Система технічного захисту інформації

Повний каталог заходів із захисту інформації (1123)

Зміст

Зміст

Анотація

Повний каталог (Bible) — містить абсолютно всі заходи, посилення та субконтролі згідно з повним скоупом НД ТЗІ.

1. AC

Клас заходів захисту AC — УПРАВЛІННЯ ДОСТУПОМ

Опис Цей клас зосереджується на обмеженні доступу до інформаційних систем, ресурсів та функцій лише для авторизованих користувачів, програм і пристроїв.

Перелік заходів захисту Політика та процедури управління доступом (AC-1); Управління обліковими записами (AC-2); Автоматизоване управління обліковими записами системи (AC-2(1)); Видалення тимчасових та екстрених облікових записів (AC-2(2)); Деактивація облікових записів (AC-2(3)); Дії при автоматизованому аудиті (AC-2(4)); Вихід із системи за відсутності активності (AC-2(5)); Динамічне управління привілеями (AC-2(6)); Схеми, засновані на ролях (AC-2(7)); Динамічне управління обліковими записами (AC-2(8)); Обмеження на використання спільних та групових облікових записів (AC-2(9)); Зміна даних спільних і групових облікових записів (AC-2(10)) [Вилучено]; Умови використання (AC-2(11)); Моніторинг нетипового використання облікових записів (AC-2(12)); Деактивація облікових записів осіб з високим рівнем ризику (AC-2(13)); Забезпечення доступу (AC-3); Обмежений доступ до привілейованих функцій (AC-3(1)) [Вилучено]; Подвійна авторизація (AC-3(2)); Мандатне управління доступом (AC-3(3)); Дискреційне управління доступом (AC-3(4)); Інформація щодо безпеки (AC-3(5)); Захист інформації користувача та системи (AC-3(6)) [Вилучено]; Управління доступом на основі ролей (AC-3(7)); Анулювання прав доступу (AC-3(8)); КЕРОВАНА ПЕРЕДАЧА

(ПУБЛІКАЦІЯ) ІНФОРМАЦІЇ (AC-3(9)); Перегляд аудитом механізмів контролю доступу (AC-3(10)); Обмеження доступу до спеціальної інформації (AC-3(11)); Встановлення та забезпечення доступу до застосунків (AC-3(12)); Управління доступом на основі атрибутів (AC-3(13)); Індивідуальний доступ (AC-3(14)); Дискреційний та обов'язковий доступ (AC-3(15)); Управління інформаційними потоками (AC-4); Атрибути безпеки об'єкту (AC-4(1)); Домени обробки даних (AC-4(2)); Динамічне управління інформаційним потоком (AC-4(3)); Управління потоком зашифрованої інформації (AC-4(4)); Вбудовування типів даних (AC-4(5)); Метадані (AC-4(6)); Механізми одностороннього потоку (AC-4(7)); Фільтри політики безпеки (AC-4(8)); Перевірки, що проводить персонал (AC-4(9)); Активація та деактивація фільтрів політики безпеки (AC-4(10)); Конфігурація фільтрів політики безпеки (AC-4(11)); Ідентифікатори типу даних (AC-4(12)); Декомпозиція на відповідні політиці субкомпоненти (AC-4(13)); Обмеження фільтра політики безпеки (AC-4(14)); Виявлення несанкціонованої інформації (AC-4(15)); Передача інформації про взаємопов'язані системи (AC-4(16)) [Вилучено]; Автентифікація домену (AC-4(17)); Прив'язка атрибуту безпеки (AC-4(18)) [Вилучено]; Перевірка метаданих (AC-4(19)); Затверджені рішення (AC-4(20)); Фізичне та логічне відділення інформаційних потоків (AC-4(21)); Єдиний доступ (AC-4(22)); Модифікована інформація, яка не підлягає оприлюдненню (AC-4(23)); Внутрішній нормалізований формат (AC-4(24)); Очищення даних (AC-4(25)); Дії з фільтрації аудиту (AC-4(26)); Надлишкові/незалежні фільтруючі механізми (AC-4(27)); Лінійні фільтрувальні канали (AC-4(28)); Фільтр механізмів оркестровки (AC-4(29)); Механізми фільтрації з використанням кількох процесів (AC-4(30)); Запобігання спробам передачі вмісту, який не пройшов перевірку фільтрації (AC-4(31)); Вимоги до процесу передачі інформації (AC-4(32)); Розмежування обов'язків (AC-5); Мінімізація повноважень (AC-6); Авторизований доступ до функцій безпеки (AC-6(1)); Непривілейований доступ до незахищених функцій (AC-6(2)); Мережевий доступ до привілейованих команд (AC-6(3)); Роздільні домени обробки (AC-6(4)); Привілейовані облікові записи (AC-6(5)); Привілейований доступ користувачами, що не належать до організації (AC-6(6)); Перегляд повноважень користувача (AC-6(7)); Рівні привілеїв для виконання коду (AC-6(8)); Аудит використання привілейованих функцій (AC-6(9)); Заборона непривілейованим користувачам виконувати привілейовані функції (AC-6(10)); Невдалі спроби входу в систему (AC-7); Автоматичне блокування облікового запису (AC-7(1)) [Вилучено]; Очищення або стирання мобільного пристрою (AC-7(2)); Обмеження на спроби біометричного входу (AC-7(3)); Використання альтернативного фактора (AC-7(4)); Попередження про використання системи (AC-8); СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) (AC-9); Невдалі спроби входу до системи (AC-9(1)); Успішні та невдалі спроби входу до системи (AC-9(2)); Повідомлення про зміни в обліковому записі (AC-9(3)); СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) – ДОДАТКОВА ІНФОРМАЦІЯ ПРО ВХІД (AC-9(4)); Управління паралельною сесією (AC-10); Блокування пристрою (AC-11); Приховані дисплеї (AC-11(1)); Припинення сеансу (AC-12); Ініційоване користувачем блокування (AC-12(1)); Повідомлення про припинення сеансу (AC-12(2)); Застережне повідомлення про те, що час сесії добігає кінця (AC-12(3)); Управління доступом (AC-13) [Вилучено]; Дозволені дії без ідентифікації або автентифікації (AC-14); Дозволені дії без ідентифікації необхідне використання (AC-14(1)) [Вилучено]; Автоматизоване маркування (AC-15) [Вилучено]; Атрибути безпеки та приватності (AC-16); Динамічне пов'язання атрибутів (AC-16(1)); Зміна значень атрибутів авторизованими особами (AC-16(2)); Підтримка системою пов'язання атрибутів (AC-16(3)); Пов'язання атрибутів авторизованими особами (AC-16(4)); Відображення атрибутів на пристроях виведення (AC-16(5)); Підтримка пов'язання атрибутів організацією (AC-16(6)); Послідовна інтерпретація атрибутів (AC-16(7)); Техніки та технології пов'язання атрибутів (AC-16(8)); Перепризначення атрибутів (AC-16(9)); Конфігурація атрибутів уповноваженими особами (AC-16(10)); Віддалений доступ (AC-17); Автоматизований моніторинг та управління (AC-17(1)); Захист конфіденційності та цілісності за допомогою шифрування (AC-17(2)); Керовані точки контролю доступу (AC-17(3)); Привілейовані команди та доступ (AC-17(4)); Моніторинг для неавторизованих підключень (AC-17(5)) [Вилучено]; Захист інформації (AC-17(6)); Додатковий захист для доступу до функцій безпеки (AC-17(7)) [Вилучено]; Деактивація незахищених протоколів мережі (AC-17(8)) [Вилучено]; Відключення або деактивація доступу (AC-17(9)); (10) автентифікація віддалених команд (AC-17(10)); Бездротовий доступ (AC-18); Автентифікація та шифрування (AC-18(1)); Моніторинг неавторизованих підключень (AC-18(2)) [Вилучено]; Відключення бездротової мережі (AC-18(3));

Обмеження налаштування користувачами (AC-18(4)); Антени та рівень потужності передачі (AC-18(5)); Контроль доступу для мобільних пристроїв (AC-19); Використання письмових та портативний пристроїв для зберігання даних (AC-19(1)) [Вилучено]; Використання персональних портативних пристроїв зберігання даних (AC-19(2)) [Вилучено]; Використання портативних пристроїв зберігання даних з неідентифікованим власником (AC-19(3)); Обмеження для засекреченої інформації (AC-19(4)); Повне шифрування пристроїв та сховищ інформації (AC-19(5)); Використання зовнішніх систем (AC-20); Обмеження на авторизоване використання (AC-20(1)); Переносні пристрої зберігання даних (AC-20(2)); Системи та компоненти, що не знаходяться у власності організації (AC-20(3)); Пристрої для зберігання даних, які можуть мати доступ до мережі (AC-20(4)); Портативні пристрої для зберігання даних – заборона використання (AC-20(5)); Розповсюдження інформації (AC-21); Автоматична підтримка ухвалення рішень (AC-21(1)); Розповсюдження інформації (AC-21(2)); Публічно доступний контент (AC-22); Захист від несанкціонованого інтелектуального аналізу даних (AC-23); Рішення щодо управління доступом (AC-24); Інформація про передачу авторизованого доступу (AC-24(1)); Відсутність ідентифікації користувача або процесу, що діє від імені користувача (AC-24(2)); Диспетчер доступу (AC-25).

1.1. ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ ДОСТУПОМ (AC-1)

a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]:
1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики контролю доступу, яка:
(a) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances);
(b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам. Процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом.
b. Призначити на посаду [Призначення: визначену організацією посадову особу] для управління, документування і розповсюдження політики та процедур контролю доступом.
c. Переглянути та оновити:
1. поточну політику управління доступом [Призначення: з визначеною організацією частотою] та [Призначення: події, визначені організацією];
2. поточні процедури управління доступом [Призначення: з визначеною організацією частотою] та [Завдання: події, визначені організацією].

No: 1
Name: ac_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюється політика контролю доступу

No: 2
Name: ac_1_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюються процедури контролю доступу

No: 3
Name: ac_1_odp_03
Type: string

Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи}

No: 4
Name: ac_1_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено посадову особу, яка керуватиме політикою та процедурами контролю доступу

No: 5
Name: ac_1_odp_05
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено частоту, з якою переглядається та оновлюється поточна політика контролю доступу

No: 6
Name: ac_1_odp_06
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено події, які вимагають перегляду та оновлення поточної політики контролю доступу

No: 7
Name: ac_1_odp_07
Type: integer
Default: 30

Визначено частоту, з якою переглядаються та оновлюються поточні процедури контролю доступу

No: 8
Name: ac_1_odp_08
Type: integer
Default: 30

Визначено події, які потребують перегляду та оновлення процедур

No: 9
Name: ac_1_a_01
Type: integer
Default: 30

Розроблено та задокументовано політику контролю доступу

No: 10
Name: ac_1_a_02
Type: integer
Default: 30

Політика контролю доступу поширюється на <AC-01_ODP[01] персонал або ролі>;

No: 11
Name: ac_1_a_03
Type: integer
Default: 30

Розроблені та задокументовані процедури контролю доступу для полегшення впровадження політики контролю доступу та пов'язаних з нею заходів захисту

No: 12
Name: ac_1_a_04

Type: integer
Default: 30

Процедури контролю доступу поширюються на <AC-01_ODP[02] персонал або ролі>

No: 13
Name: ac_1_a_1_a_01
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить мету

No: 14
Name: ac_1_a_1_a_02
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування

No: 15
Name: ac_1_a_1_a_04
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування

No: 16
Name: ac_1_a_1_a_05
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування

No: 17
Name: ac_1_a_1_a_06
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування

No: 18
Name: ac_1_a_1_a_07
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування

No: 19
Name: ac_1_a_1_b
Type: integer
Default: 30

Політика контролю доступу <AC-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам

No: 20
Name: ac_1_b
Type: integer
Default: 30

<AC-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур контролю доступу

No: 21
Name: ac_1_c_01_1
Type: integer
Default: 30

Переглядається та оновлюється поточна політика контролю доступу <AC-01_ODP[05] частота>

No: 22
Name: ac_1_c_01_2
Type: integer
Default: 30

Поточну політику контролю доступу переглянуто та оновлено після <AC-01_ODP[06] подій>

No: 23
Name: ac_1_c_02_1
Type: integer
Default: 30

Переглядаються та оновлюються поточні процедури контролю доступу <AC-01_ODP[07] частота>

No: 24
Name: ac_1_c_02_2
Type: integer
Default: 30

Поточні процедури контролю доступу переглядаються та оновлюються після <AC-01_ODP[08] подій>

1.2. УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ (AC-2)

a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації.
b. Призначити менеджерів облікових записів для управління системними обліковими записами.
c. Створити умови для групового та рольового членства.
d. Визначити авторизованих користувачів інформаційної системи, членство в групі та ролі, а також дозволи доступу (наприклад, привілеї) та інші атрибути (за потреби) для кожного облікового запису.
e. Вимагати схвалення [Призначення: визначеною організацією відповідальною особою або роллю] запитів на створення облікових записів системи.
f. Створювати, активувати, змінювати, деактивувати та видаляти системні облікові записи відповідно до [Призначення: визначених організацією політики, процедур та умов].
g. Впровадити моніторинг використання облікових записів системи.
h. Повідомляти адміністраторів облікових записів у межах [Призначення: визначеного організацією часового періоду для кожної ситуації]:
1. коли облікові записи більше не потрібні;
2. коли користувачі звільнені чи переведені;
3. коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань.
i. Авторизувати доступ до системи на основі:
1. Дійсної авторизації доступу.
2. Передбачуваного використання системи.
3. Інших атрибутів, що вимагаються організацією.
j. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами з [Призначення: визначеною організацією частотою].
k. Впровадити процес повторного випуску облікових даних спільного/групового облікового

запису (якщо він буде розгорнутий), коли особи виходять з групи.
l. Узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу.

No: 1
Name: ac_2_odp_01
Type: string
Default: nil

визначено передумови та критерії членства в групах і ролях

No: 2
Name: ac_2_odp_02
Type: string
Default: nil

визначено атрибути (за необхідності) для кожного облікового запису

No: 3
Name: ac_2_odp_03
Type: list
Default: ["admin", "security_officer"]

визначено персонал або ролі, необхідні для затвердження запитів на створення облікових записів

No: 4
Name: ac_2_odp_04
Type: string
Default: nil

визначено політику, процедури, передумови та критерії створення, активації, зміни, деактивації та видалення облікових записів

No: 5
Name: ac_2_odp_05
Type: list
Default: ["admin", "security_officer"]

визначено персонал або ролі, які мають бути повідомлені

No: 6
Name: ac_2_odp_06
Type: integer
Default: 30

визначено період часу, протягом якого адміністратори облікових записів повинні бути повідомлені про те, що облікові записи більше не потрібні

No: 7
Name: ac_2_odp_07
Type: integer
Default: 30

визначено термін, протягом якого необхідно повідомляти адміністраторів облікових записів про звільнення або переведення користувачів

No: 8
Name: ac_2_odp_08
Type: integer
Default: 30

визначено період часу, протягом якого необхідно повідомляти адміністраторів облікових записів про зміни у використанні системи або необхідність знати про зміни для окремої особи

No: 9
Name: ac_2_odp_09
Type: string
Default: nil

визначено атрибути, необхідні для авторизації доступу до системи (за потреби)

No: 10
Name: ac_2_odp_10
Type: integer
Default: 30

визначено періодичність перегляду облікових записів

No: 11
Name: ac_2_a_01
Type: string
Default: nil

визначено та задокументовано типи облікових записів, дозволених для використання в системі

No: 12
Name: ac_2_a_02
Type: string
Default: nil

визначено та задокументовано типи облікових записів, які заборонено використовувати в системі

No: 13
Name: ac_2_b
Type: string
Default: nil

призначені менеджери облікових записів

No: 14
Name: ac_2_c
Type: string
Default: nil

необхідні <AC-02_ODP[01] умови та критерії> для членства в групах та ролях

No: 15
Name: ac_2_d_01
Type: string
Default: nil

визначено авторизованих користувачів системи

No: 16
Name: ac_2_d_02
Type: string
Default: nil

вказано приналежність до групи або ролі

No: 17
Name: ac_2_d_03_01
Type: string
Default: nil

для кожного облікового запису вказуються повноваження доступу (тобто привілеї)

No: 18
Name: ac_2_d_03_02
Type: string
Default: nil

<AC-02_ODP[02] атрибути (за необхідності)> вказуються для кожного облікового запису

No: 19
Name: ac_2_e
Type: string
Default: nil

для запитів на створення облікових записів потрібні схвалення від <AC-02_ODP[03] персоналу або ролей>

No: 20
Name: ac_2_f_01
Type: string
Default: nil

облікові записи створюються відповідно до <AC-02_ODP[04] політики, процедур, передумов та критеріїв>

No: 21
Name: ac_2_f_02
Type: string
Default: nil

облікові записи активуються відповідно до <AC-02_ODP[04] політики, процедур, передумов та критеріїв>

No: 22
Name: ac_2_f_03
Type: string
Default: nil

облікові записи змінюються відповідно до <AC-02_ODP[04] політики, процедур, передумов та критеріїв>

No: 23
Name: ac_2_f_04
Type: string
Default: nil

облікові записи деактивуються відповідно до <AC-02_ODP[04] політики, процедур, передумов та критеріїв>

No: 24
Name: ac_2_f_05
Type: string
Default: nil

облікові записи видаляються відповідно до <AC-02_ODP[04] політики, процедур, передумов та критеріїв>

No: 25
Name: ac_2_g
Type: string
Default: nil

контролюється використання облікових записів

No: 26
Name: ac_2_h_01
Type: string
Default: nil

адміністратори облікових записів та <AC-02_ODP[05] персонал або ролі> отримують повідомлення протягом <AC-02_ODP[06] періоду часу>, коли облікові записи більше не потрібні

No: 27
Name: ac_2_h_02
Type: string
Default: nil

адміністратори облікових записів та <AC-02_ODP[05] персонал або ролі> отримують повідомлення протягом <AC-02_ODP[07] періоду часу>, коли користувачі звільнені чи переведені

No: 28
Name: ac_2_h_03
Type: string
Default: nil

адміністратори облікових записів та <AC-02_ODP[05] персонал або ролі> отримують повідомлення протягом <AC-02_ODP[08] періоду часу>, коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань

No: 29
Name: ac_2_i_01
Type: string
Default: nil

доступ до системи здійснюється на підставі дійсної авторизації доступу

No: 30
Name: ac_2_i_02
Type: string
Default: nil

доступ до системи авторизується на основі передбачуваного використання системи

No: 31
Name: ac_2_i_03
Type: string
Default: nil

доступ до системи авторизовано на основі атрибутів <AC-02_ODP[09] (за необхідності)>

No: 32
Name: ac_2_j
Type: string
Default: nil

облікові записи переглядаються на відповідність вимогам управління обліковими записами <AC-02_ODP[10] частота>

No: 33
Name: ac_2_k_01
Type: string
Default: nil

створено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи

No: 34
Name: ac_2_k_02
Type: string
Default: nil

впроваджено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи

No: 35
Name: ac_2_l_01

Type: string
Default: nil

процеси управління обліковими записами узгоджуються з процесами звільнення персоналу

No: 36
Name: ac_2_1_02
Type: string
Default: nil

процеси управління обліковими записами узгоджуються з процесами переводу персоналу

1.2.1. АВТОМАТИЗОВАНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ СИСТЕМИ (AC-2(1))

Використовувати автоматизовані системними обліковими записами. механізми для підтримки управління

No: 1
Name: ac_2_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Управління обліковими записами системи підтримується за допомогою автоматизовані механізми

No: 2
Name: ac_2_1_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено автоматизовані механізми, що використовуються для підтримки управління обліковими записами системи

1.2.2. ВИДАЛЕННЯ ТИМЧАСОВИХ ТА ЕКСТРЕНИХ ОБЛІКОВИХ ЗАПИСІВ (AC-2(2))

Автоматично видаляти або деактивувати тимчасові та екстрені облікові записи через [Призначення: визначений організацією період часу].

No: 1
Name: ac_2_2_odp_01
Type: string
Default: "деактивувати"

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {видаляти; деактивувати}

No: 2
Name: ac_2_2_odp_02
Type: integer
Default: 30

визначено період часу, після якого автоматично видаляються або деактивуються тимчасові або екстрені облікові записи

No: 3
Name: ac_2_2_01
Type: string
Default: nil

тимчасові та екстрені облікові записи автоматично <AC-02(02) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> через <AC-02(02) _ODP[02] період часу>

1.2.3. ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ (AC-2(3))

Автоматично деактивувати облікові записи коли:
a) їх строк дії минув;
b) вони більше не пов'язані з користувачем;
c) вони порушують організаційну політику;
d) вони були неактивними впродовж [Призначення: визначеного організацією періоду часу].

No: 1
Name: ac_2_3_odp_01
Type: integer
Default: 30

Визначено період часу, протягом якого необхідно деактивувати облікові записи

No: 2
Name: ac_2_3_odp_02
Type: integer
Default: 30

Визначено період часу неактивності, після закінчення якого облікові записи будуть деактивовані

No: 3
Name: ac_2_3_a
Type: string
Default: nil

облікові записи деактивуються протягом часового періоду, коли термін дії облікових записів минув

No: 4
Name: ac_2_3_b
Type: string
Default: nil

Облікові записи деактивуються протягом часового періоду, коли облікові записи більше не пов'язані з користувачем або фізичною особою

No: 5
Name: ac_2_3_c
Type: string
Default: nil

Облікові записи відключено протягом часового періоду, коли облікові записи порушують політику організації

No: 6
Name: ac_2_3_d
Type: string
Default: nil

облікові записи деактивуються протягом часового періоду, якщо вони були неактивними протягом визначеного періоду часу

1.2.4. ДІЇ ПРИ АВТОМАТИЗОВАНОМУ АУДИТІ (AC-2(4))

Проводити автоматизований аудит створення, модифікації, деактивації та видалення облікових записів і сповіщення про дії. ПРИ активації,

No: 1
Name: ac_2_4_01
Type: string
Default: nil

Створення облікового запису автоматично аудитується

No: 2
Name: ac_2_4_02
Type: string
Default: nil

Модифікація облікового запису автоматично аудитується

No: 3
Name: ac_2_4_03
Type: string
Default: nil

Активація облікового запису автоматично аудитується

No: 4
Name: ac_2_4_04
Type: string
Default: nil

Деактивація облікового запису автоматично аудитується

No: 5
Name: ac_2_4_05
Type: string
Default: nil

Видалення облікового запису автоматично аудитується

1.2.5. ВИХІД ІЗ СИСТЕМИ ЗА ВІДСУТНОСТІ АКТИВНОСТІ (AC-2(5))

Вимагати від користувачів виходити із системи, коли [Призначення: вичерпано визначений організацією періоду часу очікування або опис того, коли необхідно вийти із системи].

No: 1
Name: ac_2_5_01
Type: integer
Default: 30

Користувачі повинні виходити з системи, коли період очікуваної бездіяльності або опис часу, коли потрібно вийти з системи

No: 2
Name: ac_2_5_odp
Type: integer
Default: 30

Визначено часовий період очікуваної бездіяльності або опис, коли потрібно вийти з системи

1.2.6. ДИНАМІЧНЕ УПРАВЛІННЯ ПРИВІЛЕЯМИ (AC-2(6))

Реалізувати такі можливості динамічного управління привілеями: [Призначення: визначений організацією перелік можливостей динамічного управління привілеями].

No: 1
Name: ac_2_6_01
Type: string
Default: nil

Реалізовано можливості динамічного управління привілеями

No: 2
Name: ac_2_6_odp
Type: string
Default: nil

Визначено можливості динамічного управління привілеями

1.2.7. СХЕМИ, ЗАСНОВАНІ НА РОЛЯХ (AC-2(7))

a) Створювати й адмініструвати привілейовані облікові записи користувачів відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей.
b) Проводити моніторинг призначення привілейованих ролей.
c) Відстежувати зміни ролей або атрибутів.
d) Скасовувати доступ, коли призначені привілейовані ролі більше не потрібні.

No: 1
Name: ac_2_7_b
Type: string
Default: nil

Проводиться моніторинг призначення привілейованих ролей або атрибутів

No: 2
Name: ac_2_7_c
Type: string
Default: nil

Відстежуються зміни ролей або атрибутів

No: 3
Name: ac_2_7_d
Type: list
Default: ["admin", "security_officer"]

Доступ скасовується, коли призначені привілейовані ролі більше не потрібні.0

No: 4
Name: ac_2_7_odp
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {схема доступу на основі ролей; схема доступу на основі атрибутів}

1.2.8. ДИНАМІЧНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ (AC-2(8))

Створювати, активувати, управляти та деактивувати [Призначення: системні облікові записи, визначені організацією] динамічно.

No: 1
Name: ac_2_8_01
Type: string
Default: nil

УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: ac_2_8_02
Type: string
Default: nil

Облікові записи системи активуються динамічно

No: 3
Name: ac_2_8_03
Type: string
Default: nil

Облікові записи системи активуються динамічно

No: 4
Name: ac_2_8_04
Type: string
Default: nil

Облікові записи системи деактивуються динамічно

No: 5
Name: ac_2_8_odp
Type: string
Default: nil

Визначено облікові записи системи, які динамічно створюються, активуються, управляються та деактивуються

1.2.9. ОБМЕЖЕННЯ НА ВИКОРИСТАННЯ СПІЛЬНИХ ТА ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ (AC-2(9))

Використовувати лише ті спільні та групові облікові записи, які відповідають [Призначення: визначеним організацією умовам для створення спільних та групових облікових записів].

No: 1
Name: ac_2_9_01
Type: list
Default: []

Використання спільних та групових облікових записів дозволено лише за умови дотримання умов

No: 2
Name: ac_2_9_odp
Type: list
Default: []

Визначено умови створення спільних та групових облікових записів

1.2.10. ЗМІНА ДАНИХ СПІЛЬНИХ І ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ (AC-2(10)) [Вилучено]

[Вилучено: включено до AC-02(k)]

Немає параметрів для цього контролю.

1.2.11. УМОВИ ВИКОРИСТАННЯ (AC-2(11))

Забезпечити дотримання [Призначення: обставин та/або умов використання, визначених організацією] для [Призначення: визначених організацією облікових записів системи].

No: 1
Name: ac_2_11_01
Type: list
Default: []

Обставини та/або умови використання для облікових записів системи застосовуються

No: 2
Name: ac_2_11_odp_01
Type: list
Default: []

Визначено обставини та/або умови використання визначених облікових записів системи

No: 3
Name: ac_2_11_odp_02
Type: string
Default: nil

Визначені облікові записи системи, що підлягають виконанню обставин та/або умов використання

1.2.12. МОНІТОРИНГ НЕТИПОВОГО ВИКОРИСТАННЯ ОБЛІКОВИХ ЗАПИСІВ (AC-2(12))

a) Проводити моніторинг облікових записів системи на [Призначення: визначене організацією нетипове використання].
b) Повідомляти про нетипове використання облікових записів системи [Призначення: визначеного організацією персоналу або ролей].

No: 1
Name: ac_2_12_a
Type: list
Default: []

Облікові записи системи відстежуються на предмет обставини та/або умови використання

No: 2
Name: ac_2_12_b
Type: list
Default: ["admin", "security_officer"]

Про визначені обставини та/або умови використання системних облікових записів повідомляється персонал або ролі

No: 3
Name: ac_2_12_odp_01
Type: list
Default: []

Визначено обставини та/або умови використання, для яких необхідно здійснювати моніторинг облікових записів системи

No: 4
Name: ac_2_12_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким належить повідомляти про визначені обставини та/або умови використання

1.2.13. ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ ОСІБ З ВИСОКИМ РІВНЕМ РИЗИКУ (AC-2(13))

Деактивувати облікові записи користувачів, які становлять значний ризик, у межах [Призначення: визначеного організацією періоду часу] після виявлення ризику.

No: 1
Name: ac_2_13_01
Type: integer
Default: 30

Облікові записи користувачів деактивуються протягом періоду часу з моменту виявлення значних ризиків

No: 2
Name: ac_2_13_odp_01
Type: integer
Default: 30

Визначено період часу, протягом якого необхідно деактивувати облікові записи фізичних осіб, які становлять значний ризик

No: 3
Name: ac_2_13_odp_02
Type: string
Default: nil

Визначено значні ризики, що призводять до деактивації облікових записів

1.3. ЗАБЕЗПЕЧЕННЯ ДОСТУПУ (AC-3)

Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.

No: 1
Name: ac_3_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Затверджені повноваження на логічний доступ до інформації та ресурсів системи виконуються відповідно до чинних політик(правил) управління доступом

1.3.1. ОБМЕЖЕНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ (AC-3(1)) [Вилучено]

[Вилучено: включено до складу AC-06]

Немає параметрів для цього контролю.

1.3.2. ПОДВІЙНА АВТОРИЗАЦІЯ (AC-3(2))

Забезпечити подвійну авторизацію для [Призначення: визначених організацією привілейованих команд та/або інших дій, визначених організацією].

No: 1
Name: ac_3_2_01
Type: string
Default: nil

Подвійна авторизація застосовується для привілейованих команд та/або інших дій

No: 2
Name: ac_3_2_odp
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено привілейовані команди та/або інші дії, що потребують подвійної авторизації

1.3.3. МАНДАТНЕ УПРАВЛІННЯ ДОСТУПОМ (AC-3(3))

Застосовувати [Призначення: визначену організацією мандатну (mandatory) політику управління доступом] щодо всіх суб'єктів і об'єктів доступу, у яких політика:
(a) одноманітно застосовується для всіх суб'єктів і об'єктів у межах системи;
(b) вказує, що суб'єкт, якому було надано доступ до інформації, обмежений у виконанні будь-якої з таких дій:
(c) (1) передача інформації неавторизованим суб'єктам або об'єктам; (2) надання іншим суб'єктам привілеїв; (3) зміна одного чи декількох атрибутів безпеки суб'єкта, об'єкта, системи або компонентів системи; (4) вибір атрибутів безпеки та значень атрибутів, які повинні бути пов'язані з новоствореними або зміненими об'єктами; (5) зміна правил, що регулюють управління доступом; має бути вказано, що [Призначення: визначеним організацією суб'єктам] можуть бути явно надані [Призначення: визначені організацією привілеї], так що вони не обмежуються будь-яким з перелічених вище обмежень.

No: 1
Name: ac_3_3_odp_01
Type: string
Default: nil

Визначено мандатну політику контролю доступу, що застосовується до набору охоплених суб'єктів

No: 2
Name: ac_3_3_odp_02
Type: string
Default: nil

Визначено мандатну політику контролю доступу, що застосовується до набору охоплених об'єктів

No: 3
Name: ac_3_3_odp_03
Type: string
Default: nil

Визначені суб'єкти, яким явно надаються привілеї

No: 4
Name: ac_3_3_odp_04
Type: string
Default: nil

Визначено привілеї, які мають бути прямо надані суб'єктам

No: 5
Name: ac_3_3_01
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> застосовується до набору охоплених суб'єктів, зазначених у політиці

No: 6
Name: ac_3_3_02
Type: string
Default: nil

<AC-03(03)_ODP[02] мандатна політика контролю доступу> застосовується до набору охоплених об'єктів, зазначених у політиці

No: 7
Name: ac_3_3_a_01
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> застосовується одноманітно до всіх суб'єктів системи

No: 8
Name: ac_3_3_a_02
Type: string
Default: nil

<AC-03(03)_ODP[02] мандатна політика контролю доступу> застосовується одноманітно до всіх об'єктів системи

No: 9
Name: ac_3_3_b_01
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що суб'єкт, якому надано доступ до інформації, зобов'язаний не передавати інформацію неавторизованим суб'єктам або об'єктам

No: 10
Name: ac_3_3_b_02
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що суб'єкт, якому надано доступ до інформації, обмежений у наданні своїх привілеїв іншим суб'єктам

No: 11
Name: ac_3_3_b_03
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що суб'єкт, якому надано доступ до інформації, не може змінювати один або декілька атрибутів безпеки (визначених політикою) суб'єктів, об'єктів, системи або компонентів системи

No: 12
Name: ac_3_3_b_04

Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що суб'єкт, якому надано доступ до інформації, обмежений у виборі атрибутів безпеки та значень атрибутів (визначених політикою), що повинні бути пов'язані з новостворюваними або зміненими об'єктами

No: 13
Name: ac_3_3_b_05
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що суб'єкт, якому надано доступ до інформації, не має права змінювати правила, що регулюють управління доступом

No: 14
Name: ac_3_3_c
Type: string
Default: nil

<AC-03(03)_ODP[01] мандатна політика контролю доступу> та <AC-03(03)_ODP[02] мандатна політика контролю доступу> визначають, що <AC-03(03)_ODP[03] суб'єктам> можуть бути явно надані <AC-03(03)_ODP[04] привілеї> таким чином, щоб вони не були обмежені будь-якою визначеною підмножиною (або всіма) з наведених вище обмежень

1.3.4. ДИСКРЕЦІЙНЕ УПРАВЛІННЯ ДОСТУПОМ (AC-3(4))

Застосовувати [Призначення: визначену організацією дискреційну політику управління доступом] щодо визначених суб'єктів і об'єктів доступу, для яких політика визначає, що суб'єкт, якому було надано доступ до інформації, може виконати одну чи більше з таких дій:
(a) передача інформацію будь-яким іншим суб'єктам чи об'єктам;
(b) призначення своїх привілей іншим суб'єктам;
(c) зміна атрибутів безпеки суб'єктів, об'єктів, систем або компонентів системи;
(d) вибір атрибутів безпеки, які будуть пов'язані з новоствореними або переглянутими об'єктами;
(e) зміна правил, що регулюють управління доступом.

No: 1
Name: ac_3_4_odp_01
Type: string
Default: nil

Визначено дискреційну політику управління доступом, яка застосовується до набору охоплених суб'єктів

No: 2
Name: ac_3_4_odp_02
Type: string
Default: nil

Визначено дискреційну політику управління доступом, яка застосовується до набору охоплених об'єктів

No: 3
Name: ac_3_4_01
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> застосовується до набору охоплених суб'єктів, зазначених у політиці

No: 4
Name: ac_3_4_02
Type: string
Default: nil

<AC-03(04)_ODP[02] дискреційна політика управління доступом> застосовується до набору охоплених об'єктів, зазначених у політиці

No: 5
Name: ac_3_4_a
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> та <AC-03(04)_ODP[02] дискреційна політика управління доступом> визначають, що суб'єкт, якому надано доступ до інформації, може передавати інформацію будь-яким іншим суб'єктам або об'єктам

No: 6
Name: ac_3_4_b
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> та <AC-03(04)_ODP[02] дискреційна політика управління доступом> визначають, що суб'єкт, якому надано доступ до інформації, може надавати свої привілеї іншим суб'єктам

No: 7
Name: ac_3_4_c
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> та <AC-03(04)_ODP[02] дискреційна політика управління доступом> визначають, що суб'єкт, якому надано доступ до інформації, може змінювати атрибути безпеки суб'єктів, об'єктів, системи або компонентів системи

No: 8
Name: ac_3_4_d
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> та <AC-03(04)_ODP[02] дискреційна політика управління доступом> визначають, що суб'єкт, якому надано доступ до інформації, може вибирати атрибути безпеки, які будуть пов'язані з новоствореними або переглянутими об'єктами

No: 9
Name: ac_3_4_e
Type: string
Default: nil

<AC-03(04)_ODP[01] дискреційна політика управління доступом> та <AC-03(04)_ODP[02] дискреційна політика управління доступом> визначають, що суб'єкт, якому надано доступ до інформації, може змінювати правила управління доступом

1.3.5. ІНФОРМАЦІЯ ЩОДО БЕЗПЕКИ (AC-3(5))

Запобігати доступу до [Призначення: інформації щодо безпеки, яка визначена організацією], за винятком випадків, коли наявні безпечні неробочі стани системи.

No: 1
Name: ac_3_5_01

Type: string
Default: nil

Доступ до інформація щодо безпеки заборонено, за винятком випадків, коли наявні безпечні неробочі стани системи

No: 2
Name: ac_3_5_odp
Type: string
Default: nil

Визначено інформацію щодо безпеки, доступ до якої заборонено, за винятком випадків, коли наявні безпечні неробочі стани системи

1.3.6. ЗАХИСТ ІНФОРМАЦІЇ КОРИСТУВАЧА ТА СИСТЕМИ (AC-3(6)) [Вилучено]

[Вилучено: Включено в MP-04 та SC-28]

Немає параметрів для цього контролю.

1.3.7. УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ (AC-3(7))

Застосовувати політику управління доступом на основі ролей щодо визначених суб'єктів і об'єктів та управління доступом на основі [Призначення: визначених організацією ролей та користувачів, уповноважених приймати такі ролі].

No: 1
Name: ac_3_7_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Політика управління доступом на основі ролей застосовується до визначених суб'єктів

No: 2
Name: ac_3_7_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Політика управління доступом на основі ролей застосовується до визначених об'єктів

No: 3
Name: ac_3_7_03
Type: list
Default: ["admin", "security_officer"]

Доступ контролюється на основі ролей та користувачів, яким дозволено приймати такі ролі

No: 4
Name: ac_3_7_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено ролі, на яких базується управління доступом

No: 5
Name: ac_3_7_odp_02

Type: string
Default: nil

Визначено користувачів, уповноважених на прийняття ролей (визначених у AC-03(07)_ODP[01])

1.3.8. АНУЛЮВАННЯ ПРАВ ДОСТУПУ (AC-3(8))

Здійснювати анулювання прав доступу в результаті змін атрибутів безпеки суб'єктів і об'єктів на основі [Призначення: визначених організацією правил, що регулюють терміни скасування прав доступу].

No: 1
Name: ac_3_8_01
Type: string
Default: nil

Здійснюється анулювання прав доступу в результаті зміни атрибутів безпеки суб'єктів на основі правил

No: 2
Name: ac_3_8_02
Type: string
Default: nil

Здійснюється анулювання прав доступу в результаті зміни атрибутів безпеки об'єктів на основі правил

No: 3
Name: ac_3_8_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено правила, що регулюють терміни скасування дозволів на доступ

1.3.9. КЕРОВАНА ПЕРЕДАЧА (ПУБЛІКАЦІЯ) ІНФОРМАЦІЇ (AC-3(9))

Передавати (публікувати) інформацію за межами встановленої межі системи можливо, якщо: a) Приймальна [Призначення: визначена організацією система або компонент системи] забезпечує [Призначення: визначені організацією заходи безпеки]; b) [Призначення: визначені організацією заходи безпеки] використовуються для підтвердження відповідності інформації, призначеної для керованих передач (публікації).

No: 1
Name: ac_3_9_a
Type: string
Default: nil

Інформація випускається за межі системи, тільки якщо отримуюча система або компонент системи забезпечує заходи захисту

No: 2
Name: ac_3_9_b
Type: string
Default: nil

Інформація публікується за межами системи, тільки якщо заходи захисту використовуються для перевірки відповідності інформації, призначеної для публікації

1.3.10. ПЕРЕГЛЯД АУДИТОМ МЕХАНІЗМІВ КОНТРОЛЮ ДОСТУПУ (AC-3(10))

Застосувати перегляд аудитом механізмів автоматизованого управління доступу при [Призначення: визначених організацією умовах] [Призначення: визначеними організацією ролями].

No: 1
Name: ac_3_10_01
Type: string
Default: nil

За умов застосовується перегляд аудитом механізмів автоматизованого контролю доступу за допомогою ролей

No: 2
Name: ac_3_10_odp_01
Type: list
Default: []

Визначено умови, за яких можна застосовувати перегляд аудитом механізмів автоматизованого управління доступом

No: 3
Name: ac_3_10_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено ролі, яким дозволено використовувати перегляд аутом механізмів автоматизованого управління доступом

1.3.11. ОБМЕЖЕННЯ ДОСТУПУ ДО СПЕЦІАЛЬНОЇ ІНФОРМАЦІЇ (AC-3(11))

Обмежити прямий доступ до сховищ даних, що містять [Призначення: визначені організацією типи інформації].

No: 1
Name: ac_3_11_01
Type: string
Default: nil

Обмежено доступ до сховищ даних, що містять типи інформації

1.3.12. ВСТАНОВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ЗАСТОСУНКІВ (AC-3(12))

a) Вимагати від застосунків встановити в процесі інсталяції доступ до таких застосунків системи і функцій: [Призначення: визначених організацією програм та функції системи];
b) Впровадити механізм примусового застосування, щоб запобігти доступу, відмінному від заявленого.
c) Схвалити зміни доступу після початкового встановлення застосунків.

No: 1
Name: ac_3_12_a
Type: string
Default: nil

У процесі інсталяції програми повинні встановити доступ до таких системних застосунків і функцій системи: програм та функції системи

No: 2
Name: ac_3_12_b
Type: string
Default: nil

Передбачено механізм примусового застосування запобігання несанкціонованому доступу

No: 3
Name: ac_3_12_c
Type: string
Default: nil

Зміни доступу після первинної інсталяції програми схвалено

No: 4
Name: ac_3_12_odp
Type: string
Default: nil

Визначено програми та функції системи, яким необхідно встановити права доступу

1.3.13. УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ АТРИБУТІВ (AC-3(13))

Здійснювати політику управління доступу на основі атрибутів (atribute-based) для визначених суб'єктів і об'єктів доступу й управляти доступом на основі [Призначення: визначених організацією атрибутів для ухвалення рішень про доступ].

No: 1
Name: ac_3_13_1
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Політика управління доступом на здійснюється до визначених суб'єктів; основі атрибутів AC-03(13)[2] політика управління доступом на здійснюється до визначених об'єктів; основі атрибутів

No: 2
Name: ac_3_13_3
Type: string
Default: nil

Доступ контролюється на основі атрибутів

No: 3
Name: ac_3_13_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути для визначення прав доступу

1.3.14. ІНДИВІДУАЛЬНИЙ ДОСТУП (AC-3(14))

Надайте [Призначення: механізми, визначені організацією], щоб дозволити особам мати доступ до певних елементів їх особистої інформації: [Призначення: елементи, визначені організацією]

No: 1
Name: ac_3_14_01

Type: list
Default: ["admin", "security_officer"]

Механізми надаються для того, щоб дозволити особам мати доступ до елементів їхньої персональної інформації

No: 2
Name: ac_3_14_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено механізми, що дозволяють фізичним особам мати доступ до елементів їхньої персональної інформації

No: 3
Name: ac_3_14_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено елементи інформації, що ідентифікує особу, до якої мають доступ фізичні особи

1.3.15. ДИСКРЕЦІЙНИЙ ТА ОБОВ'ЯЗКОВИЙ ДОСТУП (AC-3(15))

(a) Застосовувати [Призначення: визначену організацією політику обов'язкового контролю доступу] до набору охоплених суб'єктів і об'єктів, указаних у політиці;
(b) Застосування [Призначення: визначена організацією дискреційна політика контролю доступу] до набору охоплених суб'єктів і об'єктів, указаних у політиці.

No: 1
Name: ac_3_15_a_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Політика обов'язкового контролю доступу застосовується до набору охоплених суб'єктів, зазначених у політиці

No: 2
Name: ac_3_15_a_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Політика обов'язкового контролю доступу застосовується до набору охоплених об'єктів, зазначених у політиці

No: 3
Name: ac_3_15_b_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Дискреційна політика контролю доступу застосовується до набору суб'єктів, зазначених у політиці

No: 4
Name: ac_3_15_b_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Дискреційна політика контролю доступу застосовується до набору об'єктів, зазначених у політиці

No: 5
Name: ac_3_15_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено обов'язкову політику контролю доступу, яка застосовується до набору суб'єктів, зазначених у політиці

No: 6
Name: ac_3_15_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено обов'язкову політику контролю доступу, яка застосовується до набору об'єктів, зазначених у політиці

No: 7
Name: ac_3_15_odp_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено дискреційну політику контролю доступу, яка застосовується до набору суб'єктів, зазначених у політиці

No: 8
Name: ac_3_15_odp_04
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено дискреційну політику контролю доступу, яка застосовується до набору об'єктів, зазначених у політиці

1.4. УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ (AC-4)

Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі [Призначення: визначеними організацією політиками управління інформаційним потоком].

No: 1
Name: ac_4_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Затверджені повноваження застосовуються для контролю потоку інформації всередині системи та між підключеними системами на основі політики управління інформаційними потоками

No: 2
Name: ac_4_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики управління інформаційними потоками всередині системи та між підключеними системами

1.4.1. АТРИБУТИ БЕЗПЕКИ ОБ'ЄКТУ (AC-4(1))

Використовувати [Призначення: визначені організацією атрибути безпеки], пов'язані з [Призначення: визначеними організацією інформацією, джерелами та об'єктами призначення], щоб запровадити [Призначення: визначену організацією політику управління потоками інформації] як основу для ухвалення рішень щодо управління потоками.

No: 1
Name: ac_4_1_01

Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути безпеки, пов'язані з об'єктами інформації, джерела об'єктів та об'єктами призначення, використовуються для забезпечення виконання політик управління інформаційними потоками як основи для прийняття рішень щодо управління потоками

No: 2
Name: ac_4_1_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути конфіденційності, пов'язані з об'єктами інформації, джерела об'єктів та об'єктами призначення, використовуються для забезпечення виконання політик управління інформаційними потоками як основи для прийняття рішень щодо управління потоками

No: 3
Name: ac_4_1_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути безпеки, які будуть пов'язані з інформацією, джерелом та об'єктами призначення

No: 4
Name: ac_4_1_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути конфіденційності, які будуть пов'язані з інформацією, джерелом та об'єктами призначення

No: 5
Name: ac_4_1_odp_03
Type: string
Default: nil

Визначено об'єкти інформації, які будуть пов'язані з атрибутами безпеки

No: 6
Name: ac_4_1_odp_04
Type: string
Default: nil

Визначено об'єкти інформації, які будуть пов'язані з атрибутами конфіденційності

No: 7
Name: ac_4_1_odp_05
Type: string
Default: nil

Визначено джерела об'єктів, які будуть пов'язані з атрибутами безпеки

No: 8
Name: ac_4_1_odp_06
Type: string
Default: nil

Визначено джерела об'єктів, які будуть пов'язані з атрибутами конфіденційності

No: 9
Name: ac_4_1_odp_07
Type: string
Default: nil

Визначено об'єкти призначення, які будуть пов'язані з атрибутами безпеки

No: 10
Name: ac_4_1_odp_08
Type: string
Default: nil

Визначено об'єкти призначення, які будуть пов'язані з атрибутами конфіденційності

No: 11
Name: ac_4_1_odp_09
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політику управління інформаційними потоками як основу для ухвалення рішень щодо управління потоками

1.4.2. ДОМЕНИ ОБРОБРОБКИ ДАНИХ (AC-4(2))

Використовувати захищені домени обробки даних для забезпечення [Призначення: визначеної організацією політики управління потоками інформації] як основу для ухвалення рішень щодо управління потоками.

No: 1
Name: ac_4_2_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Захищені домени обробки використовуються для забезпечення дотримання політики управління інформаційними потоками як основи для ухвалення рішень щодо управління потоками

No: 2
Name: ac_4_2_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики управління інформаційними потоками, які будуть застосовуватися з використанням захищених доменів обробки

1.4.3. ДИНАМІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ ПОТОКОМ (AC-4(3))

Здійснювати динамічне управління потоком інформації на основі [Призначення: визначених організацією політик (правил)].

No: 1
Name: ac_4_3_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Здійснюється динамічне управління потоком інформації на основі політики управління інформаційними потоками

No: 2
Name: ac_4_3_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені політики контролю інформаційних потоків, які необхідно впроваджувати

1.4.4. УПРАВЛІННЯ ПОТОКОМ ЗАШИФРОВАНОЇ ІНФОРМАЦІЇ (AC-4(4))

Запобігати обходу [Призначення: механізмів управління потоками, визначених організацією] зашифрованої інформації шляхом [Вибір (один або декілька): дешифрування інформації; блокування потоку зашифрованої інформації; завершення сеансів зв'язку, що намагаються передавати зашифровану інформацію; [Призначення: визначеними організацією процедурою або методом]].

No: 1
Name: ac_4_4_odp_01
Type: string
Default: "автоматизований засіб моніторингу"

Визначено механізми контролю інформаційних потоків, які унеможливлюють обхід зашифрованої інформації

No: 2
Name: ac_4_4_odp_02
Type: string
Default: "AES-256-GCM"

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {дешифрування інформації; блокування потоку зашифрованої інформації; завершення сеансів зв'язку що намагаються передавати зашифровану інформацію; визначена організацією процедура або метод}

No: 3
Name: ac_4_4_odp_03
Type: string
Default: "автоматизований засіб моніторингу"

Визначено організацією процедуру або метод, що використовується для запобігання обходу зашифрованої інформації через механізми контролю інформаційних потоків (якщо вибрано)

1.4.5. ВБУДОВУВАННЯ ТИПІВ ДАНИХ (AC-4(5))

Впровадити [Призначення: визначені організацією вбудовування типів даних в інші типи даних. обмеження] для

No: 1
Name: ac_4_5_odp
Type: string
Default: nil

Визначеного обмеження, які слід застосовувати щодо вбудовування типів даних в інші типи даних; обмеження накладаються на вбудовування типів даних у інші типи даних

1.4.6. МЕТАДАНІ (AC-4(6))

Здійснювати управління інформаційним потоком на основі [Призначення: визначених організацією метаданих].

No: 1
Name: ac_4_6_01
Type: string
Default: nil

Інформаційна система здійснює управління інформаційним потоком на основі метадані

No: 2
Name: ac_4_6_odp
Type: string
Default: nil

Визначено метадані, які слід використовувати як засіб управління інформаційним потоком

1.4.7. МЕХАНІЗМИ ОДНОСТОРОННЬОГО ПОТОКУ (AC-4(7))

Впровадити [Призначення: визначені організацією односторонні інформаційні потоки] за допомогою апаратних механізмів.

No: 1
Name: ac_4_7_01
Type: string
Default: nil

Односторонні інформаційні потоки забезпечуються за допомогою апаратних механізмів управління потоками.

1.4.8. ФІЛЬТРИ ПОЛІТИКИ БЕЗПЕКИ (AC-4(8))

a) Забезпечити контроль над потоком інформації, використовуючи [Призначення: визначені організацією фільтри безпеки або політики конфіденційності] як основу для рішень щодо керування потоком для [Призначення: визначені організацією потоки інформації];
b) [Вибір (один або кілька): Блокування; Зміна; Карантин] даних після помилки обробки фільтра відповідно до [Призначення: політика безпеки або конфіденційності, визначена організацією].

No: 1
Name: ac_4_8_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

ODP[02] визначено фільтри політики конфіденційності, які будуть використовуватися як основа для забезпечення керування інформаційними потоками

No: 2
Name: ac_4_8_a_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Управління інформаційними потоками здійснюється за допомогою <AC-04(08) _ODP[01] фільтр політики безпеки> як основи для прийняття рішень щодо управління потоками для <AC-04(08) _ODP[03] інформаційних потоків>; AC-04(08)(a)[01] контроль інформаційних потоків здійснюється за допомогою <AC-04(08) _ODP[02] фільтр політики конфіденційності> як основи для прийняття рішень щодо контролю потоків для <AC-04(08) _ODP[04] інформаційних потоків>

1.4.9. ПЕРЕВІРКИ, ЩО ПРОВОДИТЬ ПЕРСОНАЛ (AC-4(9))

Примусово використовувати перевірку персоналом [Призначення: потоки інформації, визначені організацією] за таких умов: [Призначення: умови, визначені організацією].

No: 1
Name: ac_4_9_01
Type: list
Default: ["admin", "security_officer"]

Перевірка персоналом використовуються для інформаційних потоків за умов

No: 2
Name: ac_4_9_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено інформаційні потоки, які потребують використання перевірку персоналом

No: 3
Name: ac_4_9_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено умови, за яких використання перевірки персоналом на інформаційні потоки має бути обов'язковим

1.4.10. АКТИВАЦІЯ ТА ДЕАКТИВАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ (AC-4(10))

Впровадити можливість для привілейованих адміністраторів активувати та деактивувати [Призначення: фільтри політики безпеки, що визначаються організацією] за таких умов: [Призначення: визначені організацією умови].

No: 1
Name: ac_4_10_01
Type: string
Default: nil

Привілейованим адміністраторам надано можливість активувати та деактивувати <AC-04(10) _ODP[01] фільтри безпеки> за <AC-04(10) _ODP[03] умов>

No: 2
Name: ac_4_10_02
Type: string
Default: nil

Привілейованим адміністраторам надано можливість активувати та деактивувати <AC-04(10) _ODP[02] фільтри конфіденційності> за <AC-04(10) _ODP[04] умов>

1.4.11. КОНФІГУРАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ (AC-4(11))

Впровадити можливість для привілейованих адміністраторів налаштувати [Призначення: визначені організацією фільтри політики безпеки] для підтримки різних політик безпеки.

No: 1
Name: ac_4_11_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Привілейованим адміністраторам надано можливість налаштовувати фільтри політики безпеки для підтримки різних політик безпеки або конфіденційності

No: 2
Name: ac_4_11_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Привілейованим адміністраторам надано можливість налаштовувати фільтри політики конфіденційності для підтримки різних політик безпеки або конфіденційності

No: 3
Name: ac_4_11_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено фільтри політики безпеки, які привілейовані адміністратори можуть налаштовувати для підтримки різних політик безпеки та конфіденційності

No: 4
Name: ac_4_11_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено фільтри політики конфіденційності, які привілейовані адміністратори можуть налаштовувати для підтримки різних політик безпеки та конфіденційності

1.4.12. ІДЕНТИФІКАТОРИ ТИПУ ДАНИХ (AC-4(12))

При передачі інформації між різними захищеними доменами використовувати [Призначення: визначені організацією ідентифікатори типів даних] для перевірки даних, необхідних для ухвалення рішень щодо інформаційного потоку.

No: 1
Name: ac_4_12_odp
Type: string
Default: nil

Визначено ідентифікатори типів даних, які будуть використовуватися для перевірки даних, необхідних для ухвалення рішень щодо інформаційних потоків; AC-04(12) при передачі інформації між різними доменами безпеки, ідентифікатори типів даних використовуються для перевірки даних, необхідних для ухвалення рішень щодо інформаційних потоків

1.4.13. ДЕКОМПОЗИЦІЯ НА ВІДПОВІДНІ ПОЛІТИЦІ СУБКОМПОНЕНТИ (AC-4(13))

При передачі інформації між різними захищеними доменами здійснювати декомпозицію інформації на [Призначення: визначені організацією субкомпоненти, що відповідають політиці] для представлення в механізмах реалізації політики.

No: 1
Name: ac_4_13_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

При передачі інформації між різними доменами безпеки інформація розкладається на субкомпоненти політики для подання механізмам забезпечення дотримання політики

No: 2
Name: ac_4_13_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено субкомпоненти політики, на які слід розкласти інформацію для подання до механізмів реалізації політики

1.4.14. ОБМЕЖЕННЯ ФІЛЬТРА ПОЛІТИКИ БЕЗПЕКИ (AC-4(14))

При передачі інформації між різними захищеними доменами реалізувати [Призначення: визначені організацією фільтри політики безпеки], що вимагають повного переліку форматів, які обмежують структуру та зміст даних.

No: 1
Name: ac_4_14_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

При передачі інформації між різними захищеними доменами, реалізовані фільтри політики безпеки вимагають повністю перелічених форматів, які обмежують структуру та вміст даних

No: 2
Name: ac_4_14_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

При передачі інформації між різними захищеними доменами, реалізовані фільтри політики конфіденційності вимагають повністю перелічених форматів, які обмежують структуру та вміст даних

No: 3
Name: ac_4_14_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено фільтри політики конфіденційності, які вимагають повного переліку форматів, що обмежують структуру та зміст даних

1.4.15. ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОЇ ІНФОРМАЦІЇ (AC-4(15))

При передачі інформації між різними захищеними доменами перевіряти інформацію на наявність [Призначення: визначеної організацією несанкціонованої інформації] та забороняти передачу такої інформації відповідно до [Призначення: визначеної організацією політики безпеки].

No: 1
Name: ac_4_15_01
Type: string
Default: nil

При передачі інформації між різними доменами безпеки інформація перевіряється на наявність <AC- 04(15)_ ODP[01] несанкціонованої інформації>

No: 2
Name: ac_4_15_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

При передачі інформації між різними доменами безпеки забороняється передача несанкціонованої інформації відповідно до політики безпеки

No: 3
Name: ac_4_15_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

При передачі інформації між різними доменами безпеки забороняється передача несанкціонованої інформації відповідно до політики конфіденційності

No: 4
Name: ac_4_15_odp_01
Type: string
Default: nil

Визначено несанкціоновану інформацію, яку потрібно виявляти

No: 5
Name: ac_4_15_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політику безпеки, яка вимагає заборонити передачу несанкціонованої інформації між різними доменами безпеки (якщо вибрано)

No: 6
Name: ac_4_15_odp_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політику конфіденційності, яка вимагає заборонити передачу визначеної організацією несанкціонованої інформації між різними доменами безпеки (якщо вибрано)

1.4.16. ПЕРЕДАЧА ІНФОРМАЦІЇ ПРО ВЗАЄМОПОВ'ЯЗАНІ СИСТЕМИ (AC-4(16)) [Вилучено]

[Вилучено: Включено в AC-04]

Немає параметрів для цього контролю.

1.4.17. АВТЕНТИФІКАЦІЯ ДОМЕНУ (AC-4(17))

Автентифікувати [Призначення: визначені організацією домени] до [Призначення: дії, визначеної організацією] з обміну інформацією.

No: 1
Name: ac_4_17_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {організація, система, програми, служби, індивід};

No: 2
Name: ac_4_17_01
Type: string
Default: nil

Для передачі інформації пункти відправлення та призначення унікально ідентифікуються та аутентифікуються за допомогою <AC-04(17)_ODP ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>

1.4.18. ПРИВ'ЯЗКА АТРИБУТУ БЕЗПЕКИ (AC-4(18)) [Вилучено]

[Вилучено: Включено в AC-16]

Немає параметрів для цього контролю.

1.4.19. ПЕРЕВІРКА МЕТАДАНИХ (AC-4(19))

Під час передачі інформації між різними захищеними доменами застосовувати до метаданих ту ж політику безпеки фільтрації, що й для корисних даних.

No: 1
Name: ac_4_19_odp_01
Type: string
Default: nil

Визначено фільтри політики безпеки, які буде застосовано до метаданих

No: 2
Name: ac_4_19_odp_02
Type: string
Default: nil

Визначено фільтри політики конфіденційності, які буде застосовано до метаданих

No: 3
Name: ac_4_19_01
Type: string
Default: nil

При передачі інформації між різними доменами безпеки, <AC-04(19)_ODP[01] фільтри політики безпеки> реалізовано на метаданих

No: 4
Name: ac_4_19_02
Type: string
Default: nil

При передачі інформації між різними доменами безпеки, <AC-04(19)_ODP[02] фільтри політики конфіденційності> реалізовано на метаданих

1.4.20. ЗАТВЕРДЖЕНІ РІШЕННЯ (AC-4(20))

Впровадити [Призначення: визначені організацією рішення про схвалені конфігурації] для керування потоком [Призначення: інформації, визначеної організацією] через захищені домени.

No: 1
Name: ac_4_20_01
Type: string
Default: nil

<AC-04(20)_ODP[01] рішення> використовуються для контролю потоку <AC-04(20)_ODP[02] інформації> між захищеними доменами

No: 2
Name: ac_4_20_odp_01
Type: string
Default: nil

Визначені рішення про схвалені конфігурації для керування потоками інформації через захищені домени

No: 3
Name: ac_4_20_odp_02

Type: string
Default: nil

Визначено інформацію, якою потрібно керувати, коли вона проходить через захищені домени

1.4.21. ФІЗИЧНЕ ТА ЛОГІЧНЕ ВІДДІЛЕННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ (AC-4(21))

Відокремлювати потоки інформації логічно або фізично, використовуючи [Призначення: визначені організацією механізми та/або методи] для досягнення [Призначення: визначеного організацією необхідного поділу за типами інформації].

No: 1
Name: ac_4_21_odp_01
Type: string
Default: "автоматизований засіб моніторингу"

Визначено механізми та/або методи, що використовуються для логічного розділення інформаційних потоків

No: 2
Name: ac_4_21_odp_02
Type: string
Default: "автоматизований засіб моніторингу"

Визначено механізми та/або методи, що використовуються для фізичного розділення інформаційних потоків

No: 3
Name: ac_4_21_odp_03
Type: string
Default: nil

Визначено необхідні поділи за типами інформації

No: 4
Name: ac_4_21_01
Type: string
Default: nil

Інформаційні потоки логічно розділені за допомогою <AC-04(21)_ODP[01] механізмів та/або методів> для досягнення <AC-04(21)_ODP[03] необхідного поділу за типами інформації>

No: 5
Name: ac_4_21_02
Type: string
Default: nil

Інформаційні потоки фізично розділені за допомогою <AC-04(21)_ODP[02] механізмів та/або методів> для досягнення <AC-04(21)_ODP[03] необхідного поділу за типами інформації>

1.4.22. ЄДИНИЙ ДОСТУП (AC-4(22))

Забезпечити доступ з одного пристрою до обчислювальних платформ, застосунків або даних, що розташовуються в декількох різних захищених доменах, одночасно запобігаючи передачі будь-якого потоку інформації між різними захищеними доменами.

No: 1
Name: ac_4_22_01
Type: integer
Default: 30

Доступ забезпечується з одного пристрою до обчислювальних платформ, застосунків або даних, що розташовуються в декількох різних захищених доменах, одночасно запобігаючи передачі інформації між різними захищеними доменами

1.4.23. МОДИФІКОВАНА ІНФОРМАЦІЯ, ЯКА НЕ ПІДЛЯГАЄ ОПРИЛЮДНЕННЮ (AC-4(23))

Під час передачі інформації між різними доменами безпеки змінюйте інформацію, яка не підлягає оприлюдненню, реалізувавши [Призначення: визначена організацією дія модифікації]

No: 1
Name: ac_4_23_odp
Type:
Default: ""

Визначено дію модифікації, що застосовується до інформації, яка не підлягає оприлюдненню;

No: 2
Name: ac_4_23_01
Type: string
Default: nil

AC-04(23) при передачі інформації між доменами безпеки інформація, що не підлягає оприлюдненню, модифікується шляхом реалізації дія модифікації

1.4.24. ВНУТРІШНІЙ НОРМАЛІЗОВАНИЙ ФОРМАТ (AC-4(24))

Під час передачі інформації між різними доменами безпеки аналізуйте вхідні дані у внутрішньому нормалізованому форматі та повторно генеруйте дані, щоб вони відповідали призначеній специфікації.

No: 1
Name: ac_4_24_1
Type: string
Default: nil

При передачі інформації між різними доменами безпеки вхідні дані розбираються у внутрішній, нормалізований формат

No: 2
Name: ac_4_24_2
Type: string
Default: nil

При передачі інформації між різними доменами безпеки дані регенеруються, щоб відповідати їхній специфікації

1.4.25. ОЧИЩЕННЯ ДАНИХ (AC-4(25))

Під час передачі інформації між різними доменами безпеки очищуйте дані, щоб мінімізувати [Вибір (один або кілька): доставка зловмисного вмісту, керування та керування зловмисним кодом, доповнення зловмисного коду та стеганографічно закодовані дані; витік конфіденційної інформації] відповідно до [Призначення: політика, визначена організацією]].

No: 1
Name: ac_4_25_odp_01
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {доставка шкідливого коду, керування та контроль шкідливого коду, доповнення шкідливого коду та даних, закодованих стеганографією; витік конфіденційної інформації}

No: 2
Name: ac_4_25_odp_02
Type: string
Default: nil

Визначено політику очищення даних

No: 3
Name: ac_4_25_01
Type: string
Default: nil

Під час передачі інформації між різними доменами безпеки дані очищуються, щоб мінімізувати <AC-04(25)_ODP[01] вибрані ризики> відповідно до <AC-04(25)_ODP[02] політики>

1.4.26. ДІЇ З ФІЛЬТРАЦІЇ АУДИТУ (AC-4(26))

Під час передачі інформації між різними доменами безпеки записуйте та перевіряйте дії фільтрації вмісту та результати для інформації, що фільтрується.

No: 1
Name: ac_4_26_01
Type: string
Default: nil

При передачі інформації між різними доменами безпеки дії з фільтрації вмісту фіксуються і перевіряються

No: 2
Name: ac_4_26_02
Type: string
Default: nil

При передачі інформації між різними доменами безпеки, результати для інформації, що фільтрується, записуються і перевіряються

1.4.27. НАДЛИШКОВІ/НЕЗАЛЕЖНІ ФІЛЬТРУЮЧІ МЕХАНІЗМИ (AC-4(27))

Під час передачі інформації між різними доменами безпеки впроваджуйте рішення фільтрації вмісту, які забезпечують надлишкові та незалежні механізми фільтрації для кожного типу даних.

No: 1
Name: ac_4_27_01
Type: integer
Default: 30

Під час передачі інформації між системами безпеки впроваджені рішення для фільтрації контенту забезпечують надлишкові та незалежні механізми фільтрації для кожного типу даних

1.4.28. ЛІНІЙНІ ФІЛЬТРУВАЛЬНІ КАНАЛИ (AC-4(28))

Під час передачі інформації між різними доменами безпеки запровадьте конвеєр лінійного фільтрування вмісту, який забезпечується дискреційним і обов'язковим контролем доступу.

No: 1
Name: ac_4_28_01
Type: string
Default: nil

При передачі інформації між доменами безпеки реалізовано лінійний конвеєр фільтрації контенту, який забезпечується дискретними та обов'язковими засобами контролю доступу

1.4.29. ФІЛЬТР МЕХАНІЗМІВ ОРКЕСТРОВКИ (AC-4(29))

Під час передачі інформації між різними доменами безпеки використовуйте механізми оркестровки фільтрів вмісту, щоб забезпечити:
a. Механізми фільтрації вмісту успішно завершують виконання без помилок;
b. Дії фільтрації вмісту виконуються в правильному порядку та відповідають [Призначення: політика, визначена організацією]

No: 1
Name: ac_4_29_a
Type: string
Default: "автоматизований засіб моніторингу"

При передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що механізми фільтрації контенту успішно завершать виконання без помилок

No: 2
Name: ac_4_29_b_01
Type: list
Default: ["login", "logout", "failed_attempt"]

При передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що дії з фільтрації контенту відбуваються в правильному порядку

No: 3
Name: ac_4_29_b_02
Type: list
Default: ["login", "logout", "failed_attempt"]

При передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що дії з фільтрації контенту відповідають політиці.

No: 4
Name: ac_4_29_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політику щодо дій з фільтрації контенту

1.4.30. МЕХАНІЗМИ ФІЛЬТРАЦІЇ З ВИКОРИСТАННЯМ КІЛЬКОХ ПРОЦЕСІВ (AC-4(30))

Під час передачі інформації між різними доменами безпеки реалізуйте механізми фільтрації вмісту за допомогою кількох процесів.

No: 1
Name: ac_4_30_01
Type: string
Default: "автоматизований засіб моніторингу"

При передачі інформації між доменами безпеки реалізовані механізми контент-фільтрації з використанням декількох процесів.

1.4.31. ЗАПОБІГАННЯ СПРОБАМ ПЕРЕДАЧІ ВМІСТУ, ЯКИЙ НЕ ПРОЙШОВ ПЕРЕВІРКУ ФІЛЬТРАЦІЇ (AC-4(31))

Під час передачі інформації між різними доменами безпеки запобігайте передачі вмісту, який не пройшов перевірку фільтрації до домену-одержувача.

No: 1
Name: ac_4_31_01
Type: string
Default: nil

При передачі інформації між різними доменами безпеки запобігається передача вмісту який не пройшов фільрацію

1.4.32. ВИМОГИ ДО ПРОЦЕСУ ПЕРЕДАЧІ ІНФОРМАЦІЇ (AC-4(32))

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації:
a. не фільтрує вміст повідомлення;
b. перевіряє метадані фільтрації;
c. забезпечує успішне завершення фільтрації вмісту, пов'язаного з метаданими фільтрації; і
d. передає вміст до цільового фільтруючого конвеєра.

No: 1
Name: ac_4_32_01
Type: string
Default: nil

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації, не фільтрує вміст повідомлення

No: 2
Name: ac_4_32_02
Type: string
Default: nil

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації, перевіряє метадані фільтрації

No: 3
Name: ac_4_32_03
Type: string
Default: nil

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації, забезпечує успішне завершення фільтрації вмісту, пов'язаного з метаданими фільтрації

No: 4
Name: ac_4_32_04
Type: string
Default: nil

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації, передає вміст до цільового фільтруючого конвеєра

1.5. РОЗМЕЖУВАННЯ ОБОВ'ЯЗКІВ (AC-5)

a. Розмежувати і документувати [Призначення: визначені організацією обов'язки окремих осіб].
b. Установити правила авторизації доступу для підтримки розмежування обов'язків.

No: 1
Name: ac_5_odp_01
Type: string
Default: nil

Визначено обов'язки осіб, які потребують розмежування

No: 2
Name: ac_5_01
Type: string
Default: nil

Обов'язки осіб <AC-05_ODP[01] визначені організацією> розмежовані та задокументовані

No: 3
Name: ac_5_02
Type: string
Default: nil

Встановлено правила авторизації доступу до системи для підтримки розмежування обов'язків

1.6. МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ (AC-6)

Впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та функцій.

No: 1
Name: ac_6_01
Type: string
Default: nil

Застосовується принцип мінімалізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання поставлених завдань організації

1.6.1. АВТОРИЗОВАНИЙ ДОСТУП ДО ФУНКЦІЙ БЕЗПЕКИ (AC-6(1))

Авторизувати доступ до [Призначення: визначені організацією функції безпеки (розгорнуті в апаратному, програмному та мікропрограмному забезпеченні)] та [Призначення: визначена організацією інформація, що має відношення до безпеки] для [Призначення: визначені організацією особи або ролі].

No: 1
Name: ac_6_1_odp_01
Type: string
Default: nil

Визначені особи або ролі з авторизованим доступом до функцій безпеки та інформації, що має відношення до безпеки

No: 2
Name: ac_6_1_odp_02
Type: string
Default: nil

Визначені функції безпеки (розгорнуті в апаратному забезпеченні) для авторизованого доступу

No: 3
Name: ac_6_1_odp_03
Type: string
Default: nil

Визначені функції безпеки (розгорнуті в програмному забезпеченні) для авторизованого доступу

No: 4
Name: ac_6_1_odp_04
Type: string
Default: nil

Визначені функції безпеки (розгорнуті в мікропрограмному забезпеченні) для авторизованого доступу

No: 5
Name: ac_6_1_odp_05
Type: string
Default: nil

Визначено інформацію, важливу для забезпечення безпеки, для авторизованого доступу

No: 6
Name: ac_6_1_a_01
Type: string
Default: nil

Авторизовано доступ для <AC-06(01)_ODP[01] осіб та ролей> до <AC-06(01)_ODP[02] функцій безпеки (розгорнутих на апаратному забезпеченні)>

No: 7
Name: ac_6_1_a_02
Type: string
Default: nil

Авторизовано доступ для <AC-06(01)_ODP[01] осіб та ролей> до <AC-06(01)_ODP[03] функцій безпеки (розгорнутих на програмному забезпеченні)>

No: 8
Name: ac_6_1_a_03
Type: string
Default: nil

Авторизовано доступ для <AC-06(01)_ODP[01] осіб та ролей> до <AC-06(01)_ODP[04] функцій безпеки (розгорнутих на мікропрограмному забезпеченні)>

No: 9
Name: ac_6_1_b
Type: string
Default: nil

Авторизовано доступ для <AC-06(01)_ODP[01] осіб та ролей> до <AC-06(01)_ODP[05] інформації, що має відношення до безпеки>

1.6.2. НЕПРИВІЛЕЙОВАНИЙ ДОСТУП ДО НЕЗАХИЩЕНИХ ФУНКЦІЙ (AC-6(2))

Вимагати від користувачів облікових записів системи або ролей, які мають доступ до [Призначення: визначених організацією функцій безпеки або інформації, що стосується безпеки], використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.

No: 1
Name: ac_6_2_01
Type: list
Default: ["admin", "security_officer"]

Користувачі облікових записів (або ролей) системи з доступом до функцій безпеки або інформації, що стосується безпеки, повинні використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій

No: 2
Name: ac_6_2_odp
Type: string
Default: nil

Визначені функції безпеки або інформація, що стосується безпеки

1.6.3. МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ КОМАНД (AC-6(3))

Авторизувати мережевий доступ до [Призначення: визначені організацією привілейовані команди] лише для [Призначення: визначені організацією потреби] та задокументувати обґрунтування такого доступу в плані безпеки системи.

No: 1
Name: ac_6_3_odp_01
Type: string
Default: nil

Визначено привілейовані команди для яких дозволяється мережевий доступ

No: 2
Name: ac_6_3_odp_02
Type: string
Default: nil

Визначено потреби для яких авторизується мережевий доступ до привілейованих команд

No: 3
Name: ac_6_3_01
Type: string
Default: nil

Мережевий доступ до <AC-06(03)_ODP[01] привілейованих команд> авторизовано лише для <AC-06(03)_ODP[02] потреб>

No: 4
Name: ac_6_3_02
Type: string
Default: nil

Обґрунтування авторизованого мережевого доступу до привілейованих команд задокументовано в плані безпеки системи

1.6.4. РОЗДІЛЬНІ ДОМЕНИ ОБРОБКИ (AC-6(4))

Надати окремі домени обробки даних для забезпечення більш точного розподілу повноважень користувача.

No: 1
Name: ac_6_4_01
Type: string
Default: nil

Надаються окремі домени обробки для більш тонкого розподілу повноважень користувачів

1.6.5. ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ (AC-6(5))

Обмежити привілейовані облікові записи в системі згідно з [Призначення: визначеним організацією персоналом або ролями].

No: 1
Name: ac_6_5_01
Type: list
Default: ["admin", "security_officer"]

Привілейовані облікові записи в системі обмежено персонал або ролі

No: 2
Name: ac_6_5_odp
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким мають бути обмежені привілейовані облікові записи в системі

1.6.6. ПРИВІЛЕЙОВАНИЙ ДОСТУП КОРИСТУВАЧАМИ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ (AC-6(6))

Заборонити привілейований доступ до системи користувачам, які не належать до організації.

No: 1
Name: ac_6_6_01
Type: string
Default: nil

Привілейований доступ до системи для користувачів, які не є членами організації, заборонено

1.6.7. ПЕРЕГЛЯД ПОВНОВАЖЕНЬ КОРИСТУВАЧА (AC-6(7))

a) Переглядати [Призначення: з визначеною організацією частотою] повноваження призначених для [Призначення: визначених організацією посад або класів користувачів] для перевірки необхідності таких повноважень; b) За необхідності перепризначити або зняти повноваження, правильного відображення цілей (місії) організації та потреб організації. для

No: 1
Name: ac_6_7_a
Type: integer
Default: 30

Повноваження, призначені ролям і класам, переглядаються з частотою для перевірки необхідності таких повноважень

No: 2
Name: ac_6_7_b
Type: string
Default: nil

Привілеї перепризначаються або знімаються, якщо це необхідно, для правильного відображення місії організації та потреб

No: 3
Name: ac_6_7_odp_01
Type: integer
Default: 30

Визначено частоту перегляду повноважень, призначених ролям або класам користувачів

No: 4
Name: ac_6_7_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено ролі або класи користувачів, яким призначено повноваження

1.6.8. РІВНІ ПРИВІЛЕЇВ ДЛЯ ВИКОНАННЯ КОДУ (AC-6(8))

Запобігати виконанню програмного забезпечення на рівні привілеїв вищому, ніж доступний користувачеві, який використовує програмне забезпечення [Призначення: визначене організацією програмне забезпечення].

No: 1
Name: ac_6_8_odp_01
Type: string
Default: nil

Визначене програмне забезпечення для якого запобігається виконання на вищому рівні привілеїв

No: 2
Name: ac_6_8_01
Type: string
Default: nil

Запобігається виконання <AC-06(08)_ODP[01] програмного забезпечення> на рівні привілеїв вищому, ніж доступний користувачеві, який його використовує

1.6.9. АУДИТ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ (AC-6(9))

Реєструвати виконання привілейованих функцій.

No: 1
Name: ac_6_9_01
Type: string
Default: nil

Проводиться аудит виконання привілейованих функцій

1.6.10. ЗАБОРОНА НЕПРИВІЛЕЙОВАНИМ КОРИСТУВАЧАМ ВИКОНУВАТИ ПРИВІЛЕЙОВАНІ ФУНКЦІЇ (AC-6(10))

Вжити заходи для запобігання можливості виконувати привілейовані функції непривілейованими користувачами.

No: 1
Name: ac_6_10_01
Type: string
Default: nil

Непривілейовані користувачі не можуть виконувати привілейовані функції

1.7. НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ (AC-7)

a. Встановити обмеження на [Призначення: визначену організацією кількість] послідовних неуспішних спроб входу користувача в систему впродовж [Призначення: визначеного організацією часового періоду].
b. Автоматично виконати [Вибір (один або декілька): блокування облікового запису/вузла на [Призначення: визначений організацією часовий період]; блокування облікового запису/вузла, доки він не буде розблокований адміністратором; затримання наступної команди входу в систему за [Надання: визначеним організацією алгоритмом затримки]; виконати [Призначення: визначені організацією дії]], коли перевищено максимальну кількість невдалих спроб входу в систему.

No: 1
Name: ac_7_odp_01
Type: integer
Default: 3

Визначено кількість послідовних неуспішних спроб входу користувача, дозволених протягом певного періоду часу

No: 2
Name: ac_7_odp_02
Type: string
Default: "15m"

Визначено період часу, яким обмежується кількість послідовних неуспішних спроб входу користувача

No: 3
Name: ac_7_odp_03
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {заблокувати обліковий запис або вузол на період часу; заблокувати обліковий запис або вузол до зняття адміністратором; затримати наступний запит на вхід за алгоритмом затримки; повідомити системного адміністратора; виконати іншу дію}

No: 4
Name: ac_7_odp_04
Type: string
Default: "15m"

Період часу, на який буде заблоковано обліковий запис або вузол (якщо вибрано)

No: 5
Name: ac_7_odp_05

Type: string
Default: nil

Визначено алгоритм затримки наступного запиту на вхід (якщо вибрано)

No: 6
Name: ac_7_odp_06
Type: string
Default: nil

Інша дія, яка буде виконана після перевищення максимальної кількості невдалих спроб (якщо вибрано)

No: 7
Name: ac_7_01
Type: string
Default: nil

Встановлено обмеження на <AC-07_ODP[01] кількість> послідовних неуспішних спроб входу користувача в систему впродовж <AC-07_ODP[02] часового періоду>

No: 8
Name: ac_7_02
Type: string
Default: nil

Автоматично виконується <AC-07_ODP[03] вибрана дія> (із врахуванням <AC-07_ODP[04] періоду блокування>, <AC-07_ODP[05] алгоритму затримки> або <AC-07_ODP[06] інших дій>), коли перевищено максимальну кількість невдалих спроб входу в систему

1.7.1. АВТОМАТИЧНЕ БЛОКУВАННЯ ОБЛІКОВОГО ЗАПИСУ (AC-7(1)) [Вилучено]

[Вилучено: Включено в AC-07]

Немає параметрів для цього контролю.

1.7.2. ОЧИЩЕННЯ АБО СТИРАННЯ МОБІЛЬНОГО ПРИСТРОЮ (AC-7(2))

Очистити або стерти інформацію з [Призначення: визначених організацією мобільних пристроїв] на основі [Призначення: визначених організацією вимог та методик очищення чи стирання] після [Призначення: визначеної організацією кількості] послідовних невдалих спроб входу в систему з пристрою.

No: 1
Name: ac_7_2_01
Type: integer
Default: 3

Інформація очищується або стирається з мобільних пристроїв на основі вимог або методів очищення або стирання після <AC-07(02)_ODP[03 кількість> послідовних, невдалих спроб входу на пристрій

No: 2
Name: ac_7_2_odp_01
Type: string
Default: nil

Визначено мобільні пристрої, які підлягають очищенню або стиранню інформації

No: 3
Name: ac_7_2_odp_02
Type: string
Default: nil

Визначено вимоги та методи очищення чи стирання інформації з мобільних пристроїв

No: 4
Name: ac_7_2_odp_03
Type: integer
Default: 3

Визначається кількість послідовних невдалих спроб входу в систему до того, як інформація буде очищена або стерта з мобільних пристроїв

1.7.3. ОБМЕЖЕННЯ НА СПРОБИ БІОМЕТРИЧНОГО ВХОДУ (AC-7(3))

Обмежити кількість невдалих спроб входу за допомогою біометрики [Призначення: визначена організацією кількість].

No: 1
Name: ac_7_3_odp_01
Type: integer
Default: 3

Визначено кількість невдалих спроб входу за допомогою біометрики

No: 2
Name: ac_7_3_01
Type: string
Default: nil

Обмежено кількість невдалих спроб входу за допомогою біометрики до <AC-07(03)_ODP[01] кількості>

1.7.4. ВИКОРИСТАННЯ АЛЬТЕРНАТИВНОГО ФАКТОРА (AC-7(4))

a) Дозволити використання [Призначення: визначені організацією фактори автентифікації], які відрізняються від основних факторів автентифікації після перевищення визначеної організацією кількості послідовних невдалих спроб входу в систему; b) Обмежити [Призначення: визначена організацією кількість] послідовних невдалих спроб входу за допомогою використання альтернативних факторів користувачем протягом [Призначення: визначеного організацією періоду часу].

No: 1
Name: ac_7_4_odp_01
Type: string
Default: nil

Визначено фактори автентифікації, які дозволено використовувати, що відрізняються від основних факторів

No: 2
Name: ac_7_4_odp_02
Type: integer
Default: 3

Визначено кількість послідовних невдалих спроб входу за допомогою альтернативних факторів

No: 3
Name: ac_7_4_odp_03
Type: string
Default: "15m"

Визначено період часу, протягом якого обмежуються спроби через альтернативні фактори

No: 4
Name: ac_7_4_a
Type: string
Default: nil

Дозволяється використання <AC-07(04)_ODP[01] факторів автентифікації> після перевищення визначеної організацією кількості послідовних невдалих спроб входу

No: 5
Name: ac_7_4_b
Type: string
Default: nil

Обмежено до <AC-07(04)_ODP[02] кількості> послідовних невдалих спроб входу за допомогою використання альтернативних факторів протягом <AC-07(04)_ODP[03] періоду часу>

1.8. ПОПЕРЕДЖЕННЯ ПРО ВИКОРИСТАННЯ СИСТЕМИ (AC-8)

a.
b. Демонструвати користувачам [Призначення: визначене організацією сповіщення або банер про використання системи] перед тим, як надавати доступ до системи, що забезпечує безпеку та приватність відповідно до чинних законів, нормативних документів, наказів, директив, політик, правил, стандартів і керівних принципів, які зазначають, що:
1. користувачі здійснюють доступ до урядової системи;
2. використання системи може контролюватися, реєструватися та підлягати аудиту;
3. несанкціоноване використання системи забороняється та приводить до кримінальної та цивільної відповідальності;
4. використання системи означає згоду на моніторинг і запис дій користувача. Зберігати сповіщення або банер на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу в систему або подальшого доступу до системи.
c. Для загальнодоступних систем:
1. демонструвати інформацію про умови використання системи [Призначення: визначені організацією умови], перш ніж надавати подальший доступ до загальнодоступної системи;
2. демонструвати посилання, якщо такі є, на моніторинг, запис або аудит, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії;
3. мати опис авторизованого використання системи.

No: 1
Name: ac_8_odp_01
Type: string
Default: nil

Визначено сповіщення або банер про використання системи

No: 2
Name: ac_8_odp_02
Type: string
Default: nil

Визначені умови використання загальнодоступної системи

No: 3
Name: ac_8_01
Type: string
Default: nil

Користувачам демонструється <AC-08_ODP[01] сповіщення або банер> перед тим, як надавати доступ до системи

No: 4
Name: ac_8_02
Type: string
Default: nil

Сповіщення зазначає: доступ до урядової системи, можливість контролю/аудиту, заборону несанкціонованого використання та згоду на моніторинг

No: 5
Name: ac_8_03
Type: string
Default: nil

Сповіщення або банер залишається на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу

No: 6
Name: ac_8_04
Type: string
Default: nil

Для загальнодоступних систем демонструється інформація про <AC-08_ODP[02] умови використання>, перш ніж надавати подальший доступ

No: 7
Name: ac_8_05
Type: string
Default: nil

Для загальнодоступних систем демонструються посилання на моніторинг, запис або аудит

No: 8
Name: ac_8_06
Type: string
Default: nil

Для загальнодоступних систем наведено опис авторизованого використання системи

1.9. СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) (AC-9)

Сповіщати користувача після успішного входу (доступу) до системи про дату та час останнього входу (доступу).

No: 1
Name: ac_9_01
Type: integer
Default: 30

Система повідомляє користувача при успішному вході (доступі) до системи про дату та час останнього входу (доступу)

1.9.1. НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ (AC-9(1))

Система сповіщає користувача після успішного входу / доступу про кількість невдалих спроб входу / доступу з моменту останнього успішного входу / доступу.

No: 1
Name: ac_9_1_01
Type: integer
Default: 3

Система сповіщає користувача після успішного входу / доступу про кількість невдалих спроб входу / доступу з моменту останнього успішного входу / доступу

1.9.2. УСПІШНІ ТА НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ (AC-9(2))

Сповіщати користувача, після успішного входу/доступу до системи про кількість [Вибір: успішних спроб доступу/входу; невдалих спроб входу/доступу; обидва варіанти] за [Призначення: визначений організацією період часу].

No: 1
Name: ac_9_2_01
Type: integer
Default: 30

Після успішного входу в систему користувач отримує повідомлення про кількість ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА протягом періоду часу

No: 2
Name: ac_9_2_odp_01
Type: integer
Default: 3

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {успішних спроб доступу/входу; невдалих спроб входу/доступу; обидва варіанти}

No: 3
Name: ac_9_2_odp_02
Type: integer
Default: 30

Визначається період часу, протягом якого система повідомляє користувача про кількість успішних спроб входу в систему, невдалих спроб входу або про обидва випадки

1.9.3. ПОВІДОМЛЕННЯ ПРО ЗМІНИ В ОБЛІКОВОМУ ЗАПИСІ (AC-9(3))

Сповіщати користувача, після успішного входу/доступу, про внесення змін до [Призначення: певних характеристик/параметрів облікового запису користувача, визначених організацією] протягом [Призначення: визначеного організацією періоду часу].

No: 1
Name: ac_9_3_odp_01
Type: string
Default: nil

Визначено характеристики або параметри облікового запису користувача, зміни яких потребують сповіщення

No: 2
Name: ac_9_3_odp_02
Type: string
Default: "15m"

Визначено період часу, протягом якого вносились зміни

No: 3
Name: ac_9_3_01
Type: string
Default: nil

Користувач сповіщається після успішного входу про внесення змін до <AC-09(03)_ODP[01] характеристик/параметрів облікового запису> протягом <AC-09(03)_ODP[02] періоду часу>

1.9.4. СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) – ДОДАТКОВА ІНФОРМАЦІЯ ПРО ВХІД (AC-9(4))

Повідомляти користувачеві, після успішного входу/доступу, наступну додаткову інформацію: [Призначення: інформація, визначена організацією, яка повинна бути включена на додаток до дати та часу останнього входу/доступу].

No: 1
Name: ac_9_4_01
Type: string
Default: nil

Після успішного входу користувач отримує повідомлення додаткова інформація

No: 2
Name: ac_9_4_odp
Type: string
Default: nil

Визначено додаткову інформацію, про яку слід повідомити користувача

1.10. УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ СЕСІЄЮ (AC-10)

Обмежити кількість одночасних сеансів для кожного [Призначення: визначеного організацією облікового запису та/або типу облікового запису] до [Призначення: визначеної організацією кількості].

No: 1
Name: ac_10_odp_01
Type: string
Default: nil

Визначено обліковий запис та/або тип облікового запису, для якого обмежуються одночасні сеанси

No: 2
Name: ac_10_odp_02
Type: integer
Default: 3

Визначено кількість одночасних сеансів, дозволених для кожного облікового запису та/або типу облікового запису

No: 3
Name: ac_10_01
Type: string
Default: nil

Кількість одночасних сеансів для кожного <AC-10_ODP[01] облікового запису та/або типу> обмежена до <AC-10_ODP[02] кількості>

1.11. БЛОКУВАННЯ ПРИСТРОЮ (AC-11)

a. Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою після [Призначення: визначеного організацією періоду] бездіяльності або після отримання запиту від користувача.
b. Зберігати блокування пристрою, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації.

No: 1
Name: ac_11_odp_01
Type: string
Default: nil

Вибрано одне або декілька з наступних значень: {ініціювання блокування пристрою після періоду неактивності; вимога до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду}

No: 2
Name: ac_11_odp_02
Type: string
Default: "15m"

Визначено часовий проміжок бездіяльності, після якого ініціюється блокування пристрою

No: 3
Name: ac_11_a
Type: string
Default: nil

Заборонено подальший доступ до системи шляхом <AC-11_ODP[01] вибору умов блокування>, зокрема після <AC-11_ODP[02] періоду> бездіяльності

No: 4
Name: ac_11_b
Type: string
Default: nil

Блокування пристрою зберігається, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації

1.11.1. ПРИХОВАНІ ДИСПЛЕЇ (AC-11(1))

Система приховує (через блокування сеансу) інформацію, попередньо видиму на дисплеї, загальнодоступним зображенням.

No: 1
Name: ac_11_1_01
Type: string
Default: nil

Система приховує (через блокування сеансу) інформацію, попередньо видиму на дисплеї, загальнодоступним зображенням

1.12. ПРИПИНЕННЯ СЕАНСУ (AC-12)

Сеанс користувача має завершуватися автоматично після [Призначення: визначених організацією умов або тригерних подій, що вимагають припинення сеансу].

No: 1
Name: ac_12_01
Type: string
Default: nil

Сеанс користувача автоматично завершується після виконання умов або подій

No: 2
Name: ac_12_odp
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено умови або події, що вимагають припинення сеансу

1.12.1. ІНІЦІЙОВАНЕ КОРИСТУВАЧЕМ БЛОКУВАННЯ (AC-12(1))

Забезпечити можливість припинення сеансів зв'язку з ініціативи користувача, коли автентифікація використовується для отримання доступу до [Призначення: визначених організацією інформаційних ресурсів].

No: 1
Name: ac_12_1_odp_01
Type: string
Default: nil

Визначено інформаційні ресурси, для доступу до яких використовується автентифікація

No: 2
Name: ac_12_1_01
Type: string
Default: nil

Забезпечується можливість припинення сеансів зв'язку з ініціативи користувача, коли автентифікація використовується для отримання доступу до <AC-12(01)_ODP[01] інформаційних ресурсів>

1.12.2. ПОВІДОМЛЕННЯ ПРО ПРИПИНЕННЯ СЕАНСУ (AC-12(2))

Відобразити виразне повідомлення для користувача, що вказує на достовірне припинення автентифікованих сеансів зв'язку.

No: 1
Name: ac_12_2_01
Type: string
Default: nil

Користувачам буде показано явне повідомлення про завершення сеансу автентифікованого зв'язку

1.12.3. ЗАСТЕРЕЖНЕ ПОВІДОМЛЕННЯ ПРО ТЕ, ЩО ЧАС СЕСІЇ ДОБІГАЄ КІНЦЯ (AC-12(3))

Відобразити виразне повідомлення користувачам, що вказує, що сесія добігає кінця [Завдання: визначений організацією час до кінця сесії].

No: 1
Name: ac_12_3_odp_01
Type: string
Default: "5m"

Визначений час до кінця сесії

No: 2
Name: ac_12_3_01
Type: string
Default: nil

Користувачам відображається виразне повідомлення, що вказує, що сесія добігає кінця за <AC-12(03)_ODP[01] визначений час>

1.13. НАГЛЯД ТА ОГЛЯД - УПРАВЛІННЯ ДОСТУПОМ (AC-13) [Вилучено]

[Вилучено: включено в AC-02 та AU-06]

Немає параметрів для цього контролю.

1.14. ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ (AC-14)

a. Визначити [Призначення: дозволені організацією дії користувачів], які можуть виконуватися в системі без ідентифікації або автентифікації відповідно до завдань та функцій організації.
b. Документувати та визначити відповідне обґрунтування в плані безпеки системи дій користувача, які не потребують ідентифікації або автентифікації.

No: 1
Name: ac_14_a
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії користувача, які можуть бути виконані в системі без ідентифікації або автентифікації, що відповідають місії та функціям організації

No: 2
Name: ac_14_a_02
Type: string
Default: nil

Обґрунтування дій користувачів, які не потребують ідентифікації або автентифікації, надається в плані захисту інформації

No: 3
Name: ac_14_b_01
Type: list
Default: ["login", "logout", "failed_attempt"]

Дії користувачів, які не потребують ідентифікації або автентифікації, задокументовані в плані захисту інформації

No: 4
Name: ac_14_odp
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії користувача, які можуть бути виконані в системі без ідентифікації або автентифікації

1.14.1. ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ НЕОБХІДНЕ ВИКОРИСТАННЯ (AC-14(1)) [Вилучено]

[Вилучено: включено до AC-14]

Немає параметрів для цього контролю.

1.15. АВТОМАТИЗОВАНЕ МАРКУВАННЯ (AC-15) [Вилучено]

[Вилучено: включено до MP-03]

Немає параметрів для цього контролю.

1.16. АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ (AC-16)

a. Визначити засоби для асоціювання (пов'язання) [Призначення: визначених організацією типів атрибутів безпеки та приватності], що приймають [Призначення: визначені організацією значення атрибутів безпеки та приватності] з інформацією, яка зберігається, обробляється та/або передається.
b. Пов'язані атрибути безпеки та приватності мають створюватися і зберігатися разом з інформацією.
c. Встановити дозволені [Призначення: визначені організацією атрибути безпеки та приватності] для [Призначення: систем, визначених організацією].
d. Визначити дозволені [Призначення: визначені організацією значення або діапазони] для кожного з встановлених атрибутів безпеки та приватності.
e. Проводити аудит змін атрибутів.
f. Переглядати атрибути безпеки та приватності на відповідність з [Призначення: визначеною організацією частотою].

No: 1
Name: ac_16_odp_01
Type: string
Default: nil

Визначено типи атрибутів безпеки

No: 2
Name: ac_16_odp_02
Type: string
Default: nil

Визначено типи атрибутів приватності (конфіденційності)

No: 3
Name: ac_16_odp_03
Type: string
Default: nil

Визначено значення атрибутів безпеки

No: 4
Name: ac_16_odp_04
Type: string
Default: nil

Визначено значення атрибутів приватності (конфіденційності)

No: 5
Name: ac_16_odp_05
Type: string
Default: nil

Визначено системи, для яких мають бути встановлені дозволені атрибути безпеки

No: 6
Name: ac_16_odp_06
Type: string
Default: nil

Визначено системи, для яких мають бути встановлені дозволені атрибути приватності

No: 7
Name: ac_16_odp_07
Type: string
Default: nil

Визначено атрибути безпеки, які дозволені для систем

No: 8
Name: ac_16_odp_08
Type: string
Default: nil

Визначено атрибути приватності, які дозволені для систем

No: 9
Name: ac_16_odp_09
Type: string
Default: nil

Визначено значення атрибутів або діапазони для встановлених атрибутів

No: 10
Name: ac_16_odp_10
Type: string
Default: "1 year"

Визначено частоту, з якою слід переглядати атрибути безпеки на предмет відповідності

No: 11
Name: ac_16_odp_11
Type: string
Default: "1 year"

Визначено частоту, з якою слід переглядати атрибути приватності на предмет відповідності

No: 12
Name: ac_16_a_01
Type: string
Default: nil

Визначено засоби для асоціювання <AC-16_ODP[01] типів атрибутів безпеки> з їх <AC-16_ODP[03] значеннями> для інформації

No: 13
Name: ac_16_a_02
Type: string
Default: nil

Визначено засоби для асоціювання <AC-16_ODP[02] типів атрибутів приватності> з їх <AC-16_ODP[04] значеннями> для інформації

No: 14
Name: ac_16_b_01
Type: string
Default: nil

Пов'язані атрибути безпеки створюються і зберігаються разом з інформацією

No: 15
Name: ac_16_b_02
Type: string
Default: nil

Пов'язані атрибути приватності створюються і зберігаються разом з інформацією

No: 16
Name: ac_16_c_01
Type: string
Default: nil

Встановлюються дозволені <AC-16_ODP[07] атрибути безпеки> для <AC-16_ODP[05] систем>

No: 17
Name: ac_16_c_02
Type: string
Default: nil

Встановлюються дозволені <AC-16_ODP[08] атрибути приватності> для <AC-16_ODP[06] систем>

No: 18
Name: ac_16_d_01
Type: string
Default: nil

Визначено дозволені <AC-16_ODP[09] значення або діапазони> для кожного з встановлених атрибутів безпеки та приватності

No: 19
Name: ac_16_e_01
Type: string
Default: nil

Проводиться аудит змін до атрибутів

No: 20
Name: ac_16_f_01
Type: string
Default: nil

Атрибути безпеки перевіряються на відповідність із <AC-16_ODP[10] частотою>

No: 21
Name: ac_16_f_02
Type: string
Default: nil

Атрибути приватності перевіряються на відповідність із <AC-16_ODP[11] частотою>

1.16.1. ДИНАМІЧНЕ ПОВ'ЯЗАННЯ АТРИБУТІВ (AC-16(1))

Атрибути безпеки динамічно пов'язуються з суб'єктами відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: політики безпеки.

No: 1
Name: ac_16_1_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути безпеки динамічно пов'язуються з суб'єктами відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: політики безпеки

No: 2
Name: ac_16_1_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути безпеки динамічно пов'язуються з об'єктами відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: політики безпеки

No: 3
Name: ac_16_1_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути конфіденційності динамічно пов'язуються з суб'єктами відповідно до наведених нижче політик конфіденційності під час створення та комбінування інформації: політики конфіденційності

No: 4
Name: ac_16_1_04
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Атрибути конфіденційності динамічно пов'язуються з об'єктами відповідно до наведених нижче політик конфіденційності під час створення та комбінування інформації: політики конфіденційності

No: 5
Name: ac_16_1_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено суб'єкти, з якими атрибути безпеки повинні динамічно пов'язуватися при створенні та комбінуванні інформації

No: 6
Name: ac_16_1_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено об'єкти, з якими атрибути безпеки повинні динамічно пов'язуватися при створенні та комбінуванні інформації

No: 7
Name: ac_16_1_odp_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені суб'єкти, з якими атрибути конфіденційності повинні динамічно пов'язуватися при створенні та комбінуванні інформації

No: 8
Name: ac_16_1_odp_04
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені об'єкти, з якими атрибути конфіденційності повинні динамічно пов'язуватися при створенні та комбінуванні інформації

No: 9
Name: ac_16_1_odp_05
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики безпеки, що вимагають динамічного пов'язування атрибутів безпеки з суб'єктами та об'єктами

No: 10
Name: ac_16_1_odp_06
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики конфіденційності, що вимагають динамічного пов'язування атрибутів безпеки з суб'єктами та об'єктами; AC-16(01)[01] атрибути безпеки динамічно пов'язуються з суб'єктами відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: політики безпеки

1.16.2. ЗМІНА ЗНАЧЕНЬ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ (AC-16(2))

Надати уповноваженим особам (або процесам, що діють від імені фізичних осіб) можливість визначати або змінювати значення відповідних атрибутів безпеки та приватності.

No: 1
Name: ac_16_2_01
Type: string
Default: nil

Уповноважені особи (або процеси, що діють від імені осіб) мають можливість визначати або змінювати значення пов'язаних з ними атрибутів безпеки

No: 2
Name: ac_16_2_02
Type: string
Default: nil

Уповноважені особи (або процеси, що діють від імені осіб) мають можливість визначати або змінювати значення пов'язаних з ними атрибутів конфіденційності

1.16.3. ПІДТРИМКА СИСТЕМОЮ ПОВ'ЯЗАННЯ АТРИБУТІВ (AC-16(3))

ПОВ'ЯЗАННЯ АТРИБУТІВ Підтримати пов'язання та цілісність [Призначення: визначених організацією атрибутів безпеки та приватності] з [Призначення: визначених організацією суб'єктів і об'єктів].

No: 1
Name: ac_16_3_01
Type: string
Default: nil

Підтримується зв'язок та цілісність атрибутів безпеки з суб'єктами

No: 2
Name: ac_16_3_02
Type: string
Default: nil

Підтримується зв'язок та цілісність атрибутів безпеки з об'єктами

No: 3
Name: ac_16_3_03
Type: string
Default: nil

Підтримується зв'язок та цілісність атрибутів конфіденційності з суб'єктами

No: 4
Name: ac_16_3_04
Type: string
Default: nil

Підтримується зв'язок та цілісність атрибутів конфіденційності з об'єктами.

No: 5
Name: ac_16_3_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути безпеки, які потребують підтримки асоціацій та цілісності

No: 6
Name: ac_16_3_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути конфіденційності, які потребують підтримки асоціації та цілісності

No: 7
Name: ac_16_3_odp_03
Type: string
Default: nil

Визначено суб'єкти, які потребують об'єднання та збереження цілісності атрибутів безпеки, що належать до таких суб'єктів

No: 8
Name: ac_16_3_odp_04

Type: string
Default: nil

Визначено об'єкти, які потребують об'єднання та збереження цілісності атрибутів безпеки, що належать до таких об'єктів

No: 9
Name: ac_16_3_odp_05
Type: string
Default: nil

Визначено суб'єктів, які потребують об'єднання та збереження цілісності атрибутів конфіденційності щодо таких суб'єктів

No: 10
Name: ac_16_3_odp_06
Type: string
Default: nil

Визначено об'єктів, які потребують об'єднання та збереження цілісності атрибутів конфіденційності щодо таких об'єктів

1.16.4. ПОВ'ЯЗАННЯ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ (AC-16(4))

Впровадити можливість пов'язувати [Призначення: визначені організацією атрибути безпеки та приватності] з [Призначення: визначеними організацією суб'єктами та об'єктами] уповноваженими особами (або процесами, що діють від імені фізичних осіб).

No: 1
Name: ac_16_4_odp_01
Type: string
Default: nil

Визначено атрибути безпеки, які пов'язуються з суб'єктами

No: 2
Name: ac_16_4_odp_02
Type: string
Default: nil

Визначено атрибути безпеки, які пов'язуються з об'єктами

No: 3
Name: ac_16_4_odp_03
Type: string
Default: nil

Визначено атрибути приватності, які пов'язуються з суб'єктами

No: 4
Name: ac_16_4_odp_04
Type: string
Default: nil

Визначено атрибути приватності, які пов'язуються з об'єктами

No: 5
Name: ac_16_4_odp_05
Type: string
Default: nil

Визначено суб'єкти, з якими пов'язуються атрибути безпеки

No: 6
Name: ac_16_4_odp_06
Type: string
Default: nil

Визначено об'єкти, з якими пов'язуються атрибути безпеки

No: 7
Name: ac_16_4_odp_07
Type: string
Default: nil

Визначено суб'єкти, з якими пов'язуються атрибути приватності

No: 8
Name: ac_16_4_odp_08
Type: string
Default: nil

Визначено об'єкти, з якими пов'язуються атрибути приватності

No: 9
Name: ac_16_4_01
Type: string
Default: nil

Впроваджено можливість уповноваженим особам (або процесам) пов'язувати <AC-16(04)_ODP[01] атрибути безпеки> з <AC-16(04)_ODP[05] суб'єктами>

No: 10
Name: ac_16_4_02
Type: string
Default: nil

Впроваджено можливість уповноваженим особам (або процесам) пов'язувати <AC-16(04)_ODP[02] атрибути безпеки> з <AC-16(04)_ODP[06] об'єктами>

No: 11
Name: ac_16_4_03
Type: string
Default: nil

Впроваджено можливість уповноваженим особам (або процесам) пов'язувати <AC-16(04)_ODP[03] атрибути приватності> з <AC-16(04)_ODP[07] суб'єктами>

No: 12
Name: ac_16_4_04
Type: string
Default: nil

Впроваджено можливість уповноваженим особам (або процесам) пов'язувати <AC-16(04)_ODP[04] атрибути приватності> з <AC-16(04)_ODP[08] об'єктами>

1.16.5. ВІДОБРАЖЕННЯ АТРИБУТІВ НА ПРИСТРОЯХ ВИВЕДЕННЯ (AC-16(5))

Відображати атрибути безпеки та приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати [Призначення: визначені організацією спеціальні інструкції щодо поширення, обробки чи наступного розподілу

інформації], використовуючи [Призначення: визначену організацією ідентифікацію, у зручній для людини формі про стандартні угоди про присвоєння імен].

No: 1
Name: ac_16_5_odp_01
Type: string
Default: nil

Визначено спеціальні інструкції щодо поширення, обробки чи наступного розподілу інформації

No: 2
Name: ac_16_5_odp_02
Type: string
Default: nil

Визначено стандартні угоди про ідентифікацію (присвоєння імен) у зручній для людини формі

No: 3
Name: ac_16_5_01
Type: string
Default: nil

Атрибути безпеки відображаються у зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати <AC-16(05)_ODP[01] спеціальні інструкції>, використовуючи <AC-16(05)_ODP[02] стандартні угоди>

No: 4
Name: ac_16_5_02
Type: string
Default: nil

Атрибути приватності відображаються у зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати <AC-16(05)_ODP[01] спеціальні інструкції>, використовуючи <AC-16(05)_ODP[02] стандартні угоди>

1.16.6. ПІДТРИМКА ПОВ'ЯЗАННЯ АТРИБУТІВ ОРГАНІЗАЦІЄЮ (AC-16(6))

Вимагати від персоналу пов'язувати та підтримувати асоціацію [Призначення: визначених організацією атрибутів безпеки та приватності] з [Призначенням: визначеними організацією суб'єктами та об'єктами] відповідно до [Призначення: визначеної організацією політики безпеки та приватності].

No: 1
Name: ac_16_6_01
Type: list
Default: ["admin", "security_officer"]

Персонал зобов'язаний пов'язувати та підтримувати зв'язок <AC-16(06)_ODP[01] атрибутів безпеки> з <AC-16(06)_ODP[05] суб'єктами> відповідно до <AC-16(06)_ODP[09] політик безпеки>

No: 2
Name: ac_16_6_02
Type: list
Default: ["admin", "security_officer"]

Персонал зобов'язаний пов'язувати та підтримувати зв'язок <AC-16(06)_ODP[02] атрибутів безпеки> з <AC-16(06)_ODP[06] об'єктами> відповідно до <AC-16(06)_ODP[09] політик безпеки>

No: 3
Name: ac_16_6_03
Type: list
Default: ["admin", "security_officer"]

Персонал зобов'язаний пов'язувати та підтримувати зв'язок <AC-16(06)_ODP[03] атрибутів конфіденційності> з <AC-16(06)_ODP[07] суб'єктами> відповідно до <AC-16(06)_ODP[10] політик безпеки>

No: 4
Name: ac_16_6_04
Type: list
Default: ["admin", "security_officer"]

Персонал зобов'язаний пов'язувати та підтримувати зв'язок <AC-16(06)_ODP[04] атрибутів конфіденційності> з <AC-16(06)_ODP[08] об'єктами> відповідно до <AC-16(06)_ODP[10] політик безпеки>

No: 5
Name: ac_16_6_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути безпеки, які будуть пов'язані з суб'єктами

No: 6
Name: ac_16_6_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути безпеки, які будуть пов'язані з об'єктами

No: 7
Name: ac_16_6_odp_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути конфіденційності, які будуть пов'язані з суб'єктами

No: 8
Name: ac_16_6_odp_04
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено атрибути конфіденційності, які будуть пов'язані з об'єктами

No: 9
Name: ac_16_6_odp_05
Type: string
Default: nil

Визначені суб'єкти, які будуть пов'язані з атрибутами безпеки

No: 10
Name: ac_16_6_odp_06
Type: string
Default: nil

Визначені об'єкти, які будуть пов'язані з атрибутами безпеки

No: 11
Name: ac_16_6_odp_07
Type: string
Default: nil

Визначені суб'єкти, які будуть пов'язані з атрибутами конфіденційності

No: 12
Name: ac_16_6_odp_08
Type: string
Default: nil

Визначені об'єкти, які будуть пов'язані з атрибутами конфіденційності

No: 13
Name: ac_16_6_odp_09
Type: list
Default: ["admin", "security_officer"]

Політики безпеки, які вимагають від персоналу пов'язувати та підтримувати зв'язок атрибутів безпеки та конфіденційності з суб'єктами та об'єктами

No: 14
Name: ac_16_6_odp_10
Type: list
Default: ["admin", "security_officer"]

Політики конфіденційності, які вимагають від персоналу пов'язувати та підтримувати зв'язок атрибутів безпеки та конфіденційності з суб'єктами та об'єктами

1.16.7. ПОСЛІДОВНА ІНТЕРПРЕТАЦІЯ АТРИБУТІВ (AC-16(7))

Забезпечити послідовну інтерпретацію атрибутів безпеки та приватності, що передаються між розподіленими компонентами системи.

No: 1
Name: ac_16_7_01
Type: string
Default: nil

Забезпечується послідовна інтерпретація атрибутів безпеки, що передаються між розподіленими компонентами системи

No: 2
Name: ac_16_7_02
Type: string
Default: nil

Забезпечується послідовна інтерпретація атрибутів приватності (конфіденційності), що передаються між розподіленими компонентами системи

1.16.8. ТЕХНІКИ ТА ТЕХНОЛОГІЇ ПОВ'ЯЗАННЯ АТРИБУТІВ (AC-16(8))

ПОВ'ЯЗАННЯ АТРИБУТІВ Реалізація [Призначення: методи та технології, визначені організацією] для пов'язування атрибутів безпеки та конфіденційності з інформацією.

No: 1
Name: ac_16_8_01
Type: string
Default: nil

Методи та технології застосовуються для пов'язування атрибутів безпеки з інформацією

No: 2
Name: ac_16_8_02

Type: string
Default: nil

Методи та технології застосовуються для пов'язування атрибутів конфіденційності з інформацією

No: 3
Name: ac_16_8_odp_01
Type: string
Default: nil

Визначено методи та технології, які необхідно застосувати для пов'язання інформації з атрибутами безпеки

No: 4
Name: ac_16_8_odp_02
Type: string
Default: nil

Визначено методи та технології, які необхідно застосувати для пов'язання інформації з атрибутами конфіденційності

1.16.9. ПЕРЕПРИЗНАЧЕННЯ АТРИБУТІВ (AC-16(9))

Перепризначення атрибутів безпеки та приватності, пов'язаних з інформацією, здійснювати лише за допомогою механізмів перегляду, перевірених з використанням [Призначення: визначених організацією технік або процедур].

No: 1
Name: ac_16_9_odp_01
Type: string
Default: "автоматизований засіб моніторингу"

Визначено техніки або процедури, що використовуються для перевірки механізмів перегляду при перепризначенні атрибутів безпеки

No: 2
Name: ac_16_9_odp_02
Type: string
Default: "автоматизований засіб моніторингу"

Визначено техніки або процедури, що використовуються для перевірки механізмів перегляду при перепризначенні атрибутів приватності (конфіденційності)

No: 3
Name: ac_16_9_01
Type: string
Default: nil

Перепризначення атрибутів безпеки, пов'язаних з інформацією, здійснюється лише за допомогою механізмів перегляду, перевірених з використанням <AC-16(09)_ODP[01] технік або процедур>

No: 4
Name: ac_16_9_02
Type: string
Default: nil

Перепризначення атрибутів приватності, пов'язаних з інформацією, здійснюється лише за допомогою механізмів перегляду, перевірених з використанням <AC-16(09)_ODP[02] технік або процедур>

1.16.10. КОНФІГУРАЦІЯ АТРИБУТІВ УПОВНОВАЖЕНИМИ ОСОБАМИ (AC-16(10))

Надати уповноваженим особам можливість визначати або змінювати тип і значення атрибутів безпеки та приватності, доступних для пов'язання із суб'єктами та об'єктами.

No: 1
Name: ac_16_10_01
Type: string
Default: nil

Уповноваженим особам надається можливість визначати або змінювати тип і значення атрибутів безпеки, доступних для пов'язання з суб'єктами та об'єктами

No: 2
Name: ac_16_10_02
Type: string
Default: nil

Уповноваженим особам надається можливість визначати або змінювати тип і значення атрибутів приватності (конфіденційності), доступних для пов'язання з суб'єктами та об'єктами

1.17. ВІДДАЛЕНИЙ ДОСТУП (AC-17)

a. Встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу.
b. Авторизувати віддалений доступ до системи, перш ніж будуть дозволені такі підключення.

No: 1
Name: ac_17_a_01
Type: string
Default: nil

Для кожного типу дозволеного віддаленого доступу встановлені та задокументовані обмеження на використання

No: 2
Name: ac_17_a_02
Type: string
Default: nil

Для кожного типу дозволеного віддаленого доступу встановлені та задокументовані вимоги до конфігурації/підключення

No: 3
Name: ac_17_a_03
Type: string
Default: nil

Для кожного типу дозволеного віддаленого доступу встановлені та задокументовані рекомендації щодо здійснення

No: 4
Name: ac_17_b_01
Type: string
Default: nil

Кожен тип віддаленого доступу до системи авторизується перед тим, як дозволити такі підключення

1.17.1. АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ТА УПРАВЛІННЯ (AC-17(1))

Проводиться моніторинг методами віддаленого доступу.

No: 1
Name: ac_17_1_01
Type: string
Default: nil

Проводиться моніторинг методами віддаленого доступу

No: 2
Name: ac_17_1_02
Type: string
Default: nil

Проводиться управління методами віддаленого доступу

1.17.2. ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ (AC-17(2))

Запроваджено криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу.

No: 1
Name: ac_17_2_01
Type: string
Default: "AES-256-GCM"

Запроваджено криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу.

1.17.3. КЕРОВАНІ ТОЧКИ КОНТРОЛЮ ДОСТУПУ (AC-17(3))

Віддалений доступ маршрутизується через авторизовані та керовані точки контролю доступу до мережі.

No: 1
Name: ac_17_3_01
Type: string
Default: nil

Віддалений доступ маршрутизується через авторизовані та керовані точки контролю доступу до мережі

1.17.4. ПРИВІЛЕЙОВАНІ КОМАНДИ ТА ДОСТУП (AC-17(4))

Виконання привілейованих команд за допомогою віддаленого доступу дозволено лише для наступних потреб: <AC-17(04)_ODP[01] потреби >.

No: 1
Name: ac_17_4_odp_01
Type: string

Default: nil

Визначено потреби, що потребують виконання привілейованих команд за допомогою віддаленого доступу

No: 2
Name: ac_17_4_odp_02
Type: string
Default: nil

Визначено потреби, що вимагають доступу до інформації, що стосується безпеки, за допомогою віддаленого доступу

No: 3
Name: ac_17_4_a_01
Type: string
Default: nil

Виконання привілейованих команд за допомогою віддаленого доступу дозволено лише для наступних потреб: <AC-17(04)_ODP[01] потреби >

No: 4
Name: ac_17_4_a_02
Type: string
Default: nil

Доступ до інформації, важливої для безпеки, за допомогою віддаленого доступу дозволяється лише для наступних потреб: <AC-17(04)_ODP[02] потреби >

No: 5
Name: ac_17_4_b
Type: string
Default: nil

Обґрунтування віддаленого доступу задокументовано в плані захисту інформації

1.17.5. МОНІТОРИНГ ДЛЯ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ (AC-17(5)) [Вилучено]

[Вилучено: Включено в CI-04]

Немає параметрів для цього контролю.

1.17.6. ЗАХИСТ ІНФОРМАЦІЇ (AC-17(6))

Інформація про механізми віддаленого доступу захищена від неавторизованого використання та розкриття.

No: 1
Name: ac_17_6_01
Type: string
Default: "автоматизований засіб моніторингу"

Інформація про механізми віддаленого доступу захищена від неавторизованого використання та розкриття

1.17.7. ДОДАТКОВИЙ ЗАХИСТ ДЛЯ ДОСТУПУ ДО ФУНКЦІЙ БЕЗПЕКИ (AC-17(7)) [Вилучено]

[Вилучено: Включено в AC-03(10)]

Немає параметрів для цього контролю.

1.17.8. ДЕАКТИВАЦІЯ НЕЗАХИЩЕНИХ ПРОТОКОЛІВ МЕРЕЖІ (AC-17(8)) [Вилучено]

[Вилучено: Включено в CM-07]

Немає параметрів для цього контролю.

1.17.9. ВІДКЛЮЧЕННЯ АБО ДЕАКТИВАЦІЯ ДОСТУПУ (AC-17(9))

Передбачена можливість відключення або деактивації віддаленого доступу до системи протягом <AC-17(09)_ODP> періоду часу>.

No: 1
Name: ac_17_9_01
Type: integer
Default: 30

Передбачена можливість відключення або деактивації віддаленого доступу до системи протягом <AC-17(09)_ODP> періоду часу>

No: 2
Name: ac_17_9_odp
Type: integer
Default: 30

Визначено період часу, протягом якого потрібно відключити або деактивувати віддалений доступ до системи

1.17.10. (10) АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД (AC-17(10))

Визначені <AC-17(10)_ODP[01] механізми> атентифікують визначені <AC-17(10)_ODP[02] віддалені команди>.

No: 1
Name: ac_17_10_01
Type: string
Default: "автоматизований засіб моніторингу"

Визначені <AC-17(10)_ODP[01] механізми> атентифікують визначені <AC-17(10)_ODP[02] віддалені команди>

No: 2
Name: ac_17_10_odp_01

Type: string
Default: "автоматизований засіб моніторингу"

Визначено механізми, реалізовані для автентифікації віддалених команд

No: 3
Name: ac_17_10_odp_02
Type: string
Default: nil

Визначено віддалені команди, які мають бути автентифіковані механізмами

1.18. БЕЗДРОТОВИЙ ДОСТУП (AC-18)

a. Установити обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення бездротового доступу.
b. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.

No: 1
Name: ac_18_a_01
Type: string
Default: nil

Встановлено обмеження на використання щодо здійснення бездротового доступу

No: 2
Name: ac_18_a_02
Type: string
Default: nil

Встановлено вимоги до конфігурації або підключення щодо здійснення бездротового доступу

No: 3
Name: ac_18_a_03
Type: string
Default: nil

Встановлено рекомендації щодо здійснення бездротового доступу

No: 4
Name: ac_18_b
Type: string
Default: nil

Авторизується бездротовий доступ до системи перед тим, як дозволяти такі з'єднання.

1.18.1. АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ (AC-18(1))

Бездротовий доступ до системи захищено за допомогою автентифікації <AC-18(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

No: 1
Name: ac_18_1_odp
Type: list
Default: ["користувачі", "пристрої"]

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {користувачі; пристрої}

No: 2
Name: ac_18_1_01
Type: string
Default: nil

Бездротовий доступ до системи захищено за допомогою автентифікації <AC-18(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>

No: 3
Name: ac_18_1_02
Type: string
Default: "AES-256-GCM"

Бездротовий доступ до системи захищений за допомогою шифрування

1.18.2. МОНІТОРИНГ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ (AC-18(2)) [Вилучено]

[Вилучено: Включено в SI-04]

Немає параметрів для цього контролю.

1.18.3. ВІДКЛЮЧЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ (AC-18(3))

Відключено, у разі відсутності необхідності у використанні, вбудовані в компоненти системи можливості бездротових мереж до їх виклику та розгортання.

No: 1
Name: ac_18_3_01
Type: string
Default: nil

Відключено, у разі відсутності необхідності у використанні, вбудовані в компоненти системи можливості бездротових мереж до їх виклику та розгортання

1.18.4. ОБМЕЖЕННЯ НАЛАШТУВАННЯ КОРИСТУВАЧАМИ (AC-18(4))

Встановлено користувачів, яким дозволено самостійно налаштовувати можливості бездротової мережі.

No: 1
Name: ac_18_4_01
Type: string
Default: nil

Встановлено користувачів, яким дозволено самостійно налаштовувати можливості бездротової мережі

No: 2
Name: ac_18_4_02
Type: string
Default: nil

Явно авторизуються визначені користувачі, яким дозволено самостійно налаштовувати можливості бездротової мережі

1.18.5. АНТЕНИ ТА РІВЕНЬ ПОТУЖНОСТІ ПЕРЕДАЧІ (AC-18(5))

Вибирано такі радіо антени, які зменшують ймовірність того, що корисні сигнали можуть прийматися за межами контрольованих організацією меж.

No: 1
Name: ac_18_5_01
Type: string
Default: nil

Вибирано такі радіо антени, які зменшують ймовірність того, що корисні сигнали можуть прийматися за межами контрольованих організацією меж

No: 2
Name: ac_18_5_02
Type: string
Default: nil

Калібруються рівні потужності передачі, щоб зменшити ймовірність того, що корисні сигнали можуть прийматися за контрольованими організацією межами

1.19. КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ (AC-19)

a. Встановити обмеження на використання, вимоги до конфігурації, вимоги до підключення і рекомендації щодо впровадження мобільних пристроїв, контрольованих організацією.
b. Авторизувати підключення мобільних пристроїв до систем, які експлуатуються організацією.

No: 1
Name: ac_19_a_01
Type: string
Default: nil

Встановлено вимоги до конфігурації мобільних пристроїв, що контролюються організацією, в тому числі, коли такі пристрої перебувають за межами контрольованої території

No: 2
Name: ac_19_a_02
Type: string
Default: nil

Встановлюються вимоги до підключення для мобільних пристроїв, що контролюються організацією, в тому числі, коли такі пристрої знаходяться за межами контрольованої території

No: 3
Name: ac_19_a_03
Type: string
Default: nil

Розроблено рекомендації щодо впровадження для мобільних пристроїв, які контролюються організацією, в тому числі, коли такі пристрої перебувають за межами контрольованої території

No: 4
Name: ac_19_b

Type: string
Default: nil

Авторизовано підключення мобільних пристроїв до систем організації

1.19.1. ВИКОРИСТАННЯ ПИСЬМОВИХ ТА ПОРТАТИВНИЙ ПРИСТРОЇВ ДЛЯ ЗБЕРІГАННЯ ДАНИХ (AC-19(1)) [Вилучено]

[Вилучено: Включено в MP-07]

Немає параметрів для цього контролю.

1.19.2. ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ (AC-19(2)) [Вилучено]

[Вилучено: Включено в MP-07]

Немає параметрів для цього контролю.

1.19.3. ВИКОРИСТАННЯ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ З НЕІДЕНТИФІКОВАНИМ ВЛАСНИКОМ (AC-19(3))

Використання портативних пристроїв зберігання даних з неідентифікованим власником (ac-19(3)).

Немає параметрів для цього контролю.

1.19.4. ОБМЕЖЕННЯ ДЛЯ ЗАСЕКРЕЧЕНОЇ ІНФОРМАЦІЇ (AC-19(4))

Обмежити доступ для мобільних пристроїв, що обробляють засекречену інформацію.

No: 1
Name: ac_19_4_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено посадових осіб із захисту інформації, відповідальних за огляд та перевірку захищених мобільних пристроїв та інформації, що зберігається на цих пристроях

No: 2
Name: ac_19_4_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики безпеки, що обмежують підключення захищених мобільних пристроїв до засекречених систем

No: 3
Name: ac_19_4_a
Type: string
Default: nil

Використання незахищених мобільних пристроїв на об'єктах, що містять системи, які обробляють, зберігають або передають секретну інформацію, заборонено, за винятком випадків, коли на це є спеціальний дозвіл уповноваженої посадової особи

No: 4
Name: ac_19_4_b_01
Type: string
Default: nil

Заборона підключення незахищених мобільних пристроїв до систем з обмеженим доступом застосовується до осіб, яким уповноважена посадова особа дозволила використовувати незахищені мобільні пристрої на об'єктах, що містять системи, які обробляють, зберігають або передають інформацію з обмеженим доступом

No: 5
Name: ac_19_4_b_02
Type: string
Default: nil

Дозвіл уповноваженої посадової особи на підключення незахищених мобільних пристроїв до незахищених систем вимагається від осіб, яким дозволено використовувати незахищені мобільні пристрої на об'єктах, що містять системи, які обробляють, зберігають або передають інформацію з обмеженим доступом

No: 6
Name: ac_19_4_b_03
Type: string
Default: nil

Заборона використання внутрішніх або зовнішніх модемів чи бездротових інтерфейсів у складі незахищених мобільних пристроїв поширюється на осіб, яким уповноваженою посадовою особою дозволено використовувати незахищені мобільні пристрої під час виконання службових обов'язків, а також на осіб, які не мають права на використання таких пристроїв

No: 7
Name: ac_19_4_b_04_01
Type: string
Default: nil

Вибірковий огляд та перевірка незахищених мобільних пристроїв та інформації, що зберігається на них, <AC-19(04)_ODP[01] посадовими особами> є обов'язковими

No: 8
Name: ac_19_4_b_04_02
Type: string
Default: nil

Дотримання політики обробки інцидентів застосовується у разі виявлення секретної інформації під час випадкового огляду та перевірки незахищених мобільних пристроїв

No: 9
Name: ac_19_4_c
Type: string
Default: nil

Підключення захищенихмобільних пристроїв до засекречених систем обмежено відповідно до <AC-19(04)_ODP[02] політики безпеки>

1.19.5. ПОВНЕ ШИФРУВАННЯ ПРИСТРОЇВ ТА СХОВИЩ ІНФОРМАЦІЇ (AC-19(5))

<AC-19(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРІВ> використовується для захисту конфіденційності та цілісності інформації на <AC-19(05)_ODP[02] мобільних пристроях>.

No: 1
Name: ac_19_5_odp_01
Type: list
Default: ["повне шифрування пристроїв", "шифрування сховищ інформації"]

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повне шифрування пристроїв; шифрування сховищ інформації}

No: 2
Name: ac_19_5_odp_02
Type: string
Default: nil

Визначено мобільні пристрої, на яких слід використовувати шифрування

No: 3
Name: ac_19_5_01
Type: string
Default: nil

<AC-19(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРІВ> використовується для захисту конфіденційності та цілісності інформації на <AC-19(05)_ODP[02] мобільних пристроях>

1.20. ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ (AC-20)

a. [Вибір (один або кілька): Встановіть [Призначення: умови, визначені організацією]; Визначте [Призначення: визначені організацією засоби контролю, які, як стверджується, будуть реалізовані на зовнішніх системах]], узгоджені з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, дозволяючи уповноваженим особам:
1. доступ до системи із зовнішніх систем;
2. обробляти, зберігати або передавати керовану організацією інформацію за допомогою зовнішніх систем;
b. Заборонити використання [Призначення: організаційно-визначені типи зовнішніх систем].

No: 1
Name: ac_20_odp_01
Type: list
Default: ["умови та положення", "заходи захисту"]

Вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {встановити <AC -20_ODP[02] умови та положення>; визначити <AC-20_ODP[03] заходи захисту>}

No: 2
Name: ac_20_odp_02
Type: list
Default: []

Визначено умови та положення, що відповідають довірчим відносинам, встановленим з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи (якщо вибрано)

No: 3
Name: ac_20_odp_03
Type: string
Default: nil

Визначено заходи захисту, які мають бути застосовані до зовнішніх систем відповідно до довірчих відносин, встановлених з іншими організаціями, що володіють, експлуатують та/або обслуговують зовнішні системи (якщо обрано)

No: 4
Name: ac_20_odp_04
Type: string
Default: nil

Визначено типи зовнішніх систем, заборонених до використання

No: 5
Name: ac_20_a_01
Type: string
Default: nil

<AC-20_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> узгоджується(ються) з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, що дозволяє уповноваженим особам отримувати доступ до системи із зовнішніх систем (якщо це застосовно)

No: 6
Name: ac_20_a_02
Type: string
Default: nil

<AC-20_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає(ють) довірчим відносинам, встановленим з іншими організаціями, які володіють, експлуатують та/або підтримують зовнішні системи, що дозволяє уповноваженим особам обробляти, зберігати або передавати інформацію, за допомогою зовнішніх систем (якщо це застосовно)

No: 7
Name: ac_20_b
Type: string
Default: nil

Заборонено використання <AC-20_ODP[04] заборонені типи зовнішніх систем> (якщо застосовно)

1.20.1. ОБМЕЖЕННЯ НА АВТОРИЗОВАНЕ ВИКОРИСТАННЯ (AC-20(1))

Авторизовані особи мають право використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після перевірки виконання заходів безпеки та конфіденційності, зазначених у політиці безпеки та конфіденційності організації, а також планах безпеки та конфіденційності (якщо такі застосовуються).

No: 1
Name: ac_20_1_a
Type: list
Default: ["admin", "security_officer"]

Авторизовані особи мають право використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після перевірки виконання заходів безпеки та конфіденційності, зазначених у політиці безпеки та конфіденційності організації, а також планах безпеки та конфіденційності (якщо такі застосовуються)

No: 2
Name: ac_20_1_b
Type: list
Default: ["admin", "security_officer"]

Авторизовані особи мають право використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після збереження погоджених угод про підключення або обробку системи з структурою організації, на якій розміщена зовнішня система

1.20.2. ПЕРЕНОСНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ (AC-20(2))

Використання портативних пристроїв носіїв інформації уповноваженими особами обмежено у зовнішніх системах за допомогою обмеження.

No: 1
Name: ac_20_2_01
Type: list
Default: ["admin", "security_officer"]

Використання портативних пристроїв носіїв інформації уповноваженими особами обмежено у зовнішніх системах за допомогою обмеження

No: 2
Name: ac_20_2_odp
Type: list
Default: ["admin", "security_officer"]

Визначено обмеження на використання авторизованими особами портативних носіїв інформації у зовнішніх системах

1.20.3. СИСТЕМИ ТА КОМПОНЕНТИ, ЩО НЕ ЗНАХОДЯТЬСЯ У ВЛАСНОСТІ ОРГАНІЗАЦІЇ (AC-20(3))

Використання систем або компонентів систем, що не належать організації, для обробки, зберігання або передачі інформації, що належить організації, обмежується за допомогою обмеження.

No: 1
Name: ac_20_3_01
Type: string
Default: nil

Використання систем або компонентів систем, що не належать організації, для обробки, зберігання або передачі інформації, що належить організації, обмежується за допомогою обмеження

No: 2
Name: ac_20_3_odp
Type: string
Default: nil

Визначено обмеження на використання систем або компонентів систем, що не належать організації, для обробки, зберігання або передачі інформації організації

1.20.4. ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ, ЯКІ МОЖУТЬ МАТИ ДОСТУП ДО МЕРЕЖІ (AC-20(4))

Заборонено використовувати <AC-20(03)_ODP мережеві носії інформації> у зовнішніх системах.

No: 1
Name: ac_20_4_odp
Type: string
Default: nil

Визначано мережеві носії інформації , які можуть мати доступ до мережі

No: 2
Name: ac_20_4_01
Type: string
Default: nil

Заборонено використовувати <AC-20(03)_ODP мережеві носії інформації> у зовнішніх системах

1.20.5. ПОРТАТИВНІ ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ – ЗАБОРОНА ВИКОРИСТАННЯ (AC-20(5))

Використання уповноваженими особами зовнішніх носіїв інформації, підконтрольних організації, на зовнішніх системах заборонено.

No: 1
Name: ac_20_5_01
Type: list
Default: ["admin", "security_officer"]

Використання уповноваженими особами зовнішніх носіїв інформації, підконтрольних організації, на зовнішніх системах заборонено

1.21. РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ (AC-21)

a. Спростити обмін інформацією, надаючи авторизованим користувачам змогу визначати, чи відповідають повноваження на доступ, що призначені партнерам для обміну, обмеженням доступу та повноваженням з приватності щодо інформації для [Призначення: визначених організацією обставин обміну інформацією, коли це необхідно користувачу].
b. Використовувати [Призначення: визначені організацією автоматизовані механізми або ручні процеси], щоб допомогти користувачам в ухваленні рішень щодо обміну інформацією та співпраці.

No: 1
Name: ac_21_a
Type: string
Default: nil

Авторизованим користувачам дозволено визначати, чи відповідають повноваження доступу, призначені партнеру з обміну, обмеженням доступу та використання інформації для обставин обміну інформацією

No: 2
Name: ac_21_b
Type: string
Default: "автоматизований засіб моніторингу"

Автоматизовані механізми використовуються для допомоги користувачам у прийнятті рішень щодо обміну інформацією та співпраці

No: 3
Name: ac_21_odp_01
Type: string
Default: nil

Визначені обставини обміну інформацією, за яких користувач повинен на власний розсуд визначати, чи відповідають повноваження доступу, надані партнеру з обміну, обмеженням доступу та використання інформації

No: 4
Name: ac_21_odp_02
Type: string
Default: "автоматизований засіб моніторингу"

Визначено автоматизовані механізми або ручні процеси, які допомагають користувачам у ухваленні рішень щодо обміну інформацією та співпраці

1.21.1. АВТОМАТИЧНА ПІДТРИМКА УХВАЛЕННЯ РІШЕНЬ (AC-21(1))

Автоматизовані механізми використовуються для забезпечення виконання рішень щодо обміну інформацією уповноваженими користувачами на основі дозволів доступу партнерів з обміну та обмежень доступу до інформації, що підлягає обміну.

No: 1
Name: ac_21_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Автоматизовані механізми використовуються для забезпечення виконання рішень щодо обміну інформацією уповноваженими користувачами на основі дозволів доступу партнерів з обміну та обмежень доступу до інформації, що підлягає обміну

No: 2
Name: ac_21_1_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено автоматизовані механізми, що застосовуються для забезпечення виконання рішень про спільний доступ до інформації авторизованими користувачами

1.21.2. РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ (AC-21(2))

Впроваджено сервіси пошуку та перевірки інформації, які застосовують е обмеження щодо обміну інформацією.

No: 1
Name: ac_21_2_01
Type: string
Default: nil

Впроваджено сервіси пошуку та перевірки інформації, які застосовують е обмеження щодо обміну інформацією

No: 2
Name: ac_21_2_odp
Type: string
Default: nil

Визначено обмеження щодо обміну інформацією

1.22. ПУБЛІЧНО ДОСТУПНИЙ КОНТЕНТ (AC-22)

a. Призначити осіб, що уповноважені на розміщення інформації в загальнодоступній системі.
b. Навчати уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом.
c. Переглядати запропонований зміст інформації до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом.
d. Переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом з [Призначення: визначеною організацією частотою]; така інформація має бути видалена в разі її виявлення.

No: 1
Name: ac_22_odp_01
Type: string
Default: nil

Визначено частоту, з якою слід переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом

No: 2
Name: ac_22_a
Type: string
Default: nil

Визначені особи уповноважені на розміщення інформації в загальнодоступній системі

No: 3
Name: ac_22_b
Type: string
Default: nil

Уповноважені особи проходять навчання, щоб гарантувати, що загальнодоступна інформація не містить інформацію з обмеженим доступом

No: 4
Name: ac_22_c
Type: string
Default: nil

Запропонований зміст інформації перевіряється до публікації в загальнодоступній системі

No: 5
Name: ac_22_d_01
Type: string
Default: nil

Зміст у загальнодоступній системі перевіряється на наявність інформації з обмеженим доступом з <AC-22_ODP[01] частотою>

No: 6
Name: ac_22_d_02
Type: string
Default: nil

Інформація з обмеженим доступом видаляється з загальнодоступної системи, якщо її виявлено

1.23. ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ (AC-23)

Використовувати [Призначення: визначені організацією техніки виявлення та попередження витоку даних] для [Призначення: визначених організацією об'єктів зберігання даних] для виявлення та захисту від несанкціонованого інтелектуального аналізу даних.

No: 1
Name: ac_23_odp_01
Type: string
Default: nil

Визначено техніки виявлення та попередження витоку даних

No: 2
Name: ac_23_odp_02
Type: string
Default: nil

Визначено об'єкти зберігання даних

No: 3
Name: ac_23_01
Type: string
Default: nil

<AC-23_ODP[01] Техніки> використовуються для <AC-23_ODP[02] об'єктів зберігання даних> для виявлення та захисту від несанкціонованого інтелектуального аналізу даних

1.24. РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ (AC-24)

[Вибір: Встановити процедури; Запровадити механізми], щоб забезпечити застосування [Призначення: визначені організацією рішення щодо контролю доступу] до кожного запиту щодо доступу до виконання доступу.

No: 1
Name: ac_24_odp_01
Type: string
Default: nil

Вибрано: встановити процедури; запровадити механізми

No: 2
Name: ac_24_odp_02
Type: string
Default: nil

Визначено рішення щодо контролю доступу

No: 3
Name: ac_24_01
Type: string
Default: nil

Відповідно до <AC-24_ODP[01] вибору>, забезпечується застосування <AC-24_ODP[02] рішень щодо контролю доступу> до кожного запиту щодо доступу до виконання доступу

1.24.1. ІНФОРМАЦІЯ ПРО ПЕРЕДАЧУ АВТОРИЗОВАНОГО ДОСТУПУ (AC-24(1))

Інформація щодо авторизації доступу передається за допомогою заходів безпеки до систем, які забезпечують ухвалення рішень щодо управління доступом. ухвалення.

No: 1
Name: ac_24_1_01
Type: string
Default: nil

Інформація щодо авторизації доступу передається за допомогою заходів безпеки до систем, які забезпечують ухвалення рішень щодо управління доступом. ухвалення

No: 2
Name: ac_24_1_odp_01
Type: string
Default: nil

Визначено інформацію щодо авторизації доступу, яка передається до систем, які забезпечують ухвалення рішень щодо управління доступом

No: 3
Name: ac_24_1_odp_02
Type: string
Default: nil

Визначено заходи безпеки, які слід використовувати, коли інформація про авторизацію передається до систем, що забезпечують виконання рішень щодо управління доступом

No: 4
Name: ac_24_1_odp_03
Type: string
Default: nil

Визначено системи, які забезпечують рішень щодо управління доступом

1.24.2. ВІДСУТНІСТЬ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА АБО ПРОЦЕСУ, ЩО ДІЄ ВІД ІМЕНІ КОРИСТУВАЧА (AC-24(2))

Здійснювати ухвалення рішень щодо управління доступом, засновуючись на [Призначення: визначених організацією атрибутах безпеки], які не охоплюють ідентифікацію користувача

або процесу, що діє від імені користувача.

No: 1
Name: ac_24_2_odp_01
Type: string
Default: nil

Визначено атрибути безпеки, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано)

No: 2
Name: ac_24_2_odp_02
Type: string
Default: nil

Визначено атрибути конфіденційності, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано)

No: 3
Name: ac_24_2_01
Type: string
Default: nil

Рішення щодо управління доступом здійснюються на основі <AC-24(02)_ODP[01] атрибутів безпеки> , які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано)

No: 4
Name: ac_24_2_02
Type: string
Default: nil

Рішення щодо управління доступом здійснюються на основі <AC-24(02)_ODP[02] атрибутів конфіденційності>, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано)

1.25. ДИСПЕТЧЕР ДОСТУПУ (AC-25)

Впровадити диспетчер доступу для [Призначення: визначеної організацією політики контролю доступу], який захищений від несанкціонованого доступу, завжди був доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована.

No: 1
Name: ac_25_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Реалізовано испетчер доступу для <AC-25_ODP політики контролю доступу>, який захищений від несанкціонованого доступу, завжди доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована

No: 2
Name: ac_25_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено політики контролю доступу, для яких реалізовано диспетчер доступу

2. AT

Клас заходів захисту AT — ОБІЗНАНІСТЬ ТА НАВЧАННЯ

Опис Цей клас спрямований на забезпечення належного рівня знань персоналу щодо загроз інформаційній безпеці та їхніх обов'язків у цій сфері.

Перелік заходів захисту Політика та процедури підвищення обізнаності та навчання (AT-1); Навчання з підвищення обізнаності (AT-2); Практичні заняття (AT-2(1)); Внутрішні загрози (AT-2(2)); Соціальна інженерія та соціальний інтелектуальний аналіз даних (AT-2(3)); Підозрілі повідомлення та аномальна поведінка системи (AT-2(4)); Вдосконалена стійка загроза (AT-2(5)); Середовище кіберзагроз (AT-2(6)); Рольове навчання (AT-3); Заходи безпеки робочого середовища (AT-3(1)); Фізичні заходи безпеки (AT-3(2)); Практичні заняття (AT-3(3)); Підозрілі зв'язки та аномальна поведінка системи (AT-3(4)); Обробка персональних даних (AT-3(5)); Навчальні записи (AT-4); Контакти з групами безпеки та асоціаціями (AT-5) [Вилучено]; Відгуки про проведені навчання (AT-6).

2.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА НАВЧАННЯ (AT-1)

a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики обізнаності та навчання у сфері забезпечення безпеки та приватності, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам.
2. Процедури, що сприяють реалізації політики підвищення обізнаності та професійної підготовки в галузі безпеки, приватності, а також пов'язаних з ними заходів захисту інформації та персональних даних.
b. Призначити [Призначення: визначену організацією посадову особу] для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та приватності.
c. Переглядати та оновлювати:
1. Поточну політика [Призначення: частота, визначена організацією] і наступне [Призначення: події, визначені організацією];
2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].

No: 1
Name: at_1_odp_01
Type: string
Default: nil

Визначено персонал або ролі, серед яких має бути поширена політика обізнаності та навчання

No: 2
Name: at_1_odp_02
Type: string
Default: nil

Визначено персонал або ролі, серед яких мають бути поширені процедури, що сприяють реалізації політики підвищення обізнаності

No: 3
Name: at_1_odp_03
Type: list
Default: ["рівень організації", "рівень місії/бізнес-процесу", "рівень системи"]

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи}

No: 4
Name: at_1_odp_04
Type: string
Default: nil

Визначено посадову особу, яка керуватиме політикою та процедурами підвищення обізнаності та навчання

No: 5
Name: at_1_odp_05
Type: string
Default: nil

Визначено частоту, з якою переглядається та оновлюється поточна політика інформування

No: 6
Name: at_1_odp_06
Type: string
Default: nil

Визначено події, які потребують перегляду та оновлення поточної політики

No: 7
Name: at_1_odp_07
Type: string
Default: nil

Визначено частоту, з якою переглядаються та оновлюються поточні процедури

No: 8
Name: at_1_odp_08
Type: string
Default: nil

Визначено події, які потребують перегляду та оновлення поточних процедур

No: 9
Name: at_1_a_01
Type: string
Default: nil

Розроблено та задокументовано політику обізнаності та навчання

No: 10
Name: at_1_a_02
Type: string
Default: nil

Політика обізнаності та навчання поширюється на <AT-01_ODP[01] персонал або ролі>

No: 11
Name: at_1_a_03
Type: string
Default: nil

Розроблені та задокументовані процедури, що сприяють впровадженню політики обізнаності та навчання і пов'язаних з нею засобів контролю доступу

No: 12
Name: at_1_a_04
Type: string
Default: nil

Процедури поширюються на <AT-01_ODP[02] персонал або ролі>

No: 13
Name: at_1_a_01_a_01
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить мету

No: 14
Name: at_1_a_01_a_02
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить сферу застосування

No: 15
Name: at_1_a_01_a_03
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить ролі

No: 16
Name: at_1_a_01_a_04
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить обов'язки

No: 17
Name: at_1_a_01_a_05
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить відповідальність керівництва

No: 18
Name: at_1_a_01_a_06
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить координацію між підрозділами організації

No: 19
Name: at_1_a_01_a_07
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання містить систему контролю відповідності

No: 20
Name: at_1_a_01_b
Type: string
Default: nil

<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика обізнаності та навчання відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам

No: 21
Name: at_1_b
Type: string
Default: nil

<AT-01_ODP[04] посадова особа> призначається для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та конфіденційності

No: 22
Name: at_1_c_01_01
Type: string
Default: nil

Переглядається та оновлюється поточна політика обізнаності та навчання з <AT-01_ODP[05] частототою>

No: 23
Name: at_1_c_01_02
Type: string
Default: nil

Переглядається та оновлюється поточна політика обізнаності та навчання після <AT-01_ODP[06] подій>

No: 24
Name: at_1_c_02_01
Type: string
Default: nil

Переглядаються та оновлюються поточні процедури обізнаності та навчання з <AT-01_ODP[07] частототою>

No: 25
Name: at_1_c_02_02
Type: string
Default: nil

Переглядаються та оновлюються поточні процедури обізнаності та навчання після <AT-01_ODP[08] подій>

2.2. НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ (AT-2)

Впровадити базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включно з менеджерами, керівниками компаній і підрядниками):
a. Забезпечити навчання грамотності з питань безпеки та конфіденційності для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників):
1. як частину початкового навчання для нових користувачів і [Призначення: частота, визначена організацією] після цього;
2. якщо цього потребують системні зміни або наступні [Призначення: події, визначені організацією].
b. Використовувати наведені нижче методи, щоб підвищити рівень безпеки та конфіденційності користувачів системи [Завдання: визначені організацією методи поінформованості];

c. Оновлювати навчання грамотності та зміст обізнаності [Завдання: частота, визначена організацією] і наступні [Завдання: події, визначені організацією];
d. Включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності.

No: 1
Name: at_2_odp_01
Type: string
Default: "щорічно"

Визначено періодичність проведення навчання грамотності з питань безпеки для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу

No: 2
Name: at_2_odp_02
Type: string
Default: "щорічно"

Визначено періодичність проведення навчання грамотності з питань конфіденційності для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу

No: 3
Name: at_2_odp_03
Type: string
Default: nil

Визначено події, які потребують навчання користувачів системи грамотності з питань безпеки

No: 4
Name: at_2_odp_04
Type: string
Default: nil

Визначено події, які потребують навчання користувачів системи грамотності з питань конфіденційності

No: 5
Name: at_2_odp_05
Type: string
Default: nil

Визначено методи, які слід застосовувати для підвищення обізнаності користувачів системи щодо безпеки та конфіденційності

No: 6
Name: at_2_odp_06
Type: string
Default: nil

Визначено частоту оновлення навчання грамотності та змісту обізнаності

No: 7
Name: at_2_odp_07
Type: string
Default: nil

Визначено події після яких необхідне оновлення навчання грамотності та змісту обізнаності

No: 8
Name: at_2_a_01_01
Type: string
Default: nil

Навчання з грамотності з питань безпеки надається користувачам системи (включаючи менеджерів, керівників вищої ланки та підрядників) як частина початкового навчання для нових користувачів

No: 9
Name: at_2_a_01_02
Type: string
Default: nil

Навчання з грамотності з питань конфіденційності надається користувачам системи (включаючи менеджерів, керівників вищої ланки та підрядників) як частина початкового навчання для нових користувачів

No: 10
Name: at_2_a_01_03
Type: string
Default: nil

Для користувачів системи (включно з менеджерами, вищим керівництвом та підрядниками) проводиться навчання з безпеки з <AT-02_ODP[01] періодичністю> після цього

No: 11
Name: at_2_a_01_04
Type: string
Default: nil

Для користувачів системи (включно з менеджерами, вищим керівництвом та підрядниками) проводиться навчання з конфіденційності з <AT-02_ODP[02] періодичністю> після цього

No: 12
Name: at_2_a_02_01
Type: string
Default: nil

Тренінги з грамотності з питань безпеки проводяться для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників), коли цього вимагають зміни в системі або після <AT-02_ODP[03] подій>

No: 13
Name: at_2_a_02_02
Type: string
Default: nil

Тренінги з грамотності з питань конфіденціності проводяться для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників), коли цього вимагають зміни в системі або після <AT-02_ODP[04] подій>

No: 14
Name: at_2_b
Type: string
Default: nil

<AT-02_ODP[05] методи> застосовуються для підвищення обізнаності користувачів системи щодо безпеки та конфіденційності

No: 15
Name: at_2_c_01
Type: string
Default: nil

Оновлюється зміст навчання грамотності та підвищення обізнаності з <AT-02_ODP[06] частотою>

No: 16
Name: at_2_c_02

Type: string
Default: nil

Оновлюється зміст навчання грамотності та підвищення обізнаності після <AT-02_ODP[07] подій>

No: 17
Name: at_2_d
Type: string
Default: nil

Уроки, отримані в результаті внутрішніх або зовнішніх інцидентів або порушень безпеки, включені в методи навчання та підвищення обізнаності

2.2.1. ПРАКТИЧНІ ЗАНЯТТЯ (AT-2(1))

Передбачені практичні вправи з тренування обізнаності, які імітують інциденти в області безпеки та конфіденційності.

No: 1
Name: at_2_1_01
Type: string
Default: nil

Передбачені практичні вправи з тренування обізнаності, які імітують інциденти в області безпеки та конфіденційності

2.2.2. ВНУТРІШНІ ЗАГРОЗИ (AT-2(2))

Ввести до програми навчання вправи з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз.

No: 1
Name: at_2_2_01
Type: string
Default: nil

Введено до програми навчання вправи з розпізнавання потенційних індикаторів внутрішніх загроз

No: 2
Name: at_2_2_02
Type: string
Default: nil

Введено до програми навчання вправи з виявлення потенційних індикаторів внутрішніх загроз

2.2.3. СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА СОЦІАЛЬНИЙ ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ (AT-2(3))

Ввести до програми навчання вправи з підвищення обізнаності щодо розпізнавання та повідомлення про потенційні та фактичні атаки, з використанням методів соціальної інженерії та інтелектуального аналізу соціальних даних.

No: 1
Name: at_2_3_01
Type: string
Default: nil

До програми навчання введено вправи з розпізнавання потенційних та фактичних випадків соціального інжинірингу

No: 2
Name: at_2_3_02
Type: string
Default: nil

До програми навчання введено вправи з повідомлення про потенційні та фактичні випадки соціального інжинірингу

No: 3
Name: at_2_3_03
Type: string
Default: nil

До програми навчання введено вправи з розпізнавання потенційних та фактичних випадків інтелектуального аналізу соціальних даних

No: 4
Name: at_2_3_04
Type: string
Default: nil

До програми навчання введено вправи з повідомлення про потенційні та фактичні випадки інтелектуального аналізу соціальних даних

2.2.4. ПІДОЗРІЛІ ПОВІДОМЛЕННЯ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ (AT-2(4))

Навчання грамотності щодо розпізнавання підозрілих повідомлень та аномальної поведінки у системах організації проводиться з використанням <AT-02(04)_ODP індикаторів>.

No: 1
Name: at_2_4_odp
Type: string
Default: nil

Визначено індикатори шкідливого коду

No: 2
Name: at_2_4_01
Type: string
Default: nil

Навчання грамотності щодо розпізнавання підозрілих повідомлень та аномальної поведінки у системах організації проводиться з використанням <AT-02(04)_ODP індикаторів>

2.2.5. ВДОСКОНАЛЕНА СТІЙКА ЗАГРОЗА (AT-2(5))

Забезпечено навчання грамотності щодо стійкої постійної загрози.

No: 1
Name: at_2_5_01
Type: string
Default: nil

Забезпечено навчання грамотності щодо стійкої постійної загрози

2.2.6. СЕРЕДОВИЩЕ КІБЕРЗАГРОЗ (AT-2(6))

Забезпечено навчання грамотності щодо середовища кіберзагроз.

No: 1
Name: at_2_6_a
Type: string
Default: nil

Забезпечено навчання грамотності щодо середовища кіберзагроз

No: 2
Name: at_2_6_b
Type: string
Default: nil

Відображається поточна інформація про кіберзагрози в операціях системи

2.3. РОЛЬОВЕ НАВЧАННЯ (AT-3)

a. Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками: [Призначення: визначені організацією ролі та обов'язки]:
1. перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і [Призначення: частота, визначена організацією] після цього;
2. коли цього потребують системні зміни.
b. Оновити навчальний контент на основі ролей [Призначення: частота, визначена організацією] і наступні [Призначення: події, визначені організацією];
c. Включіть у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки.

No: 1
Name: at_3_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено ролі та обов'язки для тренінгів з безпеки на основі ролей

No: 2
Name: at_3_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено ролі та обов'язки для тренінгів з конфіденційності на основі ролей

No: 3
Name: at_3_odp_03
Type: string
Default: nil

Визначено частоту проведення тренінгів на основі ролей з безпеки та конфіденційності для призначеного персоналу після початкової підготовки

No: 4
Name: at_3_odp_04
Type: integer
Default: 30

Визначено частоту оновлення змісту навчання на основі ролей

No: 5
Name: at_3_odp_05
Type: string
Default: nil

Визначено події, які потребують оновлення змісту навчання на основі ролей

No: 6
Name: at_3_a_01_01
Type: string
Default: nil

Навчання з безпеки на основі ролей проводиться для <AT-03_ODP[01] ролей та обов'язків> перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків

No: 7
Name: at_3_a_01_02
Type: string
Default: nil

Навчання з конфіденційності на основі ролей проводиться для <AT-03_ODP[02] ролей та обов'язків> перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків

No: 8
Name: at_3_a_01_03
Type: string
Default: nil

Навчання з безпеки на основі ролей проводиться для <AT-03_ODP[01] ролей та обов'язків> з <AT-03_ODP[03] частотою> після цього

No: 9
Name: at_3_a_01_04
Type: string
Default: nil

Навчання з конфіденційності на основі ролей проводиться для <AT-03_ODP[02] ролей та обов'язків> з <AT-03_ODP[03] частотою> після цього

No: 10
Name: at_3_a_02_01
Type: string
Default: nil

Навчання з питань безпеки на основі ролей проводиться для персоналу, який виконує певні ролі та обов'язки у сфері безпеки, коли цього вимагають зміни в системі

No: 11
Name: at_3_a_02_02
Type: string
Default: nil

Навчання з питань конфіденційності на основі ролей проводиться для персоналу, який виконує певні ролі та обов'язки у сфері безпеки, коли цього вимагають зміни в системі

No: 12
Name: at_3_b_01
Type: string
Default: nil

Оновлюється вміст навчання на основі ролей з <AT-03_ODP[04] частотою>

No: 13
Name: at_3_b_02

Type: string
Default: nil

Оновлюється вміст навчання на основі ролей після <AT-03_ODP[05] подій>

No: 14
Name: at_3_c
Type: string
Default: nil

Інформація отримана з внутрішніх чи зовнішніх інцидентів або порушень безпеки, включається в навчання на основі ролей

2.3.1. ЗАХОДИ БЕЗПЕКИ РОБОЧОГО СЕРЕДОВИЩА (AT-3(1))

<AT-03(01)_ODP[01] персонал або ролі> забезпечується підвищенням кваліфікації в галузі зайнятості та функціонування заходів захисту робочого середовища з <AT-03(01)_ODP[02] частотою>.

No: 1
Name: at_3_1_odp_01
Type: string
Default: nil

Визначено персонал або ролі, які мають бути забезпечені початковим навчанням та підвищенням кваліфікації з питань застосування та експлуатації заходів захисту робочого середовища

No: 2
Name: at_3_1_odp_02
Type: string
Default: nil

Визначено частоту проведення підвищення кваліфікації в галузі операцій та функціонування заходів захисту робочого середовища

No: 3
Name: at_3_1_01
Type: string
Default: nil

<AT-03(01)_ODP[01] персонал або ролі> забезпечується підвищенням кваліфікації в галузі зайнятості та функціонування заходів захисту робочого середовища з <AT-03(01)_ODP[02] частотою>

2.3.2. ФІЗИЧНІ ЗАХОДИ БЕЗПЕКИ (AT-3(2))

<AT-03(02)_ODP[01] персонал або ролі> забезпечуються підготовкою з питань застосування та експлуатації заходів фізичної безпеки з <AT-03(02)_ODP[02] частотою>.

No: 1
Name: at_3_2_odp_01
Type: string
Default: nil

Визначаено персонал або ролі, які мають бути забезпечені підготовкою з питань застосування та експлуатації заходів фізичної безпеки

No: 2
Name: at_3_2_odp_02
Type: string
Default: nil

Визначаеночастоту проведення підготовки з питань застосування та експлуатації заходів фізичної безпеки

No: 3
Name: at_3_2_01
Type: string
Default: nil

<AT-03(02)_ODP[01] персонал або ролі> забезпечуються підготовкою з питань застосування та експлуатації заходів фізичної безпеки з <AT-03(02)_ODP[02] частотою>

2.3.3. ПРАКТИЧНІ ЗАНЯТТЯ (AT-3(3))

Програма навчання включає практичні заняття з безпеки, які мають підкріпити досягнення цілей навчання.

No: 1
Name: at_3_3_01
Type: string
Default: nil

Програма навчання включає практичні заняття з безпеки, які мають підкріпити досягнення цілей навчання

No: 2
Name: at_3_3_02
Type: string
Default: nil

Програма навчання включає практичні заняття з конфіденційності, які мають підкріпити досягнення цілей навчання

2.3.4. ПІДОЗРІЛІ ЗВ'ЯЗКИ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ (AT-3(4))

[Вилучено: включено до AT-02(04)].

Немає параметрів для цього контролю.

2.3.5. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ (AT-3(5))

<AT-03(05)_ODP[01] персонал або ролі> навчання з <AT-03(05)_ODP[02] частотою> з використання та управління обробкою персональних даних та контролю прозорості.

No: 1
Name: at_3_5_odp_01
Type: string
Default: nil

Визначено персонал або посади, які мають пройти навчання з використання та управління обробкою персональних даних та контролю прозорості

No: 2
Name: at_3_5_odp_02
Type: string
Default: nil

Визначено періодичність проведення навчання з використання та управління обробкою персональних даних та контролю прозорості

No: 3
Name: at_3_5_01
Type: string
Default: nil

<AT-03(05)_ODP[01] персонал або ролі> навчання з <AT-03(05)_ODP[02] частотою> з використання та управління обробкою персональних даних та контролю прозорості

2.4. НАВЧАЛЬНІ ЗАПИСИ (AT-4)

a. Документувати та відстежувати індивідуальні навчальні заходи із забезпечення безпеки та приватності, включно з базовою підготовкою з питань безпеки та приватності, а також спеціальною підготовкою з питань безпеки та приватності визначених посадових осіб.
b. Зберігати індивідуальні записи про навчання впродовж [Призначення: визначеного організацією періоду часу].

No: 1
Name: at_4_a_01
Type: string
Default: nil

Задокументовані індивідуальні навчальні заходи із забезпечення безпеки та конфіденційності інформації, включно з базовою підготовкою з питань безпеки та конфіденційності, а також спеціальною підготовкою з безпеки та конфіденційності

No: 2
Name: at_4_a_02
Type: string
Default: nil

Відстежуються індивідуальні навчальні заходи із забезпечення безпеки та конфіденційності інформації, включно з базовою підготовкою з питань безпеки та конфіденційності, а також спеціальною підготовкою з безпеки та конфіденційності

No: 3
Name: at_4_b
Type: integer
Default: 30

Індивідуальні записи про навчання зберігаються протягом період часу

No: 4
Name: at_4_odp
Type: integer
Default: 30

Визначено період зберігання індивідуальних записів про навчання

2.5. КОНТАКТИ З ГРУПАМИ БЕЗПЕКИ ТА АСОЦІАЦІЯМИ (AT-5) [Вилучено]

[Вилучено: включено в PM-15]

Немає параметрів для цього контролю.

2.6. ВІДГУКИ ПРО ПРОВЕДЕНІ НАВЧАННЯ (AT-6)

Надати відгук про результати організаційного навчання наступному персоналу [Призначення: з визначеною організацією частотою та визначеному організацією персоналу]

No: 1
Name: at_6_01
Type: list
Default: ["admin", "security_officer"]

Відгуки про результати навчання надаються з визначеною частотою до персоналу

No: 2
Name: at_6_odp_01
Type: integer
Default: 30

Визначено частоту надання відгуків щодо результатів навчання в організації

No: 3
Name: at_6_odp_02
Type: list
Default: ["admin", "security_officer"]

Призначено персонал, якому надаватиметься відгуки щодо результатів навчання в організації

3. AU

Клас заходів захисту AU — АУДИТ ТА ПІДЗВІТНІСТЬ

Опис Цей клас забезпечує можливість відстеження дій у системі, генерування, захист та аналіз записів аудиту для виявлення порушень політики безпеки.

Перелік заходів захисту Політика та процедури аудиту та підзвітності (AU-1); Події аудиту (AU-2); Узагальнення записів про аудит з декількох джерел (AU-2(1)) [Вилучено]; Вибір події аудиту за компонентами (AU-2(2)) [Вилучено]; Перегляд та оновлення (AU-2(3)) [Вилучено]; Привілейовані функції (AU-2(4)) [Вилучено]; Зміст записів аудиту (AU-3); Додаткова інформація про аудит (AU-3(1)); Централізоване управління плановaним змістом записів аудиту (AU-3(2)) [Вилучено]; Обмеження елементів персональних даних (AU-3(3)); Місткість сховища записів аудиту (AU-4); Передача до альтернативного сховища (AU-4(1)); Реагування на відмови обробки даних аудиту (AU-5); Місткість сховища записів аудиту (AU-5(1)); Тривожне сповіщення в реальному часі (AU-5(2)); Налаштування порогового обсягу трафіку (AU-5(3)); Вимкнення у разі відмови (AU-5(4)); Можливість альтернативного журналювання аудиту (AU-5(5)); Огляд, аналіз і звітність аудиту (AU-6); Автоматизована інтеграція процесів

(AU-6(1)); Огляд, аналіз і звітність аудиту сповіщення про порушення безпеку (AU-6(2)) [Вилучено]; Зіставляння сховищ аудиту (AU-6(3)); Централізований перегляд та аналіз (AU-6(4)); Інтегрований аналіз записів аудиту (AU-6(5)); Кореляція з фізичним моніторингом (AU-6(6)); Дозволені дії (AU-6(7)); Аналіз повного тексту привілейованих команд (AU-6(8)); Кореляція з інформацією з нетехнічних джерел (AU-6(9)); Регулювання рівня аудиту (AU-6(10)) [Вилучено]; Скорочення записів аудиту та формування звіту (AU-7); Автоматична обробка (AU-7(1)); Автоматичне сортування та пошук (AU-7(2)) [Вилучено]; Позначка часу (AU-8); Синхронізація з авторитетним джерелом часу (AU-8(1)) [Вилучено]; Вторинне авторитетне джерело часу (AU-8(2)) [Вилучено]; Захист інформації аудиту (AU-9); Апаратні носії інформації одноразового запису (AU-9(1)); Зберігання на окремих фізичних системах або компонентах (AU-9(2)); Криптографічний захист (AU-9(3)); Доступ, який надається через членство в підмножини привілейованих користувачів (AU-9(4)); Подвійна авторизація (AU-9(5)); Доступ тільки для читання (AU-9(6)); Зберігання на компоненті іншої операційної системи (AU-9(7)); Неспростовність (AU-10); Асоціація ідентичності (AU-10(1)); Ратифікація прив'язки інформації про ідентичність виробника (AU-10(2)); Ланцюжок збереження доказів (AU-10(3)); Валідація зв'язку ідентичності перегля- (AU-10(4)); Цифрові підписи (AU-10(5)) [Вилучено]; Збереження записів аудиту (AU-11); Довгострокова можливість отримання (AU-11(1)); Генерація даних аудиту (AU-12); Загальносистемний та синхронізований за часом журналу аудиту (AU-12(1)); Стандартизовані формати (AU-12(2)); Зміни, що вносять авторизовані особи (AU-12(3)); Аудит запитів персональних даних (AU-12(4)); Моніторинг розкриття інформації (AU-13); Використання автоматичних засобів (AU-13(1)); Огляд сайтів, що підлягають моніторингу (AU-13(2)); Авторизоване копіювання інформації (AU-13(3)); Аудит сесії (AU-14); Система запуску (AU-14(1)); Захоплення та запис інформації (AU-14(2)) [Вилучено]; Віддалений перегляд та прослуховування (AU-14(3)); Альтернативна можливість аудиту (AU-15) [Вилучено]; Міжорганізаційний аудит (AU-16); Збереження ідентичності (AU-16(1)); Обмін інформацією аудиту (AU-16(2)); Розмежування (AU-16(3)).

3.1. ПОЛІТИКА ТА ПРОЦЕДУРИ АУДИТУ ТА ПІДЗВІТНОСТІ (AU-1)

a. Розробити, задокументувати та поширити [Призначення: серед персоналу або ролей, що їх визначила організація]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика аудиту та підзвітності, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам.
2. Процедури, що сприяють здійсненню політики аудиту та підзвітності, а також пов'язані з ними заходи аудиту та підзвітності.
b. Призначити [Призначення: визначену організацією старшу посадову особу] для управління політикою та процедурами аудиту та підзвітності.
c. Переглядати та оновлювати поточний аудит та підзвітність:
1. політику [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією];
2. процедури аудиту [Призначення: визначеною організацією частотою] та [Завдання: події, визначені організацією].

No: 1
Name: au_1_a_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Розроблено та задокументовано політику аудиту та підзвітності

No: 2
Name: au_1_a_02
Type: list
Default: ["admin", "security_officer"]

Політика аудиту та підзвітності доведена до персонал або ролі

No: 3
Name: au_1_a_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Розроблені та задокументовані процедури аудиту та підзвітності, що сприяють впровадженню політики аудиту та підзвітності, а також відповідні заходи контролю аудиту та підзвітності

No: 4
Name: au_1_b
Type: list
Default: ["admin", "security_officer"]

Посадова особа призначається для управління політикою та процедурами аудиту та підзвітності AU-01(c)[01][01] переглядається та оновлюється поточна політика аудиту та підзвітності з частота; AU-01(c)[01][02] переглядається та оновлюється поточна політика аудиту та підзвітності після подій; AU-01(c)[02][01] переглядається та оновлюється поточні процедури аудиту та підзвітності з частота; AU-01(c)[02][02] переглядається та оновлюється поточні процедури аудиту та підзвітності після подій

No: 5
Name: au_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, до яких має бути доведена політика аудиту та підзвітності

No: 6
Name: au_1_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюються процедури аудиту та підзвітності

No: 7
Name: au_1_odp_03
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи}

No: 8
Name: au_1_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено посадову особу, яка управлятиме політикою та процедурами аудиту та підзвітності

No: 9
Name: au_1_odp_05
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено частоту, з якою переглядається та оновлюється поточна політика аудиту та підзвітності

No: 10
Name: au_1_odp_06

Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено події, які потребують перегляду та оновлення поточної політики аудиту та підзвітності

No: 11
Name: au_1_odp_07
Type: integer
Default: 30

Визначено частоту, з якою переглядаються та оновлюються поточні процедури аудиту та підзвітності

No: 12
Name: au_1_odp_08
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено події, які потребують перегляду та оновлення поточної процедури аудиту та підзвітності

3.2. ПОДІЇ АУДИТУ (AU-2)

a. Визначити типи подій, які система може реєструвати для підтримки функції аудиту: [Призначення: типи подій, визначені організацією, які система здатна реєструвати];
b. Координувати функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації, пов'язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються;
c. Визначити, які типи подій підлягають аудиту: [Призначення: визначені організацією події, що підлягають аудиту (підмножина подій, що підлягають аудиту, визначених в AU-2 a.), а також частота (або ситуація, що вимагає) проведення аудиту для кожної ідентифікованої події]
d. Обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю;
e. Перегляньте й оновіть типи подій, вибрані для журналювання [Призначення: частота, визначена організацією].

No: 1
Name: au_2_a
Type: string
Default: nil

Типи подій, які система здатна реєструвати, визначено для підтримки функції аудиту

No: 2
Name: au_2_b
Type: string
Default: nil

Функція аудиту безпеки координується з іншими підрозділами організації, які вимагають інформації, пов'язаної з аудитом, длдля посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються

No: 3
Name: au_2_c_01
Type: string
Default: nil

Типи подій (підмножина 02_ODP[01]) визначаються для реєстрації у системі; AU-

No: 4
Name: au_2_c_02

Type: string
Default: "щорічно"

Зазначені типи подій реєструються 02_ODP[03] частота або ситуація>; <AU-

No: 5
Name: au_2_d
Type: string
Default: nil

Надається обґрунтування, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та конфіденційністю

No: 6
Name: au_2_e
Type: string
Default: "щорічно"

Переглядаються та оновлюються типи подій, вибрані для реєстрації, частота. у системі

No: 7
Name: au_2_odp_01
Type: string
Default: nil

Визначено типи подій, які система може реєструвати для підтримки функції аудиту

No: 8
Name: au_2_odp_02
Type: string
Default: nil

Визначено типи подій (підмножина AU-02_ODP[01]) що підлягають аудиту у системі

No: 9
Name: au_2_odp_03
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено частоту або ситуацію, що вимагає проведення аудиту для кожної ідентифікованої події

No: 10
Name: au_2_odp_04
Type: string
Default: "щорічно"

Частота перегляду та оновлення типів подій, обраних для журналювання

3.2.1. УЗАГАЛЬНЕННЯ ЗАПИСІВ ПРО АУДИТ З ДЕКІЛЬКОХ ДЖЕРЕЛ (AU-2(1)) [Вилучено]

[Вилучено: Включено в AU-12]

Немає параметрів для цього контролю.

3.2.2. ВИБІР ПОДІЇ АУДИТУ ЗА КОМПОНЕНТАМИ (AU-2(2)) [Вилучено]

[Вилучено: Включено в AU-12]

Немає параметрів для цього контролю.

3.2.3. ПЕРЕГЛЯД ТА ОНОВЛЕННЯ (AU-2(3)) [Вилучено]

[Вилучено: Включено в AU-02]

Немає параметрів для цього контролю.

3.2.4. ПРИВІЛЕЙОВАНІ ФУНКЦІЇ (AU-2(4)) [Вилучено]

[Вилучено: Включено в AC-06(09)]

Немає параметрів для цього контролю.

3.3. ЗМІСТ ЗАПИСІВ АУДИТУ (AU-3)

Переконатися, що записи аудиту містять інформацію, яка встановлює наступне:
a. який тип події стався;
b. коли відбулася подія;
c. де відбулася подія;
d. джерело події;
e. наслідки події;
f. результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.

No: 1
Name: au_3_a
Type: list
Default: ["login", "logout", "failed_attempt"]

Записи аудиту містять інформацію, яка встановлює який тип події стався

No: 2
Name: au_3_b
Type: string
Default: nil

Записи аудиту містять інформацію, яка встановлює коли подія сталася

No: 3
Name: au_3_c
Type: string
Default: nil

Записи аудиту містять інформацію, яка встановлює де відбулася подія

No: 4
Name: au_3_d
Type: list
Default: ["login", "logout", "failed_attempt"]

Записи аудиту містять інформацію, яка встановлює джерело події

No: 5
Name: au_3_e

Type: list
Default: ["login", "logout", "failed_attempt"]

Записи аудиту містять інформацію, яка встановлює наслідки події

No: 6
Name: au_3_f
Type: list
Default: ["login", "logout", "failed_attempt"]

Записи аудиту містять інформацію, яка встановлює результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією

3.3.1. ДОДАТКОВА ІНФОРМАЦІЯ ПРО АУДИТ (AU-3(1))

Сформовані записи аудиту містять наступну <AU-03(01)_ODP додаткова інформація>.

No: 1
Name: au_3_1_01
Type: string
Default: nil

Сформовані записи аудиту містять наступну <AU-03(01)_ODP додаткова інформація>

No: 2
Name: au_3_1_odp
Type: string
Default: nil

Визначено додаткову інформацію, яка має бути включена до записів аудиту

3.3.2. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПЛАНОВАНИМ ЗМІСТОМ ЗАПИСІВ АУДИТУ (AU-3(2)) [Вилучено]

[Вилучено: Включено до PL-09]

Немає параметрів для цього контролю.

3.3.3. ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ (AU-3(3))

Обмежити персональні дані, що міститься в записах аудиту, до таких елементів, які визначені в оцінці ризику приватності: [Призначення: визначені організацією елементи].

No: 1
Name: au_3_3_01
Type: list
Default: ["admin", "security_officer"]

Інформація, щщо ідентифікує особу, яка міститься в записах аудиту, обмежується <AU-03(03)_ODP елементами>, визначеними в оцінці ризиків конфіденційності

No: 2
Name: au_3_3_odp
Type: string
Default: nil

Визначаються елементи, визначені конфіденційності; в оцінці ризику

3.4. МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ (AU-4)

Розподіляти місткість сховища записів аудиту у відповідності до [Призначення: визначених організацією вимог до зберігання записів аудиту].

No: 1
Name: au_4_01
Type: string
Default: nil

Розподілено ємність для зберігання записів аудиту відповідно до вимог

No: 2
Name: au_4_odp
Type: string
Default: nil

Визначено вимоги до зберігання записів аудиту

3.4.1. ПЕРЕДАЧА ДО АЛЬТЕРНАТИВНОГО СХОВИЩА (AU-4(1))

Записи аудиту вивантажуються на іншу систему або носій інформації, з системи, що перевіряється, з частотою.

No: 1
Name: au_4_1_01
Type: integer
Default: 30

Записи аудиту вивантажуються на іншу систему або носій інформації, з системи, що перевіряється, з частотою

No: 2
Name: au_4_1_odp
Type: integer
Default: 30

Визначено частоту завантаження записів аудиту на іншу систему чи носій інформації, з системи що перевіряється

3.5. РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ (AU-5)

a. Сповіщати [Призначення: визначені організацією персонал або посади] у разі збою обробки даних аудиту в [Призначення: визначений організацією період часу].
b. Виконати наступні додаткові дії: [Призначення: визначені організацією дії, які необхідно зробити].

No: 1
Name: au_5_a
Type: list
Default: ["admin", "security_officer"]

Персонал або ролі отримують сповіщення у разі збою процесу обробки даних аудиту періоду часу

No: 2
Name: au_5_b
Type: list
Default: ["login", "logout", "failed_attempt"]

Додаткові дії виконуються у разі збою процесу обробки даних аудиту

No: 3
Name: au_5_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, які отримують сповіщення про збої в процесі обробки даних аудиту

No: 4
Name: au_5_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено період часу, протягом якого персонал або ролі отримують сповіщення про збої в процесі обробки даних аудиту

No: 5
Name: au_5_odp_03
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено додаткові дії, яких слід вжити у випадку збою в процесі обробки даних аудиту

3.5.1. МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ (AU-5(1))

Попередження надається <AU-05(01)_ODP[01] персоналу або ролям> протягом <AU-05(01)_ODP[02] періоду часу>, коли виділений обсяг сховища журналів аудиту досягає <AU-05(01)_ODP[03] відсотків> від максимального обсягу сховища журналів аудиту.

No: 1
Name: au_5_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, які мають бути попереджені, коли обсяг записів аудиту, що зберігаються, досягає максимуму місткості сховища

No: 2
Name: au_5_1_odp_02
Type: string
Default: nil

Визначено період часу, протягом якого визначений персонал або ролі будуть попереджені

No: 3
Name: au_5_1_odp_03
Type: string
Default: nil

Визначено відсоток максимальної ємності сховища для зберігання журналів аудиту

No: 4
Name: au_5_1_01
Type: string
Default: nil

Попередження надається <AU-05(01)_ODP[01] персоналу або ролям> протягом <AU-05(01)_ODP[02] періоду часу>, коли виділений обсяг сховища журналів аудиту досягає <AU-05(01)_ODP[03] відсотків> від максимального обсягу сховища журналів аудиту

3.5.2. ТРИВОЖНЕ СПОВІЩЕННЯ В РЕАЛЬНОМУ ЧАСІ (AU-5(2))

Забезпечити сповіщення в [Призначення: визначений організацією період реального часу] [Призначення: визначених організацією персоналу, ролей та/або місць], коли відбуваються такі події збою аудиту: [Призначення: визначені організацією події, пов'язані зі збоями та помилками аудиту, які вимагають тривоги в реальному часі].

No: 1
Name: au_5_2_01
Type: list
Default: ["admin", "security_officer"]

Протягом періоду реального часу надається сповіщення персоналу або ролям, коли виникають події

No: 2
Name: au_5_2_odp_01
Type: integer
Default: 30

Визначено період реального часу, за який потрібно надсилати сповіщення при виникненні подій збою аудиту (визначених у AU-05(02)_ODP[03])

No: 3
Name: au_5_2_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, які мають бути сповіщені при виникненні подій збоїв в аудиті (визначених в AU05(02)_ODP[03])

No: 4
Name: au_5_2_odp_03
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено події, пов'язані зі збоями та помилками аудиту

3.5.3. НАЛАШТУВАННЯ ПОРОГОВОГО ОБСЯГУ ТРАФІКУ (AU-5(3))

Здійснювати налаштування порогових значень обсягу трафіку комунікаційних мереж, що відображають обмеження на можливості аудиту та [Вибір: відхиляти; затримувати] мережевий трафік, якщо він перевищує цей поріг.

No: 1
Name: au_5_3_odp

Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {відхилити; затримати}

No: 2
Name: au_5_3_01
Type: string
Default: nil

Застосовуються налаштовані порогові значення обсягу трафіку комунікаційних мереж, що відображають обмеження на можливості аудиту

No: 3
Name: au_5_3_02
Type: string
Default: nil

Мережевий трафік <AU-05(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>, якщо обсяг мережевого трафіку перевищує налаштовані порогові значення

3.5.4. ВИМКНЕННЯ У РАЗІ ВІДМОВИ (AU-5(4))

Застосовувати [Вибір: повне вимикання системи; часткове вимикання системи; знижений режим роботи з обмеженням доступної/цільової функціональності] у разі [Призначення: визначених організацією збоїв аудиту], якщо немає альтернативної можливості аудиту.

No: 1
Name: au_5_4_odp_01
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повне вимикання системи; часткове вимикання системи; знижений режим роботи з обмеженням доступної/цільової функціональності}

No: 2
Name: au_5_4_odp_02
Type: string
Default: nil

Визначено збої аудиту, які спричиняють зміну режиму роботи

No: 3
Name: au_5_4_01
Type: string
Default: nil

<AU-05(04)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> викликається/викликаються у випадку <AU-05(04)_ODP[02] збоїв аудиту>, якщо не існує альтернативної можливості ведення аудиту

3.5.5. МОЖЛИВІСТЬ АЛЬТЕРНАТИВНОГО ЖУРНАЛЮВАННЯ АУДИТУ (AU-5(5))

Надання альтернативної можливості журналювання аудиту в разі збою основної можливості журналювання аудиту, яка реалізується [Призначення: визначена організацією функція альтернативного журналювання аудиту]

No: 1
Name: au_5_5_odp

Type: string
Default: nil

Визначено альтернативний функціонал ведення журналу аудиту на випадок збою в роботі основної функції ведення журналу аудиту

No: 2
Name: au_5_5_01
Type: string
Default: nil

Альтернативна можливість ведення журналу аудиту надається на випадок відмови основної можливості ведення журналу аудиту, який реалізує <AU-05(05)_ODP визначений альтернативний функціонал ведення журналу аудиту>

3.6. ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ (AU-6)

a. Переглядати та аналізувати записи системного аудиту [Призначення: з визначеною організацією частотою] для виявлення [Призначення: визначеної організацією неналежної або незвичайної діяльності].
b. Відправляти звіт про аудит [Призначення: визначеним організацією персоналу або посадам].
c. Налаштувати рівні огляду аудиту, аналізу та звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації.

No: 1
Name: au_6_a
Type: string
Default: "щотижня"

Записи аудиту системи переглядаються та аналізуються частота для виявлення ознак неналежної або незвичної діяльності та потенційного впливу неналежної або незвичної діяльності

No: 2
Name: au_6_b
Type: list
Default: ["admin", "security_officer"]

Звіт аудиту відправляється персоналу або ролям

No: 3
Name: au_6_c
Type: string
Default: nil

Рівень перевірки, аналізу та звітування записів аудиту в системі коригується у разі зміни ризиків на основі інформації правоохоронних органів, розвідувальної інформації або інших достовірних джерел інформації

No: 4
Name: au_6_odp_01
Type: integer
Default: 30

Визначено частоту, з якою переглядаються та аналізуються записи аудиту системи

No: 5
Name: au_6_odp_02
Type: string
Default: nil

Визначена неналежна або незвична діяльність

No: 6
Name: au_6_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі які отримують результати оглядів та аналізів системних записів

3.6.1. АВТОМАТИЗОВАНА ІНТЕГРАЦІЯ ПРОЦЕСІВ (AU-6(1))

Процеси перегляду, аналізу та звітності інтегровані з використанням автоматизованих механізмів.

No: 1
Name: au_6_1_01
Type: string
Default: nil

Процеси перегляду, аналізу та звітності інтегровані з використанням автоматизованих механізмів

No: 2
Name: au_6_1_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено автоматизовані механізми, що використовуються для інтеграції процесів перегляду, аналізу та звітності записів аудиту

3.6.2. ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ БЕЗПЕКУ (AU-6(2)) [Вилучено]

[Вилучено: Включено до SI-4]

Немає параметрів для цього контролю.

3.6.3. ЗІСТАВЛЯННЯ СХОВИЩ АУДИТУ (AU-6(3))

Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.

No: 1
Name: au_6_3_01
Type: string
Default: nil

Аналізуються та зіставляються записи аудиту в різних сховищах, задля забезпечення ситуативної обізнаності в масштабах організації

3.6.4. ЦЕНТРАЛІЗОВАНИЙ ПЕРЕГЛЯД ТА АНАЛІЗ (AU-6(4))

Забезпечити та впровадити можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі.

No: 1
Name: au_6_4_01
Type: string
Default: nil

Забезпечино можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі

No: 2
Name: au_6_4_02
Type: string
Default: nil

Впроваджено можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі

3.6.5. ІНТЕГРОВАНИЙ АНАЛІЗ ЗАПИСІВ АУДИТУ (AU-6(5))

Інтегрувати аналіз записів аудиту з аналізом [Вибір (один або більше): інформації про сканування уразливостей; даних про продуктивність; інформації про моніторинг системи; [Призначення: визначених організацією даних/інформації, зібраних з інших джерел]] для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність.

No: 1
Name: au_6_5_odp_01
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {інформація про сканування вразливостей; дані про продуктивність; інформація про моніторинг системи; <AU-06(05)_ODP[02] дані/інформація, зібрана з інших джерел>}

No: 2
Name: au_6_5_odp_02
Type: string
Default: nil

Визначено дані/інформацію, зібрані з інших джерел, що підлягають аналізу (якщо вони були обрані)

No: 3
Name: au_6_5_01
Type: string
Default: nil

Аналіз записів аудиту інтегровано з аналізом <AU-06(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>, для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність

3.6.6. КОРЕЛЯЦІЯ З ФІЗИЧНИМ МОНІТОРИНГОМ (AU-6(6))

Зіставляти інформацію із записів аудиту з інформацією, отриманою від моніторингу фізичного доступу, для подальшого підвищення здатності ідентифікувати підозрілу, неприйнятну, незвичайну або зловмисну діяльність.

No: 1
Name: au_6_6_01
Type: string
Default: nil

Інформація з записів аудиту співвідноситься з інформацією, отриманою в результаті моніторингу фізичного доступу, для подальшого посилення здатності виявляти підозрілу, невідповідну, незвичну або зловмисну

діяльність

3.6.7. ДОЗВОЛЕНІ ДІЇ (AU-6(7))

Визначити дозволені дії для кожного [Вибір (один або кілька): системного процесу; ролі; користувача], пов'язаного з переглядом, аналізом та поданням інформації про аудит.

No: 1
Name: au_6_7_odp
Type: list
Default: ["admin"]

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {процес системи; роль; користувач};

No: 2
Name: au_6_7_01
Type: string
Default: nil

визначено дозволені дії для кожного <AU-06(07)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> , пов'язані з переглядом, аналізом та поданням інформації про аудит.

3.6.8. АНАЛІЗ ПОВНОГО ТЕКСТУ ПРИВІЛЕЙОВАНИХ КОМАНД (AU-6(8))

Виконувати повний аналіз тексту привілейованих команд аудиту у фізично окремому компоненті чи підсистемі або іншій системі, яка може виконувати такий аналіз.

No: 1
Name: au_6_8_01
Type: string
Default: nil

виконується повний аналіз тексту привілейованих команд аудиту у фізично окремому компоненті чи підсистемі або іншій системі, яка може виконувати такий аналіз.

3.6.9. КОРЕЛЯЦІЯ З ІНФОРМАЦІЄЮ З НЕТЕХНІЧНИХ ДЖЕРЕЛ (AU-6(9))

Зіставляти інформацію з нетехнічних джерел з інформацією аудиту з метою посилення організаційної обізнаності.

No: 1
Name: au_6_9_01
Type: string
Default: nil

Зіставляється інформація з нетехнічних джерел з інформацією аудиту з метою посилення організаційної обізнаності.

3.6.10. РЕГУЛЮВАННЯ РІВНЯ АУДИТУ (AU-6(10)) [Вилучено]

[Вилучено: Включено до AU-06]

Немає параметрів для цього контролю.

3.7. СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ (AU-7)

Забезпечити та реалізувати можливості скорочення записів перевірок аудитом і звітів, до рівня, який:
a. підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;
b. не змінює оригінальний вміст або час упорядкування записів аудиту.

No: 1
Name: au_7_a_1
Type: string
Default: nil

забезпечено можливість скорочення записів перевірок аудитом та звітів, до рінвня що підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;

No: 2
Name: au_7_a_2
Type: string
Default: nil

реалізовано можливість скорочення записів перевірок аудитом та звітів, до рінвня що підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;

No: 3
Name: au_7_b_1
Type: string
Default: nil

забезпечено можливість скорочення записів перевірок аудитом та звітів, які не змінюють оригінальний зміст або час упорядкування записів аудиту;

No: 4
Name: au_7_b_2
Type: string
Default: nil

реалізовано можливість скорочення записів перевірок аудитом та звітів, які не змінюють оригінальний зміст або час упорядкування записів аудиту;

3.7.1. АВТОМАТИЧНА ОБРОБКА (AU-7(1))

Забезпечити можливість обробки записів аудиту для подій, що представляють інтерес, на основі <AU-07(01)_ODP полей в записах аудиту>.

No: 1
Name: au_7_1_odp
Type: string
Default: nil

визначено поля в записах аудиту, які можна обробляти, сортувати або шукати;

No: 2
Name: au_7_1_1
Type: string
Default: nil

забезпечити можливість обробки записів аудиту для подій, що представляють інтерес, на основі <AU-07(01)_ODP полей в записах аудиту>

No: 3
Name: au_7_1_2
Type: string
Default: nil

реалізувати можливість обробки записів аудиту для подій, що представляють інтерес, на основі <AU-07(01)_ODP полей в записах аудиту>

3.7.2. АВТОМАТИЧНЕ СОРТУВАННЯ ТА ПОШУК (AU-7(2)) [Вилучено]

[Вилучено: Включено до AU-07(01)]

Немає параметрів для цього контролю.

3.8. ПОЗНАЧКА ЧАСУ (AU-8)

a. Використовувати внутрішньосистемний годинник для створення позначок часу для записів аудиту.
b. Застосовувати позначки часу, які відповідають [Призначення: деталізація вимірювання часу, визначена організацією] і використовують всесвітній координований час, мають фіксоване зміщення місцевого часу відносно всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.

No: 1
Name: au_8_odp
Type: string
Default: nil

визначено деталізацію вимірювання часу для часових позначок записів аудиту;

No: 2
Name: au_8_a
Type: string
Default: nil

внутрішній системний годинник використовується для створення позначок часу для записів аудиту;

No: 3
Name: au_8_b
Type: string
Default: nil

позначки часу застосовуються для записів аудиту, які відповідають <AU-08_ODP деталізація вимірювання часу> і які використовують всесвітній координований час, мають фіксоване місцеве зміщення місцевого часу від всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.

3.8.1. СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ (AU-8(1)) [Вилучено]

[Вилучено: Включено до SC-45(01)]

Немає параметрів для цього контролю.

3.8.2. ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ (AU-8(2)) [Вилучено]

[Вилучено: Включено до SC-45(02)]

Немає параметрів для цього контролю.

3.9. ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ (AU-9)

a. Захист інформації аудиту та інструментів несанкціонованого доступу, зміни та видалення; журналювання аудиту від
b. Сповіщення [Призначення: персонал або ролі, визначені організацією] у разі виявлення несанкціонованого доступу, зміни або видалення інформації аудиту.

No: 1
Name: au_9_odp
Type: list
Default: ["admin"]

визначено персонал або ролі, які мають бути сповіщені при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту;

No: 2
Name: au_9_a
Type: string
Default: nil

інформація про аудит та інструменти журналювання аудиту захищені від несанкціонованого доступу, зміни та видалення;

No: 3
Name: au_9_b
Type: list
Default: ["admin"]

<AU-09_ODP персонал або ролі> отримують сповіщення при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту.

3.9.1. АПАРАТНІ НОСІЇ ІНФОРМАЦІЇ ОДНОРАЗОВОГО ЗАПИСУ (AU-9(1))

Журнали аудиту записані на апаратні носії інформації з одноразовим записом.

No: 1
Name: au_9_1_01
Type: string
Default: nil

журнали аудиту записані на апаратні носії інформації з одноразовим записом.

3.9.2. ЗБЕРІГАННЯ НА ОКРЕМИХ ФІЗИЧНИХ СИСТЕМАХ АБО КОМПОНЕНТАХ (AU-9(2))

Зберігати записи аудиту з [Призначення: визначеною організацією з частотою] у репозиторії, який є частиною фізично іншої системи або компонента системи, ніж система або компонент, який перевіряється.

No: 1
Name: au_9_2_odp
Type: integer
Default: 30

визначено частоту з якою необхідно зберігати записи аудиту;

No: 2
Name: au_9_2_01
Type: string
Default: nil

зберігати записи аудиту з <AU-09(02)_ODP частотою> у репозиторії, який є частиною іншої системи або компонента системи, не частиною системи або компонента системи, який перевіряється.

3.9.3. КРИПТОГРАФІЧНИЙ ЗАХИСТ (AU-9(3))

Запровадити криптографічні механізми для захисту цілісності інформації аудиту та інструментів аудиту.

No: 1
Name: au_9_3_01
Type: string
Default: nil

впроваджено криптографічні механізми для захисту цілісності інформації аудиту

3.9.4. ДОСТУП, ЯКИЙ НАДАЄТЬСЯ ЧЕРЕЗ ЧЛЕНСТВО В ПІДМНОЖИНИ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ (AU-9(4))

Авторизувати доступ до управління функціональністю аудиту тільки для [Призначення: визначеної організацією підмножини привілейованих користувачів].

No: 1
Name: au_9_4_odp
Type: string
Default: nil

визначено підмножину привілейованих користувачів;

No: 2
Name: au_9_4_01
Type: string
Default: nil

авторизувати доступ до управління функціональністю аудиту тільки для <AU-09(04)_ODP підмножини привілейованих користувачів>.

3.9.5. ПОДВІЙНА АВТОРИЗАЦІЯ (AU-9(5))

Здійснювати подвійну авторизацію для [Вибір (один або кілька): переміщення; видалення] [Призначення: визначеної організацією інформації аудиту].

No: 1
Name: au_9_5_odp_1
Type: integer
Default: 30

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {переміщення; видалення};

No: 2
Name: au_9_5_odp_2
Type: string
Default: nil

визначено інформацію аудиту, для якої має бути застосована подвійна авторизація;

No: 3
Name: au_9_5_01
Type: string
Default: nil

подвійна авторизація застосовується для <AU09(05)_ODP[01] ВИБІРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> з <AU-09(05)_ODP[02] інформації аудиту>.

3.9.6. ДОСТУП ТІЛЬКИ ДЛЯ ЧИТАННЯ (AU-9(6))

Авторизувати доступ лише для читання інформації аудиту для [Призначення: визначеної організацією підмножини привілейованих користувачів].

No: 1
Name: au_9_6_odp
Type: string
Default: nil

визначено підмножину привілейованих користувачів для яких доступ авторизовано тільки для читання.

No: 2
Name: au_9_6_01
Type: string
Default: nil

авторизувати доступ лише для читання інформації аудиту для <AU-09(06)_ODP підмножини привілейованих користувачів>.

3.9.7. ЗБЕРІГАННЯ НА КОМПОНЕНТІ ІНШОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ (AU-9(7))

Зберігати інформацію про аудит на компоненті, що працює з іншою операційною системою, ніж система або компонент, який проходить аудит.

No: 1
Name: au_9_7_01
Type: string
Default: nil

інформація про аудит зберігається на компоненті, що працює з іншою операційною системою, ніж система або компонент, який проходить аудит

3.10. НЕСПРОСТОВНІСТЬ (AU-10)

Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала [Призначення: дії, визначені організацією, на які поширюється принцип неспростовності].

No: 1
Name: au_10_odp
Type: string
Default: nil

визначено дії, на які поширюється принцип неспростовності;

No: 2
Name: au_10_01
Type: string
Default: nil

надаються неспростовні докази того, що особа (або процес, що діє від імені особи) виконала <AU-10_ODP дії>.

3.10.1. АСОЦІАЦІЯ ІДЕНТИЧНОСТІ (AU-10(1))

Особистість джерела інформації зв'язується з інформацією з <AU-10(01)_ODP сила зв'язування>;.

No: 1
Name: au_10_1_odp
Type: string
Default: nil

визначено міцність зв'язку між особистістю джерела інформації та інформацією;

No: 2
Name: au_10_1_a
Type: string
Default: nil

особистість джерела інформації зв'язується з інформацією з <AU-10(01)_ODP сила зв'язування>;

No: 3
Name: au_10_1_b
Type: string
Default: nil

впроваджено засоби, якими уповноважені особи можуть визначити особу виробника інформації.

3.10.2. РАТИФІКАЦІЯ ПРИВ'ЯЗКИ ІНФОРМАЦІЇ ПРО ІДЕНТИЧНІСТЬ ВИРОБНИКА (AU-10(2))

a) Підтвердити прив'язку інформації про ідентичність джерела до інформації з [Призначення: визначеною організацією частотою]. b) Виконати [Призначення: визначені організацією дії] у разі помилки перевірки.

No: 1
Name: au_10_2_01
Type: string
Default: nil

НЕСПРОСТОВНІСТЬ - РАТИФІКАЦІЯ ПРИВ'ЯЗКИ ІНФОРМАЦІЇ ПРО ІДЕНТИЧНІСТЬ ВИРОБНИКА МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: au_10_2_a
Type: integer
Default: 30

Прив'язка інформації про ідентичність джерела до інформації підтвержується з частотою

No: 3
Name: au_10_2_b
Type: list
Default: ["login", "logout", "failed_attempt"]

Виконуються дії у разі помилки перевірки

No: 4
Name: au_10_2_odp_01
Type: integer
Default: 30

Визначено частоту, з якою необхідно підтверджувати прив'язку інформації про ідентичність джерела до інформації

3.10.3. ЛАНЦЮЖОК ЗБЕРЕЖЕННЯ ДОКАЗІВ (AU-10(3))

Підтримувати перегляд і випуск ідентичності та повноважень у межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації.

No: 1
Name: au_10_3_01
Type: string
Default: nil

Підтримується перегляд і випуск ідентичності та повноважень у межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації

3.10.4. ВАЛІДАЦІЯ ЗВ'ЯЗКУ ІДЕНТИЧНОСТІ ПЕРЕГЛЯ- (AU-10(4))

ЗВ'ЯЗКУ ІДЕНТИЧНОСТІ a) Підтвердити прив'язку особистості рецензента до інформації в точках передачі або видачі до її випуску або передачі між [Призначення: визначеними організацією домени безпеки]. b) Виконати [Призначення: визначені організацією дії] у разі помилки перевірки.

No: 1
Name: au_10_4_a
Type: list
Default: ["admin", "security_officer"]

Прив'язка особистості рецензента інформації до інформації в точках передачі або видачі до її випуску або передачі між доменами безпеки підтверджується

No: 2
Name: au_10_4_b
Type: list
Default: ["login", "logout", "failed_attempt"]

Дії виконуються у випадку помилки перевірки

No: 3
Name: au_10_4_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено домени безпеки, для яких прив'язка особи рецензента інформації до інформації повинна бути підтверджена в точках передачі або видачі

No: 4
Name: au_10_4_odp_02
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії, які мають бути виконані у випадку помилки перевірки

3.10.5. ЦИФРОВІ ПІДПИСИ (AU-10(5)) [Вилучено]

[Вилучено: Включено до SI-07]

Немає параметрів для цього контролю.

3.11. ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ (AU-11)

Зберігати записи аудиту впродовж [Призначення: визначеного організацією періоду часу, відповідно політиці зберігання записів], щоб забезпечити підтримку розслідувань (постфактум) інцидентів безпеки та приватності, а також для задоволення вимог нормативних і документів організації щодо збереження даних аудиту.

No: 1
Name: au_11_odp
Type: string
Default: nil

визначено період часу для зберігання записів аудиту, який узгоджується з політикою зберігання записів;

No: 2
Name: au_11_01
Type: string
Default: nil

записи аудиту зберігаються впродовж <AU-11_ODP період часу>, щоб забезпечити підтримку розслідування (постфактум) інцидентів безпеки та конфіденційності, а також відповідати нормативним та вимогам організації щодо збереження даних аудиту.

3.11.1. ДОВГОСТРОКОВА МОЖЛИВІСТЬ ОТРИМАННЯ (AU-11(1))

Впровадити <AU-11(01)_ODP заходи>, щоб гарантувати, що довгострокові записи аудиту, можуть бути отримані.

No: 1
Name: au_11_1_odp
Type: string
Default: nil

визначено заходи, необхідні для реалізації довгострокової можливості отримання записів аудиту

No: 2
Name: au_11_1_01
Type: string
Default: nil

впровадити <AU-11(01)_ODP заходи>, щоб гарантувати, що довгострокові записи аудиту, можуть бути отримані.

3.12. ГЕНЕРАЦІЯ ДАНИХ АУДИТУ (AU-12)

a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [Призначення: визначених організацією компонентах системи].
b. Дозволити [Призначення: визначеному організацією персоналу або посадам] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи;
c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.

No: 1
Name: au_12_odp_1
Type: string
Default: nil

визначено компоненти системи, які забезпечують можливість

No: 2
Name: au_12_odp_2
Type: list
Default: ["admin"]

визначено персонал або ролі, яким дозволено обирати типи подій, що мають реєструватися певними компонентами системи;

No: 3
Name: au_12_a
Type: string
Default: nil

можливість генерації записів аудиту для типів подій, які система

No: 4
Name: au_12_b
Type: list
Default: ["admin"]

<AU-12_ODP[02] персонал або ролі> може/можуть вибирати типи подій, які будуть реєструватися певними компонентами системи;

No: 5
Name: au_12_c
Type: string
Default: nil

згенеровано записи аудиту для типів подій, визначених у AU02_ODP[02], які включають вміст записів аудиту, визначений у AU03.

3.12.1. ЗАГАЛЬНОСИСТЕМНИЙ ТА СИНХРОНІЗОВАНИЙ ЗА ЧАСОМ ЖУРНАЛУ АУДИТУ (AU-12(1))

(01)[01] записи аудиту з <AU-12(01)_ODP[01] компонентів системи> збираються у загальносистемний (логічний або фізичний) журнал аудиту, який синхронізується у часі в межах <AU-12(01)_ODP[02] рівня взаємозв'язку>.

No: 1
Name: au_12_1_odp_1
Type: string
Default: nil

AU-12(01)_ODP[01] визначено компоненти системи, з яких записи аудиту мають бути зібрані в загальносистемний (логічний або фізичний) журнал аудиту;

No: 2
Name: au_12_1_odp_2
Type: string
Default: nil

AU-12(01)_ODP[02] визначено рівень взаємозв'язку між мітками часу окремих записів у журналах аудиту;

No: 3
Name: au_12_1_01
Type: string
Default: nil

AU-12(01)[01] записи аудиту з <AU-12(01)_ODP[01] компонентів системи> збираються у загальносистемний (логічний або фізичний) журнал аудиту, який синхронізується у часі в межах <AU-12(01)_ODP[02] рівня взаємозв'язку>.

3.12.2. СТАНДАРТИЗОВАНІ ФОРМАТИ (AU-12(2))

Створити загальносистемний (логічний або фізичний) журнал аудиту, що складається із записів аудиту в стандартизованому форматі.

No: 1
Name: au_12_2_01
Type: string
Default: nil

Створюється загальносистемний (логічний) журнал аудиту, що складається з записів аудиту в стандартизованому форматі

3.12.3. ЗМІНИ, ЩО ВНОСЯТЬ АВТОРИЗОВАНІ ОСОБИ (AU-12(3))

Забезпечити та реалізувати можливість для [Призначення: визначених організацією окремих осіб або ролей] змінити аудит, який виконуватиметься на [Призначення: визначених організацією компонентах системи] на основі [Призначення: визначених організацією критеріїв вибору подій] у межах [Призначення: визначених організацією часових порогів].

No: 1
Name: au_12_3_odp_1
Type: list
Default: ["admin"]

Визначено осіб або ролі, яким дозволено змінювати аудит компонентів системи;

No: 2
Name: au_12_3_odp_2
Type: string
Default: nil

Визначено компоненти системи, на яких має виконуватися аудит;

No: 3
Name: au_12_3_odp_3
Type: string
Default: nil

Визначено критерії вибору подій;

No: 4
Name: au_12_3_odp_4
Type: string
Default: nil

Визначено часові пороги, в яких мають змінюватися аудит;

No: 5
Name: au_12_3_1
Type: string
Default: nil

Забезпечено можливість <AU-12(03)_ODP[01] особам або часових порогів>;

No: 6
Name: au_12_3_2
Type: string
Default: nil

Реалізовано можливість <AU-12(03)_ODP[01] особам або часових порогів>;

3.12.4. АУДИТ ЗАПИТІВ ПЕРСОНАЛЬНИХ ДАНИХ (AU-12(4))

Забезпечити та реалізувати можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональні дані.

No: 1
Name: au_12_4_1
Type: list
Default: ["admin"]

забезпечена можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію.

No: 2
Name: au_12_4_2
Type: list
Default: ["admin"]

реалізувана можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію.

3.13. МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ (AU-13)

a. Моніторинг [Завдання: визначена організацією інформація з відкритих джерел та/або інформаційних сайтів] [Завдання: частота, визначена організацією] на наявність доказів неавторизованого розголошення конфіденційної інформації;
b. Якщо виявлено розголошення інформації:
1. Повідомити [Призначення: персонал або ролі, визначені організацією];
2. Виконайте такі додаткові дії: [Призначення: додаткові дії, визначені організацією].

No: 1
Name: au_13_odp_1
Type: string
Default: nil

визначено інформацію з відкритих джерел та/або інформаційні сайти, що підлягають моніторингу на наявність доказів неавторизованого розголошення конфіденційної інформації;

No: 2
Name: au_13_odp_2
Type: integer
Default: 30

визначено частоту моніторингу інформації з відкритих джерел та/або інформаційних сайтів на наявність доказів неавторизованого розголошення конфіденційної інформації;

No: 3
Name: au_13_odp_3
Type: list
Default: ["admin"]

визначено персонал або ролі, які мають бути повідомлені в разі виявлення розголошення інформації;

No: 4
Name: au_13_odp_4
Type: string
Default: nil

визначено додаткові дії, як і необхідно вжити у разі виявлення розголошення інформації;

No: 5
Name: au_13_a
Type: string
Default: nil

<AU-13_ODP[01] інформація з відкритих джерел та/або інформаційні сайти> відстежуються <AU-13_ODP[02] частота> на наявність доказів неавторизованого розголошення конфіденційної інформації;

No: 6
Name: au_13_b_1
Type: list
Default: ["admin"]

<AU-13_ODP[03] персонал або ролі> буде повідомлено, якщо буде виявлено розголошення інформації;

No: 7
Name: au_13_b_2
Type: string
Default: nil

<AU-13_ODP[04] додаткові дії> вживаються, якщо виявлено розголошення інформації.

3.13.1. ВИКОРИСТАННЯ АВТОМАТИЧНИХ ЗАСОБІВ (AU-13(1))

Моніторинг інформації з відкритих джерел та інформаційних сайтів здійснюється за допомогою <AU-13(01)_ODP автоматизовані механізми>.

No: 1
Name: au_13_1_odp
Type: string
Default: nil

визначено автоматизовані механізми моніторингу інформації з відкритих джерел та інформаційних сайтів;

No: 2
Name: au_13_1_01
Type: string
Default: nil

моніторинг інформації з відкритих джерел та інформаційних сайтів здійснюється за допомогою <AU-13(01)_ODP автоматизовані механізми>.

3.13.2. ОГЛЯД САЙТІВ, ЩО ПІДЛЯГАЮТЬ МОНІТОРИНГУ (AU-13(2))

Проводити огляд відкритих інформаційних сайтів, що підлягають моніторингу [Призначення: з визначеною організацією частотою].

No: 1
Name: au_13_2_odp
Type: integer
Default: 30

визначено частоту з якою проводять огляд відкритих інформаційних сайтів, що підлягають моніторингу

No: 2
Name: au_13_2_01
Type: string
Default: nil

проводиться огляд відкритих інформаційних сайтів, що підлягають моніторингу з <AU-13(02)_ODP частотою>.

3.13.3. АВТОРИЗОВАНЕ КОПІЮВАННЯ ІНФОРМАЦІЇ (AU-13(3))

Використовуйте методи виявлення, процеси та інструменти, щоб визначити, чи зовнішні суб'єкти копіюють організаційну інформацію неавторизованим способом.

No: 1
Name: au_13_3_01
Type: string
Default: nil

застосовуються методи, процеси та інструменти виявлення, щоб визначити, чи не копіюють зовнішні суб'єкти інформацію організації в несанкціонований спосіб.

3.14. АУДИТ СЕСІЇ (AU-14)

a. Надавати та реалізувати можливість для [Призначення: користувачів або ролей, визначених організацією] для [Вибору (одного або кількох): збору/запису або перегляду/прослуховування] вмісту сесії користувача в [Призначення: обставини, визначені організацією];
b. Розробляти, інтегрувати та використовувати діяльність з аудиту сесії, консультуючись із юрисконсультантом щодо її відповідності до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів і вказівок.

No: 1
Name: au_14_odp_1
Type: list
Default: ["admin"]

визначено користувачів або ролі, які можуть перевіряти вміст сесії користувача;

No: 2
Name: au_14_odp_2
Type: integer
Default: 30

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {збору/запису або перегляду/прослуховування};

No: 3
Name: au_14_odp_3
Type: list
Default: ["admin"]

визначено обставини, за яких вміст сесії користувача може бути перевірено;

No: 4
Name: au_14_a_1
Type: list
Default: ["admin"]

<AU-14_ODP[01] користувачам або ролям> надається можливість

No: 5
Name: au_14_a_2
Type: list
Default: ["admin"]

реалізовано можливість для <AU-14_ODP[01] користувачів або

No: 6
Name: au_14_b_1
Type: string
Default: nil

діяльність з аудиту сесій розробляється після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;

No: 7
Name: au_14_b_2
Type: string
Default: nil

діяльність з аудиту сесій інтегрується після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;

No: 8
Name: au_14_b_3

Type: string
Default: nil

діяльність з аудиту сесій використовується після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;

3.14.1. СИСТЕМА ЗАПУСКУ (AU-14(1))

Аудит сесії при запуску системи автоматично ініціюється.

No: 1
Name: au_14_1_01
Type: string
Default: nil

аудит сесії при запуску системи автоматично ініціюється

3.14.2. ЗАХОПЛЕННЯ ТА ЗАПИС ІНФОРМАЦІЇ (AU-14(2)) [Вилучено]

[Вилучено: Включено до AU-14] [Вилучено: Включено до AU-14]

Немає параметрів для цього контролю.

3.14.3. ВІДДАЛЕНИЙ ПЕРЕГЛЯД ТА ПРОСЛУХОВУВАННЯ (AU-14(3))

Забезпечити та реалізувати можливість авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, у режимі реального часу.

No: 1
Name: au_14_3_1
Type: list
Default: ["admin"]

забезпечується можливість для авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, в режимі реального часу;

No: 2
Name: au_14_3_2
Type: list
Default: ["admin"]

реалізовано можливість для авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, в режимі реального часу;

3.15. АЛЬТЕРНАТИВНА МОЖЛИВІСТЬ АУДИТУ (AU-15) [Вилучено]

[Вилучено: Включено до AU-05(05)]

Немає параметрів для цього контролю.

3.16. МІЖОРГАНІЗАЦІЙНИЙ АУДИТ (AU-16)

Використовувати [Призначення: визначені організацією методи] для координації [Призначення: визначеної організацією інформації] серед зовнішніх організацій, коли інформація аудиту передається за межі організації.

No: 1
Name: au_16_odp_1
Type: string
Default: nil

визначено методи для координації інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи);

No: 2
Name: au_16_odp_2
Type: string
Default: nil

визначено інформацію для координації інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи);

No: 3
Name: au_16_01
Type: string
Default: nil

організація використовує <AU-16_ODP[01] методи> для координації <AU-16_ODP[02] інформації> серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи).

3.16.1. ЗБЕРЕЖЕННЯ ІДЕНТИЧНОСТІ (AU-16(1))

Вимагається, щоб ідентичність особистості зберігалася в міжорганізаційних журналах аудиту.

No: 1
Name: au_16_1_01
Type: string
Default: nil

вимагається, щоб ідентичність особистості зберігалася в міжорганізаційних журналах аудиту.

3.16.2. ОБМІН ІНФОРМАЦІЄЮ АУДИТУ (AU-16(2))

Надавати інформацію про міжорганізаційний аудит до [Призначення: організацій, визначених організацією] на основі [Призначення: визначеної організацією міжорганізаційної угоди про обмін].

No: 1
Name: au_16_2_odp_1
Type: string
Default: nil

визначено організації до яких надають інформацію про міжорганізаційний аудит

No: 2
Name: au_16_2_odp_2
Type: string
Default: nil

визначено міжорганізаційну угоду про розподіл.

No: 3
Name: au_16_2_01
Type: string
Default: nil

надати інформацію про міжорганізаційний аудит до <AU16(02)_ODP[01] організацій> організацією на основі <AU16(02)_ODP[02] угоди про розподіл>.

3.16.3. РОЗМЕЖУВАННЯ (AU-16(3))

Запровадити [Призначення: заходи, визначені організацією], щоб розмежувати людей від інформації аудиту, що передається в межах організації.

No: 1
Name: au_16_3_odp
Type: string
Default: nil

визначено заходи для розмежування окремих осіб від інформації аудиту, що передається в межах організації;

No: 2
Name: au_16_3_01
Type: string
Default: nil

<AU-16(03)_ODP заходи> впроваджуються для того, щоб розмежування окремих осіб від інформації аудиту, що передається в межах організації;

4. CA

Клас заходів захисту CA — ОЦІНЮВАННЯ,

Опис Цей клас регламентує процеси перевірки ефективності заходів захисту, авторизації систем та їх безперервного моніторингу.

Перелік заходів захисту Політика і процедури оцінювання, акредитація та моніторинг безпеки (CA-1); Оцінювання (CA-2); Незалежні експерти (CA-2(1)); Спеціалізовані оцінки (CA-2(2)); Зовнішні організації (CA-2(3)); Взаємодія систем (CA-3); Незахищені з'єднання системи (CA-3(1)) [Вилучено]; Захищені з'єднання системи (CA-3(2)); Несекретні з'єднання системи безпеки, що не є національними (CA-3(3)) [Вилучено]; Підключення до загальнодоступних мереж (CA-3(4)) [Вилучено]; Обмеження зв'язку із зовнішніми системами (CA-3(5)) [Вилучено]; Передача дозволів (CA-3(6)); Транзитивний обмін інформацією (CA-3(7)); Сертифікація безпеки (CA-4) [Вилучено]; План усунення недоліків та контрольні показники (CA-5); Автоматизація підтримки задля точності та вживаності (CA-5(1)); Акредитація (CA-6); Спільна акредитація - одна і та сама організація (CA-6(1)); Спільна акредитація - різні організації (CA-6(2)); Безперервний моніторинг (CA-7); Незалежне оцінювання (CA-7(1)); Види оцінок (CA-7(2)) [Вилучено]; Аналіз тенденції (CA-7(3)); Моніторинг ризику (CA-7(4)); Узгоджений аналіз (CA-7(5)); Безперервний моніторингу (CA-7(6)); Тестування на проникнення (CA-8); Незалежна команда

або агент на проникнення (CA-8(1)); Червона команда (CA-8(2)); Можливості перевірки на проникнення (CA-8(3)); Внутрішні системні зв'язки (CA-9); Відповідність заходів безпеки (CA-9(1)).

4.1. ПОЛІТИКА І ПРОЦЕДУРИ ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ БЕЗПЕКИ (CA-1)

a. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посад]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика оцінювання, авторизації та моніторингу, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинним законам, нормативним документам, наказам, положенням, політиці, стандартам і керівним принципам.
2. Процедури, що сприяють реалізації політики оцінювання, авторизації та моніторингу безпеки та приватності, а також пов'язаних з ними заходів оцінювання, авторизації та моніторингу безпеки та приватності.
b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;
c. Переглядати та оновлювати поточне оцінювання, авторизацію та моніторинг:
1. Політику [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією];
2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].

No: 1
Name: ca_1_odp_1
Type: list
Default: ["admin"]

визначено персонал або ролі, серед яких має бути поширена політика оцінювання, авторизації та моніторингу;

No: 2
Name: ca_1_odp_2
Type: list
Default: ["admin"]

визначено персонал або ролі, серед яких мають бути поширені процедури оцінювання, авторизації та моніторингу;

No: 3
Name: ca_1_odp_3
Type: integer
Default: 30

вибрано одне або декілька з наступних ЗНА ЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: ca_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка управлятиме розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;

No: 5
Name: ca_1_odp_5
Type: integer
Default: 30

визначено частоту, з якою переглядається та оновлюється поточна політика оцінювання, авторизації та моніторингу;

No: 6
Name: ca_1_odp_6
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення поточної політики оцінки, авторизації та моніторингу;

No: 7
Name: ca_1_odp_7
Type: integer
Default: 30

визначено частоту, з якою переглядається та оновлюється поточні процедури оцінювання, авторизації та моніторингу;

No: 8
Name: ca_1_odp_8
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення поточні процедури оцінки, авторизації та моніторингу;

No: 9
Name: ca_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику оцінювання, авторизації та моніторингу;

No: 10
Name: ca_1_a_2
Type: string
Default: nil

політика оцінювання, авторизації та моніторингу поширюється

No: 11
Name: ca_1_a_3
Type: list
Default: ["admin"]

розроблені та задокументовані процедури оцінювання, авторизації та моніторингу, що сприяють впровадженню політики оцінювання, авторизації та моніторингу, а також пов'язані з ними засоби контролю оцінювання, авторизації та моніторингу;

No: 12
Name: ca_1_a_4
Type: list
Default: ["admin"]

процедури оцінювання, авторизації та моніторингу поширюються серед <CA-01_ODP[02] персоналу або ролей>;

No: 13
Name: ca_1_a_1_a_1
Type: string
Default: nil

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить мету;

No: 14
Name: ca_1_a_1_a_2
Type: string
Default: nil

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить сферу застосування;

No: 15
Name: ca_1_a_1_a_3
Type: list
Default: ["admin"]

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить ролі;

No: 16
Name: ca_1_a_1_a_4
Type: string
Default: nil

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить обов'язки;

No: 17
Name: ca_1_a_1_a_5
Type: string
Default: nil

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить відповідальність керівництва;

No: 18
Name: ca_1_a_1_a_6
Type: string
Default: nil

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить координацію між підрозділами організації;

No: 19
Name: ca_1_a_1_a_7
Type: list
Default: ["admin"]

політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить систему контролю відповідності;

No: 20
Name: ca_1_a_1_b
Type: string
Default: nil

<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політика оцінювання, надання дозволів та моніторингу відповідає чинним законам, нормативним документам, наказа м, положенням, політиці, стандартам

і керівним принципам;

No: 21
Name: ca_1_b
Type: string
Default: nil

<CA-01_ODP[04] посадова особа > призначається для управління розробкою, документуванням та розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;

No: 22
Name: ca_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика оцінки, авторизації та моніторингу з <CA-01_ODP[05] частотою>;

No: 23
Name: ca_1_c_1_2
Type: string
Default: nil

переглядається та оновлюється поточна політика оцінки, авторизації та моніторингу після <CA-01_ODP[06] подій>;

No: 24
Name: ca_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури оцінки, авторизації та моніторингу з <CA-01_ODP[07] частотою>;

No: 25
Name: ca_1_c_2_2
Type: string
Default: nil

переглядаються та оновлюються поточні процедури оцінки, авторизації та моніторингу після <CA-01_ODP[07] подій>;

4.2. ОЦІНЮВАННЯ (CA-2)

a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися;
b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі:
1. заходи захисту та посилені заходи, що підлягають оцінюванню;
2. процедури оцінювання, ефективності заходів; які використовуватимуться для визначення
3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.
c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником;
d. Оцінити заходи захисту в системі та в її середовищі функціонування з [Призначення: визначеною організацією частотою] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності;
e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання;
f. Надати результати оцінювання з безпеки [Призначення: особам або ролям, визначеним організацією].

No: 1
Name: ca_2_odp_1
Type: list
Default: ["admin"]

визначено частоту, з якою слід оцінювати засоби контролю в системі та середовищі її функціонування;

No: 2
Name: ca_2_odp_2
Type: list
Default: ["admin"]

визначені особи або ролі, яким мають бути надані результати оцінювання з безпеки;

No: 3
Name: ca_2_a
Type: string
Default: nil

обрано відповідного оцінювача або команду оцінювачів для проведення оцінювання;

No: 4
Name: ca_2_b_1
Type: list
Default: ["admin"]

розроблено план контрольної оцінки, який описує обсяг оцін ки, включаючи заходи захисту та посилені заходи, що підлягають оцінюванню.

No: 5
Name: ca_2_b_2
Type: list
Default: ["admin"]

розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи процедури оцінювання, які використовуватимуться для визначення ефективності заходів.

No: 6
Name: ca_2_b_3_1
Type: string
Default: nil

розроблено план контро льної оцінки, який описує обсяг оцінки, включаючи середовище оцінювання.

No: 7
Name: ca_2_b_3_2
Type: list
Default: ["admin"]

розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи групу оцінювання.

No: 8
Name: ca_2_b_3_3
Type: list
Default: ["admin"]

розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи ролі й обов'язки з оцінювання.

No: 9
Name: ca_2_c
Type: string
Default: nil

план оцінки заходів захисту розглядається та затверджується уповноваженою посадовою особою або призначеним представником перед проведенням оцінки;

No: 10
Name: ca_2_d_1
Type: string
Default: nil

заходи захисту оцінюються в системі та середовищі її визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до безпеки;

No: 11
Name: ca_2_d_2
Type: string
Default: nil

заходи захисту оцінюються в системі та середовищі її визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до конфіденційності;

No: 12
Name: ca_2_e
Type: string
Default: nil

готується звіт оцінювання , який документує результати оцінювання;

No: 13
Name: ca_2_f
Type: list
Default: ["admin"]

результати оцінювання з безпеки надаються <CA-02_ODP[02] особам або ролям>.

4.2.1. НЕЗАЛЕЖНІ ЕКСПЕРТИ (CA-2(1))

Для проведення контрольних оцінок залучаються незалежні експерти або групи експертів.

No: 1
Name: ca_2_1_01
Type: list
Default: ["admin"]

Для проведення контрольних оцінок залучаються незалежні експерти або групи експертів.

4.2.2. СПЕЦІАЛІЗОВАНІ ОЦІНКИ (CA-2(2))

Ввести як частину оцінювання заходів безпеки та приватності, [Призначення: з визначеною організацією частотою], [Вибір: з попередженням; без попередження], [Вибір (один або кілька): поглиблений моніторинг; сканування уразливостей; тестування на шкідливих користувачів; оцінювання внутрішньої загрози; тестування продуктивності та навантаження; [Призначення: організаційно визначені інші форми оцінювання]].

No: 1
Name: ca_2_2_odp_1
Type: integer
Default: 30

визначено частоту, з якою слід включати спеціалізовані оцінки як частину оцінювання безпеки та конфіденційності;

No: 2
Name: ca_2_2_odp_2
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {з попередженням; без попередження};

No: 3
Name: ca_2_2_odp_3
Type: list
Default: ["admin"]

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {поглиблений моніторинг; сканування уразливостей; тестування на шкідливих користувачів; оцінювання внутрішньої загрози; тестування продуктивності та навантаження; };

No: 4
Name: ca_2_2_odp_4
Type: string
Default: nil

визначаються інші форми оцінювання (якщо вони були обрані);

No: 5
Name: ca_2_2_01
Type: string
Default: nil

<CA-02(02)_ODP[01] періодичність оцінювання> <CA02(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> ПАРАМЕТРА(ів)> включаються як частина оцінювання заходів безпеки та конфіденційності;

4.2.3. ЗОВНІШНІ ОРГАНІЗАЦІЇ (CA-2(3))

Використовуйте результати контрольного оцінювання, які виконує [Призначення: зовнішня організація, визначена організацією] на [Призначення: система, визначена організацією], коли оцінювання відповідає [Завдання: вимоги, визначені організацією].

No: 1
Name: ca_2_3_odp_1
Type: string
Default: nil

визначено організацію, яка надає результати оцінок заходів захисту інформації та персональних даних

No: 2
Name: ca_2_3_odp_2
Type: string
Default: nil

визначено систему, яка приймає результати оцінок заходів захисту інформації та персональних даних

No: 3
Name: ca_2_3_odp_3
Type: string
Default: nil

визначено вимоги до результатів оцінок заходів захисту інформації та персональних даних

No: 4
Name: ca_2_3_01

Type: string
Default: nil

прийняти результати оцінок заходів захисту інформації та

4.3. ВЗАЄМОДІЯ СИСТЕМ (CA-3)

a. схвалити та керувати обміном інформацією між системою та іншими системами за допомогою [Вибір (один або кілька): угоди безпеки взаємозв'язку; договори безпеки обміну інформацією; меморандуми про взаєморозуміння; угоди про рівень обслуговування; угоди користувача; угоди про нерозголошення; [Доручення: тип договору, визначений організацією]];.
b. документувати, як частину угоди про обмін, характеристики інтерфейсу, вимоги до безпеки та приватності, засоби контролю та відповідальність для кожної системи, а також характер переданої інформації;
c. здійснювати перегляд та оновлення угод з [Призначення: визначеною організацією частотою].

No: 1
Name: ca_3_odp_1
Type: list
Default: ["admin"]

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {}: угоди безпеки взаємозв'язку; договори безпеки обміну інформацією; меморандуми про взаєморозуміння; угоди про рівень обслуговування; угоди користувача; угоди

No: 2
Name: ca_3_odp_2
Type: string
Default: nil

визначено тип угоди, який використовується для схвалення та керування обміном інформацією (якщо вибрано);

No: 3
Name: ca_3_odp_3
Type: integer
Default: 30

визначено частоту, з якою необхідно переглядати та оновлювати угоди;

No: 4
Name: ca_3_a
Type: string
Default: nil

обмін інформацією між системою та іншими системами схвалюється та керується за допомогою <CA-03_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;

No: 5
Name: ca_3_b_1
Type: string
Default: nil

характеристики інтерфейсу задокументовані як частина кожної угоди про обмін;

No: 6
Name: ca_3_b_2
Type: string
Default: nil

вимоги до безпеки задокументовані як частина кожної угоди про обмін;

No: 7
Name: ca_3_b_3
Type: string
Default: nil

вимоги щодо конфіденційності задокументовані як частина кожної угоди про обмін;

No: 8
Name: ca_3_b_4
Type: string
Default: nil

заходи захисту задокументовані як частина кожної угоди про обмін;

No: 9
Name: ca_3_b_5
Type: string
Default: nil

відповідальність за кожну сист ему задокументована як частина кожної угоди про обмін;

No: 10
Name: ca_3_b_6
Type: string
Default: nil

характер переданої інформації документується як частина кожної угоди про обмін;

No: 11
Name: ca_3_c
Type: string
Default: nil

угоди переглядаються та оновлюються <CA-03_ODP[03] частота>.

4.3.1. НЕЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ (CA-3(1)) [Вилучено]

[Вилучено: Включено до SC-07(25)]

Немає параметрів для цього контролю.

4.3.2. ЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ (CA-3(2))

Захищені з'єднання системи (ca-3(2)).

Немає параметрів для цього контролю.

4.3.3. НЕСЕКРЕТНІ З'ЄДНАННЯ СИСТЕМИ БЕЗПЕКИ, ЩО НЕ Є НАЦІОНАЛЬНИМИ (CA-3(3)) [Вилучено]

[Вилучено: Включено до SC-07(27)]

Немає параметрів для цього контролю.

4.3.4. ПІДКЛЮЧЕННЯ ДО ЗАГАЛЬНОДОСТУПНИХ МЕРЕЖ (CA-3(4)) [Вилучено]

[Вилучено: Включено до SC-07(28)]

Немає параметрів для цього контролю.

4.3.5. ОБМЕЖЕННЯ ЗВ'ЯЗКУ ІЗ ЗОВНІШНІМИ СИСТЕМАМИ (CA-3(5)) [Вилучено]

[Вилучено: Включено до SC-07(05)]

Немає параметрів для цього контролю.

4.3.6. ПЕРЕДАЧА ДОЗВОЛІВ (CA-3(6))

Переконатися, що особи або системи, які передають дані між взаємопов'язаними системами, мають необхідні повноваження (тобто дозволи на запис або привілеї), до прийняття таких даних.

No: 1
Name: ca_3_6_01
Type: string
Default: nil

особи або системи, які передають дані між системами, що з'єднуються, мають необхідні повноваження (тобто дозволи на запис або привілеї) перед тим, як приймати такі дані.

4.3.7. ТРАНЗИТИВНИЙ ОБМІН ІНФОРМАЦІЄЮ (CA-3(7))

a) Визначити транзитивний (низхідний) обмін інформацією з іншими системами через системи, визначені в CA-3a; b) Вжити заходів для забезпечення припинення транзитивного (низхідного) обміну інформацією, коли засоби контролю ідентифікованих транзитивних (низхідних) систем не можуть бути перевірені або підтверджені.

No: 1
Name: ca_3_7_a
Type: string
Default: nil

визначено транзитний обмін інформацією з іншими системами через системи, визначені в CA-03a;

No: 2
Name: ca_3_7_b
Type: list
Default: ["admin"]

вживаються заходи для забезпечення припинення транзитного обміну інформацією, коли засоби контролю над ідентифікованими транзитними системами не можуть бути перевірені або підтверджені.

4.4. СЕРТИФІКАЦІЯ БЕЗПЕКИ (CA-4) [Вилучено]

[Вилучено: Включено до CA-02]

Немає параметрів для цього контролю.

4.5. ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ (CA-5)

a. Розробити для системи план усунення недоліків та контрольні показники з метою документування запланованих коригувальних дій організації для усунення недоліків і зауважень, які виявлені в ході оцінювання заходів захисту, а також для зменшення або усунення відомих вразливостей у системі.
b. Оновлювати чинний план усунення недоліків та контрольні показники з [Призначення: визначеною організацією частотою] на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.

No: 1
Name: ca_5_odp
Type: list
Default: ["admin"]

визначено частоту оновлення чинного плану усунення недоліків та контрольних показників на основі результатів оцінювання заходів захисту, незалежних аудитів та постійного моніторингу;

No: 2
Name: ca_5_a
Type: list
Default: ["admin"]

розроблено план усунення недоліків та контрольні показники для системи, та задокументувано заплановані дії організації з коригування, спрямовані на усунення недоліків та зауважень, виявлених під час оцінки заходів захисту, а також на зменшення або усунення відомих вразливостей в системі;

No: 3
Name: ca_5_b
Type: string
Default: nil

існуючий план оновлюються <CA-05_ODP частота> на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.

4.5.1. АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ (CA-5(1))

<CA-05(01)_ODP автоматизовані механізми> використовуються для забезпечення точності, актуальності та доступності плану усунення недоліків і основних етапів для системи.

No: 1
Name: ca_5_1_odp
Type: string
Default: nil

визначено автоматизовані механізми, які використовуються для забезпечення точності, актуальності та доступності плану усунення недоліків і основних етапів для системи;

No: 2
Name: ca_5_1_01

Type: string
Default: nil

<CA-05(01)_ODP автоматизовані механізми> використовуються для забезпечення точності, актуальності та доступності плану усунення недоліків і основних етапів для системи.

4.6. АКРЕДИТАЦІЯ (CA-6)

a. Призначити старшого керівника, який відповідає за систему;
b. Призначити старшого керівника, відповідального за систему, та будь-які загальні заходи захисту, успадковані системою.
c. Переконатися перед початком функціонування системи, що посадова особа:
1. акредитує загальні заходи захисту, що успадковані системою;
2. акредитує систему на функціонування за призначенням.
d. Переконайтеся, що посадова особа, яка акредитує засоби захисту, дозволяє використання цих засобів захисту для успадкування організаційними системами;
e. Оновлювати акредитацію [Призначення: з визначеною організацією частотою].

No: 1
Name: ca_6_odp
Type: integer
Default: 30

визначено частоту, з якою потрібно оновлювати акредитації;

No: 2
Name: ca_6_a
Type: string
Default: nil

призначено старшого керівника, який відповідає за систему;

No: 3
Name: ca_6_b
Type: string
Default: nil

призначено старшого керівника, відповідального за систему, та будь-які загальні заходи захисту, успадковані системою;

No: 4
Name: ca_6_c_1
Type: string
Default: nil

перед початком функціонування системи посадова особа, яка відповідає за систему, акредитує загальні заходи захисту, що успадковані системою;

No: 5
Name: ca_6_c_2
Type: string
Default: nil

перед початком функціонування системи посадова особа, яка відповідає за систему, акредитує систему на функціонування за призначенням;

No: 6
Name: ca_6_d
Type: string
Default: nil

посадова особа, яка акредитує заходи захисту, дозволяє використання цих заходів захисту для успадкування системами організації;

No: 7
Name: ca_6_e
Type: string
Default: nil

акредитації оновлюються <CA-06_ODP частота>.

4.6.1. СПІЛЬНА АКРЕДИТАЦІЯ - ОДНА І ТА САМА ОРГАНІЗАЦІЯ (CA-6(1))

Для системи впроваджено спільний процес акредитації;.

No: 1
Name: ca_6_1_1
Type: string
Default: nil

для системи впроваджено спільний процес акредитації;

No: 2
Name: ca_6_1_2
Type: string
Default: nil

спільний процес акредитації, який використовується в системі, включає в себе кілька посадових осіб з однієї організації , які надають акредитацію.

4.6.2. СПІЛЬНА АКРЕДИТАЦІЯ - РІЗНІ ОРГАНІЗАЦІЇ (CA-6(2))

Впровадити спільний процес акредитації для системи, що має кількох уповноважених посадових осіб з принаймні однією уповноваженою посадовою особою з організації, яка є зовнішньою організацією, що здійснює акредитацію.

No: 1
Name: ca_6_2_1
Type: string
Default: nil

для системи впроваджено спільний процес акредитації;

No: 2
Name: ca_6_2_2
Type: string
Default: nil

спільний процес акредитації, що використовується в системі, передбачає наявність кількох посадових осіб, які надають акредитації, принаймні одна з яких є посадовою особою з організації, що не належить до організації, яка здійснює акредитацію.

4.7. БЕЗПЕРЕРВНИЙ МОНІТОРИНГ (CA-7)

Розробити стратегію безперервного моніторингу безпеки та приватності й упровадити програму безперервного моніторингу безпеки та приватності, яка охоплює:

a. встановлення показників безпеки та приватності, які необхідно відстежувати: [Призначення: визначені організацією метрики];
b. встановлення [Призначення: визначена організацією частота] для моніторингу та [Призначення: визначена організацією частота] для безперервного оцінювання ефективності заходів захисту;
c. поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу організації;
d. постійний моніторинг стану безпеки та приватності відповідно до встановлених організацією метрик і відповідно до стратегії безперервного моніторингу організації;
e. зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки та приватності;
f. дії реагування за результатами аналізу інформації, пов'язаної з безпекою та приватністю;
g. повідомлення про статус безпеки та приватності системи [Призначення: визначені організацією персонал або ролі] з [Призначення: визначеною організацією частотою].

No: 1
Name: ca_7_odp_1
Type: string
Default: nil

визначено метрики системного рівня, які підлягають моніторингу;

No: 2
Name: ca_7_odp_2
Type: integer
Default: 30

визначено частоту, з якою слід моніторити ефективність заходів захисту;

No: 3
Name: ca_7_odp_3
Type: integer
Default: 30

визначено частоту, з якою слід оцінювати ефективність заходів захисту;

No: 4
Name: ca_7_odp_4
Type: list
Default: ["admin"]

визначено персонал або ролі, яким повідомляється про стан безпеки системи;

No: 5
Name: ca_7_odp_5
Type: integer
Default: 30

визначено частоту, з якою повідомляється про стан безпеки системи;

No: 6
Name: ca_7_odp_6
Type: list
Default: ["admin"]

визначено персонал або ролі, яким повідомляється про стан конфіденційності системи;

No: 7
Name: ca_7_odp_7
Type: integer
Default: 30

визначено частоту, з якою повідомляється про стан конфіденційності системи;

No: 8
Name: ca_7_1
Type: string
Default: nil

розроблено стратегію безперервного моніторингу на системному рівні;

No: 9
Name: ca_7_2
Type: string
Default: nil

безперервний моніторинг на рівні системи здійснюється відповідно до стратегії безперервного моніторингу на рівні організації;

No: 10
Name: ca_7_a
Type: string
Default: nil

безперервний моніторинг на рівні системи включає встановлення наступних метрик на рівні системи, які підлягають моніторингу:

No: 11
Name: ca_7_b_1
Type: string
Default: nil

безперервний моніторинг на рівні системи включає встановлені захисту;

No: 12
Name: ca_7_b_2
Type: string
Default: nil

безперервний моніторинг на рівні системи включає встановлені

No: 13
Name: ca_7_c
Type: list
Default: ["admin"]

безперервний моніторинг на рівні системи включає поточні контрольні оцінки відповідно до стратегії безперервного моніторингу;

No: 14
Name: ca_7_d
Type: string
Default: nil

безперервний моніторинг на рівні системи включає постійний моніторинг визначених системою та організацією показників відповідно до стратегії безперервного моніторингу;

No: 15
Name: ca_7_e
Type: string
Default: nil

безперервний моніторинг на рівні системи включає зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу;

No: 16
Name: ca_7_f
Type: string
Default: nil

безперервний моніторинг на рівні системи включає в себе дії з реагування на результати аналізу інформації, пов'язаної з безпекою та приватністю;

No: 17
Name: ca_7_g_1
Type: string
Default: nil

безперервний моніторинг на рівні системи включає повідомлення

No: 18
Name: ca_7_g_2
Type: string
Default: nil

безперервний моніторинг на рівні системи включає повідомлення

4.7.1. НЕЗАЛЕЖНЕ ОЦІНЮВАННЯ (CA-7(1))

Для постійного моніторингу заходів захисту в системі залучаються незалежні експертів або групи з оцінювання.

No: 1
Name: ca_7_1_01
Type: string
Default: nil

для постійного моніторингу заходів захисту в системі залучаються незалежні експертів або групи з оцінювання.

4.7.2. ВИДИ ОЦІНОК (CA-7(2)) [Вилучено]

[Вилучено: Включено до CA-02]

Немає параметрів для цього контролю.

4.7.3. АНАЛІЗ ТЕНДЕНЦІЇ (CA-7(3))

Впровадити аналіз тенденцій, щоб визначити, чи потрібно змінювати реалізацію заходу захисту, частоту постійних моніторингових заходів і види діяльності, що використовуються в процесі безперервного моніторингу, на основі емпіричних даних.

No: 1
Name: ca_7_3_1
Type: string
Default: nil

аналіз тенденцій використовується для визначення того, чи потрібно змінювати реалізацію заходів захисту, які використовуються в процесі безперервного моніторингу, на основі емпіричних даних;

No: 2
Name: ca_7_3_2

Type: string
Default: nil

аналіз тенденцій застосовується для того, щоб на основі емпіричних даних визначити, чи потрібно змінювати частоту постійного моніторингу;

No: 3
Name: ca_7_3_3
Type: string
Default: nil

аналіз тенденцій застосовується для того, щоб на основі емпіричних даних визначити, чи потрібно змінювати види діяльності, які використовуються в процесі безперервного моніторингу.

4.7.4. МОНІТОРИНГ РИЗИКУ (CA-7(4))

Забезпечити моніторинг ризиків, що є невід'ємною частиною стратегії постійного моніторингу та включає:
(a) моніторинг ефективності;
(b) моніторинг відповідності;
(c) моніторинг змін.

No: 1
Name: ca_7_4_01
Type: string
Default: nil

моніторинг ризиків є невід'ємною частиною стратегії безперервного моніторингу;

No: 2
Name: ca_7_4_a
Type: string
Default: nil

моніторинг ефективності включено до моніторингу ризиків;

No: 3
Name: ca_7_4_b
Type: string
Default: nil

моніторинг відповідності включено до моніторингу ризиків;

No: 4
Name: ca_7_4_c
Type: string
Default: nil

моніторинг змін включений до моніторингу ризиків.

4.7.5. УЗГОДЖЕНИЙ АНАЛІЗ (CA-7(5))

Застосуйте наступні дії, щоб перевірити, що політики встановлені, а запроваджені заходи захисту працюють узгоджено: [Призначення: дії, визначені організацією].

No: 1
Name: ca_7_5_odp_1
Type: string
Default: nil

визначені дії для підтвердження того, що політики встановлені;

No: 2
Name: ca_7_5_odp_2
Type: string
Default: nil

визначені дії для підтвердження того, що впроваджені заходи захисту працюють узгоджено;

No: 3
Name: ca_7_5_1
Type: string
Default: nil

<CA-07(05)_ODP[01] дії> використовуються для перевірки того, що політики встановлено;

No: 4
Name: ca_7_5_2
Type: string
Default: nil

<CA-07(05)_ODP[02] дії> використовуються для перевірки того, що впроваджені заходи захисту працюють узгоджено

4.7.6. БЕЗПЕРЕРВНИЙ МОНІТОРИНГУ (CA-7(6))

Забезпечити точність, актуальність і доступність результатів моніторингу для системи за допомогою [Завдання: автоматизовані механізми, визначені організацією]

No: 1
Name: ca_7_6_odp
Type: string
Default: nil

визначено автоматизовані механізми забезпечення точності, актуальності та доступності результатів моніторингу системи;

No: 2
Name: ca_7_6_01
Type: string
Default: nil

<CA-07(06)_ODP автоматизовані механізми > використовуються для забезпечення точності, актуальності та доступності результатів моніторингу системи.

4.8. ТЕСТУВАННЯ НА ПРОНИКНЕННЯ (CA-8)

Проводити тестування на проникнення з [Призначення: визначеною організацією частотою] у [Призначення: визначеній організацією інформаційній системі чи системному компоненті].

No: 1
Name: ca_8_odp_1
Type: integer
Default: 30

визначено частоту з якою проводить тестування на проникнення.

No: 2
Name: ca_8_odp_2
Type: string
Default: nil

визначено систему у якій проводить тестування на проникнення

No: 3
Name: ca_8_01
Type: string
Default: nil

проводиться тестування на проникнення з <CA-08_ODP[01] частотою> у <CA-08_ODP[02] системі>.

4.8.1. НЕЗАЛЕЖНА КОМАНДА АБО АГЕНТ НА ПРОНИКНЕННЯ (CA-8(1))

Для проведення тестування на проникнення в систему або компонентів системи залучається незалежний агент або команда з тестування на проникнення.

No: 1
Name: ca_8_1_01
Type: string
Default: nil

для проведення тестування на проникнення в систему або компонентів системи залучається незалежний агент або команда з тестування на проникнення.

4.8.2. ЧЕРВОНА КОМАНДА (CA-8(2))

Використовувати наступні вправи червоної команди, для імітації спроб супротивників скомпрометувати системи організації відповідно до прийнятих правил ведення бойових дій: [Завдання: визначені організацією вправи червоної команди].

No: 1
Name: ca_8_2_odp
Type: string
Default: nil

визначено вправи червоної команди для імітації спроби супротивників скомпрометувати системи організації;

No: 2
Name: ca_8_2_01
Type: string
Default: nil

залучити <CA-08(02)_ODP вправи червоної команди>, щоб імітувати спроби супротивників скомпрометувати системи організації.

4.8.3. МОЖЛИВОСТІ ПЕРЕВІРКИ НА ПРОНИКНЕННЯ (CA-8(3))

Впровадити процес тестування на проникнення, який охоплює [Призначення: визначену організацією частоту] [Вибір: з попередженням; без попередження] спроб обійти чи зламати заходи захисту, пов'язані з фізичними точками доступу до об'єкта.

No: 1
Name: ca_8_3_odp_1
Type: integer
Default: 30

визначено частоту спроби обійти або зламати заходи захисту, пов'язані з фізичними точками доступу до об'єкта в тестуванні на проникнення

No: 2
Name: ca_8_3_odp_2
Type: integer
Default: 30

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {з попередженням; без попередження};

No: 3
Name: ca_8_3_01
Type: string
Default: nil

впроваджено процес тестування на проникнення, який

4.9. ВНУТРІШНІ СИСТЕМНІ ЗВ'ЯЗКИ (CA-9)

a. Авторизувати внутрішні підключення [Призначення: системні компоненти або класи компонентів, що організація визначила] до системи;
b. Задокументувати, для кожного внутрішнього з'єднання, характеристики інтерфейсу, вимоги безпеки та приватності, а також характер переданої інформації;
c. Розірвати внутрішні системні підключення після [Призначення: умови, визначені організацією];
d. Переглядати [Призначення: частота, визначена організацією] постійну потребу в кожному внутрішньому з'єднанні.

No: 1
Name: ca_9_odp_1
Type: string
Default: nil

визначено компоненти системи або класи компонентів, що потребують внутрішніх підключень до системи;

No: 2
Name: ca_9_odp_2
Type: string
Default: nil

визначено умови, за яких необхідно розірвати внутрішні підключення;

No: 3
Name: ca_9_odp_3
Type: integer
Default: 30

визначено частоту, з якою необхідно переглядати постійну потребу в кожному внутрішньому з'єднанні;

No: 4
Name: ca_9_a
Type: string
Default: nil

внутрішні підключення <CA-09_ODP[01] компонентів системи> до системи є авторизовані;

No: 5
Name: ca_9_b_1
Type: string
Default: nil

для кожного внутрішнього з'єднання задокументовані характеристики інтерфейсу;

No: 6
Name: ca_9_b_2
Type: string
Default: nil

для кожного внутрішнього з'єднання задокументовані вимоги безпеки;

No: 7
Name: ca_9_b_3
Type: string
Default: nil

для кожного внутрішнього з'єднання задокументовані вимоги конфіденційності;

No: 8
Name: ca_9_b_4
Type: string
Default: nil

для кожного внутрішнього з'єднання задокументовані характер переданої інформації;

No: 9
Name: ca_9_c
Type: string
Default: nil

внутрішні з'єднання системи розриваються після виконання <CA09_ODP[02] умов>;

No: 10
Name: ca_9_d
Type: string
Default: nil

переглядається подальша потреба у кожному внутрішньому з'єднанні <CA-09_ODP[03] частота>.

4.9.1. ВІДПОВІДНІСТЬ ЗАХОДІВ БЕЗПЕКИ (CA-9(1))

Забезпечується надання результатів внутрішніх підключень до компонентів системи.

No: 1
Name: ca_9_1_1
Type: string
Default: nil

перед встановленням внутрішнього з'єднання виконується перевірка на відповідність вимогам безпеки складових компонентів системи;

No: 2
Name: ca_9_1_2
Type: string
Default: nil

перед встановленням внутрішнього з'єднання виконується перевірка на відповідність вимогам конфіденційності складових компонентів системи;

5. CM

Клас заходів захисту CM — УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

Опис Цей клас гарантує створення та підтримання базових налаштувань системи, а також строгий контроль за змінами в апаратному та програмному забезпеченні.

Перелік заходів захисту Політика та процедури управління конфігурацією (CM-1); Базова конфігурація (CM-2); Перегляд та оновлення (CM-2(1)) [Вилучено]; Автоматизація підтримки задля точності та вживаності (CM-2(2)); Зберігання попередніх версій конфігурацій (CM-2(3)); Неавторизоване програмне забезпечення (CM-2(4)); Авторизоване програмне забезпечення (CM-2(5)) [Вилучено]; Розробка та середовище тестування (CM-2(6)); Конфігурація систем та компонентів для сфер з високим ризиком (CM-2(7)); Управління змінами конфігурації (CM-3); Автоматизоване документування, повідомлення та заборона внесення змін (CM-3(1)); Тестування, валідація та документування змін (CM-3(2)); Автоматизована реалізація змін (CM-3(3)); Представник безпеки (CM-3(4)); Автоматичне реагування безпеки (CM-3(5)); Управління засобами криптографічного захисту (CM-3(6)); Перегляд змін у системі (CM-3(7)); Запобігання чи обмеження змін конфігурації (CM-3(8)); Аналіз впливу на безпеку та приватність (CM-4); Відокремлені випробувальні середовища (CM-4(1)); Верифікація функцій безпеки та приватності (CM-4(2)); Обмеження доступу до зміни (CM-5); Аудит і здійснення автоматичного доступу (CM-5(1)); Перегляд змін у системі (CM-5(2)) [Вилучено]; Підписані компоненти (CM-5(3)) [Вилучено]; Подвійна авторизація (CM-5(4)); Обмеження повноважень для виробництва та експлуатації (CM-5(5)); Обмеження повноважень для бібліотек (CM-5(6)); Обмеження доступу до зміни вадження заходів захисту (CM-5(7)) [Вилучено]; Налаштування конфігурації (CM-6); Автоматизоване управління, застосування та верифікація (CM-6(1)); Налаштування конфігурації санкціоновані зміни (CM-6(2)); Демонстрація відповідності (CM-6(4)) [Вилучено]; Мінімально необхідна функціональність (CM-7); Періодичний перегляд (CM-7(1)); Заборона виконання програми (CM-7(2)); Відповідність реєстрації (CM-7(3)); Неавторизоване програмне забезпечення - чорний список (CM-7(4)); Авторизоване програмне забезпечення – білий список (CM-7(5)); Замкнуті середовища з обмеженими привілеями (CM-7(6)); Виконуваний код у захищеному середовищі (CM-7(7)); Бінарний або машинний виконуваний код (CM-7(8)); Заборона використання неавторизованого обладнання (CM-7(9)); Інвентаризація компонентів системи (CM-8); Оновлення під час встановлення та видалення (CM-8(1)); Автоматизована підтримка (CM-8(2)); Автоматизоване виявлення неавторизованих компонентів (CM-8(3)); Інформація про підзвітність (CM-8(4)); Інвентаризація компонентів системи дублювання компонентів обліку (CM-8(5)); Перевірені налаштування та затверджені відхилення (CM-8(6)); Централізоване сховище (CM-8(7)); Автоматизоване відстеження місця розташування (CM-8(8)); Призначення компонентів системам (CM-8(9)); План управління конфігурацією (CM-9); Встановлення відповідальності (CM-9(1)); Обмеження використання програмного забезпечення (CM-10); Обмеження використання програмного забезпечення програмне забезпечення з відкритим вихідним кодом (CM-10(1)); Встановлене користувачем програмне забезпечення (CM-11); Встановлене користувачем програмне забезпечення попередження про несанкціоновану інсталяцію (CM-11(1)); Встановлене користувачем програмне забезпечення встановлення програмного забезпечення з привілейованим статусом (CM-11(2)); Встановлене користувачем програмне забезпечення автоматичне виконання і моніторинг (CM-11(3)); Розташування інформації (CM-12); Автоматизовані інструменти підтримки розташування інформації (CM-12(1)); Відображення дій даних (CM-13); Підписані компоненти (CM-14).

5.1. ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM-1)

a. Розробити, задокументувати та поширити серед [Призначення: визначених організацією персоналу або ролей]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики управління конфігурацією, яка:
2.
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам; процедури, що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією.
b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією.
c. Переглядати та оновлювати поточну політику управління конфігурацією:
1. Політика [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією];
2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].

No: 1
Name: cm_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, на яких поширюється політика управління конфігурацією;

No: 2
Name: cm_1_odp_2
Type: string
Default: nil

визначено персонал або ролі, на яких поширюється процедури управління конфігурацією;

No: 3
Name: cm_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: cm_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка управляє розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією;

No: 5
Name: cm_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика управління конфігурацією;

No: 6
Name: cm_1_odp_6
Type: string
Default: nil

визначено події, після яких переглядається та оновлюється поточна політика управління конфігурацією;

No: 7
Name: cm_1_odp_7
Type: string
Default: nil

визначено частоту, з якою перегляда ються та оновлюються поточні процедури управління конфігурацією;

No: 8
Name: cm_1_odp_8
Type: string
Default: nil

визначено події, після яких переглядаються та оновлюються поточні процедури управління конфігурацією;

No: 9
Name: cm_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику управління конфігурацією;

No: 10
Name: cm_1_a_2
Type: string
Default: nil

політика управління конфігурацією поширюється на <CM01_ODP[01] персонал або ролі>;

No: 11
Name: cm_1_a_3
Type: string
Default: nil

розроблені та задокументовані процедури управління , що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією;

No: 12
Name: cm_1_a_4
Type: string
Default: nil

процедури управління конфігурацією поширюються на <CM01_ODP[02] персонал або ролі>;

No: 13
Name: cm_1_a_1_a_1
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить мету;

No: 14
Name: cm_1_a_1_a_2
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить сферу застосування;

No: 15
Name: cm_1_a_1_a_3
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить ролі;

No: 16
Name: cm_1_a_1_a_4
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить обов'язки;

No: 17
Name: cm_1_a_1_a_5
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить відповідальність керівництва;

No: 18
Name: cm_1_a_1_a_6
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить координацію між підрозділами організації;

No: 19
Name: cm_1_a_1_a_7
Type: string
Default: nil

<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> політики управління конфігурацією містить систему контролю відповідності;

No: 20
Name: cm_1_a_1_b
Type: string
Default: nil

політика управління конфігурацією відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам;

No: 21
Name: cm_1_b
Type: string
Default: nil

<CM-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією;

No: 22
Name: cm_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика управління

No: 23
Name: cm_1_c_1_2
Type: string
Default: nil

переглядається та оновлюється поточна політика управління

No: 24
Name: cm_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури управління

No: 25
Name: cm_1_c_2_2
Type: string
Default: nil

переглядаються та оновлюються поточні процедури управління

5.2. БАЗОВА КОНФІГУРАЦІЯ (CM-2)

a. Розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи.
b. Переглядати та оновлювати базові налаштування системи:
1. з [Призначення: визначеною організацією частотою];
2. за потреби внаслідок [Призначення: визначених організацією обставин];
3. коли встановлені нові або оновлені компоненти системи.

No: 1
Name: cm_2_odp_1
Type: string
Default: nil

визначено частоту перегляду та оновлення базових налаштувань;

No: 2
Name: cm_2_odp_2
Type: string
Default: nil

визначено обставини, що вимагають перегляду та оновлення базових налаштувань;

No: 3
Name: cm_2_a_1
Type: string
Default: nil

розроблено та задокументовано поточні базові налаштування системи;

No: 4
Name: cm_2_a_2
Type: string
Default: nil

поточні базові налаштування системи підтримуються за допомогою заходів конфігурації;

No: 5
Name: cm_2_b_1
Type: string
Default: nil

переглядаються та оновлюються базові налаштування системи

No: 6
Name: cm_2_b_2
Type: string
Default: nil

переглядаються та оновлюються базові налаштування системи

No: 7
Name: cm_2_b_3
Type: string
Default: nil

переглядаються та оновлюються базові налаштування системи коли встановлюються або модернізуються компоненти системи.

5.2.1. ПЕРЕГЛЯД ТА ОНОВЛЕННЯ (CM-2(1)) [Вилучено]

[Вилучено: Включено до CM-02]

Немає параметрів для цього контролю.

5.2.2. АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ (CM-2(2))

Підтримувати актуальність, повноту, точність і доступність базової конфігурації системи за допомогою [Призначення: автоматизовані механізми, визначені організацією].

No: 1
Name: cm_2_2_odp
Type: string
Default: nil

визначено автоматизовані механізми підтримки базової конфігурації системи;

No: 2
Name: cm_2_2_1
Type: string
Default: nil

актуальність базової конфігурації системи підтримується за допомогою <CM-02(02)_ODP автоматизовані механізми>;

No: 3
Name: cm_2_2_2
Type: string
Default: nil

повнота базової конфігурації системи підтримується за допомогою <CM-02(02)_ODP автоматизовані механізми>;

No: 4
Name: cm_2_2_3

Type: string
Default: nil

точність базової конфігурації системи підтримується за допомогою <CM-02(02)_ODP автоматизовані механізми>;

No: 5
Name: cm_2_2_4
Type: string
Default: nil

доступність базової конфігурації системи підтримується за допомогою <CM-02(02)_ODP автоматизовані механізми>;

5.2.3. ЗБЕРІГАННЯ ПОПЕРЕДНІХ ВЕРСІЙ КОНФІГУРАЦІЙ (CM-2(3))

Зберігати [Призначення: кількість, визначена організацією] попередніх версій базових конфігурацій системи для підтримки відкату.

No: 1
Name: cm_2_3_odp
Type: string
Default: nil

визначено попередні версії базових конфігурацій системи необхідні для підтримки відкату

No: 2
Name: cm_2_3_01
Type: string
Default: nil

зберігати <CM-02(03)_ODP попередні версії> для підтримки відкату

5.2.4. НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ (CM-2(4))

Неавторизоване програмне забезпечення (cm-2(4)).

Немає параметрів для цього контролю.

5.2.5. АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ (CM-2(5)) [Вилучено]

[Вилучено: Включено до CM-07(05)]

Немає параметрів для цього контролю.

5.2.6. РОЗРОБКА ТА СЕРЕДОВИЩЕ ТЕСТУВАННЯ (CM-2(6))

Підтримувати базову конфігурацію для розробки системи та тестових середовищ, які керуються окремо від робочої базової конфігурації.

No: 1
Name: cm_2_6_1
Type: string
Default: nil

підтримується базова конфігурація для розробки системи, які керуються окремо від робочої базової конфігурації.

No: 2
Name: cm_2_6_2
Type: string
Default: nil

підтримується базова конфігурація для розробки тестових середовищ, які керуються окремо від робочої базової конфігурації.

5.2.7. КОНФІГУРАЦІЯ СИСТЕМ ТА КОМПОНЕНТІВ ДЛЯ СФЕР З ВИСОКИМ РИЗИКОМ (CM-2(7))

(a) Видавати [Призначення: визначених організацією систем або компонентів систем] з [Призначенням: визначеними організацією конфігураціями] особам, що перебувають у місцях, які організація вважає місцями зі значним ризиком;
(b) Застосувати [Призначення: визначені організацією запобіжні заходи безпеки] до компонентів, коли особи повертаються з поїздки.

No: 1
Name: cm_2_7_odp_1
Type: string
Default: nil

CM-02(07)_ODP[01] визначено системи або компоненти систем, які мають видаватися особам, що перебувають у місцях зі значним ризиком;

No: 2
Name: cm_2_7_odp_2
Type: string
Default: nil

CM-02(07)_ODP[02] визначено конфігурації систем або компонентів систем, що видаються у місцях зі значним ризиком;

No: 3
Name: cm_2_7_odp_3
Type: string
Default: nil

CM-02(07)_ODP[03] визначено заходи безпеки, які мають застосовуватися після повернення осіб з поїздки;

No: 4
Name: cm_2_7_a
Type: string
Default: nil

CM-02(07)[01] <CM-02(07)_ODP[01] системи або компоненти системи> з <CM-02(07)_ODP[02] конфігураціями> видаються особам, що перебувають у місцях, які організація вважає, становлять значний ризик;

No: 5
Name: cm_2_7_b
Type: string
Default: nil

CM-02(07)[02] <CM-02(07)_ODP[03] заходи безпеки> застосовуються до систем або компонентів системи, коли особи повертаються з поїздки.

5.3. УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ (CM-3)

a. Визначити типи змін у системі, які контролюються конфігурацією.
b. Переглядати запропоновані зміни в конфігурації, контрольовані системою, і схвалити або відхилити ці зміни з явним урахуванням аналізу наслідків безпеки.
c. Документувати рішення зі зміни конфігурації системи.
d. Впровадити схвалені зміни конфігурації в систему.
e. Зберігати записи змін конфігурації системі впродовж [Призначення: певного періоду часу, визначеного організацією].
f. Здійснювати моніторинг і аналіз дій, пов'язаних зі змінами конфігурації системи.
g. Координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою [Призначення: елементу управління змінами конфігурації, визначеного організацією], який викликається [Вибір (один або кілька): [Призначення: з визначеною організацією частотою]; [Призначення: визначені організацією умови зміни конфігурації]].

No: 1
Name: cm_3_odp_1
Type: string
Default: nil

визначено період часу, протягом якого зберігатимуться записи про зміни конфігурації;

No: 2
Name: cm_3_odp_2
Type: string
Default: nil

визначено елементи управління змінами конфігурації, відповідальні за координацію та нагляд за діяльністю з управління змінами;

No: 3
Name: cm_3_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ

No: 4
Name: cm_3_odp_4
Type: string
Default: nil

визначено частоту, з якою викликаються елементи управління змінами конфігурації (якщо вибрано);

No: 5
Name: cm_3_odp_5
Type: string
Default: nil

визначено умови, за яких викликаються елементи управління змінами конфігурації (якщо вибрано);

No: 6
Name: cm_3_a
Type: string
Default: nil

визначено та задокументовано типи змін до системи, які контролюються конфігурацією;

No: 7
Name: cm_3_b_1
Type: string
Default: nil

розглядаються запропоновані зміни в конфігурації, що контролюються системою;

No: 8
Name: cm_3_b_2
Type: string
Default: nil

запропоновані зміни в конфігурації, що контролюються системою, схвалюються або відхиляються з урахуванням аналізу наслідків безпеки;

No: 9
Name: cm_3_c
Type: string
Default: nil

рішення про зміну конфігурації системи документуються;

No: 10
Name: cm_3_d
Type: string
Default: nil

впроваджуються схвалені зміни до конфігурації в систему;

No: 11
Name: cm_3_e
Type: string
Default: nil

записи про зміни конфігурації у системі зберігаються протягом

No: 12
Name: cm_3_f_1
Type: string
Default: nil

здійснюється моніторинг дій, пов'язаних зі змінами конфігурації системи;

No: 13
Name: cm_3_f_2
Type: string
Default: nil

здійснюється аналіз дій, пов'язаних зі змінами конфігурації системи;

No: 14
Name: cm_3_g_1
Type: string
Default: nil

діяльність з управління змінами конфігурації координується та

No: 15
Name: cm_3_g_2
Type: string
Default: nil

елемент управління зміною конфігурації викликається <CM03_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

5.3.1. АВТОМАТИЗОВАНЕ ДОКУМЕНТУВАННЯ, ПОВІДОМЛЕННЯ ТА ЗАБОРОНА ВНЕСЕННЯ ЗМІН (CM-3(1))

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для документування запропонованих змін до системи;.

No: 1
Name: cm_3_1_odp_1
Type: string
Default: nil

визначено механізми, що використовуються для ав181 томатизації управління змінами конфігурації

No: 2
Name: cm_3_1_odp_2
Type: string
Default: nil

визначені уповноважені органи, про які необхідно повідомляти та узгоджувати пропоновані зміни в системі;

No: 3
Name: cm_3_1_odp_3
Type: string
Default: nil

визначено період часу, після якого слід виділяти зміни, які не були схвалені або відхилені;

No: 4
Name: cm_3_1_odp_4
Type: string
Default: nil

визначено персонал, який буде повідомлений про завершення затверджених змін;

No: 5
Name: cm_3_1_a
Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для документування запропонованих змін до системи;

No: 6
Name: cm_3_1_b
Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для повідомлення <CM03(01)_ODP[02] уповноважені органи> про запропоновані зміни в системі та запиту на затвердження змін;

No: 7
Name: cm_3_1_c
Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для виділення запропонованих змін до системи, які не були схвалені або відхилені протягом

No: 8
Name: cm_3_1_d

Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для заборони внесення змін до системи до отримання відповідних погоджень;

No: 9
Name: cm_3_1_e
Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для документування всіх змін в системі;

No: 10
Name: cm_3_1_f
Type: string
Default: nil

<CM-03(01)_ODP[01] автоматизовані механізми> використовуються для повідомлення <CM03(01)_ODP[04] персоналу> про завершення погоджених змін у системі.

5.3.2. ТЕСТУВАННЯ, ВАЛІДАЦІЯ ТА ДОКУМЕНТУВАННЯ ЗМІН (CM-3(2))

Тестувати, перевіряти та документувати зміни в системі до повної їх реалізації.

No: 1
Name: cm_3_2_1
Type: string
Default: nil

зміни в системі тестуються перед повним впровадженням змін;

No: 2
Name: cm_3_2_2
Type: string
Default: nil

зміни в системі перевіряються перед повним впровадженням змін;

No: 3
Name: cm_3_2_3
Type: string
Default: nil

зміни в системі документуються перед повним впровадженням змін.

5.3.3. АВТОМАТИЗОВАНА РЕАЛІЗАЦІЯ ЗМІН (CM-3(3))

Внести зміни в поточний базову план системи та розгорнути оновлений базовий план на встановленій базі за допомогою [Призначення: автоматизовані механізми, визначені організацією].

No: 1
Name: cm_3_3_odp
Type: string
Default: nil

визначено автоматизовані механізми для внесення змін та розгортання оновленого базового плану по всій встановленій базі;

No: 2
Name: cm_3_3_1
Type: string
Default: nil

зміни до поточного базового плану системи реалізуються за допомогою <CM-03(03)_ODP автоматизовані механізми>;

No: 3
Name: cm_3_3_2
Type: string
Default: nil

оновлений базовий план розгортається по всій встановленій базі за допомогою <CM-03(03)_ODP автоматизовані механізми>.

5.3.4. ПРЕДСТАВНИК БЕЗПЕКИ (CM-3(4))

Вимагати від [Призначення: визначеного організацією представника з інформаційної безпеки] бути членом [Призначення: визначеного організацією елементу керування зміною конфігурацій].

No: 1
Name: cm_3_4_odp_1
Type: string
Default: nil

визначено представника з безпеки, який має бути членом елементу керування змінами конфігурації;

No: 2
Name: cm_3_4_odp_2
Type: string
Default: nil

визначено представника з конфіденційності, який має бути членом елементу керування змінами конфігурації;

No: 3
Name: cm_3_4_odp_3
Type: string
Default: nil

визначено елемент керування змінами конфігурації, членами якого мають бути представники безпеки та конфіденційності;

No: 4
Name: cm_3_4_1
Type: string
Default: nil

<CM-03(04)_ODP[01] представники безпеки> повинні бути членами <CM-03(04)_ODP[03] елемента керування змінами конфігурації>;

No: 5
Name: cm_3_4_2
Type: string
Default: nil

<CM-03(04)_ODP[02] представники конфіденційності> повинні бути членами <CM-03(04)_ODP[03] елемента керування змінами конфігурації>.

5.3.5. АВТОМАТИЧНЕ РЕАГУВАННЯ БЕЗПЕКИ (CM-3(5))

Реалізувати автоматичне [Призначення: визначене організацією реагування безпеки], якщо базова конфігурація системи змінюється несанкціонованим чином.

No: 1
Name: cm_3_5_odp
Type: string
Default: nil

визначено реагування безпеки, які мають бути застосовані автоматично;

No: 2
Name: cm_3_5_01
Type: string
Default: nil

<CM-03(05)_ODP реагування безпеки> автоматично застосовуються, якщо базова конфігурація системи змінюється несанкціонованим чином.

5.3.6. УПРАВЛІННЯ ЗАСОБАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ (CM-3(6))

Забезпечити, щоб криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебували під управлінням конфігурацією [Призначення: визначених організацією заходів безпеки].

No: 1
Name: cm_3_6_odp
Type: string
Default: nil

визначено заходи захисту;

No: 2
Name: cm_3_6_01
Type: string
Default: nil

криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебува ють під управлінням конфігурацією <CM-03(06)_ODP заходи захисту>.

5.3.7. ПЕРЕГЛЯД ЗМІН У СИСТЕМІ (CM-3(7))

Перегляньте зміни в системі [Призначення: частота, визначена організацією] або коли [Призначення: обставини, визначені організацією], щоб визначити, чи відбулися неавторизовані зміни.

No: 1
Name: cm_3_7_odp_1
Type: string
Default: nil

визначено частоту, з якою необхідно переглядати зміни;

No: 2
Name: cm_3_7_odp_2
Type: string
Default: nil

визначено обставини, за яких зміни мають бути переглянуті;

No: 3
Name: cm_3_7_01
Type: string
Default: nil

зміни в системі переглядаються < CM-03(07)_ODP[01] визначити, чи відбулися неавторизовані зміни.

5.3.8. ЗАПОБІГАННЯ ЧИ ОБМЕЖЕННЯ ЗМІН КОНФІГУРАЦІЇ (CM-3(8))

Запобігати або обмежити зміни конфігурації системи за таких обставин: [Призначення: обставини, визначені організацією].

No: 1
Name: cm_3_8_odp
Type: string
Default: nil

визначено обставини, за яких зміни мають бути запобіжені або обмежені;

No: 2
Name: cm_3_8_01
Type: string
Default: nil

зміни конфігурації системи запобігають або обмежують за <CM-03(08)_ODP обставин>.

5.4. АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ (CM-4)

Аналізувати зміни в системі, щоб визначити потенційну загрозу безпеці та приватності перед реалізацією змін.

No: 1
Name: cm_4_1
Type: string
Default: nil

аналізуються зміни в системі, щоб визначити потенційну загрозу безпеці перед реалізацією змін

No: 2
Name: cm_4_2
Type: string
Default: nil

аналізуються зміни в системі, щоб визначити потенційну загрозу конфіденційності перед реалізацією змін

5.4.1. ВІДОКРЕМЛЕНІ ВИПРОБУВАЛЬНІ СЕРЕДОВИЩА (CM-4(1))

Зміни в системі аналізуються в окремому тестовому середовищі перед впровадженням в операційному середовищі;.

No: 1
Name: cm_4_1_1
Type: string
Default: nil

зміни в системі аналізуються в окремому тестовому середовищі перед впровадженням в операційному середовищі;

No: 2
Name: cm_4_1_2
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на безпеку через недоліки;

No: 3
Name: cm_4_1_3
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на конфіденційність через недоліки;

No: 4
Name: cm_4_1_4
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на безпеку через слабкості;

No: 5
Name: cm_4_1_5
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на конфіденційність через слабкості;

No: 6
Name: cm_4_1_6
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на безпеку через несумістність;

No: 7
Name: cm_4_1_7
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на конфіденційність через несумістність;

No: 8
Name: cm_4_1_8
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на безпеку через навмисне спричинення шкоди;

No: 9
Name: cm_4_1_9
Type: string
Default: nil

зміни в системі аналізуються на предмет впливу на конфіденційність через навмисне спричинення шкоди;

5.4.2. ВЕРИФІКАЦІЯ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ (CM-4(2))

Після змін у системі переконайтеся, що відповідні заходи захисту реалізовано правильно і вони функціонують належним чином та дають бажаний результат щодо дотримання вимог безпеки та приватності для системи.

No: 1
Name: cm_4_2_1
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, реалізовані правильно з точки зору відповідності вимогам безпеки системи після внесення змін до системи;

No: 2
Name: cm_4_2_2
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, реалізовані правильно з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;

No: 3
Name: cm_4_2_3
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, функціонують належним чином з точки зору відповідності вимогам безпеки системи після внесення змін до системи;

No: 4
Name: cm_4_2_4
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, функціонують належним чином з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;

No: 5
Name: cm_4_2_5
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, дають бажаний результат з точки зору відповідності вимогам безпеки системи після внесення змін до системи;

No: 6
Name: cm_4_2_6
Type: string
Default: nil

заходи захисту, на які було здійснено вплив, дають бажаний результат з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;

5.5. ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ (CM-5)

Визначити, задокументувати, затвердити та забезпечити застосування фізичних і логічних обмежень доступу, пов'язаних зі змінами в системі.

No: 1
Name: cm_5_1
Type: string
Default: nil

визначені та задокументовані фізичні обмеження доступу, пов'язані зі змінами в системі;

No: 2
Name: cm_5_2
Type: string
Default: nil

затверджені фізичні обмеження доступу, пов'язані зі змінами в системі;

No: 3
Name: cm_5_3
Type: string
Default: nil

застосовуються фізичні обмеження доступу, пов'язані зі змінами в системі;

No: 4
Name: cm_5_4
Type: string
Default: nil

визначені та задокументовані логічні обмеження доступу, пов'язані зі змінами в системі;

No: 5
Name: cm_5_5
Type: string
Default: nil

затверджені логічні обмеження доступу, пов'язані зі змінами в системі;

No: 6
Name: cm_5_6
Type: string
Default: nil

застосовуються логічні обмеження доступу, пов'язані зі змінами в системі;

5.5.1. АУДИТ І ЗДІЙСНЕННЯ АВТОМАТИЧНОГО ДОСТУПУ (CM-5(1))

Обмеження доступу до змін застосовуються за допомогою <CM-05(01)_ODP автоматизованих механізмів>;.

No: 1
Name: cm_5_1_odp
Type: string
Default: nil

визначено механізми, що використовуються для автоматизації застосування обмежень доступу;

No: 2
Name: cm_5_1_a
Type: string
Default: nil

обмеження доступу до змін застосовуються за допомогою <CM-05(01)_ODP автоматизованих механізмів>;

No: 3
Name: cm_5_1_b
Type: string
Default: nil

автоматично формуються записи аудиту для виконаних дій.

5.5.2. ПЕРЕГЛЯД ЗМІН У СИСТЕМІ (CM-5(2)) [Вилучено]

[Вилучено: перенесено до CM-03(07)]

Немає параметрів для цього контролю.

5.5.3. ПІДПИСАНІ КОМПОНЕНТИ (CM-5(3)) [Вилучено]

[Вилучено: перенесено до CM-14]

Немає параметрів для цього контролю.

5.5.4. ПОДВІЙНА АВТОРИЗАЦІЯ (CM-5(4))

Здійснювати подвійну авторизацію для внесення змін до [Призначення: компонентів системи та інформації на рівні системи, визначених організацією].

No: 1
Name: cm_5_4_odp_1
Type: string
Default: nil

визначено компоненти системи, що потребують подвійної авторизації для внесення змін;

No: 2
Name: cm_5_4_odp_2
Type: string
Default: nil

визначено інформацію на рівні системи , що потребують подвійної авторизації для внесення змін;

No: 3
Name: cm_5_4_1
Type: string
Default: nil

запроваджено подвійну авторизацію для внесення змін

No: 4
Name: cm_5_4_2
Type: string
Default: nil

запроваджено подвійну авторизацію для внесення змін

5.5.5. ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ ВИРОБНИЦТВА ТА ЕКСПЛУАТАЦІЇ (CM-5(5))

(a) обмежити повноваження для зміни компонентів системи та інформації, пов'язаної із системою, у виробничому або операційному середовищі;

(b) переглядати та переоцінювати повноваження [Призначення: визначеною організацією з частотою].

No: 1
Name: cm_5_5_odp_1
Type: string
Default: nil

визначено частоту перегляду повноважень;

No: 2
Name: cm_5_5_odp_2
Type: string
Default: nil

визначено частоту переоцінення повноважень;

No: 3
Name: cm_5_5_a_1
Type: string
Default: nil

повноваження для зміни компонентів системи у виробничому або операційному середовищі обмежені;

No: 4
Name: cm_5_5_a_2
Type: string
Default: nil

повноваження для зміни інформації, пов'язаної із системою у виробничому або операційному середовищі обмежені;

No: 5
Name: cm_5_5_b_1
Type: string
Default: nil

переглядаються повноваження <CM-05(05)_ODP[01] частота>;

No: 6
Name: cm_5_5_b_2
Type: string
Default: nil

переоцінюються повноваження <CM-05(05)_ODP[02] частота>;

5.5.6. ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ БІБЛІОТЕК (CM-5(6))

Обмежити повноваження для зміни програмного забезпечення, яке перебуває в бібліотеках програмного забезпечення.

No: 1
Name: cm_5_6_01
Type: string
Default: nil

обмежено повноваження для зміни програмного забезпечення, яке перебуває в бібліотеках програмного забезпечення

5.5.7. ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ ВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ (CM-5(7)) [Вилучено]

[Вилучено: включено до SI-07]

Немає параметрів для цього контролю.

5.6. НАЛАШТУВАННЯ КОНФІГУРАЦІЇ (CM-6)

a. Встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, які відображають найбільш обмежений режим, що відповідає експлуатаційним вимогам, використовуючи [Призначення: визначені організацією загальні безпечні конфігурації].
b. Реалізувати конфігураційні установки.
c. Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для [Призначення: визначених організацією компонентів системи] на основі [Призначення: визначених організацією експлуатаційних вимог].
d. Відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур.

No: 1
Name: cm_6_odp_1
Type: string
Default: nil

визначено загальні безпечні конфігурації для встановлення та документування параметрів конфігурації компонентів, які застосовуються в системі;

No: 2
Name: cm_6_odp_2
Type: string
Default: nil

визначено компоненти системи, для яких необхідно затвердити відхилення;

No: 3
Name: cm_6_odp_3
Type: string
Default: nil

визначені експлуатаційні вимоги, що вимагають затвердження відхилень;

No: 4
Name: cm_6_a
Type: string
Default: nil

налаштування конфігурації, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам, встановлені та задокументовані для компонентів, що застосовуються

No: 5
Name: cm_6_b
Type: string
Default: nil

реалізовано установки конфігурації, задокументовані в CM-06a;

No: 6
Name: cm_6_c_1

Type: string
Default: nil

будь-які відхилення від встановлених параметрів конфігурації вимог>;

No: 7
Name: cm_6_c_2
Type: string
Default: nil

будь-які відхилення від встановлених налаштувань конфігурації

No: 8
Name: cm_6_d_1
Type: string
Default: nil

зміни в налаштуваннях конфігурації відстежуються відповідно до політики та процедур організації;

No: 9
Name: cm_6_d_2
Type: string
Default: nil

зміни налаштувань конфігурації керуються відповідно до політики та процедур організації.

5.6.1. АВТОМАТИЗОВАНЕ УПРАВЛІННЯ, ЗАСТОСУВАННЯ ТА ВЕРИФІКАЦІЯ (CM-6(1))

Налаштування конфігурації для <CM-06(01)_ODP[01].

No: 1
Name: cm_6_1_odp_1
Type: string
Default: nil

визначено компоненти системи, для яких можна керувати, застосовувати та перевіряти налаштування конфігурації;

No: 2
Name: cm_6_1_odp_2
Type: string
Default: nil

визначено автоматизовані механізми керування налаштуваннями конфігурації;

No: 3
Name: cm_6_1_odp_3
Type: string
Default: nil

визначено автоматизовані механізми застосування налаштувань конфігурації;

No: 4
Name: cm_6_1_odp_4
Type: string
Default: nil

визначено автоматизовані механізми перев ірки налаштувань конфігурації;

No: 5
Name: cm_6_1_1

Type: string
Default: nil

налаштування конфігурації для <CM-06(01)_ODP[01]

No: 6
Name: cm_6_1_2
Type: string
Default: nil

налаштування конфігурації для <CM-06(01)_ODP[01] компонентів системи> застосовуються за допомогою

No: 7
Name: cm_6_1_3
Type: string
Default: nil

налаштування конфігурації для <CM-06(01)_ODP[01] компонентів системи> перевіряються за допомогою

5.6.2. НАЛАШТУВАННЯ КОНФІГУРАЦІЇ САНКЦІОНОВАНІ ЗМІНИ (CM-6(2))

Виконайте такі дії у відповідь на неавторизовані зміни в [Призначення: параметри конфігурації, визначені організацією]: [Призначення: дії, визначені організацією].

No: 1
Name: cm_6_2_01
Type: string
Default: nil

<CM-06(02)_ODP[01] дії> виконуються у відповідь на конфігурації>.

5.6.3. ДЕМОНСТРАЦІЯ ВІДПОВІДНОСТІ (CM-6(4)) [Вилучено]

[Вилучено: Включено до CM-04]

Немає параметрів для цього контролю.

5.7. МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ (CM-7)

a. Налаштуйте систему для забезпечення лише [Призначення: основні функції, визначені організацією для місії];
b. Заборонити або обмежити використання таких функцій, портів, протоколів, програмного забезпечення та/або служб: [Призначення: визначені організацією заборонені або обмежені функції, системні порти, протоколи, програмне забезпечення та/або служби].

No: 1
Name: cm_7_odp_1
Type: string
Default: nil

визначено основні функції системи, необхідні для виконання місії;

No: 2
Name: cm_7_odp_2
Type: string
Default: nil

визначено функції, які необхідно заборонити або обмежити;

No: 3
Name: cm_7_odp_3
Type: string
Default: nil

визначено системні порти, які необхідно заборонити або обмежити;

No: 4
Name: cm_7_odp_4
Type: string
Default: nil

визначено протоколи, які необхідно заборонити або обмежити;

No: 5
Name: cm_7_odp_5
Type: string
Default: nil

визначено програмне забезпечення, яке необхідно заборонити або обмежити;

No: 6
Name: cm_7_odp_6
Type: string
Default: nil

визначено служби, які необхідно заборонити або обмежити;

No: 7
Name: cm_7_a
Type: string
Default: nil

система налаштована на забезпечення лише <CM-07_ODP[01] основні функції системи >;

No: 8
Name: cm_7_b_1
Type: string
Default: nil

використання <CM-07_ODP[02] функцій> заборонено або обмежено;

No: 9
Name: cm_7_b_2
Type: string
Default: nil

використання <CM-07_ODP[03] порти> заборонено або обмежено;

No: 10
Name: cm_7_b_3
Type: string
Default: nil

використання <CM-07_ODP[04] протоколи> заборонено або обмежено;

No: 11
Name: cm_7_b_4

Type: string
Default: nil

використання <CM-07_ODP[05] програмне забезпечення > заборонено або обмежено;

No: 12
Name: cm_7_b_5
Type: string
Default: nil

використання <CM-07_ODP[06] служби> заборонено або обмежено;

5.7.1. ПЕРІОДИЧНИЙ ПЕРЕГЛЯД (CM-7(1))

Система переглядається <CM-07(01)_ODP[01] частота> для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;.

No: 1
Name: cm_7_1_odp_1
Type: string
Default: nil

визначено частоту, з якою слід переглядати систему для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;

No: 2
Name: cm_7_1_odp_2
Type: string
Default: nil

визначено функції, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;

No: 3
Name: cm_7_1_odp_3
Type: string
Default: nil

визначено порти, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;

No: 4
Name: cm_7_1_odp_4
Type: string
Default: nil

визначено протоколи, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;

No: 5
Name: cm_7_1_odp_5
Type: string
Default: nil

визначено послуги, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;

No: 6
Name: cm_7_1_a
Type: string
Default: nil

система переглядається <CM-07(01)_ODP[01] частота> для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;

No: 7
Name: cm_7_1_b_1
Type: string
Default: nil

<CM-07(01)_ODP[02] функції> , які вважаються непотрібними та/або незахищеними, вимкнено;

No: 8
Name: cm_7_1_b_2
Type: string
Default: nil

<CM-07(01)_ODP[03] порти> , які вважаються непотрібними та/або незахищеними, вимкнено;

No: 9
Name: cm_7_1_b_3
Type: string
Default: nil

<CM-07(01)_ODP[04] протоколи> , які вважаються непотрібними та/або незахищеними, вимкнено;

No: 10
Name: cm_7_1_b_4
Type: string
Default: nil

<CM-07(01)_ODP[05] послуги>, які вважаються непотрібними та/або незахищеними, вимкнено;

5.7.2. ЗАБОРОНА ВИКОНАННЯ ПРОГРАМИ (CM-7(2))

Заборонити виконання програми відповідно до [Вибір (один або кілька): [Призначення: визначеної організацією політики, правил поведінки та/або угод про доступ щодо використання програмного забезпечення та обмежень]; правил, що встановлюють терміни та умови використання програмного забезпечення].

No: 1
Name: cm_7_2_odp_1
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ стання програмного забезпечення та обмежень>; правила, що встановлюють терміни та умови використання програмного забезпечення};

No: 2
Name: cm_7_2_odp_2
Type: string
Default: nil

визначені політики, правил поведінки та/або угод про доступ щодо використання програмного забезпечення та обмежень (якщо вибрано);

No: 3
Name: cm_7_2_01
Type: string
Default: nil

виконання програми заборонено відповідно до <CM07(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

5.7.3. ВІДПОВІДНІСТЬ РЕЄСТРАЦІЇ (CM-7(3))

Забезпечити відповідність [Призначення: визначеним організацією вимогам до реєстрації для функцій, портів, протоколів і послуг].

No: 1
Name: cm_7_3_odp
Type: string
Default: nil

визначено вимоги до реєстрації функцій, портів, протоколів та сервісів;

No: 2
Name: cm_7_3_01
Type: string
Default: nil

<CM-07(03)_ODP вимоги до реєстрації> дотримано.

5.7.4. НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ЧОРНИЙ СПИСОК (CM-7(4))

(a) Визначити [Призначення: визначені організацією програмне забезпечення, що не має дозволу виконуватися в системі].
(b) Впровадити політику «дозволу всього, за винятком деяких» для заборони виконання неавторизованих програм у системі
(c) Переглядати та оновлювати список неавторизованих програм [Призначення: з визначеною організацією частотою].

No: 1
Name: cm_7_4_odp_1
Type: string
Default: nil

визначено програмне забезпечення, яке не має дозволу на виконання в системі;

No: 2
Name: cm_7_4_odp_2
Type: string
Default: nil

визначено частоту, з якою слід переглядати та оновлювати список неавторизованих програм;

No: 3
Name: cm_7_4_a
Type: string
Default: nil

визначено <CM-07(04)_ODP[01] програмне забезпечення>;

No: 4
Name: cm_7_4_b
Type: string
Default: nil

політика "дозволу всього, за винятком деяких" застосовується для заборони виконання неавторизованих програм у системі;

No: 5
Name: cm_7_4_c

Type: string
Default: nil

переглядається та оновлюється список неавторизованих

5.7.5. АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ – БІЛИЙ СПИСОК (CM-7(5))

(a) Визначити [Призначення: визначені організацією програмне забезпечення, яке авторизовано виконується в системі]
(b) Впровадити політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм у системі.
(c) Переглядати та оновлювати список авторизованих програм [Призначення: з визначеною організацією частотою].

No: 1
Name: cm_7_5_odp_1
Type: string
Default: nil

визначено програмне забезпечення, яке авторизовано для виконання в системі;

No: 2
Name: cm_7_5_odp_2
Type: string
Default: nil

визначено частоту перегляду та оновлення списку авторизованих програм;

No: 3
Name: cm_7_5_a
Type: string
Default: nil

визначено <CM-07(05)_ODP[01] програмне забезпечення>;

No: 4
Name: cm_7_5_b
Type: string
Default: nil

політика "заборонити все, дозволити за винятком" застосовуэться, щоб дозволити виконання авторизованих програм у системі;

No: 5
Name: cm_7_5_c
Type: string
Default: nil

переглядається та оновлюється список авторизованих

5.7.6. ЗАМКНУТІ СЕРЕДОВИЩА З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ (CM-7(6))

Вимагайте, щоб визначене програмне забезпечення, встановлене користувачем, виконувалося в обмеженому середовищі фізичної або віртуальної машини з обмеженими привілеями: [Призначення: програмне забезпечення, встановлене користувачем, визначене організацією]

No: 1
Name: cm_7_6_odp
Type: string
Default: nil

визначено встановлене користувачем програмне забезпечення, яке потрібно виконувати в обмеженому середовищі;

No: 2
Name: cm_7_6_01
Type: string
Default: nil

<CM-07(06)_ODP програмне забезпечення, встановлене користувачем> має виконуватися в обмеженому середовищі фізичної або віртуальної машини з обмеженими привілеями.

5.7.7. ВИКОНУВАНИЙ КОД У ЗАХИЩЕНОМУ СЕРЕДОВИЩІ (CM-7(7))

Дозволити виконання двійкового або машинно-виконуваного коду лише в обмеженому фізичному або віртуальному машинному середовищі та за явного дозволу [Призначення: персонал або ролі, визначені організацією], якщо такий код: a) Отримано з джерел з обмеженою гарантією або без неї; та/або b) Без надання вихідного коду.

No: 1
Name: cm_7_7_odp
Type: string
Default: nil

визначено персонал або ролі для явного дозволу на виконання двійкового або машинно-виконуваного коду;

No: 2
Name: cm_7_7_01
Type: string
Default: nil

виконання двійкового або машинного коду дозволено лише в обмеженому середовищі фізичної або віртуальної машини;

No: 3
Name: cm_7_7_a
Type: string
Default: nil

виконання двійкового або машинного коду, отриманого з джерел з обмеженою гарантією або без неї, дозволяється лише з явного дозволу <CM-07(07)_ODP персонал або ролі>;

No: 4
Name: cm_7_7_b
Type: string
Default: nil

виконання двійкового або машинного коду без надання вихідного коду дозволяється лише з явного дозволу < CM07(07)_ODP персонал або ролі>.

5.7.8. БІНАРНИЙ АБО МАШИННИЙ ВИКОНУВАНИЙ КОД (CM-7(8))

a) Заборонити використання двійкового або машинно-виконуваного коду з джерел з обмеженою гарантією або без неї або без надання вихідного коду; і b) Дозволяти винятки лише для

обов'язкових місій або оперативних вимог і за погодженням з уповноваженою посадовою особою.

No: 1
Name: cm_7_8_a
Type: string
Default: nil

використання двійкового або машинного коду заборонено, якщо він походить з джерел з обмеженою гарантією або без неї, або без надання вихідного коду;

No: 2
Name: cm_7_8_b_1
Type: string
Default: nil

винятки із заборони на використання двійкового або машинного коду з джерел з обмеженою гарантією або без неї, або без надання вихідного коду допускаються лише для обов'язкових місій або оперативних вимог;

No: 3
Name: cm_7_8_b_2
Type: string
Default: nil

винятки із заборони на використання двійкового або машинного коду з джерел з обмеженою гарантією або без неї, або без надання вихідного коду допускаються лише у разі погодження з уповноваженою посадовою особою;

5.7.9. ЗАБОРОНА ВИКОРИСТАННЯ НЕАВТОРИЗОВАНОГО ОБЛАДНАННЯ (CM-7(9))

a.
b. c. ЗАБОРОНА Визначити [Призначення: апаратні компоненти, визначені організацією, авторизовані для використання в системі]; Заборонити використання або підключення неавторизованих апаратних компонентів; Перегляд та оновлення списку авторизованих апаратних компонентів [Призначення: частота, визначена організацією].

No: 1
Name: cm_7_9_odp_1
Type: string
Default: nil

визначено апаратні компоненти, дозволені для використання в системі;

No: 2
Name: cm_7_9_a
Type: string
Default: nil

ідентифіковано < CM-07(09)_ODP[01] апаратні компоненти>;

No: 3
Name: cm_7_9_b
Type: string
Default: nil

використання або підключення несанкціонованих апаратних компонентів заборонено;

No: 4
Name: cm_7_9_c

Type: string
Default: nil

список дозволених апаратних компонентів переглядається та оновлюється з <CM-07(09)_ODP[02] частота>;.

5.8. ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ (CM-8)

a.
b. Розробити та задокументувати процес інвентаризації компонентів системи, який:
1. точно описує поточну систему;
2. охоплює всі компоненти в межах акредитації системи;
3. не включає повторний облік компонентів або компонентів, будь-якої іншої системи;
4. визначає рівень деталізації, який є необхідним для відстеження та звітування;
5. включає інформацію для досягнення підзвітності компонентів системи: [Призначення: визначена організацією інформація, необхідна для досягнення ефективної підзвітності компонентів системи]. Переглядати та оновлювати опис компонентів системи з [Призначення: визначеною організацією частотою].

No: 1
Name: cm_8_odp_1
Type: string
Default: nil

визначено інформацію, яка вважається необхідною для досягнення ефективної підзвітності компонентів системи;

No: 2
Name: cm_8_odp_2
Type: string
Default: nil

визначено частоту перегляду та оновлення опису компонентів системи;

No: 3
Name: cm_8_a_1
Type: string
Default: nil

розроблено та задокументовано процес інвентаризації компонентів системи, який точно описує поточну систему;

No: 4
Name: cm_8_a_2
Type: string
Default: nil

розроблено та задокументовано процес інвентаризації компонентів системи, який охоплює всі компоненти в межах акредитації системи;

No: 5
Name: cm_8_a_3
Type: string
Default: nil

розроблено та задокументовано процес інвентаризації компонентів системи, який не включає повторний облік компонентів або компонентів, будь-якої іншої системи;

No: 6
Name: cm_8_a_4

Type: string
Default: nil

розроблено та задокументовано процес інвентаризації компонентів системи, який визначає рівень деталізації, який є необхідним для відстеження та звітування;

No: 7
Name: cm_8_a_5
Type: string
Default: nil

розроблено та задокументовано процес інвентаризації компонентів системи, який включає <CM-08_ODP[01] інформацію>;

No: 8
Name: cm_8_b
Type: string
Default: nil

переглядається та оновлюється опис компонентів системи

5.8.1. ОНОВЛЕННЯ ПІД ЧАС ВСТАНОВЛЕННЯ ТА ВИДАЛЕННЯ (CM-8(1))

Інвентаризація компонентів системи оновлюється в рамках інсталяцій компонентів системи;.

No: 1
Name: cm_8_1_1
Type: string
Default: nil

інвентаризація компонентів системи оновлюється в рамках інсталяцій компонентів системи;

No: 2
Name: cm_8_1_2
Type: string
Default: nil

інвентаризація компонентів системи оновлюється в рамках видалення компонентів системи;

No: 3
Name: cm_8_1_3
Type: string
Default: nil

інвентаризація компонентів системи оновлюється в рамках оновлення компонентів системи;

5.8.2. АВТОМАТИЗОВАНА ПІДТРИМКА (CM-8(2))

<CM-08(02)_ODP[01] автоматизовані механізми> використовуються для підтримки актуальності інвентаризації компонентів системи;.

No: 1
Name: cm_8_2_odp_1
Type: string
Default: nil

визначено автоматизовані механізми підтримки актуальності інвентаризації компонентів системи;

No: 2
Name: cm_8_2_odp_2
Type: string
Default: nil

визначено автоматизовані механізми підтримки повноти інвентаризації компонентів системи;

No: 3
Name: cm_8_2_odp_3
Type: string
Default: nil

визначено автоматизовані механізми підтримки точності інвентаризації компонентів системи;

No: 4
Name: cm_8_2_odp_4
Type: string
Default: nil

визначено автоматизовані механізми підтримки доступності інвентаризації компонентів системи;

No: 5
Name: cm_8_2_1
Type: string
Default: nil

<CM-08(02)_ODP[01] автоматизовані механізми> використовуються для підтримки актуальності інвентаризації компонентів системи;

No: 6
Name: cm_8_2_2
Type: string
Default: nil

<CM-08(02)_ODP[02] автоматизовані механізми> використовуються для підтримки повноти інвентаризації компонентів системи;

No: 7
Name: cm_8_2_3
Type: string
Default: nil

<CM-08(02)_ODP[03] автоматизовані механізми> використовуються для підтримки точності інвентаризації компонентів системи;

No: 8
Name: cm_8_2_4
Type: string
Default: nil

<CM-08(02)_ODP[04] автоматизовані механізми> використовуються для підтримки доступності інвентаризації компонентів системи;

5.8.3. АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМПОНЕНТІВ (CM-8(3))

Наявність несанкціонованого обладнання в системі виявляється за допомогою <CM-08(03)_ODP[01] частота>;.

No: 1
Name: cm_8_3_odp_1

Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованого обладнання в системі;

No: 2
Name: cm_8_3_odp_2
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованого програмного забезпечення в системі;

No: 3
Name: cm_8_3_odp_3
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованих мікропрограмних компонентів в системі;

No: 4
Name: cm_8_3_odp_4
Type: string
Default: nil

визначено частоту, з якою використовуються автоматизовані механізми для виявлення присутності несанкціонованих компонентів системи в системі;

No: 5
Name: cm_8_3_odp_5
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ

No: 6
Name: cm_8_3_odp_6
Type: string
Default: nil

визначено персонал або ролі, я кі мають бути повідомлені при виявленні несанкціонованих компонентів (якщо вибрано);

No: 7
Name: cm_8_3_a_1
Type: string
Default: nil

наявність несанкціонованого обладнання в системі виявляється за допомогою <CM-08(03)_ODP[01] частота>;

No: 8
Name: cm_8_3_a_2
Type: string
Default: nil

наявність несанкціонованого програмного забезпечення

No: 9
Name: cm_8_3_a_3
Type: string
Default: nil

наявність несанкціонованих мікропрограмних компонентів в системі виявляється за допомогою <CM08(03)_ ODP[03] автоматизованих механізмів> <CM 08(03)_ODP[04] частота>;

No: 10
Name: cm_8_3_b_1
Type: string
Default: nil

<CM-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> приймаються при виявленні несанкціонованого обладнання;

No: 11
Name: cm_8_3_b_2
Type: string
Default: nil

<CM-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПА206 РАМЕТРА(ів)> приймаються при виявленні несанкціонованого програмного забезпечення;

No: 12
Name: cm_8_3_b_3
Type: string
Default: nil

<CM-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> приймаються при виявленні несанкціонованих мікропрограмних компонентів;

5.8.4. ІНФОРМАЦІЯ ПРО ПІДЗВІТНІСТЬ (CM-8(4))

Впровадженно в інвентаризацію компонент ів системи засіб для ідентифікації <CM-08(04)_ ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> осіб, відповідальних і підзвітних за управління цими компонентами.

No: 1
Name: cm_8_4_odp
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {ім'я; позиція; роль};

No: 2
Name: cm_8_4_01
Type: string
Default: nil

впровадженно в інвентаризацію компонент ів системи засіб для ідентифікації <CM-08(04)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> осіб, відповідальних і підзвітних за управління цими компонентами.

5.8.5. ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ ДУБЛЮВАННЯ КОМПОНЕНТІВ ОБЛІКУ (CM-8(5))

Інвентаризація компонентів системи дублювання компонентів обліку (cm-8(5)).

Немає параметрів для цього контролю.

5.8.6. ПЕРЕВІРЕНІ НАЛАШТУВАННЯ ТА ЗАТВЕРДЖЕНІ ВІДХИЛЕННЯ (CM-8(6))

Включено перевірені налаштування компонентів до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи;.

No: 1
Name: cm_8_6_1
Type: string
Default: nil

включено перевірені налаштування компонентів до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи;

No: 2
Name: cm_8_6_2
Type: string
Default: nil

включено будь-які затверджені відхилення до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи.

5.8.7. ЦЕНТРАЛІЗОВАНЕ СХОВИЩЕ (CM-8(7))

Впровадити централізоване компонентів системи. сховище СИСТЕМИ для ЦЕНТРАЛІЗОВАНЕ інвентаризаційного обліку

No: 1
Name: cm_8_7_01
Type: string
Default: nil

впроваджено централізоване сховище для інвентаризаційного обліку компонентів системи.

5.8.8. АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ МІСЦЯ РОЗТАШУВАННЯ (CM-8(8))

Використовуютья <CM-08(08)_ODP автоматизовані механізми> для підтримки відстеження компонентів системи за географічним розташуванням.

No: 1
Name: cm_8_8_odp
Type: string
Default: nil

визначено автоматизовані механізми відстеження компонентів;

No: 2
Name: cm_8_8_01
Type: string
Default: nil

використовуютья <CM-08(08)_ODP автоматизовані механізми> для підтримки відстеження компонентів системи за географічним розташуванням

5.8.9. ПРИЗНАЧЕННЯ КОМПОНЕНТІВ СИСТЕМАМ (CM-8(9))

Компоненти системи призначаються системі;.

No: 1
Name: cm_8_9_odp
Type: string
Default: nil

визначено персонал або ролі, від яких слід отримувати підтвердження;

No: 2
Name: cm_8_9_a
Type: string
Default: nil

компоненти системи призначаються системі;

No: 3
Name: cm_8_9_b
Type: string
Default: nil

отримано підтвердження призначення компонента від <CM-08(09)_ODP персонал або ролі>.

5.9. ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM-9)

Унікально ідентифікувати та автентифікувати користувачів або процеси, що діють від імені користувачів.

No: 1
Name: cm_9_odp
Type: string
Default: nil

визначено персонал або ролі для розгляду та затвердження плану управління конфігурацією;

No: 2
Name: cm_9_01
Type: string
Default: nil

CM-09[01] розроблено та задокументовано план управління конфігурацією системи;

No: 3
Name: cm_9_02
Type: string
Default: nil

CM-09[02] реалізовано план управління конфігурацією системи;

No: 4
Name: cm_9_a_1
Type: string
Default: nil

план управління конфігурацією описує ролі;

No: 5
Name: cm_9_a_2
Type: string
Default: nil

план управління конфігурацією описує відповідальність;

No: 6
Name: cm_9_a_3
Type: string
Default: nil

план управління конфігурацією описує процеси та процедури управління конфігурацією;

No: 7
Name: cm_9_b_1
Type: string
Default: nil

план управління конфігурацією встановлює процес ідентифікації елементів конфігурації протягом всього життєвого циклу розробки системи;

No: 8
Name: cm_9_b_2
Type: string
Default: nil

план управління конфігурацією встановлює процес управління конфігурацією елементів;

No: 9
Name: cm_9_c_1
Type: string
Default: nil

план управління конфігурацією визначає елементи конфігурації системи;

No: 10
Name: cm_9_c_2
Type: string
Default: nil

план управління конфігурацією розміщує елементи конфігурації під управлінням конфігурацією;

No: 11
Name: cm_9_d
Type: string
Default: nil

план управління конфігурацією розглянуто та затверджено <CM09_ODP персонал або ролі>;

No: 12
Name: cm_9_e_1
Type: string
Default: nil

план управління конфігурацією захищений від несанкціонованого розкриття;

No: 13
Name: cm_9_e_2
Type: string
Default: nil

план управління конфігурацією захищений від несанкціонованої модифікації.

5.9.1. ВСТАНОВЛЕННЯ ВІДПОВІДАЛЬНОСТІ (CM-9(1))

Встановлено відповідальність за реалізацію процесу управління конфігурацією персоналу, який безпосередньо не бере участь у розробці системи.

No: 1
Name: cm_9_1_01
Type: string
Default: nil

встановлено відповідальність за реалізацію процесу управління конфігурацією персоналу, який безпосередньо не бере участь у розробці системи.

5.10. ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (CM-10)

Програмне забезпечення та супутня документація використовуються відповідно до договірних угод та законів про авторські права;.

No: 1
Name: cm_10_a
Type: string
Default: nil

програмне забезпечення та супутня документація використовуються відповідно до договірних угод та законів про авторські права;

No: 2
Name: cm_10_b
Type: string
Default: nil

використання програмного забезпечення та пов'язаної з ним документації, захищеної ліцензіями, відстежується для контролю за копіюванням та розповсюдженням;

No: 3
Name: cm_10_c
Type: string
Default: nil

використання технології однорангового обміну файлами контролюється та документується, щоб гарантувати, що одноранговий обмін файлами не використовується для несанкціонованого розповсюдження, відображення, виконання або відтворен ня програмного забезпечення, захищеного авторським правом.

5.10.1. ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ (CM-10(1))

Встановлено <CM-10(01)_ODP обмеження> на використання програмного забезпечення з відкритим вихідним кодом.

No: 1
Name: cm_10_1_odp
Type: string
Default: nil

визначено обмеження на використання програмного забезпечення з відкритим вихідним кодом

No: 2
Name: cm_10_1_01
Type: string
Default: nil

встановлено <CM-10(01)_ODP обмеження> на використання програмного забезпечення з відкритим вихідним кодом.

5.11. ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ (CM-11)

Встановлено <CM-11_ODP[01] правила (політики)>, що регулюють встановлення програмного забезпечення користувачами;.

No: 1
Name: cm_11_odp_1
Type: string
Default: nil

визначено правила (політики), що регулюють встановлення програмного забезпечення користувачами;

No: 2
Name: cm_11_odp_2
Type: string
Default: nil

визначено методи, що використовуються для забезпечення дотримання правил (політик) встановлення програмного забезпечення;

No: 3
Name: cm_11_odp_3
Type: string
Default: nil

визначено частоту, з якою слід контролювати відповідність правил (політик);

No: 4
Name: cm_11_a
Type: string
Default: nil

встановлено <CM-11_ODP[01] правила (політики)>, що регулюють встановлення програмного забезпечення користувачами;

No: 5
Name: cm_11_b
Type: string
Default: nil

правила (політики) встановлення програмного забезпечення

No: 6
Name: cm_11_c
Type: string
Default: nil

дотримання <CM-11_ODP[01] політик> контролюється <CM11_ODP[03] частота>.

5.11.1. ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПОПЕРЕДЖЕННЯ ПРО НЕСАНКЦІОНОВАНУ ІНСТАЛЯЦІЮ (CM-11(1))

Встановлене користувачем програмне забезпечення попередження про несанкціоновану інсталяцію (cm-11(1)).

Немає параметрів для цього контролю.

5.11.2. ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПРИВІЛЕЙОВАНИМ СТАТУСОМ (CM-11(2))

Встановлювати програмне забезпечення дозволено користувачеві лише при наявності привілейованого статусу.

No: 1
Name: cm_11_2_01
Type: string
Default: nil

встановлювати програмне забезпечення дозволено користувачеві лише при наявності привілейованого статусу.

5.11.3. ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЧНЕ ВИКОНАННЯ І МОНІТОРИНГ (CM-11(3))

Дотримання політик виконання програмного забезпечення забезпечується за допомогою <CM11(03)_ODP[01] автоматизованих механізмів>;.

No: 1
Name: cm_11_3_odp_1
Type: string
Default: nil

визначено автоматизовані механізми для забезпечення дотримання політик виконання програмного забезпечення;

No: 2
Name: cm_11_3_odp_2
Type: string
Default: nil

визначено автоматизовані механізми для забезпечення дотримання політик контролю програмного забезпечення;

No: 3
Name: cm_11_3_1
Type: string
Default: nil

дотримання політик виконання програмного забезпечення забезпечується за допомогою <CM11(03)_ODP[01] автоматизованих механізмів>;

No: 4
Name: cm_11_3_2
Type: string
Default: nil

дотримання політик контролю програмного забезпечення контролюється за допомогою <CM-11(03)_ODP[02] автоматизованих механізмів>.

5.12. РОЗТАШУВАННЯ ІНФОРМАЦІЇ (CM-12)

Місцезнаходження <CM-12_ODP інформація> визначено та задокументовано;.

No: 1
Name: cm_12_odp
Type: string
Default: nil

визначено інформацію, місцезнаходження якої має бути визначено та задокументовано;

No: 2
Name: cm_12_a_1
Type: string
Default: nil

місцезнаходження <CM-12_ODP інформація> визначено та задокументовано;

No: 3
Name: cm_12_a_2
Type: string
Default: nil

визначено та задокументовано конкретні компоненти системи, на яких обробляється <CM-12_ODP інформація>;

No: 4
Name: cm_12_a_3
Type: string
Default: nil

визначено та задокументовано конкретні компоненти системи, на яких зберігається <CM-12_ODP інформація>;

No: 5
Name: cm_12_b_1
Type: string
Default: nil

визначено та задокументовано користувачів, які мають доступ до системи та компонентів системи, де обробляється <CM-12_ODP інформація>;

No: 6
Name: cm_12_b_2
Type: string
Default: nil

визначено та задокументовано користувачів, які мають доступ до системи та компонентів системи, де зберігає ться <CM-12_ODP інформація>;

No: 7
Name: cm_12_c_1
Type: string
Default: nil

задокументовано зміни розташування (наприклад, системи або компонентів системи), де обробляється <CM-12_ODP інформація>;

No: 8
Name: cm_12_c_2
Type: string
Default: nil

задокументовано зміни розташування (наприклад, системи або компонентів сис теми), де зберігається <CM-12_ ODP інформація>;

5.12.1. АВТОМАТИЗОВАНІ ІНСТРУМЕНТИ ПІДТРИМКИ РОЗТАШУВАННЯ ІНФОРМАЦІЇ (CM-12(1))

Автоматизовані інструменти використовуються для ідентифікації <CM-12(01)_ODP[01] інформації за типом> забезпечити впровадження належних за ходів захисту щодо інформації про організацію і персональних даних.

No: 1
Name: cm_12_1_odp_1
Type: string
Default: nil

інформація визначена за типом;

No: 2
Name: cm_12_1_odp_2
Type: string
Default: nil

визначено компоненти системи, де знаходиться інформація;

No: 3
Name: cm_12_1_01
Type: string
Default: nil

автоматизовані інструменти використовуються для ідентифікації <CM-12(01)_ODP[01] інформації за типом> забезпечити впровадження належних за ходів захисту щодо інформації про організацію і персональних даних.

5.13. ВІДОБРАЖЕННЯ ДІЙ ДАНИХ (CM-13)

Розроблено та задокументовано карту дій з даними системи.

No: 1
Name: cm_13_01
Type: string
Default: nil

розроблено та задокументовано карту дій з даними системи.

5.14. ПІДПИСАНІ КОМПОНЕНТИ (CM-14)

Інсталяція < CM-14_ODP[01] програмне забезпечення > попередньо запобігається, якщо не буде перевірено, що програмне забезпечення було підписано цифровим підписом за допомогою сертифіката, визнаного та затвердженого організацією;.

No: 1
Name: cm_14_odp_1
Type: string
Default: nil

визначено програмне забезпечення, яке потребує перевірки сертифікату з цифровим підписом перед встановленням;

No: 2
Name: cm_14_odp_2
Type: string
Default: nil

визначено мікропрограмні компоненти, які потребує перевірки сертифікату з цифровим підписом перед встановленням;

No: 3
Name: cm_14_1
Type: string
Default: nil

інсталяція < CM-14_ODP[01] програмне забезпечення > попередньо запобігається, якщо не буде перевірено, що програмне забезпечення було підписано цифровим підписом за допомогою сертифіката, визнаного та затвердженого організацією;

No: 4
Name: cm_14_2
Type: string
Default: nil

інсталяція < CM-14_ODP[02] мікропрограмні компоненти > попередньо запобігається, якщо не буде перевірено, що мікропрограмні компоненти були підписані цифровим підписом за допомогою сертифіката, визнаного та затвердженого організацією;

6. CP

Клас заходів захисту CP — ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

Опис Цей клас описує заходи для відновлення функціонування інформаційної системи та забезпечення її безперебійної роботи у разі надзвичайних ситуацій.

Перелік заходів захисту Політика та процедури планування безперервної роботи (CP-1); План забезпечення безперервної роботи та відновлення функціонування (CP-2); Координація з пов'язаними планами (CP-2(1)); Навчання із забезпечення безперервної роботи (CP-3); Тестування плану забезпечення безперервної роботи та відновлення функціонування (CP-4); Альтернативна платформа тестування (CP-4(2)); Автоматичне тестування (CP-4(3)); Повне відновлення (CP-4(4)); Застосовуються для порушення та негативного впливу на (CP-4(5)); Оновлення плану забезпечення безперервної роботи та відновлення функціонування (CP-5) [Вилучено]; Альтернативне місце зберігання (CP-6); Відділення від первинного сховища (CP-6(1)); Час відновлення та встановлення цілей відновлення (CP-6(2)); Доступність (CP-6(3)); Альтернативний майданчик роботи (CP-7); Відділення від основного майданчика (CP-7(1)); Доступність (CP-7(2)); Пріоритет обслуговування (CP-7(3)); Підготовка для використання (CP-7(4)); Нездатність повернутися на основний майданчик (CP-7(6)); Комунікаційні послуги (CP-8); Пріоритет постачання послуг (CP-8(1)); Єдині точки відмови (CP-8(2)); Відділення основних та альтернативних провайдерів (CP-8(3)); План забезпечення безперервної роботи постачальника комунікаційних послуг (CP-8(4)); Тестування альтернативних комунікаційних послуг (CP-8(5)); Резервне копіювання (CP-9); Випробування на надійність та цілісність (CP-9(1)); Тестування відновлення з використанням зразків (CP-9(2)); Відокремлене сховище критичної інформації (CP-9(3)); Передача на альтернативне сховище зберігання (CP-9(5)); Надлишкова вторинна система (CP-9(6)); Подвійна авторизація (CP-9(7)); Криптографічний захист (CP-9(8)); Відновлення та відтворення системи (CP-10); Відновлення транзакцій (CP-10(2)); Відновлення в межах часового періоду (CP-10(4)); Здатність відмовостійкості (CP-10(5)) [Вилучено]; Альтернативні протоколи зв'язку (CP-11); Безпечний режим (CP-12); Альтернативні механізми безпеки (CP-13).

6.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP-1)

Розроблено та задокументовано політику планування безперервної роботи на випадок надзвичайних ситуацій;.

No: 1
Name: cp_1_odp_1
Type: string
Default: nil

визначено персонал або посади, на які поширюється політика планування безперервної роботи на випадок надзвичайних ситуацій;

No: 2
Name: cp_1_odp_2
Type: string
Default: nil

визначено персонал або посади, на які поширюється процедури планування безперервної роботи на випадок надзвичайних ситуацій;

No: 3
Name: cp_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: cp_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка кер уватиме політикою та процедурами планування безперервної роботи на випадок надзвичайних ситуацій;

No: 5
Name: cp_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика;

No: 6
Name: cp_1_odp_6
Type: string
Default: nil

визначено події, після яких переглядається та оновлюється поточна політика;

No: 7
Name: cp_1_odp_7
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються поточні процедури;

No: 8
Name: cp_1_odp_8
Type: string
Default: nil

визначено події, після яких переглядаються та оновлюються поточні процедури;

No: 9
Name: cp_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику планування безперервної роботи на випадок надзвичайних ситуацій;

No: 10
Name: cp_1_a_2
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій поширюється на <CP-01_ODP[01] персонал або посади>;

No: 11
Name: cp_1_a_3
Type: string
Default: nil

розроблені та задокументовані процедури планування безперервної роботи на випадок надзвичайних ситуацій, що сприяють впровадженню політики планування безперервної роботи на випадок надзвичайних ситуацій та пов'язаних з нею заходів захисту на випадок надзвичайних ситуацій;

No: 12
Name: cp_1_a_4
Type: string
Default: nil

процедури планування безперервної роботи на випадок надзвичайних ситуацій поширюються на <CP-01_ODP[02] персонал або посади>;

No: 13
Name: cp_1_a_1_a_1
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить мету;

No: 14
Name: cp_1_a_1_a_2
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування;

No: 15
Name: cp_1_a_1_a_3
Type: string
Default: nil

політика план ування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить ролі;

No: 16
Name: cp_1_a_1_a_4
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить обов'язки;

No: 17
Name: cp_1_a_1_a_5
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить відповідальність керівництва;

No: 18
Name: cp_1_a_1_a_6
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить координацію між підрозділами організації;

No: 19
Name: cp_1_a_1_a_7
Type: string
Default: nil

політика планування безперервної роботи на випадок надзвичайних ситуацій <CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить систему контролю відповідності;

No: 20
Name: cp_1_a_1_b
Type: string
Default: nil

<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика планування безперервної роботи на випадок надзвичайних ситуацій в ідповідає чинним законам, виконавчим розпорядженням, директивам, положенням, політикам, стандартам і керівним принципам;

No: 21
Name: cp_1_b
Type: string
Default: nil

<CP-01_ODP[04] посадова особа> призначається для управління , документуванням та розповсюдженням політики та процедур планування безперервної роботи на випадок надзвичайних ситуацій;

No: 22
Name: cp_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика планування

No: 23
Name: cp_1_c_1_2
Type: string
Default: nil

переглядається т а оновлюється поточна політика планування безперервної роботи на випадок надзвичайних ситуацій після

No: 24
Name: cp_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури планування безперервної роботи на випадок надзвичайних ситуацій

No: 25
Name: cp_1_c_2_2
Type: string
Default: nil

переглядаються та оновлюються поточні процедури планування безперервної роботи на випадок надзвичайних ситуацій

6.2. ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ (CP-2)

Розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який визначає основні завдання, функції та пов’язані з ними вимоги щодо безперервної роботи;.

No: 1
Name: cp_2_odp_1
Type: string
Default: nil

визначено персонал або ролі для перегляду плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 2
Name: cp_2_odp_2
Type: string
Default: nil

визначено персонал або ролі для затвердження плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 3
Name: cp_2_odp_3
Type: string
Default: nil

визначено ключовий резервний персонал (ідентифікований за іменами та/або за ролями), якому поширюються копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій;

No: 4
Name: cp_2_odp_4
Type: string
Default: nil

визначено ключові елементи, на які поширюються копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій;

No: 5
Name: cp_2_odp_5
Type: string
Default: nil

визначено періодичність перегляду плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 6
Name: cp_2_odp_6
Type: string
Default: nil

визначено ключовий резервний персонал (ідентифікований за іменами та/або ролями), якому необхідно повідомити про зміни;

No: 7
Name: cp_2_odp_7
Type: string
Default: nil

визначено ключові елементи організації, і які необхідно повідомити про зміни;

No: 8
Name: cp_2_a_1
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи;

No: 9
Name: cp_2_a_2_1
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує цілі;

No: 10
Name: cp_2_a_2_2

Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує пріорітети;

No: 11
Name: cp_2_a_2_3
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує відповідні показники;

No: 12
Name: cp_2_a_3_1
Type: string
Default: nil

розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено ролі;

No: 13
Name: cp_2_a_3_2
Type: string
Default: nil

розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено обов'язки;

No: 14
Name: cp_2_a_3_3
Type: string
Default: nil

розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено відповідальних осіб з контактною інформацією;

No: 15
Name: cp_2_a_4
Type: string
Default: nil

розроблено план забезпечення безперервної роботи на випадок непередбачених обставин для системи, який спрямований на підтримку основних завдань і функції, попри системні збої, компрометації або помилки;

No: 16
Name: cp_2_a_5
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації та персональних даних;

No: 17
Name: cp_2_a_6
Type: string
Default: nil

розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, який вирішує питання обміну інформацією про надзвичайні ситуації;

No: 18
Name: cp_2_a_7_1
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який переглядається <CP-02_ODP[01] персоналом або ролями>;

No: 19
Name: cp_2_a_7_2
Type: string
Default: nil

розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який затверджено <CP-02_ODP[02] персоналом або ролями>;

No: 20
Name: cp_2_b_1
Type: string
Default: nil

копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій розповсюджуються серед <CP-02_ODP[03] персоналу>;

No: 21
Name: cp_2_b_2
Type: string
Default: nil

копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій розповсюджуються серед <CP-02_ODP[04] елементів>;

No: 22
Name: cp_2_c
Type: string
Default: nil

діяльність з планування безперервної роботи координується з діяльністю із заходами по усуненню інцидентів;

No: 23
Name: cp_2_d
Type: string
Default: nil

переглядається план забезпечення безперервної роботи у надзвичайних ситуаціях для системи <CP-02_ODP[05] частота>;

No: 24
Name: cp_2_e_1
Type: string
Default: nil

план забезпечення безперервної роботи на випадок надзвичайних ситуацій оновлюється з урахуванням змін в організації, системі або середовищі функціонування;

No: 25
Name: cp_2_e_2
Type: string
Default: nil

план забезпечення безперервної роботи на випадок надзвичайних ситуацій оновлюється для вирішення проблем, що виникають під час впровадження, виконання або тестування плану дій на випадок надзвичайних ситуацій;

No: 26
Name: cp_2_f_1
Type: string
Default: nil

зміни в плані забезпечення безперервної роботи на випадок

No: 27
Name: cp_2_f_2
Type: string
Default: nil

зміни в плані забезпечення безперервної роботи на випадок

No: 28
Name: cp_2_g_1
Type: string
Default: nil

уроки, отримані під час тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях або фактичних дій у надзвичайних ситуаціях, включаються в навчання;

No: 29
Name: cp_2_g_2
Type: string
Default: nil

уроки, отримані під час тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях або фактичних дій у надзвичайних ситуаціях, включаються в тестування;

No: 30
Name: cp_2_h_1
Type: string
Default: nil

план забезпечення безперервної роботи у надзвичайних ситуаціях захищений від несанкціонованого доступу;

No: 31
Name: cp_2_h_2
Type: string
Default: nil

план забезпечення безперервної роботи у надзвичайних ситуаціях захищений від несанкціонованих змін;

6.2.1. КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ (CP-2(1))

Розробка плану забезпечення безперервної роботи у надзвичайних ситуаціях координується зі структурними підрозділами, які відповідають за розробку та реалізацію пов'язаних планів.

No: 1
Name: cp_2_1_01
Type: string
Default: nil

розробка плану забезпечення безперервної роботи у надзвичайних ситуаціях координується зі структурними підрозділами, які відповідають за розробку та реалізацію пов'язаних планів.

6.3. НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP-3)

Підготовка на випадок надзвичайних ситуацій надається користувачам системи відповідно до призначених ролей та обов'язків протягом <CP-03_ODP[01] періоду часу> з моменту прийняття на себе надзвичайної ролі або обов'язку;.

No: 1
Name: cp_3_odp_1
Type: string
Default: nil

визначено період часу, протягом якого необхідно провести тренінг з підготовки до дій в умовах надзвичайних ситуацій після прийняття на себе ролі або відповідальності в умовах надзвичайних ситуацій;

No: 2
Name: cp_3_odp_2
Type: string
Default: nil

визначено частоту проведення тренінгів для користувачів системи, які виконують непередбачувану роль або несуть відповідальність;

No: 3
Name: cp_3_odp_3
Type: string
Default: nil

визначено частоту, з якою необхідно переглядати та оновлювати зміст тренувань на випадок надзвичайних ситуацій;

No: 4
Name: cp_3_odp_4
Type: string
Default: nil

визначено події, які потребують перегля ду та оновлення тренувань на випадок надзвичайних ситуацій;

No: 5
Name: cp_3_a_1
Type: string
Default: nil

підготовка на випадок надзвичайних ситуацій надається користувачам системи відповідно до призначених ролей та обов'язків протягом <CP-03_ODP[01] періоду часу> з моменту прийняття на себе надзвичайної ролі або обов'язку;

No: 6
Name: cp_3_a_2
Type: string
Default: nil

навчання на випадок надзвичайних ситуацій проводиться для користувачів системи відповідно до призначених ролей та обов'язків, якщо цього вимагають зміни в системі;

No: 7
Name: cp_3_a_3
Type: string
Default: nil

користувачам системи надається навчання на випадок надзвичайних ситуацій відповідно до призначених ролей та обов'язків

No: 8
Name: cp_3_b_1
Type: string
Default: nil

переглядається та оновлюється зміст тренувань за планом реагування на надзвичайні ситуації <CP-03_ODP[03] частота>;

No: 9
Name: cp_3_b_2
Type: string
Default: nil

зміст тренувань за планом реагування на надзвичайні ситуації

6.4. ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ (CP-4)

Тестується план забезпечення безперервної робо ти у надзвичайних ситуаціях для системи <CP-04_ODP[01] частота>;.

No: 1
Name: cp_4_odp_1
Type: string
Default: nil

визначено частоту тестування плану забезпечення безперервної роботи у надзвичайних ситуаціях для системи;

No: 2
Name: cp_4_odp_2
Type: string
Default: nil

визначено тести для визначення ефективності плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 3
Name: cp_4_odp_3
Type: string
Default: nil

визначені тести для визначення готовності до виконання плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 4
Name: cp_4_a_1
Type: string
Default: nil

тестується план забезпечення безперервної робо ти у надзвичайних ситуаціях для системи <CP-04_ODP[01] частота>;

No: 5
Name: cp_4_a_2
Type: string
Default: nil

<CP-04_ODP[02] тести> використовуються для визначення ефективності плану;

No: 6
Name: cp_4_a_3
Type: string
Default: nil

<CP-04_ODP[03] тести> використовуються для визначення готовності до виконання плану;

No: 7
Name: cp_4_b
Type: string
Default: nil

переглядаються результати тестування плану забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 8
Name: cp_4_c
Type: string
Default: nil

за необхідності ініціюються коригувальні дії.

6.4.1. АЛЬТЕРНАТИВНА ПЛАТФОРМА ТЕСТУВАННЯ (CP-4(2))

План забезпечення безперервної роботи у надзвичайних ситуаціях тестується на альтернативній платформі для ознайомлення персоналу з об'єктом та наявними ресурсами;.

No: 1
Name: cp_4_2_a
Type: string
Default: nil

план забезпечення безперервної роботи у надзвичайних ситуаціях тестується на альтернативній платформі для ознайомлення персоналу з об'єктом та наявними ресурсами;

No: 2
Name: cp_4_2_b
Type: string
Default: nil

план забезпечення безперервної роботи у надзвичайних ситуаціях тестується на альтернативній платформі для оцінки можливостей альтернативної платформи;

6.4.2. АВТОМАТИЧНЕ ТЕСТУВАННЯ (CP-4(3))

План забезпечення безперервної роботи на випадок надзвичайних ситуацій тестується за допомогою <CP-04(03)_ODP автоматизованих механізмів>.

No: 1
Name: cp_4_3_odp

Type: string
Default: nil

визначено автоматизовані механізми тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях;

No: 2
Name: cp_4_3_01
Type: string
Default: nil

план забезпечення безперервної роботи на випадок надзвичайних ситуацій тестується за допомогою <CP-04(03)_ODP автоматизованих механізмів>.

6.4.3. ПОВНЕ ВІДНОВЛЕННЯ (CP-4(4))

Включено повне відновлення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування.

No: 1
Name: cp_4_4_1
Type: string
Default: nil

включено повне відновлення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування

No: 2
Name: cp_4_4_2
Type: string
Default: nil

включено повне повернення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування

6.4.4. ЗАСТОСОВУЮТЬСЯ ДЛЯ ПОРУШЕННЯ ТА НЕГАТИВНОГО ВПЛИВУ НА (CP-4(5))

<CP-04(05)_ODP[01] механізми> застосовуються для порушення та негативного впливу на <CP-04(05)_ODP[02] систему або компонент системи>.

No: 1
Name: cp_4_5_odp_1
Type: string
Default: nil

визначено механізми, що застосовуються для порушення та негативного впливу на систему або на компонент системи;

No: 2
Name: cp_4_5_odp_2
Type: string
Default: nil

визначено систему або компонент системи, до яких застосовуються механізми порушення та негативного впливу

No: 3
Name: cp_4_5_01
Type: string
Default: nil

<CP-04(05)_ODP[01] механізми> застосовуються для порушення та негативного впливу на <CP-04(05)_ODP[02] систему або компонент системи>.

6.5. ОНОВЛЕННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ (CP-5) [Вилучено]

[Вилучено: Включено до CP-02]

Немає параметрів для цього контролю.

6.6. АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ (CP-6)

Створено альтернативне місце зберігання;.

No: 1
Name: cp_6_a_1
Type: string
Default: nil

створено альтернативне місце зберігання;

No: 2
Name: cp_6_a_2
Type: string
Default: nil

створення альтернативного місця зберігання включає в себе необхідні угоди, що дозволяють зберігати та видавати інформацію резервного копіювання системи;

No: 3
Name: cp_6_b
Type: string
Default: nil

в альтернативному місці зберігання впроваджені заходи захисту, аналогічні заходам захисту основної локації.

6.6.1. ВІДДІЛЕННЯ ВІД ПЕРВИННОГО СХОВИЩА (CP-6(1))

Визначено альтернативне місце зберігання, яке відокремлено від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз.

No: 1
Name: cp_6_1_01
Type: string
Default: nil

визначено альтернативне місце зберігання, яке відокремлено від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз.

6.6.2. ЧАС ВІДНОВЛЕННЯ ТА ВСТАНОВЛЕННЯ ЦІЛЕЙ ВІДНОВЛЕННЯ (CP-6(2))

Налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до часу відновлення;.

No: 1
Name: cp_6_2_1
Type: string
Default: nil

налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до часу відновлення;

No: 2
Name: cp_6_2_2
Type: string
Default: nil

налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до встановлених цілей відновлення.

6.6.3. ДОСТУПНІСТЬ (CP-6(3))

Визначено потенційні проблеми доступності для альтернативного місця зберігання в разі збоїв або стихійних лих по всьому регіоні;.

No: 1
Name: cp_6_3_1
Type: string
Default: nil

визначено потенційні проблеми доступності для альтернативного місця зберігання в разі збоїв або стихійних лих по всьому регіоні;

No: 2
Name: cp_6_3_2
Type: string
Default: nil

в загальних рисах окреслено дії щодо пом'якшення наслідків

6.7. АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК РОБОТИ (CP-7)

Альтернативний майданчик для роботи, включно з необхідними.

No: 1
Name: cp_7_odp_1

Type: string
Default: nil

визначені операції системи для основних завдань і функцій;

No: 2
Name: cp_7_odp_2
Type: string
Default: nil

визначено період часу, відповідно термінам відновлення та встановленим цілям відновлення;

No: 3
Name: cp_7_a
Type: string
Default: nil

альтернативний майданчик для роботи, включно з необхідними

No: 4
Name: cp_7_b_1
Type: string
Default: nil

обладнання та прилади, необхідні для передачі, доступні на альтернативному місці роботи або якщо укладені контракти на періоду часу> для передачі;

No: 5
Name: cp_7_b_2
Type: string
Default: nil

обладнання та прилади, необхідні для відновлення, доступні на альтернативному місці роботи або якщо укладені контракти на періоду часу> для передачі;

No: 6
Name: cp_7_c
Type: string
Default: nil

впроваджено на альтернативному майданчику роботи заходи захисту, еквівалентні тим, що впровадженні на основному майданчику.

6.7.1. ВІДДІЛЕННЯ ВІД ОСНОВНОГО МАЙДАНЧИКА (CP-7(1))

Визначено альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення сприйнятливості до тих самих загроз.

No: 1
Name: cp_7_1_01
Type: string
Default: nil

визначено альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення сприйнятливості до тих самих загроз

6.7.2. ДОСТУПНІСТЬ (CP-7(2))

Визначено потенційні проблеми доступності для альтернативного майданчика для роботи в разі збоїв або катастрофи по всьому регіону.

No: 1
Name: cp_7_2_1
Type: string
Default: nil

визначено потенційні проблеми доступності для альтернативного майданчика для роботи в разі збоїв або катастрофи по всьому регіону

No: 2
Name: cp_7_2_2
Type: string
Default: nil

окреслено чіткі заходи щодо пом'якшення наслідків

6.7.3. ПРІОРИТЕТ ОБСЛУГОВУВАННЯ (CP-7(3))

Розроблено угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог стосовно доступності (включно з вимогами щодо часу відно237 влення).

No: 1
Name: cp_7_3_01
Type: string
Default: nil

розроблено угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог стосовно доступності (включно з вимогами щодо часу відно237 влення).

6.7.4. ПІДГОТОВКА ДЛЯ ВИКОРИСТАННЯ (CP-7(4))

Підготовлено альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання основних завдань та функцій.

No: 1
Name: cp_7_4_01
Type: string
Default: nil

підготовлено альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання основних завдань та функцій

6.7.5. НЕЗДАТНІСТЬ ПОВЕРНУТИСЯ НА ОСНОВНИЙ МАЙДАНЧИК (CP-7(6))

Розроблено план до обставин, які виключають повернення на основне місце роботи;.

No: 1
Name: cp_7_6_1
Type: string
Default: nil

розроблено план до обставин, які виключають повернення на основне місце роботи;

No: 2
Name: cp_7_6_2
Type: string
Default: nil

підготувалися до обставин, які виключають повернення на основне місце роботи;

6.8. КОМУНІКАЦІЙНІ ПОСЛУГИ (CP-8)

Альтернативні комунікаційні послуги, включно з необхідними угодами, що дозволяють відновити <CP-08_ODP[01] операції системи>, створюються для основних завдань та функцій протягом <CP08_ODP[02] періоду часу>, коли основні комунікаційні можливості недоступн і на основному або альтернативному місцях роботи або зберігання.

No: 1
Name: cp_8_odp_1
Type: string
Default: nil

визначено операції системи, які необхідно відновити для виконання основних завдань та функцій;

No: 2
Name: cp_8_odp_2
Type: string
Default: nil

визначено період часу, протягом якого необхідно відновити основні завдання та функції, коли основні комунікаційні можливості недоступні;

No: 3
Name: cp_8_01
Type: string
Default: nil

альтернативні комунікаційні послуги, включно з необхідними угодами, що дозволяють відновити <CP-08_ODP[01] операції системи>, створюються для основних завдань та функцій протягом <CP08_ODP[02] періоду часу>, коли основні комунікаційні можливості недоступн і на основному або альтернативному місцях роботи або зберігання.

6.8.1. ПРІОРИТЕТ ПОСТАЧАННЯ ПОСЛУГ (CP-8(1))

Розроблено угоди про надання основних комунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог щодо доступності (включно з вимогами щодо часу відновлення);.

No: 1
Name: cp_8_1_a_1
Type: string
Default: nil

розроблено угоди про надання основних комунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог щодо доступності (включно з вимогами щодо часу відновлення);

No: 2
Name: cp_8_1_a_2
Type: string
Default: nil

розроблено альтернативні угоди про надання комунікаційних послуг, які містять положення про пріоритетність надання послуг відповідно до вимог доступності (включно з вимогами щодо часу відновлення);

No: 3
Name: cp_8_1_b
Type: string
Default: nil

надсилається запит про пріоритети комуніка ційних послуг для всіх комунікаційних послуг, що використовуються для забезпечення безперервності роботи, якщо основні та/або альтернативні комунікаційні послуги надаються загальним оператором.

6.8.2. ЄДИНІ ТОЧКИ ВІДМОВИ (CP-8(2))

Отримано альтернативні комунікаційні послуги з метою зменшення ймовірності спільного використання єдиної точки відмови з основними комунікаційними послугами.

No: 1
Name: cp_8_2_01
Type: string
Default: nil

отримано альтернативні комунікаційні послуги з метою зменшення ймовірності спільного використання єдиної точки відмови з основними комунікаційними послугами.

6.8.3. ВІДДІЛЕННЯ ОСНОВНИХ ТА АЛЬТЕРНАТИВНИХ ПРОВАЙДЕРІВ (CP-8(3))

Отримуються альтернативні комунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тих самих загроз.

No: 1
Name: cp_8_3_01
Type: string
Default: nil

отримуються альтернативні комунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тих самих загроз.

6.8.4. ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ПОСТАЧАЛЬНИКА КОМУНІКАЦІЙНИХ ПОСЛУГ (CP-8(4))

Постачальники основних комунікаційних послуг зобов'язані мати плани забезпечення безперервної роботи;.

No: 1
Name: cp_8_4_odp_1
Type: string
Default: nil

визначено частоту, з якою постачальники послуг повинні надавати свідчення про тестування планів забезпечення безперервної роботи;

No: 2
Name: cp_8_4_odp_2
Type: string
Default: nil

визначено частоту, з якою постачальники послуг повинні надавати свідчення про тренування з планів забезпечення безперервної роботи;

No: 3
Name: cp_8_4_a_1
Type: string
Default: nil

постачальники основних комунікаційних послуг зобов'язані мати плани забезпечення безперервної роботи;

No: 4
Name: cp_8_4_a_2
Type: string
Default: nil

постачальники альтернативних комунікаційних послуг зобов'язані мати плани забезпечення безперервної роботи;

No: 5
Name: cp_8_4_b
Type: string
Default: nil

переглядаються плани забезпечення безперервної роботи постачальників комунікаційних послуг для забезпечення відповідності планам забе зпечення безперервної роботи організації;

No: 6
Name: cp_8_4_c_1
Type: string
Default: nil

отримано свідчення про тестування планів забезпечення

No: 7
Name: cp_8_4_c_2
Type: string
Default: nil

отримано свідчення про тренування з планів забезпечення

6.8.5. ТЕСТУВАННЯ АЛЬТЕРНАТИВНИХ КОМУНІКАЦІЙНИХ ПОСЛУГ (CP-8(5))

Тестування надання альтернативних комунікаційних послуг з <CP-08(05)_ODP частотою>.

No: 1
Name: cp_8_5_odp

Type: string
Default: nil

визначено частоту з якою необхідно тестувати надання альтернативних комунікаційних послуг;

No: 2
Name: cp_8_5_01
Type: string
Default: nil

тестування надання альтернативних комунікаційних послуг з <CP-08(05)_ODP частотою>.

6.9. РЕЗЕРВНЕ КОПІЮВАННЯ (CP-9)

Резервне копіювання інформації кор истувача, що міститься в.

No: 1
Name: cp_9_odp_1
Type: string
Default: nil

визначено компоненти системи, для яких необхідно проводити резервне копіювання інформації користувачів;

No: 2
Name: cp_9_odp_2
Type: string
Default: nil

визначено частоту, з якою слід проводити резервне копіювання інформації користувача відповідно до часу відновлення та цілей відновлення;

No: 3
Name: cp_9_odp_3
Type: string
Default: nil

визначено частоту проведення резервного копіювання інформації системи, що відповідає завдань відновлення і встановлених цілей відновлення;

No: 4
Name: cp_9_odp_4
Type: string
Default: nil

визначено частоту, з якою слід проводити резервне копіювання документації системи відповідно до часу відновлення та цілей точки відновлення;

No: 5
Name: cp_9_a
Type: string
Default: nil

резервне копіювання інформації кор истувача, що міститься в

No: 6
Name: cp_9_b
Type: string
Default: nil

виконується резервне копіювання інформації системи, що CP-09(c) створюються резервні копії документації системи, включаючи

No: 7
Name: cp_9_d_1
Type: string
Default: nil

конфіденційність резервних копій інформації захищена;

No: 8
Name: cp_9_d_2
Type: string
Default: nil

цілісність резервних копій інформації захищена;

No: 9
Name: cp_9_d_3
Type: string
Default: nil

доступність резервних копій інформації захищена.

6.9.1. ВИПРОБУВАННЯ НА НАДІЙНІСТЬ ТА ЦІЛІСНІСТЬ (CP-9(1))

Носії резервних копій інформації тестується <CP09(01)_ODP[01] частота> для перевірки надійності;.

No: 1
Name: cp_9_1_odp_1
Type: string
Default: nil

визначено частоту тестування на надійність носіїв резервних копій інформації;

No: 2
Name: cp_9_1_odp_2
Type: string
Default: nil

визначено частоту тестування на цілісність носіїв резервних копій інформації;

No: 3
Name: cp_9_1_1
Type: string
Default: nil

носії резервних копій інформації тестується <CP09(01)_ODP[01] частота> для перевірки надійності;

No: 4
Name: cp_9_1_2
Type: string
Default: nil

носії резервних копій інформації тестується <CP09(01)_ODP[02] частота> для перевірки цілісності;

6.9.2. ТЕСТУВАННЯ ВІДНОВЛЕННЯ З ВИКОРИСТАННЯМ ЗРАЗКІВ (CP-9(2))

Використовується зразок резервної копії інформації при відновленні вибраних функцій системи як частину тестування плану забезпечення безперервної роботи та відновлення функціонування.

No: 1
Name: cp_9_2_01
Type: string
Default: nil

використовується зразок резервної копії інформації при відновленні вибраних функцій системи як частину тестування плану забезпечення безперервної роботи та відновлення функціонування

6.9.3. ВІДОКРЕМЛЕНЕ СХОВИЩЕ КРИТИЧНОЇ ІНФОРМАЦІЇ (CP-9(3))

Резервні копії <CP-09(03)_ODP критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою> зберігаються в окремому сховищі або у вогнетривкому контейнері, не пов'язаному з системою.

No: 1
Name: cp_9_3_odp
Type: string
Default: nil

визначено критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою яке має зберігатися в окремому сховищі або у вогнетривкому контейнері;

No: 2
Name: cp_9_3_01
Type: string
Default: nil

резервні копії <CP-09(03)_ODP критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою> зберігаються в окремому сховищі або у вогнетривкому контейнері, не пов'язаному з системою.

6.9.4. ПЕРЕДАЧА НА АЛЬТЕРНАТИВНЕ СХОВИЩЕ ЗБЕРІГАННЯ (CP-9(5))

Інформація резервної копії системи передається до альтернативного сховища протягом <CP-09(05)_ODP[01] періоду часу>;.

No: 1
Name: cp_9_5_odp_1
Type: string
Default: nil

визначено період часу, що відповідає часу відновлення та цілям відновлення;

No: 2
Name: cp_9_5_odp_2

Type: string
Default: nil

визначено швидкість передачі даних, що відповідає часу відновлення та цілям відновлення;

No: 3
Name: cp_9_5_1
Type: string
Default: nil

інформація резервної копії системи передається до альтернативного сховища протягом <CP-09(05)_ODP[01] періоду часу>;

No: 4
Name: cp_9_5_2
Type: string
Default: nil

інформація резервної копії системи передається до альтернативного сховища з <CP-09(05)_ODP[02] швидкість передачі >;

6.9.5. НАДЛИШКОВА ВТОРИННА СИСТЕМА (CP-9(6))

Резервне копіювання системи здійснюється шляхом підтримки надлишкової вторинної системи, яка не пов'язана з первинною системою;.

No: 1
Name: cp_9_6_1
Type: string
Default: nil

резервне копіювання системи здійснюється шляхом підтримки надлишкової вторинної системи, яка не пов'язана з первинною системою;

No: 2
Name: cp_9_6_2
Type: string
Default: nil

резервне копіювання системи здійснюється шляхом підтримки резервної вторинної системи, яка може бути активована без втрати інформації або порушення роботи.

6.9.6. ПОДВІЙНА АВТОРИЗАЦІЯ (CP-9(7))

Застосовано подвійну авторизацію для видалення або знищення <CP-09(07)_ODP резервної інформації>.

No: 1
Name: cp_9_7_odp
Type: string
Default: nil

визначено резервну інформацію, для якої необхідно застосувати подвійну авторизацію з метою видалення або знищення;

No: 2
Name: cp_9_7_01

Type: string
Default: nil

застосовано подвійну авторизацію для видалення або знищення <CP-09(07)_ODP резервної інформації>.

6.9.7. КРИПТОГРАФІЧНИЙ ЗАХИСТ (CP-9(8))

Реалізовано криптографічні механізми для запобігання несанкціонованому розкриттю та зміні <CP-09(08)_ODP резервної інформації>.

No: 1
Name: cp_9_8_odp
Type: string
Default: nil

визначено резервні копії інформації для захисту від несанкціонованого розкриття та змін;

No: 2
Name: cp_9_8_01
Type: string
Default: nil

реалізовано криптографічні механізми для запобігання несанкціонованому розкриттю та зміні <CP-09(08)_ODP резервної інформації>.

6.10. ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ (CP-10)

Відновлення системи до відомого стану забезпечується протягом.

No: 1
Name: cp_10_odp_1
Type: string
Default: nil

визначено період часу для відновлення, часу та цілям відновлення системи;

No: 2
Name: cp_10_odp_2
Type: string
Default: nil

визначено період часу для відтворення, часу та цілям відновлення системи;

No: 3
Name: cp_10_1
Type: string
Default: nil

відновлення системи до відомого стану забезпечується протягом

No: 4
Name: cp_10_2
Type: string
Default: nil

відтворення системи до відомого стану забезпечується протягом

6.10.1. ВІДНОВЛЕННЯ ТРАНЗАКЦІЙ (CP-10(2))

Реалізовано відновлення транзакцій для систем, що базуються на транзакціях.

No: 1
Name: cp_10_2_01
Type: string
Default: nil

реалізовано відновлення транзакцій для систем, що базуються на транзакціях

6.10.2. ВІДНОВЛЕННЯ В МЕЖАХ ЧАСОВОГО ПЕРІОДУ (CP-10(4))

Забезпечено можливість відновлення компонентів системи протягом <CP-10(04)_ODP період часу відновлення> з інформації управління конфігурацією та захищеною цілісністю, яка описує відомий робочий стан компонентів.

No: 1
Name: cp_10_4_odp
Type: string
Default: nil

визначено період часу відновлення, протягом якого компоненти системи відновлюються до відомого, робочого стану;

No: 2
Name: cp_10_4_01
Type: string
Default: nil

забезпечено можливість відновлення компонентів системи протягом <CP-10(04)_ODP період часу відновлення> з інформації управління конфігурацією та захищеною цілісністю, яка описує відомий робочий стан компонентів.

6.10.3. ЗДАТНІСТЬ ВІДМОВОСТІЙКОСТІ (CP-10(5)) [Вилучено]

[Вилучено: Включено до SI-13]

Немає параметрів для цього контролю.

6.11. АЛЬТЕРНАТИВНІ ПРОТОКОЛИ ЗВ'ЯЗКУ (CP-11)

Організація забезпечує можливість застосування <CP-11_ODP альтернативних протоколів зв'язку > для підтримки збереження безперервності функціонування.

No: 1
Name: cp_11_odp
Type: string
Default: nil

організація визначає альтернативні протоколи зв'язку для підтримки збереження безперервності функціонування

No: 2
Name: cp_11_01
Type: string
Default: nil

організація забезпечує можливість застосування <CP-11_ODP альтернативних протоколів зв'язку > для підтримки збереження безперервності функціонування

6.12. БЕЗПЕЧНИЙ РЕЖИМ (CP-12)

При виявлені <CP-12_ODP[01] умови>, вводиться безпечний режим роботи з <CP-12_ODP[02] обмеженням>.

No: 1
Name: cp_12_odp_1
Type: string
Default: nil

визначено умови, за яких організація вводить безпечний режим роботи;

No: 2
Name: cp_12_odp_2
Type: string
Default: nil

визначено обмеження в безпечному режимі роботи;

No: 3
Name: cp_12_01
Type: string
Default: nil

при виявлені <CP-12_ODP[01] умови>, вводиться безпечний режим роботи з <CP-12_ODP[02] обмеженням>.

6.13. АЛЬТЕРНАТИВНІ МЕХАНІЗМИ БЕЗПЕКИ (CP-13)

<CP-13_ODP[01] альтернативні або додаткові механізми безпеки> використовуються для реалізації <CP-13_ODP[02] функцій безпеки> , коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані.

No: 1
Name: cp_13_odp_1
Type: string
Default: nil

визначені альтернативні або додаткові механізми безпеки;

No: 2
Name: cp_13_odp_2

Type: string
Default: nil

визначені функції безпеки;

No: 3
Name: cp_13_01
Type: string
Default: nil

<CP-13_ODP[01] альтернативні або додаткові механізми безпеки> використовуються для реалізації <CP-13_ODP[02] функцій безпеки> , коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані.

7. IA

Клас заходів захисту IA — ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

Опис Цей клас відповідає за однозначне розпізнавання користувачів або пристроїв та підтвердження їхньої справжності перед наданням доступу до системи.

Перелік заходів захисту Політика та процедури ідентифікації та автентифікації (IA-1); ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) (IA-2); Багатофакторна автентифікація привілейованих облікових записів (IA-2(1)); Багатофакторна автентифікація непривілейованих (IA-2(2)); Локальний доступ до привілейованих облікових записів (IA-2(3)) [Вилучено]; Локальний доступ до непривілейованих облікових записів (IA-2(4)) [Вилучено]; Індивідуальна автентифікація з груповою автентифікацією (IA-2(5)); Мережевий доступ до непривілейованих облікових записів – окремий пристрій (IA-2(7)) [Вилучено]; Доступ до облікових записів – стійкість до відтворення (IA-2(8)); Доступ до непривілейованих облікових записів – стійкість до відтворення (IA-2(9)) [Вилучено]; Єдина точка входу (IA-2(10)); Віддалений доступ - окремий пристрій (IA-2(11)) [Вилучено]; ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12)); Автентифікація по зовнішньому каналу (IA-2(13)); Ідентифікація та автентифікація пристроїв (IA-3); Криптографічна двобічна автентифікація (IA-3(1)); Криптографічний двобічна мережа автентифікація [виключено: включено до ia-03(01)]. (IA-3(2)); Динамічний розподіл адреси (IA-3(3)); Ідентифікація та автентифікація пристрою виконується на основі атестації за допомогою (IA-3(4)); Управління ідентифікацією (IA-4); Заборона використання ідентифікаторів облікових записів таки самих, як й публічні ідентифікатори (IA-4(1)); Авторизація супервайзера [виключено: включено до ia-12(01)]. (IA-4(2)); Множинні форми сертифікації (IA-4(3)); Ідентифікація статусу користувача (IA-4(4)); Динамічне управління (IA-4(5)); Кросорганізаційне управління (IA-4(6)); Особиста реєстрація [виключено: включено до ia-12(04)]. (IA-4(7)); Попарні псевдонімні ідентифікатори (IA-4(8)); Попарні псевдонімні ідентифікатори (IA-4(9)); Управління автентифікатором (IA-5); Автентифікація на основі пароля (IA-5(1)); Автентифікація на основі відкритого ключа (IA-5(2)); Особиста або довірча автентифікація зовнішньої сторони [виключено: включено до ia-12(04)]. (IA-5(3)); Автоматизована підтримка для визначення міцності пароля [виключено: включено до ia-05(01)]. (IA-5(4)); Зміна автентифікаторів до доставки (IA-5(5)); Захист автентифікаторів (IA-5(6)); Відсутність вбудованих незашифрованих статичних автентифікаторів (IA-5(7)); Багатосистемні облікові записи (IA-5(8)); Управління об'єднанням автентифікаторів (IA-5(9)); Динамічне зв'язування мандатів (IA-5(10)); Автентифікація на основі апаратних токенів (IA-5(11)) [Вилучено]; Ефективність біометричної автентифікації (IA-5(12)); Закінчення терміну шування автентифікаторів (IA-5(13)); Управління змістом довірчих сховищ інфраструктури відкритих ключів (IA-5(14)); Продукти та послуги, затверджені уповноваженим органом (IA-5(15)); Передача особистої або довірчої автентифікації зовнішньої сторони (IA-5(16)); Автоматизовані засоби виявлення атак із використанням біометричних автентифікаторів (IA-5(17)); Менеджер паролів (IA-5(18));

ПРИХОВУВАННЯ ЗВОРОТНОГО ЗВ'ЯЗКУ АВТЕНТИФІКАТОРА; Автентифікація криптографічного модуля (IA-7); ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) (IA-8); Використання затверджених продуктів (IA-8(3)) [Вилучено]; ВИЗНАННЯ ПОСВІДЧЕНЬ ОСОБИ (PIV-I) (IA-8(5)); Розмежування (IA-8(6)); Послуги ідентифікації та автентифікації (IA-9); Обмін інфо- (IA-9(1)); Передача рішень [виключено: перенесено до ia-09] (IA-9(2)); Адаптивна автентифікація (IA-10); Повторна автентифікація (IA-11); ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) (IA-12); Авторизація супервайзера (IA-12(1)); Посвідчення особи (IA-12(2)); Очна перевірка та верифікація (IA-12(4)); Підтвердження адреси (IA-12(5)); Прийняття ідентифікацій схвалених третьою стороною (IA-12(6)).

7.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ (IA-1)

Розроблено та задокументовано політику ідентифікації та автентифікації;.

No: 1
Name: ia_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, на які поширюється політика ідентифікації та автентифікації;

No: 2
Name: ia_1_odp_2
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури ідентифікації та автентифікації;

No: 3
Name: ia_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесів; рівень системи};

No: 4
Name: ia_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка управляє політикою та процедурами ідентифікації та автентифікації;

No: 5
Name: ia_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика ідентифікації та автентифікації;

No: 6
Name: ia_1_odp_6
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення поточної політики ідентифікації та автентифікації;

No: 7
Name: ia_1_odp_7
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються поточні процедури ідентифікації та автентифікації;

No: 8
Name: ia_1_odp_8
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення процедур ідентифікації та автентифікації;

No: 9
Name: ia_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику ідентифікації та автентифікації;

No: 10
Name: ia_1_a_2
Type: string
Default: nil

політика ідентифікації та автентифікації поширюється на <IA01_ODP[01] персонал або ролі>;

No: 11
Name: ia_1_a_3
Type: string
Default: nil

розроблені та задокументовані процедури ідентифікації та автентифікації, що сприяють впровадженню політики ідентифікації та автентифікації, а також відповідні заходи ідентифікації та перевірки автентичності;

No: 12
Name: ia_1_a_4
Type: string
Default: nil

процедури ідентифікації та автентифікації поширюються на <IA01_ODP[02] персонал або ролі>;

No: 13
Name: ia_1_a_1_a_1
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить мету;

No: 14
Name: ia_1_a_1_a_2
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить сферу застосування;

No: 15
Name: ia_1_a_1_a_3
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить ролі;

No: 16
Name: ia_1_a_1_a_4
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить обов'язки;

No: 17
Name: ia_1_a_1_a_5
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить відповідальність керівництва;

No: 18
Name: ia_1_a_1_a_6
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить координацію між підрозділами організації;

No: 19
Name: ia_1_a_1_a_7
Type: string
Default: nil

<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політики ідентифікації та автентифікації містить систему контролю відповідності;

No: 20
Name: ia_1_a_1_b
Type: string
Default: nil

політика ідентифікації та автентифікації <IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинному законодавству, виконавчим розпорядженням, директивам, положенням, політиці, стандартам і керівним принципам;

No: 21
Name: ia_1_b
Type: string
Default: nil

<IA-01_ODP[04] посадова особа> призначається для управління політикою та процедурами ідентифікації та автентифікації;

No: 22
Name: ia_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика ідентифікації та

No: 23
Name: ia_1_c_1_2
Type: string
Default: nil

переглядається та оновлюється поточна політика ідентифікації та

No: 24
Name: ia_1_c_2_1
Type: string
Default: nil

переглядаються та оновлю ються поточні процедури ідентифікації

No: 25
Name: ia_1_c_2_2
Type: string
Default: nil

переглядаються та оновлю ються поточні процедури ідентифікації

7.2. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) (IA-2)

Користувачі унікально ідентифіковані та автентифіковані;.

No: 1
Name: ia_2_1
Type: string
Default: nil

користувачі унікально ідентифіковані та автентифіковані;

No: 2
Name: ia_2_2
Type: string
Default: nil

процеси що діють від імені користувачів унікально ідентифіковані та автентифіковані;

7.2.1. БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ (IA-2(1))

Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів.

No: 1
Name: ia_2_1_01
Type: string
Default: nil

реалізувано багатофакторну автентифікацію для доступу до привілейованих облікових записів

7.2.2. БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ НЕПРИВІЛЕЙОВАНИХ (IA-2(2))

Реалізувати багатофакторну автентифікацію для доступу до непривілейованих облікових записів.

No: 1
Name: ia_2_2_01

Type: string
Default: nil

реалізовано багатофакторну автентифікацію для доступу до непривілейованих облікових записів

7.2.3. ЛОКАЛЬНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ (IA-2(3)) [Вилучено]

[Вилучено: Включено до IA-02(01)]

Немає параметрів для цього контролю.

7.2.4. ЛОКАЛЬНИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ (IA-2(4)) [Вилучено]

[Вилучено: Включено до IA-02(02)]

Немає параметрів для цього контролю.

7.2.5. ІНДИВІДУАЛЬНА АВТЕНТИФІКАЦІЯ З ГРУПОВОЮ АВТЕНТИФІКАЦІЄЮ (IA-2(5))

Користувачі повинні пройти індивідуальну автентифікацію перед наданням доступу до спільних облікових записів або ресурсів, якщо використовуються спільні облікові записи або автентифікатори.

No: 1
Name: ia_2_5_01
Type: string
Default: nil

користувачі повинні пройти індивідуальну автентифікацію перед наданням доступу до спільних облікових записів або ресурсів, якщо використовуються спільні облікові записи або автентифікатори.

7.2.6. МЕРЕЖЕВИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – ОКРЕМИЙ ПРИСТРІЙ (IA-2(7)) [Вилучено]

[Вилучено: Включено до IA-02(01)]

Немає параметрів для цього контролю.

7.2.7. ДОСТУП ДО ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ (IA-2(8))

Реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до <IA-02(08)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

No: 1
Name: ia_2_8_odp
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {привілейовані облікові записи; непривілейовані облікові записи};

No: 2
Name: ia_2_8_01
Type: string
Default: nil

реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до <IA-02(08)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

7.2.8. ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ (IA-2(9)) [Вилучено]

[Вилучено: Включено до IA-02(08)]

Немає параметрів для цього контролю.

7.2.9. ЄДИНА ТОЧКА ВХОДУ (IA-2(10))

Забезпечено можливість єдиного входу для <IA-02(10)_ODP облікових записів і послуг системи>.

No: 1
Name: ia_2_10_odp
Type: string
Default: nil

визначено облікові записи та послуги системи, для яких має бути забезпечена можливість єдиного входу;

No: 2
Name: ia_2_10_01
Type: string
Default: nil

забезпечено можливість єдиного входу для <IA-02(10)_ODP облікових записів і послуг системи>.

7.2.10. ВІДДАЛЕНИЙ ДОСТУП - ОКРЕМИЙ ПРИСТРІЙ (IA-2(11)) [Вилучено]

[Вилучено: Включено до IA-02(06)]

Немає параметрів для цього контролю.

7.2.11. ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12))

Забезпечити прийняття повноважень для верифікації особистої інформації (PIV CREDENTIALS).

No: 1
Name: ia_2_12_01
Type: string
Default: nil

приймаються та електронним шляхом підтверджуються повноваження облікових даних особистої ідентифікації.

7.2.12. АВТЕНТИФІКАЦІЯ ПО ЗОВНІШНЬОМУ КАНАЛУ (IA-2(13))

<IA-02(13)_ODP[01] механізми зовнішньої автентифікації> застосовано за <IA-02(13)_ODP[02] умов>.

No: 1
Name: ia_2_13_odp_1
Type: string
Default: nil

визначено механізми зовнішньої автентифікації;

No: 2
Name: ia_2_13_odp_2
Type: string
Default: nil

визначено умови, за яких має бути реалізована зовнішня автентифікація;

No: 3
Name: ia_2_13_01
Type: string
Default: nil

<IA-02(13)_ODP[01] механізми зовнішньої автентифікації> застосовано за <IA-02(13)_ODP[02] умов>.

7.3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ (IA-3)

<IA-03_ODP[01] пристрої та/або типи пристроїв> унікально ідентифіковані та автентифіковано перед встановленням підключення.

No: 1
Name: ia_3_odp_1
Type: string
Default: nil

визначені пристрої та/або типи пристроїв, які повинні бути унікально ідентифіковані та автентифіковані перед установкою підключення;

No: 2
Name: ia_3_odp_2
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {локальний; віддалений; мережевий};

No: 3
Name: ia_3_01
Type: string
Default: nil

<IA-03_ODP[01] пристрої та/або типи пристроїв> унікально ідентифіковані та автентифіковано перед встановленням підключення

7.3.1. КРИПТОГРАФІЧНА ДВОБІЧНА АВТЕНТИФІКАЦІЯ (IA-3(1))

<IA-03(01)_ODP[01] пристрої та/або типи пристроїв> автентифікуються перед встановленням підключення <IA03(01)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах.

No: 1
Name: ia_3_1_odp_1
Type: string
Default: nil

визначено пристрої та/або типи пристроїв, які потребують використання двобічної автентифікації яка заснована на криптографічних механізмах для автентифікації перед встановленням підключення;

No: 2
Name: ia_3_1_odp_2
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {локальний; віддалений; мережевий};

No: 3
Name: ia_3_1_01
Type: string
Default: nil

<IA-03(01)_ODP[01] пристрої та/або типи пристроїв> автентифікуються перед встановленням підключення <IA03(01)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах.

7.3.2. КРИПТОГРАФІЧНИЙ ДВОБІЧНА МЕРЕЖА АВТЕНТИФІКАЦІЯ [Виключено: включено до IA-03(01)]. (IA-3(2))

Криптографічний двобічна мережа автентифікація [виключено: включено до ia-03(01)]. (ia-3(2)).

Немає параметрів для цього контролю.

7.3.3. ДИНАМІЧНИЙ РОЗПОДІЛ АДРЕСИ (IA-3(3))

Інформація про оренду динамічного розподілу адрес, що призначається пристроям з динамічним розподілом адрес,.

No: 1
Name: ia_3_3_odp_1
Type: string
Default: nil

визначено інформацію про оренду, яку буде використано для стандартизації динамічного розподілу адрес для пристроїв;

No: 2
Name: ia_3_3_odp_2
Type: string
Default: nil

визначено тривалість оренди, яка буде використовуватися для стандартизації динамічного виділення адрес для пристроїв;

No: 3
Name: ia_3_3_a_1
Type: string
Default: nil

інформація про оренду динамічного розподілу адрес, що призначається пристроям з динамічним розподілом адрес,

No: 4
Name: ia_3_3_a_2
Type: string
Default: nil

тривалість оренди динамічного виділення адреси, що призначається пристроям з динамічним виділенням адреси, стандартизовано відповідно до <IA-03(03)_ODP[02] тривалість оренди>;

No: 5
Name: ia_3_3_b
Type: string
Default: nil

інформація про оренду перевіряється, коли її призначено пристрою.

7.3.4. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЮ ВИКОНУЄТЬСЯ НА ОСНОВІ АТЕСТАЦІЇ ЗА ДОПОМОГОЮ (IA-3(4))

Ідентифікація та автентифікація пристрою виконується на основі атестації за допомогою <IA-03(04)_ODP процес управління конфігурацією>.

No: 1
Name: ia_3_4_odp

Type: string
Default: nil

визначено процес управління конфігурацією, який буде використовуватися для ідентифікації та автентифікації пристроїв на основі атестації;

No: 2
Name: ia_3_4_01
Type: string
Default: nil

ідентифікація та автентифікація пристрою виконується на основі атестації за допомогою <IA-03(04)_ODP процес управління конфігурацією>.

7.4. УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ (IA-4)

Управління ідентифікаторами здійснюється шляхом отримання дозволу від <IA-04_ODP[01] персоналу або ролей> на призначення ідентифікатора особі, групі, ролі або пристрою;.

No: 1
Name: ia_4_odp_1
Type: string
Default: nil

визначено персонал або ролі, від яких необхідно отримати дозвіл на призначення ідентифікатора;

No: 2
Name: ia_4_odp_2
Type: string
Default: nil

визначено період часу для запобігання повторному використанню ідентифікаторів;

No: 3
Name: ia_4_a
Type: string
Default: nil

управління ідентифікаторами здійснюється шляхом отримання дозволу від <IA-04_ODP[01] персоналу або ролей> на призначення ідентифікатора особі, групі, ролі або пристрою;

No: 4
Name: ia_4_b
Type: string
Default: nil

управління ідентифікаторами здійснюється шляхом вибору ідентифікатора, який ідентифікує окрему особу, групу, ролі або пристрій;

No: 5
Name: ia_4_c
Type: string
Default: nil

управління ідентифікаторами здійснюється шляхом призначення ідентифікатора особі, групі, ролі або пристрою;

No: 6
Name: ia_4_d
Type: string
Default: nil

ідентифікатори управляються шляхом запобігання повторному використанню ідентифікаторів впродовж <IA-04_ODP[02] період часу>.

7.4.1. ЗАБОРОНА ВИКОРИСТАННЯ ІДЕНТИФІКАТОРІВ ОБЛІКОВИХ ЗАПИСІВ ТАКИ САМИХ, ЯК Й ПУБЛІЧНІ ІДЕНТИФІКАТОРИ (IA-4(1))

Заборонено використання ідентифікаторів облікових записів системи, які збігаються із загальнодоступними ідентифікаторами для індивідуальних облікових записів.

No: 1
Name: ia_4_1_01
Type: string
Default: nil

заборонено використання ідентифікаторів облікових записів системи, які збігаються із загальнодоступними ідентифікаторами для індивідуальних облікових записів.

7.4.2. АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА [Виключено: Включено до IA-12(01)]. (IA-4(2))

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА [Виключено: Включено до IA-12(01)].

No: 1
Name: ia_4_2_01
Type: string
Default: nil

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА [Виключено: Включено до IA-12(01)]

7.4.3. МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ (IA-4(3))

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ [Виключено: Включено до IA-12(02)].

No: 1
Name: ia_4_3_01
Type: string
Default: nil

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ [Виключено: Включено до IA-12(02)]

7.4.4. ІДЕНТИФІКАЦІЯ СТАТУСУ КОРИСТУВАЧА (IA-4(4))

Управління індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума <IA-04(04)_ODP ознака>, що ідентифікує індивідуальний статус.

No: 1
Name: ia_4_4_odp
Type: string
Default: nil

визначено ознаку, що ідентифікує індивідуальний статус;

No: 2
Name: ia_4_4_01
Type: string
Default: nil

управління індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума <IA-04(04)_ODP ознака>, що ідентифікує індивідуальний статус.

7.4.5. ДИНАМІЧНЕ УПРАВЛІННЯ (IA-4(5))

Індивідуальні ідентифікатори динамічно управляються відповідно до <IA-04(05)_ODP політика динамічних ідентифікаторів>.

No: 1
Name: ia_4_5_odp
Type: string
Default: nil

визначено політику динамічних ідентифікаторів для управління індивідуальними ідентифікаторами;

No: 2
Name: ia_4_5_01
Type: string
Default: nil

індивідуальні ідентифікатори динамічно управляються відповідно до <IA-04(05)_ODP політика динамічних ідентифікаторів>.

7.4.6. КРОС-ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ (IA-4(6))

Здійснюється координація з <IA-04(06)_ODP зовнішні організації> для крос-організаційного управління ідентифікаторами.

No: 1
Name: ia_4_6_odp
Type: string
Default: nil

визначено зовнішні організації з якими необхідно здійснювати координацію для крос-організаційного управління ідентифікаторами;

No: 2
Name: ia_4_6_01
Type: string
Default: nil

здійснюється координація з <IA-04(06)_ODP зовнішні організації> для крос-організаційного управління ідентифікаторами.

7.4.7. ОСОБИСТА РЕЄСТРАЦІЯ [Виключено: Включено до IA-12(04)]. (IA-4(7))

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОСОБИСТА РЕЄСТРАЦІЯ [Виключено: Включено до IA-12(04)].

No: 1
Name: ia_4_7_01
Type: list
Default: ["admin", "security_officer"]

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОСОБИСТА РЕЄСТРАЦІЯ [Виключено: Включено до IA-12(04)]

7.4.8. ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ (IA-4(8))

Створено попарні псевдонімні ідентифікатори.

No: 1
Name: ia_4_8_01
Type: string
Default: nil

створено попарні псевдонімні ідентифікатори.

7.4.9. ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ (IA-4(9))

Атрибути для кожної унікально ідентифікованої особи, пристрою або служби зберігаються у <IA-04(09)_ODP захищеному центральному сховищі>.

No: 1
Name: ia_4_9_odp
Type: string
Default: nil

визначено захищене центральне сховище, яке використовується для зберігання атрибутів для кожної унікально ідентифікованої особи, пристрою або служби;

No: 2
Name: ia_4_9_01
Type: string
Default: nil

атрибути для кожної унікально ідентифікованої особи, пристрою або служби зберігаються у <IA-04(09)_ODP захищеному центральному сховищі>.

7.5. УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ (IA-5)

Управління системними автентифікаторами здійснюється шляхом перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор;.

No: 1
Name: ia_5_odp_1
Type: string
Default: nil

визначено період часу для зміни або оновлення автентифікаторів за типом автентифікатора;

No: 2
Name: ia_5_odp_2
Type: string
Default: nil

визначено події, які викликають зміну або оновлення автентифікаторів;

No: 3
Name: ia_5_a
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор;

No: 4
Name: ia_5_b
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом створення вихідного вмісту автентифікатора для будь -яких автентифікаторів, виданих організацією;

No: 5
Name: ia_5_c
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом забезпечення того, щоб автентифікатори мали достатню стійкість механізму для їх використання за призначенням;

No: 6
Name: ia_5_d
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом створення та реалізація адміністративних процедур для первинного розповсюдження автентифікаторів, для втрачених/ск омпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів;

No: 7
Name: ia_5_e
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом зміни типових автентифікаторів перед першим використанням;

No: 8
Name: ia_5_f
Type: string
Default: nil

управління системними ав тентифікаторами здійснюється шляхом

No: 9
Name: ia_5_g

Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом захисту вмісту автентифікатора від несанкціонованого розкриття та модифікацій;

No: 10
Name: ia_5_h
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом вимоги до осіб, які використовують пристрої, використовувати спеціальні заходи безпеки для захисту автентифікаторів;

No: 11
Name: ia_5_i
Type: string
Default: nil

управління системними автентифікаторами здійснюється шляхом вимоги змінювати автентифікатори для облікових записів груп/ролей при зміні членства в цих облікових записах.

7.5.1. АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПАРОЛЯ (IA-5(1))

Для автентифікації на основі паролів підтримується та оновлюється список часто використовуваних, очікуваних або також коли є підозра, що паролі організації були скомпрометовані прямо чи опосередковано;.

No: 1
Name: ia_5_1_odp_1
Type: string
Default: nil

визначено частоту оновлення списку часто використовуваних, очікуваних або скомпрометованих паролів;

No: 2
Name: ia_5_1_odp_2
Type: string
Default: nil

визначено склад та правила складності автентифікатора;

No: 3
Name: ia_5_1_a
Type: string
Default: nil

для автентифікації на основі паролів підтримується та оновлюється список часто використовуваних, очікуваних або також коли є підозра, що паролі організації були скомпрометовані прямо чи опосередковано;

No: 4
Name: ia_5_1_b
Type: string
Default: nil

для автентифікації на основі паролів, коли паролі створюються або оновлюються користувачами, паролі перевіряються на відсутність у списку загальновживаних, очікуваних або скомпрометованих паролів в IA-05(01)(a);

No: 5
Name: ia_5_1_c

Type: string
Default: nil

для автентифікації на основі паролів, паролі передаються лише криптографічно захищеними каналами;

No: 6
Name: ia_5_1_d
Type: string
Default: nil

для автентифікації на основі паролів паролі зберігаються за допомогою затвердженого алгоритму гешування, переважно використовуючи ключову геш-функцію;

No: 7
Name: ia_5_1_e
Type: string
Default: nil

для автентифікації на основі пароля після відновлення облікового запису потрібно негайно вибрати новий пароль;

No: 8
Name: ia_5_1_f
Type: string
Default: nil

для автентифікації на основі пароля дозволяється вибір користувачем довгих паролів і фраз, що включають пробіли та всі друковані символи;

No: 9
Name: ia_5_1_g
Type: string
Default: nil

для автентифікації на основі пароля використовуються автоматизовані інструменти, які допомагають користувачеві у виборі надійних автентифікаторів паролів;

No: 10
Name: ia_5_1_h
Type: string
Default: nil

для автентифікації на основі пароля застосовуються <IA05(01)_ODP[02] склад та правила складності>.

7.5.2. АВТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА (IA-5(2))

Реалізувати автентифікацію на основі відкритого ключа.

Немає параметрів для цього контролю.

7.5.3. ОСОБИСТА АБО ДОВІРЧА АВТЕНТИФІКАЦІЯ ЗОВНІШНЬОЇ СТОРОНИ [Виключено: Включено до IA-12(04)]. (IA-5(3))

УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ОСОБИСТА АБО ДОВІРЧА АВТЕНТИФІКАЦІЯ ЗОВНІШНЬОЇ СТОРОНИ [Виключено: Включено до IA-12(04)].

No: 1
Name: ia_5_3_01
Type: list
Default: ["admin", "security_officer"]

УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ОСОБИСТА АБО ДОВІРЧА АВТЕНТИФІКАЦІЯ ЗОВНІШНЬОЇ СТОРОНИ [Виключено: Включено до IA-12(04)]

7.5.4. АВТОМАТИЗОВАНА ПІДТРИМКА ДЛЯ ВИЗНАЧЕННЯ МІЦНОСТІ ПАРОЛЯ [Виключено: Включено до IA-05(01)]. (IA-5(4))

УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНА ПІДТРИМКА ДЛЯ ВИЗНАЧЕННЯ МІЦНОСТІ ПАРОЛЯ [Виключено: Включено до IA-05(01)].

No: 1
Name: ia_5_4_01
Type: string
Default: nil

УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНА ПІДТРИМКА ДЛЯ ВИЗНАЧЕННЯ МІЦНОСТІ ПАРОЛЯ [Виключено: Включено до IA-05(01)]

7.5.5. ЗМІНА АВТЕНТИФІКАТОРІВ ДО ДОСТАВКИ (IA-5(5))

Розробники та інсталятори компонентів системи зобов'язані надавати унікальні автентифікатори або змінювати автентифікатори за замовчуванням до доставки та встановлення.

No: 1
Name: ia_5_5_01
Type: string
Default: nil

розробники та інсталятори компонентів системи зобов'язані надавати унікальні автентифікатори або змінювати автентифікатори за замовчуванням до доставки та встановлення.

7.5.6. ЗАХИСТ АВТЕНТИФІКАТОРІВ (IA-5(6))

Автентифікатори захищені відповідно до категорії безпеки інформації, до якої дозволяє доступ використання автентифікатора.

No: 1
Name: ia_5_6_01
Type: string
Default: nil

автентифікатори захищені відповідно до категорії безпеки інформації, до якої дозволяє доступ використання автентифікатора.

7.5.7. ВІДСУТНІСТЬ ВБУДОВАНИХ НЕЗАШИФРОВАНИХ СТАТИЧНИХ АВТЕНТИФІКАТОРІВ (IA-5(7))

Незашифровані статичні автентифікатори не вбудовуються в застосунки або сценарії доступу та не збережені на функціональній клавіші.

No: 1
Name: ia_5_7_01
Type: string
Default: nil

незашифровані статичні автентифікатори не вбудовуються в застосунки або сценарії доступу та не збережені на функціональній клавіші.

7.5.8. БАГАТОСИСТЕМНІ ОБЛІКОВІ ЗАПИСИ (IA-5(8))

<IA-05(08)_ODP заходи захисту> впроваджені для управління ризиком компрометації через наявність облікових записів у декількох системах.

No: 1
Name: ia_5_8_odp
Type: string
Default: nil

визначено заходи захисту, впроваджені для управління ризиком компрометації через те, що користувачі мають облікові записи в декількох системах.

No: 2
Name: ia_5_8_01
Type: string
Default: nil

<IA-05(08)_ODP заходи захисту> впроваджені для управління ризиком компрометації через наявність облікових записів у декількох системах.

7.5.9. УПРАВЛІННЯ ОБ'ЄДНАННЯМ АВТЕНТИФІКАТОРІВ (IA-5(9))

<IA-05(09)_ODP зовнішні організації> використовуються для об'єднання автентифікаторів.

No: 1
Name: ia_5_9_odp
Type: string
Default: nil

визначено зовнішні організації, які будуть використовуватися для об'єднання автентифікаторів;

No: 2
Name: ia_5_9_01
Type: string
Default: nil

<IA-05(09)_ODP зовнішні організації> використовуються для об'єднання автентифікаторів.

7.5.10. ДИНАМІЧНЕ ЗВ'ЯЗУВАННЯ МАНДАТІВ (IA-5(10))

Ідентифікатори та автентифікатори динамічно зв'язуються за допомогою <IA-05(10)_ODP правила для динамічного зв'язування >.

No: 1
Name: ia_5_10_odp
Type: string
Default: nil

визначено правила для динамічного зв'язування ідентифікаторів та автентифікаторів;

No: 2
Name: ia_5_10_01
Type: string
Default: nil

ідентифікатори та автентифікатори динамічно зв'язуються за допомогою <IA-05(10)_ODP правила для динамічного зв'язування >.

7.5.11. АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ (IA-5(11)) [Вилучено]

[Вилучено: Включено до IA-02(01), IA-02(02)]

Немає параметрів для цього контролю.

7.5.12. ЕФЕКТИВНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ (IA-5(12))

Забезпечити ефективність біометричної автентифікації.

No: 1
Name: ia_5_12_odp
Type: string
Default: nil

визначено вимоги до якості біометрії;

No: 2
Name: ia_5_12_01
Type: string
Default: nil

для біометричної автентифікації використовувати механізми, які задовольняють <IA-05(12)_ODP вимоги>.

7.5.13. ЗАКІНЧЕННЯ ТЕРМІНУ ШУВАННЯ АВТЕНТИФІКАТОРІВ (IA-5(13))

Забороняється використання кешованих автентифікаторів після <IA-05(13)_ODP періоду часу>.

No: 1
Name: ia_5_13_odp
Type: string
Default: nil

визначено періоду часу після якого необхідно заборонити використання кешованих автентифікаторів

No: 2
Name: ia_5_13_01
Type: string
Default: nil

забороняється використання кешованих автентифікаторів після <IA-05(13)_ODP періоду часу>.

7.5.14. УПРАВЛІННЯ ЗМІСТОМ ДОВІРЧИХ СХОВИЩ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ (IA-5(14))

Для автентифікації на основі інфраструктури з відкритим ключем використовується загальноорганізаційна методологія управління вмістом довірених сховищ інфраструктури відкритого ключа, встановлених на всіх платформах, включно з мережами, операційними системами, браузерами та застосунками.

No: 1
Name: ia_5_14_01
Type: string
Default: nil

для автентифікації на основі інфраструктури з відкритим ключем використовується загальноорганізаційна методологія управління вмістом довірених сховищ інфраструктури відкритого ключа, встановлених на всіх платформах, включно з мережами, операційними системами, браузерами та застосунками.

7.5.15. ПРОДУКТИ ТА ПОСЛУГИ, ЗАТВЕРДЖЕНІ УПОВНОВАЖЕНИМ ОРГАНОМ (IA-5(15))

Використовувати продукти та послуги автентифікації, затверджені уповноваженим органом.

No: 1
Name: ia_5_15_01
Type: string
Default: nil

використовуються лише схвалені та затверджені уповноваженим органом продукти та послуги.

7.5.16. ПЕРЕДАЧА ОСОБИСТОЇ АБО ДОВІРЧОЇ АВТЕНТИФІКАЦІЇ ЗОВНІШНЬОЇ СТОРОНИ (IA-5(16))

Передача <IA-05(16)_ODP[01] типів та/або конкретних.

No: 1
Name: ia_5_16_odp_1
Type: string
Default: nil

визначено типи та/або конкретні автентифікатори, які будуть передаватися;

No: 2
Name: ia_5_16_odp_2
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {особисто; довіреною зовнішньою стороною};

No: 3
Name: ia_5_16_odp_3
Type: string
Default: nil

визначено зареєстрований орган, який приймає автентифікатори;

No: 4
Name: ia_5_16_odp_4
Type: string
Default: nil

визначено персонал або ролі, які уповноважують передачу автентифікаторів;

No: 5
Name: ia_5_16_01
Type: string
Default: nil

передача <IA-05(16)_ODP[01] типів та/або конкретних

7.5.17. АВТОМАТИЗОВАНІ ЗАСОБИ ВИЯВЛЕННЯ АТАК ІЗ ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ АВТЕНТИФІКАТОРІВ (IA-5(17))

Використовувати автоматизовані засоби виявлення атак із використанням біометричних автентифікаторів.

No: 1
Name: ia_5_17_01
Type: string
Default: nil

використовуються механізми виявлення атак із використанням штучно виготовлених артефактів для біометричних автентифікаторів.

7.5.18. МЕНЕДЖЕР ПАРОЛІВ (IA-5(18))

<IA-05(18)_ODP[01] менеджери паролів> використовуються для створення та керування паролями;.

No: 1
Name: ia_5_18_odp_1
Type: string
Default: nil

визначено менеджери паролів, які використовуються для створення та керування паролями;

No: 2
Name: ia_5_18_odp_2

Type: string
Default: nil

визначено елементи керування для захисту паролів;

No: 3
Name: ia_5_18_a
Type: string
Default: nil

<IA-05(18)_ODP[01] менеджери паролів> використовуються для створення та керування паролями;

No: 4
Name: ia_5_18_b
Type: string
Default: nil

паролі зах ищені за допомогою <IA-05(18)_ODP[02] елементи керування >

7.6. ПРИХОВУВАННЯ ЗВОРОТНОГО ЗВ'ЯЗКУ АВТЕНТИФІКАТОРА

Забезпечино приховану зворотну передачу інформації автентифікації в про277 цесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.

No: 1
Name: ia_6_01
Type: string
Default: nil

забезпечино приховану зворотну передачу інформації автентифікації в про277 цесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.

7.7. АВТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНОГО МОДУЛЯ (IA-7)

Забезпечити сувору автентифікацію самого криптографічного модуля.

No: 1
Name: ia_7_01
Type: string
Default: nil

впроваджено механізми автентифікації в криптографічний модуль, який відповідає вимогам чинних законів, виконавчих розпоряджень, директив, політик, правил, стандартів та рекомендацій для такої автентифікації.

7.8. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) (IA-8)

Унікально ідентифіку ються та автентифікуються користувачі, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.

No: 1
Name: ia_8_01
Type: string
Default: nil

унікально ідентифіку ються та автентифікуються користувачі, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.

7.8.1. ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ (IA-8(3)) [Вилучено]

[Вилучено: Включено до IA-08(02)]

Немає параметрів для цього контролю.

7.8.2. ВИЗНАННЯ ПОСВІДЧЕНЬ ОСОБИ (PIV-I) (IA-8(5))

Приймаються облікові дані або дані PKI, які відповідають <IA-08(05)_ODP політика>;.

No: 1
Name: ia_8_5_odp
Type: string
Default: nil

визначено політику використання ативних облікових даних або облікових даних PKI;

No: 2
Name: ia_8_5_1
Type: string
Default: nil

приймаються облікові дані або дані PKI, які відповідають <IA-08(05)_ODP політика>;

No: 3
Name: ia_8_5_2
Type: string
Default: nil

підтверджуються облікові дані або дані PKI, які відповідають <IA-08(05)_ODP політика>.

7.8.3. РОЗМЕЖУВАННЯ (IA-8(6))

Впроваджено <IA-08(06)_ODP заходи> щоб розмежувати атрибути користува ча або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними сторонами.

No: 1
Name: ia_8_6_odp
Type: string
Default: nil

визначено заходи, щоб розмежувати атрибути користувача або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними сторонами;

No: 2
Name: ia_8_6_01
Type: string
Default: nil

впроваджено <IA-08(06)_ODP заходи> щоб розмежувати атрибути користува ча або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними сторонами.

7.9. ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ (IA-9)

<IA-09_ODP системні служби та застосунки> унікально ідентифікуються та автентифікуються перед встановленням зв'язку з пристроями, користувачами або іншими службами чи застосунками.

No: 1
Name: ia_9_odp
Type: string
Default: nil

визначено системні служби та застосунки, які мають бути унікально ідентифіковані та автентифіковані;

No: 2
Name: ia_9_01
Type: string
Default: nil

<IA-09_ODP системні служби та застосунки> унікально ідентифікуються та автентифікуються перед встановленням зв'язку з пристроями, користувачами або іншими службами чи застосунками.

7.9.1. ОБМІН ІНФО- (IA-9(1))

ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ОБМІН ІНФОРМАЦІЄЮ [Виключено: перенесено до IA-09].

No: 1
Name: ia_9_1_01
Type: string
Default: nil

ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ОБМІН ІНФОРМАЦІЄЮ [Виключено: перенесено до IA-09]

7.9.2. ПЕРЕДАЧА РІШЕНЬ [Виключено: перенесено до IA-09] (IA-9(2))

ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ПЕРЕДАЧА РІШЕНЬ [Виключено: перенесено до IA-09].

No: 1
Name: ia_9_2_01
Type: string
Default: nil

ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ПЕРЕДАЧА РІШЕНЬ [Виключено: перенесено до IA-09]

7.10. АДАПТИВНА АВТЕНТИФІКАЦІЯ (IA-10)

Особи, які отримують доступ до системи, повинні використовувати <IA-10_ODP[01] додаткові методи або механізми автентифікації> за певних <IA-10_ODP[02] обставин або ситуацій>.

No: 1
Name: ia_10_odp_1
Type: string
Default: nil

IA-10_ODP[01] визначені додаткові методи або механізми автентифікації, які будуть застосовуватися при доступі до системи за певних обставин або ситуацій;

No: 2
Name: ia_10_odp_2
Type: string
Default: nil

IA-10_ODP[02] визначені обставини або ситуації, які вимагають від осіб, що отримують доступ до системи, використання додаткових методів або механізмів автентифікації;

No: 3
Name: ia_10_01
Type: string
Default: nil

IA-10[01] особи, які отримують доступ до системи, повинні використовувати <IA-10_ODP[01] додаткові методи або механізми автентифікації> за певних <IA-10_ODP[02] обставин або ситуацій>.

7.11. ПОВТОРНА АВТЕНТИФІКАЦІЯ (IA-11)

Користувачі повинні повторно автентифікуватися, коли <IA-11_ODP обставини або ситуації>.

No: 1
Name: ia_11_odp
Type: string
Default: nil

визначено обставини або ситуації, що вимагають повторної автен283 тифікації;

No: 2
Name: ia_11_01
Type: string
Default: nil

користувачі повинні повторно автентифікуватися, коли <IA-11_ODP обставини або ситуації>.

7.12. ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) (IA-12)

Користувачі, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях, мають підтверджену ідентичність;.

No: 1
Name: ia_12_a
Type: string
Default: nil

користувачі, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях, мають підтверджену ідентичність;

No: 2
Name: ia_12_b
Type: string
Default: nil

встановлені ідентифікатори користувачів унікальні для особи;

No: 3
Name: ia_12_c_1
Type: string
Default: nil

збираються докази ідентичності особи;

No: 4
Name: ia_12_c_2
Type: string
Default: nil

затверджуються докази ідентичності особи;

No: 5
Name: ia_12_c_3
Type: string
Default: nil

перевіряються докази ідентичності особи;

7.12.1. АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА (IA-12(1))

Процес реєстрації для отримання облікового запису для логічного доступу включає авторизацію супервайзера.

No: 1
Name: ia_12_1_01
Type: string
Default: nil

процес реєстрації для отримання облікового запису для логічного доступу включає авторизацію супервайзера.

7.12.2. ПОСВІДЧЕННЯ ОСОБИ (IA-12(2))

Документи, що посвідчують особу пред'являються до реєстраційного органу.

No: 1
Name: ia_12_2_01
Type: string
Default: nil

документи, що посвідчують особу пред'являються до реєстраційного органу.

7.12.3. ОЧНА ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ (IA-12(4))

Підтвердження та перевірка посвідчення особи проводиться особисто в призначеному органі реєстрації.

No: 1
Name: ia_12_4_01
Type: string
Default: nil

підтвердження та перевірка посвідчення особи проводиться особисто в призначеному органі реєстрації.

7.12.4. ПІДТВЕРДЖЕННЯ АДРЕСИ (IA-12(5))

Підтвердження адреси (ia-12(5)).

No: 1
Name: ia_12_5_odp
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {реєстраційний код; повідомлення про перевірку}; доставляється через зовнішні канали для перевірки адреси (фізичної або цифрової) користувача.

7.12.5. ПРИЙНЯТТЯ ІДЕНТИФІКАЦІЙ СХВАЛЕНИХ ТРЕТЬОЮ СТОРОНОЮ (IA-12(6))

Приймаються зовнішньо підтверджені ідентифікатори <IA12(06)_ODP рівень гарантії ідентичності>.

No: 1
Name: ia_12_6_odp
Type: string
Default: nil

визначено рівень гарантії ідентичності для прийняття зовнішньо підтверджених ідентифікаторів;

No: 2
Name: ia_12_6_01
Type: string
Default: nil

приймаються зовнішньо підтверджені ідентифікатори <IA12(06)_ODP рівень гарантії ідентичності>.

8. IR

Клас заходів захисту IR — РЕАГУВАННЯ НА ІНЦИДЕНТИ

Опис Цей клас визначає процедури виявлення, аналізу, локалізації та усунення наслідків інцидентів інформаційної безпеки.

Перелік заходів захисту Політика та процедури реагування на інциденти (IR-1); Навчання з реагування на інциденти (IR-2); Моделювання подій (IR-2(1)); Злам (IR-2(3)); Перевірка реагувань на інциденти (IR-3); Координація з пов'язаними планами (IR-3(2)); Постійне покращення (IR-3(3)); Обробка інциденту (IR-4); Динамічна реконфігурація (IR-4(2)); Безперервність операцій (IR-4(3)); Інформаційна кореляція (IR-4(4)); Внутрішні загрози - особливі можливості (IR-4(6)); Координація з зовнішніми організаціями (IR-4(8)); Здатність динамічного реагування (IR-4(9)); Координація ланцюга постачання (IR-4(10)); Інтегрована група реагування на інцеденти (IR-4(11)); Зловмисний код та криміналістичний аналіз (IR-4(12)); Аналіз поведінки (IR-4(13)); Центр безпеки (IR-4(14)); Зв'язки з громадкістю та відновлення репутації (IR-4(15)); Моніторинг інциденту (IR-5); Автоматизоване відстеження, збір даних і аналіз (IR-5(1)); Звітність про інциденти (IR-6); Автоматичне звітування (IR-6(1)); Координація ланцюжка постачання (IR-6(3)); Підтримка реагування на інциденти (IR-7); Автоматизація підтримки для забезпечення доступності інформації та підтримки (IR-7(1)); Координація з зовнішніми постачальниками (IR-7(2)); План реагування на інциденти (IR-8); Обробка персональних даних (IR-8(1)); Реагування на витік інформації (IR-9); Відповідальний персонал (IR-9(1)) [Вилучено]; Тренування (IR-9(2)); Робота після витоку (IR-9(3)); Викриття неавторизованого персоналу (IR-9(4)); Інтегрована команда аналізу інформаційної безпеки (IR-10) [Вилучено].

8.1. ПОЛІТИКА ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-1)

a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]:
1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики реагування на інциденти, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; процедури, що забезпечують реалізацію політики реагування на інциденти та пов'язані з нею заходи реагування на інциденти.
b. Призначити [Призначення: визначену організацією посадову особу вищого керівництва] для управління, документування і розповсюдження політики та процедур реагування на інциденти.
c. Переглядати та оновлювати поточні:
1. політику реагування на інциденти [Призначення: з визначеною організацією частотою] і

наступні [Призначення: події, визначені організацією];
2. процедури реагування на інциденти [Призначення: з визначеною організацією частотою] та наступні [Призначення: події, визначені організацією].

No: 1
Name: ir_1_odp_1
Type: string
Default: "Визначено організацією"

визначено персонал або ролі, до яких має бути доведена політика реагування на інциденти;

No: 2
Name: ir_1_odp_2
Type: string
Default: "Визначено організацією"

визначено персонал або ролі, до яких мають бути доведені процедури реагування на інциденти;

No: 3
Name: ir_1_odp_3
Type: string
Default: "Визначено організацією"

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: ir_1_odp_4
Type: string
Default: "Визначено організацією"

визначено посадову особу, яка керуватиме політикою та процедурами реагування на інциденти;

No: 5
Name: ir_1_odp_5
Type: string
Default: "Визначено організацією"

визначено частоту, з якою переглядається та оновлюється поточна політика реагування на інциденти;

No: 6
Name: ir_1_odp_6
Type: string
Default: "Визначено організацією"

визначаються події, які потребують перегляду та оновлення поточної політики реагування на інциденти;

No: 7
Name: ir_1_odp_7
Type: string
Default: "Визначено організацією"

визначено частоту, з якою переглядаються та оновлюються поточні процедури реагування на інциденти;

No: 8
Name: ir_1_odp_8
Type: string
Default: "Визначено організацією"

визначено події, які пот ребують перегляду та оновлення процедур реагування на інциденти;

No: 9
Name: ir_1_a_1

Type: string
Default: "Визначено організацією"

розроблено та задокументовано політику реагування на інциденти;

No: 10
Name: ir_1_a_2
Type: string
Default: "Визначено організацією"

політика реагування на інциденти поширюється серед <IR01_ODP[01] персоналу або ролей>;

No: 11
Name: ir_1_a_3
Type: string
Default: "Визначено організацією"

розроблені та задокументовані процедури реагування на інциденти, що сприяють впровадженню політики реагування на інциденти та пов'язаних з нею заходів захисту з реагування на інциденти;

No: 12
Name: ir_1_a_4
Type: string
Default: "Визначено організацією"

процедури реагування на інциденти поширюються серед <IR01_ODP[02] персоналу або ролей>;

No: 13
Name: ir_1_a_1_a_1
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить мету;

No: 14
Name: ir_1_a_1_a_2
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить сферу застосування;

No: 15
Name: ir_1_a_1_a_3
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить ролі;

No: 16
Name: ir_1_a_1_a_4
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить обов'язки;

No: 17
Name: ir_1_a_1_a_5
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить відповідальність керівництва;

No: 18
Name: ir_1_a_1_a_6
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить координацію між підрозділами організації;

No: 19
Name: ir_1_a_1_a_7
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить систему контролю відповідності;

No: 20
Name: ir_1_a_1_b
Type: string
Default: "Визначено організацією"

політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;

No: 21
Name: ir_1_b
Type: string
Default: "Визначено організацією"

<IR-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур реагування на інциденти;

No: 22
Name: ir_1_c_1_1
Type: string
Default: "Визначено організацією"

переглядається та оновлюється поточна політика реагування на

No: 23
Name: ir_1_c_1_2
Type: string
Default: "Визначено організацією"

поточна політика реагування на інциденти переглядається та

No: 24
Name: ir_1_c_2_1
Type: string
Default: "Визначено організацією"

переглядаються та оновлюються поточні процедури реагування на

No: 25
Name: ir_1_c_2_2
Type: string
Default: "Визначено організацією"

поточні процедури реагування на інциденти переглядаються та

8.2. НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-2)

a. Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків:
1. у рамках [Призначення: визначеного організацією періоду часу], впродовж якого авторизована роль або відповідальність за реагування на інциденти;
2. у разі внесення змін у систему;
3. з визначеною [Призначення: визначена організацією частота] у подальшому.
b. Переглядайте та оновлюйте навчальний контент із реагування на інциденти [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].

No: 1
Name: ir_2_odp_1
Type: string
Default: "Визначено організацією"

визначено період часу, протягом якого має бути проведено навчання з реагування на інциденти для користувачів системи, які беруть на себе роль або відповідальність за реагування на інциденти;

No: 2
Name: ir_2_odp_2
Type: string
Default: "Визначено організацією"

визначено частоту, з якою користувачі повинні п роходити навчання з реагування на інциденти;

No: 3
Name: ir_2_odp_3
Type: string
Default: "Визначено організацією"

визначено частоту перегляду та оновлення змісту навчання з реагування на інциденти;

No: 4
Name: ir_2_odp_4
Type: string
Default: "Визначено організацією"

визначено події, які ініціюють перегляд змісту навчання з реагування на інциденти;

No: 5
Name: ir_2_a_1
Type: string
Default: "Визначено організацією"

навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків протягом або обов'язків з реагування на інциденти або отримання доступу до системи;

No: 6
Name: ir_2_a_2
Type: string
Default: "Визначено організацією"

навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків, коли цього вимагають зміни в системі;

No: 7
Name: ir_2_a_3

Type: string
Default: "Визначено організацією"

користувачам системи надається навчання з реагування на інциденти відповідно до призначених ролей та обов'язків <IR02_ODP[02] частота>;

No: 8
Name: ir_2_b_1
Type: string
Default: "Визначено організацією"

зміст навчання з реагування на інциденти переглядається та

No: 9
Name: ir_2_b_2
Type: string
Default: "Визначено організацією"

зміст навчання з реагування на інциденти переглядається та

8.2.1. МОДЕЛЮВАННЯ ПОДІЙ (IR-2(1))

Моделювання подій включається в процес навчання з реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях.

No: 1
Name: ir_2_1_01
Type: string
Default: nil

моделювання подій включається в процес навчання з реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях.

8.2.2. ЗЛАМ (IR-2(3))

Проводиться навчання з реагування на інциденти щодо виявлення та реагування на порушення;.

No: 1
Name: ir_2_3_1
Type: string
Default: nil

проводиться навчання з реагування на інциденти щодо виявлення та реагування на порушення;

No: 2
Name: ir_2_3_2
Type: string
Default: nil

проводиться навчання з реагування на інциденти щодо процесу повідомлення про порушення в організації.

8.3. ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ (IR-3)

Перевіряти ефективність реагування системи на інциденти [Призначення: з визначеною організацією частотою] за допомогою [Призначення: визначених організацією тестів].

No: 1
Name: ir_3_odp_1
Type: string
Default: "Визначено організацією"

визначено частоту, з якою необхідно перевіряти ефективність реагування системи на інциденти;

No: 2
Name: ir_3_odp_2
Type: string
Default: "Визначено організацією"

визначено тести, що використовуються для перевірки ефективності реагування на інциденти в системі;

No: 3
Name: ir_3_01
Type: string
Default: "Визначено організацією"

ефективність реагування системи на інциденти перевіряється тестів>.

8.3.1. КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ (IR-3(2))

Тестування реагування на інциденти координується з елементами організації, відповідальними за пов'язані плани.

No: 1
Name: ir_3_2_01
Type: string
Default: nil

Тестування реагування на інциденти координується з елементами організації, відповідальними за пов'язані плани

8.3.2. ПОСТІЙНЕ ПОКРАЩЕННЯ (IR-3(3))

Якісні дані тестування використовуються для визначення ефективності процесів реагування на інциденти;.

No: 1
Name: ir_3_3_a_1
Type: string
Default: nil

якісні дані тестування використовуються для визначення ефективності процесів реагування на інциденти;

No: 2
Name: ir_3_3_a_2

Type: string
Default: nil

кількісні дані тестування використовуються для визначення ефективності процесів реагування на інциденти;

No: 3
Name: ir_3_3_b_1
Type: string
Default: nil

якісні дані тестування використовуються для постійного вдосконалення процесів реагування на інциденти;

No: 4
Name: ir_3_3_b_2
Type: string
Default: nil

кількісні дані тестування використовуються для постійного вдосконалення процесів реагування на інциденти;

No: 5
Name: ir_3_3_c_1
Type: string
Default: nil

якісні дані, отримані за результатами тестування , використовуються для забезпечення точних показників та метрик реагування на інциденти;

No: 6
Name: ir_3_3_c_2
Type: string
Default: nil

кількісні дані, отримані за результатами тестування , використовуються для забезпечення точних показників та метрик реагування на інциденти;

No: 7
Name: ir_3_3_c_3
Type: string
Default: nil

якісні дані, отримані за результатами тестування , використовуються для забезпе чення послідовності показників та метрик реагування на інциденти;

No: 8
Name: ir_3_3_c_4
Type: string
Default: nil

кількісні дані, отримані за результатами тестування , використовуються для забезпечення послідовності показників та метрик реагування на інциденти;

No: 9
Name: ir_3_3_c_5
Type: string
Default: nil

якісні дані, отримані за результатами тестування , використовуються для забезпечення відтворюваносні показників та метрик реагування на інциденти;

No: 10
Name: ir_3_3_c_6
Type: string
Default: nil

кількусні дані, отримані за результатами тестування , використовуються для забезпечення ві дтворюваносні показників та метрик реагування на інциденти;

8.4. ОБРОБКА ІНЦИДЕНТУ (IR-4)

a. Впровадити можливості обробки інцидентів безпеки та приватності, включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням.
b. Координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування.
c. Включити засвоєні уроки від поточних дій з обробки інцидентів до процедур реагування, навчання та перевірки інцидентів і реалізувати відповідні зміни.
d. Встановлюйте строгість заходів з обробки інцидентів у порівнянній та передбачуваній формі в межах всієї організації.

No: 1
Name: ir_4_a_1
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з підготовкою;

No: 2
Name: ir_4_a_2
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з виявленням;

No: 3
Name: ir_4_a_3
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з аналізом;

No: 4
Name: ir_4_a_4
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з локалізацією;

No: 5
Name: ir_4_a_5
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з ліквідацією;

No: 6
Name: ir_4_a_6
Type: string
Default: "Визначено організацією"

впроваджено можливість обробки інцидентів безпеки включно з відновленням;

No: 7
Name: ir_4_b

Type: string
Default: "Визначено організацією"

діяльність з обробки інцидентів координується із заходами із забезпечення безперервності функціонування;

No: 8
Name: ir_4_c_1
Type: string
Default: "Визначено організацією"

уроки, отримані з поточних дій з обробки інцидентів, включаються в процедури реагування на інциденти, навчання та тестування;

No: 9
Name: ir_4_c_2
Type: string
Default: "Визначено організацією"

зміни, що випливають з отриманих уроків, впроваджуються відповідним чином;

No: 10
Name: ir_4_d_1
Type: string
Default: "Визначено організацією"

строгість заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;

No: 11
Name: ir_4_d_2
Type: string
Default: "Визначено організацією"

інтенсивність заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;

No: 12
Name: ir_4_d_3
Type: string
Default: "Визначено організацією"

обсяг заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;

No: 13
Name: ir_4_d_4
Type: string
Default: "Визначено організацією"

результати діяльності заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;

8.4.1. ДИНАМІЧНА РЕКОНФІГУРАЦІЯ (IR-4(2))

<IR-04(02)_ODP[01] типи динамічної реконфігурації> для частина здатності реагування на інциденти.

No: 1
Name: ir_4_2_odp_1
Type: string
Default: nil

визначено типи динамічної реконфігурації для компонентів системи;

No: 2
Name: ir_4_2_odp_2

Type: string
Default: nil

визначено компоненти системи, які потребують динамічної реконфігурації;

No: 3
Name: ir_4_2_01
Type: string
Default: nil

<IR-04(02)_ODP[01] типи динамічної реконфігурації> для частина здатності реагування на інциденти.

8.4.2. БЕЗПЕРЕРВНІСТЬ ОПЕРАЦІЙ (IR-4(3))

Ідентифіковано <IR-04(03)_ODP[01] класи інцидентів>;.

No: 1
Name: ir_4_3_odp_1
Type: string
Default: nil

визначено класи інцидентів, що вимагають вживання

No: 2
Name: ir_4_3_odp_2
Type: string
Default: nil

визначено дії, які необхідно вжити у відповідь на визначені організацією класи інцидентів;

No: 3
Name: ir_4_3_1
Type: string
Default: nil

ідентифіковано <IR-04(03)_ODP[01] класи інцидентів>;

No: 4
Name: ir_4_3_2
Type: string
Default: nil

<IR-04(03)_ODP[02] дії> вживаються у відповідь на ці інциденти (визначені в IR-04(03)_ODP[01]) для забезпечення продовження виконання завдань та функцій організації.

8.4.3. ІНФОРМАЦІЙНА КОРЕЛЯЦІЯ (IR-4(4))

Інформація про інциденти та індивідуальне реагування на інциденти зіставляється з метою досягнення загальноорганізаційного бачення на обізнаність про інциденти та реагування на них.

No: 1
Name: ir_4_4_01
Type: string
Default: nil

інформація про інциденти та індивідуальне реагування на інциденти зіставляється з метою досягнення загальноорганізаційного бачення на обізнаність про інциденти та реагування на них.

8.4.4. ВНУТРІШНІ ЗАГРОЗИ - ОСОБЛИВІ МОЖЛИВОСТІ (IR-4(6))

Реалізовано можливість обробки інцидентів, пов'язаних з внутрішніми загрозами.

No: 1
Name: ir_4_6_01
Type: string
Default: nil

реалізовано можливість обробки інцидентів, пов'язаних з внутрішніми загрозами

8.4.5. КООРДИНАЦІЯ З ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ (IR-4(8))

Здійснюється координація з <IR-04(08)_ODP[01] нення міжорганізаційного бачення щодо обізнаності про інциденти та більш ефективного реагування на інциденти.

No: 1
Name: ir_4_8_odp_1
Type: string
Default: nil

визначено зовнішні організації, з якими необхідно координувати та обмінюватися інформацією про інциденти в організації;

No: 2
Name: ir_4_8_odp_2
Type: string
Default: nil

визначено інформацію про інциденти, яку необхідно зіставляти та поширювати із зовнішніми організаціями;

No: 3
Name: ir_4_8_01
Type: string
Default: nil

здійснюється координація з <IR-04(08)_ODP[01] нення міжорганізаційного бачення щодо обізнаності про інциденти та більш ефективного реагування на інциденти.

8.4.6. ЗДАТНІСТЬ ДИНАМІЧНОГО РЕАГУВАННЯ (IR-4(9))

Використуються <IR-04(09)_ODP можливості динамічного реагування> для ефективного реагування на інциденти безпеки.

No: 1
Name: ir_4_9_odp
Type: string
Default: nil

визначено можливості динамічного реагування для ефективного реагування на інциденти безпеки.

No: 2
Name: ir_4_9_01

Type: string
Default: nil

використуються <IR-04(09)_ODP можливості динамічного реагування> для ефективного реагування на інциденти безпеки.

8.4.7. КООРДИНАЦІЯ ЛАНЦЮГА ПОСТАЧАННЯ (IR-4(10))

Координується діяльність з обробки інцидентів, пов'язана з подіями ланцюжка постачання, з іншими організаціями, що беруть участь у ланцюжку постачання.

No: 1
Name: ir_4_10_01
Type: string
Default: nil

координується діяльність з обробки інцидентів, пов'язана з подіями ланцюжка постачання, з іншими організаціями, що беруть участь у ланцюжку постачання.

8.4.8. ІНТЕГРОВАНА ГРУПА РЕАГУВАННЯ НА ІНЦЕДЕНТИ (IR-4(11))

Створена та підтримується інтегрована група реагування на інциденти;.

No: 1
Name: ir_4_11_odp
Type: string
Default: nil

визначено період часу, протягом якого може бути розгорнута інтегрована група реагування на інцидент;

No: 2
Name: ir_4_11_1
Type: string
Default: nil

створена та підтримується інтегрована група реагування на інциденти;

No: 3
Name: ir_4_11_2
Type: string
Default: nil

інтегрована група реагування на інциденти може бути розгорнута в будь -якому місці, визначеному організацією протягом <IR04(11)_ODP часового періоду>.

8.4.9. ЗЛОВМИСНИЙ КОД ТА КРИМІНАЛІСТИЧНИЙ АНАЛІЗ (IR-4(12))

Шкідливий код, що залишився в системі, аналізується після інциденту;.

No: 1
Name: ir_4_12_1
Type: string
Default: nil

шкідливий код, що залишився в системі, аналізується після інциденту;

No: 2
Name: ir_4_12_2
Type: string
Default: nil

інші залишкові артефакти, що залишилися в системі (якщо такі є), аналізуються після інциденту.

8.4.10. АНАЛІЗ ПОВЕДІНКИ (IR-4(13))

Аналізується аномальна або підозрювана ворожа поведінка в <IR-04(13)_ODP середовищах або ресурсах > або пов'язана з ними.

No: 1
Name: ir_4_13_odp
Type: string
Default: nil

визначаються середовища або ресурси, які можуть містити або можуть бути пов'язані з аномальною або підозрілою ворожою поведінкою;

No: 2
Name: ir_4_13_01
Type: string
Default: nil

аналізується аномальна або підозрювана ворожа поведінка в <IR-04(13)_ODP середовищах або ресурсах > або пов'язана з ними.

8.4.11. ЦЕНТР БЕЗПЕКИ (IR-4(14))

Створено оперативний центр безпеки;.

No: 1
Name: ir_4_14_1
Type: string
Default: nil

створено оперативний центр безпеки;

No: 2
Name: ir_4_14_2
Type: string
Default: nil

підтримується оперативний центр безпеки;

8.4.12. ЗВ'ЯЗКИ З ГРОМАДКІСТЮ ТА ВІДНОВЛЕННЯ РЕПУТАЦІЇ (IR-4(15))

Зв'язки з громадкістю та відновлення репутації (ir-4(15)).

Немає параметрів для цього контролю.

8.5. МОНІТОРИНГ ІНЦИДЕНТУ (IR-5)

Відстежувати та документувати інциденти безпеки та приватності.

No: 1
Name: ir_5_1
Type: string
Default: "Визначено організацією"

відстежуються інциденти безпеки та приватності;

No: 2
Name: ir_5_2
Type: string
Default: "Визначено організацією"

документуються інциденти безпеки та приватності.

8.5.1. АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ, ЗБІР ДАНИХ І АНАЛІЗ (IR-5(1))

Інциденти відстежуються за допомогою <IR05(01)_ODP[01] автоматизованих механізмів>;.

No: 1
Name: ir_5_1_odp_1
Type: string
Default: nil

визначено автоматизовані механізми відстеження інцидентів;

No: 2
Name: ir_5_1_odp_2
Type: string
Default: nil

визначено автоматизовані механізми збору інформації про інциденти;

No: 3
Name: ir_5_1_odp_3
Type: string
Default: nil

визначено автоматизовані механізми аналізу інформації про інциденти;

No: 4
Name: ir_5_1_1
Type: string
Default: nil

інциденти відстежуються за допомогою <IR05(01)_ODP[01] автоматизованих механізмів>;

No: 5
Name: ir_5_1_2
Type: string
Default: nil

інформація про інциденти збирається за допомогою <IR05(01)_ODP[02] автоматизованих механізмів>;

No: 6
Name: ir_5_1_3
Type: string
Default: nil

інформація про інциденти аналізується за допомогою <IR05(01)_ODP[03] автоматизованих механізмів>.

8.6. ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ (IR-6)

a. Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж [Призначення: визначеного організацією періоду часу].
b. Звітувати про інциденти безпеки, приватності та ланцюжки постачання в [Призначення: визначений організацією уповноважений орган].

No: 1
Name: ir_6_odp_1
Type: string
Default: "Визначено організацією"

визначено період часу, протягом якого персонал повинен повідомляти про підозрілі інциденти до уповноваженого органу;

No: 2
Name: ir_6_odp_2
Type: string
Default: "Визначено організацією"

визначені органи, до яких слід повідомляти інформацію про інцидент;

No: 3
Name: ir_6_a
Type: string
Default: "Визначено організацією"

персонал зобов'язаний повідомляти про підозрілі інциде нти протягом <IR-06_ODP[01] періоду часу>;

No: 4
Name: ir_6_b
Type: string
Default: "Визначено організацією"

інформацію про інцидент повідомляється <IR-06_ODP[02] органам>.

8.6.1. АВТОМАТИЧНЕ ЗВІТУВАННЯ (IR-6(1))

Використовуються <IR-06(01)_ODP автоматичні механізми> звітування про інциденти.

No: 1
Name: ir_6_1_odp
Type: string
Default: nil

визначені автоматичні механізми звітування про інциденти;

No: 2
Name: ir_6_1_01

Type: string
Default: nil

використовуються <IR-06(01)_ODP автоматичні механізми> звітування про інциденти.

8.6.2. КООРДИНАЦІЯ ЛАНЦЮЖКА ПОСТАЧАННЯ (IR-6(3))

Інформація про інцидент надається постачальнику продукту або послуги та іншим організаціям, які беруть участь у ланцюжку постачання систем або компонентів системи, пов'язаних з інцидентом.

No: 1
Name: ir_6_3_01
Type: string
Default: nil

інформація про інцидент надається постачальнику продукту або послуги та іншим організаціям, які беруть участь у ланцюжку постачання систем або компонентів системи, пов'язаних з інцидентом.

8.7. ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-7)

Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною спроможностей організації реагування на інциденти, які являють собою поради та допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності.

No: 1
Name: ir_7_a
Type: string
Default: "Визначено організацією"

IR-07(a) надається ресурс підтримки реагування на інциденти, що є невід'ємною частиною спроможності організації реагувати на інциденти;

No: 2
Name: ir_7_b
Type: string
Default: "Визначено організацією"

IR-07(b) ресурс підтримки реагування на інциденти містить поради та допомогу користувачам системи для обробки та формування звітності про інциденти.

8.7.1. АВТОМАТИЗАЦІЯ ПІДТРИМКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ ТА ПІДТРИМКИ (IR-7(1))

Підвищено доступність інформації та підтримки реагування на інциденти з використанням <IR-07(01)_ODP автоматизованих механізмів>.

No: 1
Name: ir_7_1_odp

Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для збільшення доступності інформації та підтримки при реагуванні на інциденти;

No: 2
Name: ir_7_1_01
Type: string
Default: nil

підвищено доступність інформації та підтримки реагування на інциденти з використанням <IR-07(01)_ODP автоматизованих механізмів>.

8.7.2. КООРДИНАЦІЯ З ЗОВНІШНІМИ ПОСТАЧАЛЬНИКАМИ (IR-7(2))

Встановлено прямі відносини кооперації між здатністю реагування на інциденти та зовнішніми постачальниками можливостей захисту системи.

No: 1
Name: ir_7_2_a
Type: string
Default: nil

встановлено прямі відносини кооперації між здатністю реагування на інциденти та зовнішніми постачальниками можливостей захисту системи.

No: 2
Name: ir_7_2_b
Type: string
Default: nil

визначено членів команди реагування на інциденти в організації для зовнішніх постачальників послуг.

8.8. ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-8)

a. Розробити план реагування на інциденти, який:
1. надає організації дорожню карту для впровадження її можливостей реагування на інциденти;
2. описує структуру та організацію спроможності реагування на інциденти;
3. надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;
4. відповідає вимогам керівництва організації;
5. визначає інциденти, що вимагають звітування, а також метрики для їх вимірювання в організації;
6. визначає ресурси й керівні принципи управління, необхідні для ефективного функціонування та підтримки спроможності реагування на інциденти.
b. Розповсюдити копії плану реагування на інциденти [Призначення: серед визначеного організацією персоналу або ролей].
c. Переглядати план реагування на інциденти [Призначення: з визначеною організацією частотою].
d. Оновлювати план реагування на інциденти для розв'язання проблем із системою й організацією під час перевірок та реагування.
e. Повідомляти про зміни у плані реагування на інциденти [Призначення: визначеному організацією персоналу або ролям].

f. Захищати план реагування на інциденти від несанкціонованого розголошення та зміни.

No: 1
Name: ir_8_odp_1
Type: string
Default: "Визначено організацією"

визначено персонал або ролі, які переглядають та затверджують план реагування на інциденти;

No: 2
Name: ir_8_odp_2
Type: string
Default: "Визначено організацією"

визначено періодичність перегляду та затвердження плану реагування на інциденти;

No: 3
Name: ir_8_odp_3
Type: string
Default: "Визначено організацією"

визначені організації, персонал або ролі, які несуть відповідальність за реагування на інциденти;

No: 4
Name: ir_8_odp_4
Type: string
Default: "Визначено організацією"

визначено персонал з реагування на інцидент (ідентифікований за іменами та/або за ролями), якому мають бути роздані копії плану реагування на інцидент;

No: 5
Name: ir_8_odp_5
Type: string
Default: "Визначено організацією"

визначено елементи організації, серед яких мають бути розповсюджені копії плану реагування на інцидент;

No: 6
Name: ir_8_odp_6
Type: string
Default: "Визначено організацією"

визначено персонал з реагування на інцидент (ідентифікований за іменами та/або ролями), якому повідомляються зміни до плану реагування на інцидент;

No: 7
Name: ir_8_odp_7
Type: string
Default: "Визначено організацією"

визначено елементи організації, яким повідомляється про зміни в плані реагування на інцидент;

No: 8
Name: ir_8_a_1
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який надає організації дорожню карту для впровадження її можливостей реагування на інциденти;

No: 9
Name: ir_8_a_2

Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який описує структуру та організацію спроможності реагування на інциденти;

No: 10
Name: ir_8_a_3
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;

No: 11
Name: ir_8_a_4
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який відповідає унікальним вимогам організації, які пов'язані із завданнями, розміром, структурою і функціями;

No: 12
Name: ir_8_a_5
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який визначає підзвітні інциденти;

No: 13
Name: ir_8_a_6
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який надає показники для вимірювання можливостей реагування на інциденти всередині організації;

No: 14
Name: ir_8_a_7
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти;

No: 15
Name: ir_8_a_8
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, який вирішує питання обміну інформацією про інциденти;

No: 16
Name: ir_8_a_9
Type: string
Default: "Визначено організацією"

розроблено план реагування на інцидент, який розглядається та затверджується <IR-08_ODP[01] персоналом або ролями> < IR08_ODP[02] частота>;

No: 17
Name: ir_8_a_10
Type: string
Default: "Визначено організацією"

розроблено план реагування на інциденти, в якому чітко визначено організацій, персоналу або ролей>.

No: 18
Name: ir_8_b_1
Type: string
Default: "Визначено організацією"

копії плану реагування на інцидент розповсюджуються серед <IR309

No: 19
Name: ir_8_b_2
Type: string
Default: "Визначено організацією"

копії плану реагування на інцидент розповсюджуються серед <IR08_ODP[05] елементів організації>;

No: 20
Name: ir_8_c
Type: string
Default: "Визначено організацією"

план реагування на інциденти оновлюється з урахуванням змін у системі та організації або проблем, що виникають під час впровадження, виконання або тестування плану;

No: 21
Name: ir_8_d_1
Type: string
Default: "Визначено організацією"

зміни в плані реагування на інцидент повідомляються <IR08_ODP[06] персоналу з реагування на інциденти>;

No: 22
Name: ir_8_d_2
Type: string
Default: "Визначено організацією"

зміни в плані реагування на інциденти надсилаються до <IR08_ODP[07] елементів організації>;

No: 23
Name: ir_8_e_1
Type: string
Default: "Визначено організацією"

план реагування на інциденти захищений від несанкціонованого розкриття;

No: 24
Name: ir_8_e_2
Type: string
Default: "Визначено організацією"

план реагування на інциденти захищений від несанкціонованої модифікації.

8.8.1. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ (IR-8(1))

План реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає процес визначення доцільності повідомлення наглядових організацій і надання такого повідомлення, якщо це доречно;.

No: 1
Name: ir_8_1_a
Type: string
Default: nil

план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає процес визначення доцільності повідомлення наглядових організацій і надання такого повідомлення, якщо це доречно;

No: 2
Name: ir_8_1_b
Type: string
Default: nil

план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає процес оцінювання для визначення ступеня шкоди, труднощів, незручностей або несправедливості щодо постраждалих осіб та будь-які механізми пом'якшення такої шкоди;

No: 3
Name: ir_8_1_c
Type: string
Default: nil

план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає ідентифікацію застосовних вимог щодо конфіденційності.

8.9. РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ (IR-9)

<IR-09_ODP[01] персонал або ролі> призначено відповідальним за реагування на витоки інформації;.

No: 1
Name: ir_9_odp_1
Type: string
Default: nil

визначено персонал або ролі, на які покладено відповідальність за реагування на витоки інформації;

No: 2
Name: ir_9_odp_2
Type: string
Default: nil

визначено персонал або ролі, які мають бути сповіщені про витік інформації за допомогою методу зв'язку, не пов'язаного з витоком;

No: 3
Name: ir_9_odp_3
Type: string
Default: nil

визначені дії, які необхідно виконати;

No: 4
Name: ir_9_a
Type: string
Default: nil

<IR-09_ODP[01] персонал або ролі> призначено відповідальним за реагування на витоки інформації;

No: 5
Name: ir_9_b
Type: string
Default: nil

у відповідь на витік інформації визначається конкретна інформація, пов'язана з джерелом витоку в системі;

No: 6
Name: ir_9_c
Type: string
Default: nil

<IR-09_ODP[02] персонал або ролі> попереджається про витік інформації за допомогою методу зв'язку, не пов'язаного з витоком;

No: 7
Name: ir_9_d
Type: string
Default: nil

ізоляцюється система або компонент системи де відбувся витік інформації;

No: 8
Name: ir_9_e
Type: string
Default: nil

інформація видаляється із зараженої системи або компонента у відповідь на витік інформації;

No: 9
Name: ir_9_f
Type: string
Default: nil

у відповідь на витік інформації визначаються інші системи або компоненти системи, які могли бути згодом джерелом витоку інформації;

No: 10
Name: ir_9_g
Type: string
Default: nil

<IR-09_ODP[03] дії> виконуються у відповідь на витік інформації.

8.9.1. ВІДПОВІДАЛЬНИЙ ПЕРСОНАЛ (IR-9(1)) [Вилучено]

[Вилучено: включено до IR-09]

Немає параметрів для цього контролю.

8.9.2. ТРЕНУВАННЯ (IR-9(2))

Забезпечено навчання з реагування на витік інформації <IR09(02)_ODP частота>.

No: 1
Name: ir_9_2_odp
Type: string
Default: nil

визначено частоту навчання з реагування на витік інформації;

No: 2
Name: ir_9_2_01
Type: string
Default: nil

забезпечено навчання з реагування на витік інформації <IR09(02)_ODP частота>.

8.9.3. РОБОТА ПІСЛЯ ВИТОКУ (IR-9(3))

Реалізувано <IR-09(03)_ODP процедури>, з метою забезпечення спроможності для персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригу312 вальних дій.

No: 1
Name: ir_9_3_odp
Type: string
Default: nil

визначено процедури з метою забезпечення спроможності персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригувальних дій.

No: 2
Name: ir_9_3_01
Type: string
Default: nil

реалізувано <IR-09(03)_ODP процедури>, з метою забезпечення спроможності для персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригу312 вальних дій.

8.9.4. ВИКРИТТЯ НЕАВТОРИЗОВАНОГО ПЕРСОНАЛУ (IR-9(4))

Застосовуються <IR-09(04)_ODP механізми захисту > для персоналу, що має доступ до інформації, яка не відпов ідає призначеним правам доступу.

No: 1
Name: ir_9_4_odp
Type: string
Default: nil

визначено механізми захисту для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу;

No: 2
Name: ir_9_4_01
Type: string
Default: nil

застосовуються <IR-09(04)_ODP механізми захисту > для персоналу, що має доступ до інформації, яка не відпов ідає призначеним правам доступу.

8.10. ІНТЕГРОВАНА КОМАНДА АНАЛІЗУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (IR-10) [Вилучено]

[Вилучено: перенесено до IR-04(11)]

Немає параметрів для цього контролю.

9. MA

Клас заходів захисту MA — ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

Опис Цей клас регулює процеси планового та позапланового технічного обслуговування компонентів системи для запобігання збоям.

Перелік заходів захисту Політика та процедури технічного обслуговування (MA-1); Зміст запису (MA-2(1)) [Вилучено]; Автоматизована технічна діяльність (MA-2(2)); Інструменти для обслуговування (MA-3); Перевірка інструментів (MA-3(1)); Перевірка носіїв інформації (MA-3(2)); Запобігання несанкціонованому переміщенню (MA-3(3)); Обмеження використання інструмента (MA-3(4)); Привілейоване виконання (MA-3(5)); Оновлення програм- (MA-3(6)); Віддалене обслуговування (MA-4); Аудит та огляд (MA-4(1)); Документування віддаленого обслуговування (MA-4(2)) [Вилучено]; Порівняльна безпека і очищення (MA-4(3)); Схвалення та повідомлення (MA-4(5)); Віддалене обслуговування роз'єднання (MA-4(7)); Технічний персонал (MA-5); Особи без належного доступу (MA-5(1)); Оформлення допуску для систем, що обробляють інформацію з обмеженим доступом (MA-5(2)); Вимоги до громадянства (MA-5(3)); Іноземні громадяни (MA-5(4)); Несистемне обслуговування (MA-5(5)); Своєчасне обслуговування (MA-6); Профілактичне обслуговування (MA-6(1)); Планове технічне обслуговування (MA-6(2)); Автоматизована підтримка планового технічного обслуговування (MA-6(3)); Технічне обслуговування в польових умовах (MA-7).

9.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ (MA-1)

a. Планувати, документувати та переглядати записи з технічного обслуговування, ремонту або заміни компонентів системи відповідно до вимог виробника та постачальників та/або вимог організації.
b. Затвердити та здійснювати моніторинг усіх заходів з технічного обслуговування, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці, чи переміщуються в інше місце.
c. Вимагати, щоб [Призначення: визначені організацією персонал чи ролі] явно схвалили видалення системи або компоненту системи з організаційного обладнання для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації.
d. Очищати обладнання з погляду видалення всієї інформації з носіїв до вилучення обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації.
e. Перевірити всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше, працюють належним чином після дій з обслуговування, ремонту або заміни.
f. Вносити [Призначення: визначену організацією інформацію, пов'язану з технічним обслуговуванням] до записів з технічного обслуговування.

No: 1
Name: ma_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, на які поширюється політика технічного обслуговування;

No: 2
Name: ma_1_odp_2
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури технічного обслуговування;

No: 3
Name: ma_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: ma_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка керуватиме політикою та процедурами технічного обслуговування;

No: 5
Name: ma_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика технічного обслуговування;

No: 6
Name: ma_1_odp_6
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення поточної політики технічного обслуговування;

No: 7
Name: ma_1_odp_7
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються поточні процедури технічного обслуговування;

No: 8
Name: ma_1_odp_8
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення процедур технічного обслуговування;

No: 9
Name: ma_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику технічного обслуговування;

No: 10
Name: ma_1_a_2
Type: string
Default: nil

політика технічного обслуговування поширюється на <MA01_ODP[01] персонал або ролі>;

No: 11
Name: ma_1_a_3
Type: string
Default: nil

розроблені та задокументовані процедури технічного обслуговування, що сприяють впровадженню політики технічного обслуговування та пов'язаних з нею заходів технічного обслуговування;

No: 12
Name: ma_1_a_4
Type: string
Default: nil

процедури технічного обслуговування розповсюджуються серед <MA-01_ODP[02] персоналу або ролей>;

No: 13
Name: ma_1_a_1_a_1
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить мету;

No: 14
Name: ma_1_a_1_a_2
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування;

No: 15
Name: ma_1_a_1_a_3
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить ролі;

No: 16
Name: ma_1_a_1_a_4
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить обов'язки;

No: 17
Name: ma_1_a_1_a_5
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить відповідальність керівництва;

No: 18
Name: ma_1_a_1_a_6
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить координацію між підрозділами організації;

No: 19
Name: ma_1_a_1_a_7
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить систему контролю відповідності;

No: 20
Name: ma_1_a_1_b
Type: string
Default: nil

політика технічного обслуговування <MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам;

No: 21
Name: ma_1_b
Type: string
Default: nil

<MA-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур технічного обслуговування;

No: 22
Name: ma_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика обслуговування <MA-01_ODP[05] частота>;

No: 23
Name: ma_1_c_1_2
Type: string
Default: nil

переглядається та оновлюється поточна політика обслуговування після <MA-01_ODP[06] подій>;

No: 24
Name: ma_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури технічного

No: 25
Name: ma_1_c_2_2
Type: string
Default: nil

переглядаються та оновлюються поточні процедури технічного

9.1.1. ЗМІСТ ЗАПИСУ (MA-2(1)) [Вилучено]

[Вилучено: Включено до MA-02]

Немає параметрів для цього контролю.

9.1.2. АВТОМАТИЗОВАНА ТЕХНІЧНА ДІЯЛЬНІСТЬ (MA-2(2))

<MA-02(02)_ODP[01] автоматизовані механізми> використовуються для планування дій з технічного обслуговування, ремонту та заміни системи;.

No: 1
Name: ma_2_2_odp_1
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для планування дій з технічного обслуговування, ремонту та заміни системи;

No: 2
Name: ma_2_2_odp_2
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для проведення дій з технічного обслуговування, ремонту та заміни системи;

No: 3
Name: ma_2_2_odp_3
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для документування дій з технічного обслуговування, ремонту та заміни системи;

No: 4
Name: ma_2_2_a_1
Type: string
Default: nil

<MA-02(02)_ODP[01] автоматизовані механізми> використовуються для планування дій з технічного обслуговування, ремонту та заміни системи;

No: 5
Name: ma_2_2_a_2
Type: string
Default: nil

<MA-02(02)_ODP[02] автоматизовані механізми> використовуються для проведення дій з технічного обслуговування, ремонту та заміни системи;

No: 6
Name: ma_2_2_a_3
Type: string
Default: nil

<MA-02(02)_ODP[03] автоматизовані механізми> використовуються для документування дій з технічного обслуговування, ремонту та заміни системи;

No: 7
Name: ma_2_2_b_1
Type: string
Default: nil

надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії з технічного обслуговування;

No: 8
Name: ma_2_2_b_2
Type: string
Default: nil

надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії ремонту;

No: 9
Name: ma_2_2_b_3
Type: string
Default: nil

надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії з заміни;

9.2. ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ (MA-3)

a. Затвердити, контролювати та відстежувати використання засобів технічного обслуговування.
b. Переглядати раніше затверджені інструменти технічного [Призначення: з частотою, визначеною організацією]. обслуговування

No: 1
Name: ma_3_odp
Type: string
Default: nil

визначено частоту, з якою слід переглядати раніше затверджені інструменти технічного обслуговування;

No: 2
Name: ma_3_a_1
Type: string
Default: nil

використання засобів технічного обслуговування затверджено;

No: 3
Name: ma_3_a_2
Type: string
Default: nil

використання засобів технічного обслуговування контролюється;

No: 4
Name: ma_3_a_3
Type: string
Default: nil

використання засобів технічного обслуговування відстажуються;

No: 5
Name: ma_3_b
Type: string
Default: nil

переглядаються раніше затверджені інструменти технічного обслуговування <MA-03_ODP частота>.

9.2.1. ПЕРЕВІРКА ІНСТРУМЕНТІВ (MA-3(1))

Оглядаються інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних або несанкціонованих модифікацій.

No: 1
Name: ma_3_1_01
Type: string
Default: nil

оглядаються інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних або несанкціонованих модифікацій.

9.2.2. ПЕРЕВІРКА НОСІЇВ ІНФОРМАЦІЇ (MA-3(2))

Перед використанням носіїв у системі перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду.

No: 1
Name: ma_3_2_01
Type: string
Default: nil

перед використанням носіїв у системі перевіряються носії, що містять діагностичні та тестові програми на наявність шкідливого коду.

9.2.3. ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ПЕРЕМІЩЕННЮ (MA-3(3))

Запобігти переміщенню обладнання для технічного обслуговування, що містить організаційну інформацію, шляхом:
(a) перевірки відсутності організаційної інформації, розміщеної на обладнанні;
(b) очищення або знищення обладнання;
(c) утримання обладнання на об'єкті;
(d) отримання дозволу від [Призначення: визначених організацією персоналу чи ролей], які явно дозволяють переміщення обладнання з об'єкта.

No: 1
Name: ma_3_3_odp
Type: string
Default: nil

визначено персонал або ролі, які можуть надавати дозвіл на переміщення обладнання з об'єкту;

No: 2
Name: ma_3_3_a
Type: string
Default: nil

переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом перевірки того, що на обладнанні не міститься ніякої інформації організації; або

No: 3
Name: ma_3_3_b
Type: string
Default: nil

переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом очищення або знищення обладнання; або

No: 4
Name: ma_3_3_c
Type: string
Default: nil

переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом утримання обладнання на об'єкті; або

No: 5
Name: ma_3_3_d
Type: string
Default: nil

переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом отримання дозволу від <MA-03(03)_ODP персонал або ролі>.

9.2.4. ОБМЕЖЕННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТА (MA-3(4))

Обмежити використання інструментів авторизованим персоналом. технічного ОБМЕЖЕННЯ обслуговування лише

No: 1
Name: ma_3_4_01
Type: string
Default: nil

обмежено використання інструментів технічного обслуговування лише авторизованим персоналом.

9.2.5. ПРИВІЛЕЙОВАНЕ ВИКОНАННЯ (MA-3(5))

(a) вимагати схвалення кожного віддаленого сеансу технічного обслуговування [Призначення: персоналом або роллю, що визначила організація];
(b) повідомити [Призначення: персонал або ролі, що визначила організація] про дату та час запланованого віддаленого обслуговування.

No: 1
Name: ma_3_5_01
Type: string
Default: nil

відстежується використання інструментів обслуговування, які виконуються з підвищеними привілеями.

9.2.6. ОНОВЛЕННЯ ПРОГРАМ- (MA-3(6))

Запровадити криптографічні механізми для захисту цілісності та конфіденційності віддаленого обслуговування та діагностичних комунікацій.

No: 1
Name: ma_3_6_01
Type: string
Default: nil

інструменти технічного обслуговування перевіряються, щоб переконатися, що встановлені найновіші оновлення програмного забезпечення та патчі.

9.3. ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ (MA-4)

Впроваджено віддалені дії з обслуговування та діагностики;.

No: 1
Name: ma_4_a_1
Type: string
Default: nil

впроваджено віддалені дії з обслуговування та діагностики;

No: 2
Name: ma_4_a_2
Type: string
Default: nil

відстежуються віддалені дії з обслуговування та діагностики;

No: 3
Name: ma_4_b_1
Type: string
Default: nil

використання віддалених засобів технічного обслуговування та діагностики дозволено лише відповідно до політики організації;

No: 4
Name: ma_4_b_2
Type: string
Default: nil

використання віддалених засобів технічного обслуговування та діагностики задокументовано в плані захисту інформації;

No: 5
Name: ma_4_c
Type: string
Default: nil

надійна автентифікація використовується при встановленні віддалених технічних та діагностичних сеансів;

No: 6
Name: ma_4_d
Type: string
Default: nil

ведеться облік віддалених дій з обслуговування та діагностики;

No: 7
Name: ma_4_e_1
Type: string
Default: nil

сесія припиняється, коли завершено віддалене обслуговування

No: 8
Name: ma_4_e_2
Type: string
Default: nil

мережеве з'єднання припиняється, коли завершено віддалене обслуговування

9.3.1. АУДИТ ТА ОГЛЯД (MA-4(1))

<MA-04(01)_ODP[01] події аудиту> журналюються для віддалених сеансів обслуговування;.

No: 1
Name: ma_4_1_odp_1
Type: string
Default: nil

визначено події аудиту, які слід журналювати для віддалених сеансів обслуговування;

No: 2
Name: ma_4_1_odp_2
Type: string
Default: nil

визначено події аудиту, які слід журналювати для віддалених сеансів діагностики;

No: 3
Name: ma_4_1_a_1
Type: string
Default: nil

<MA-04(01)_ODP[01] події аудиту> журналюються для віддалених сеансів обслуговування;

No: 4
Name: ma_4_1_a_2
Type: string
Default: nil

<MA-04(01)_ODP[02] події аудиту> журналюються для віддалених сеансів діагностики;

No: 5
Name: ma_4_1_b_1
Type: string
Default: nil

здійснюється огляд записів про сеанси віддаленого обслуговування;

No: 6
Name: ma_4_1_b_2
Type: string
Default: nil

здійснюється огляд записів про сеанси віддаленої діагностики.

9.3.2. ДОКУМЕНТУВАННЯ ВІДДАЛЕНОГО ОБСЛУГОВУВАННЯ (MA-4(2)) [Вилучено]

[Вилучено: включено до MA-01 та MA-04]

Немає параметрів для цього контролю.

9.3.3. ПОРІВНЯЛЬНА БЕЗПЕКА І ОЧИЩЕННЯ (MA-4(3))

Віддалені послуги з технічного обслуговування повинні виконуватися з системи, яка реалізує заходи захисту, співставні з заходами захисту, реалізованими в системі, що обслуговується;.

No: 1
Name: ma_4_3_a_1
Type: string
Default: nil

віддалені послуги з технічного обслуговування повинні виконуватися з системи, яка реалізує заходи захисту, співставні з заходами захисту, реалізованими в системі, що обслуговується;

No: 2
Name: ma_4_3_a_2
Type: string
Default: nil

віддалені послуги з діагностики повинні виконуватися з системи, яка реалізує заходи захисту, співставні з заходами захисту, реалізованими в системі, що обслуговується;

No: 3
Name: ma_4_3_b_1
Type: string
Default: nil

компонент, що підлягає обслуговуванню, видаляється з системи перед проведенням віддаленого технічного обслуговування або діагностики;

No: 4
Name: ma_4_3_b_2
Type: string
Default: nil

компонент, що підлягає обслуговуванню, пройшов процедуру очищення (від інф ормації організації);

No: 5
Name: ma_4_3_b_3
Type: string
Default: nil

компонент перевіряється та очищується (на наявність потенційно шкідливого програмного забезпечення) після виконання послуги та перед повторним підключенням компонента до системи.

9.3.4. СХВАЛЕННЯ ТА ПОВІДОМЛЕННЯ (MA-4(5))

Схвалення кожного віддаленого сеансу обслуговування.

No: 1
Name: ma_4_5_odp_1
Type: string
Default: nil

визначено персонал або ролі, необхідні для затвердження кожного віддаленого сеансу технічного обслуговування;

No: 2
Name: ma_4_5_odp_2
Type: string
Default: nil

визначено персонал та ролі, які мають бути повідомлені про дату та час запланованого віддаленого технічного обслуговування;

No: 3
Name: ma_4_5_a

Type: string
Default: nil

схвалення кожного віддаленого сеансу обслуговування

No: 4
Name: ma_4_5_b
Type: string
Default: nil

<MA-04(05)_ODP[02] персонал і ролі> повідомлено про дату і час запланованого віддаленого технічного обслуговування.

9.3.5. ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ РОЗ'ЄДНАННЯ (MA-4(7))

Реалізувано перевірку роз'єднання у разі припинення віддалених сеансів обслуговування.

No: 1
Name: ma_4_7_1
Type: string
Default: nil

реалізувано перевірку роз'єднання у разі припинення віддалених сеансів обслуговування

No: 2
Name: ma_4_7_2
Type: string
Default: nil

реалізувано перевірку роз'єднання у разі припинення віддалених сеансів діагностики

9.4. ТЕХНІЧНИЙ ПЕРСОНАЛ (MA-5)

a. Встановити процедуру авторизації технічного персоналу та вести перелік авторизованих організацій технічного обслуговування або персоналу.
b. Перевіряти, що персонал, який не супроводжується та виконує технічне обслуговування в системі, має необхідні дозволи на доступ.
c. Визначити персонал організації з необхідними повноваженнями щодо доступу та технічною компетенцією для нагляду за персоналом з технічного обслуговування, який не має необхідних дозволів на доступ.

No: 1
Name: ma_5_a_1
Type: string
Default: nil

запроваджено процес авторизації технічного персоналу;

No: 2
Name: ma_5_a_2
Type: string
Default: nil

ведеться перелік авторизованих організацій або персоналу з технічного обслуговування;

No: 3
Name: ma_5_b
Type: string
Default: nil

персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ;

No: 4
Name: ma_5_c
Type: string
Default: nil

персонал організації з необхідними повноваженнями доступу та технічною компетентністю призначений/призначені для нагляду за діяльністю з технічного обслуговування персоналу, який не має необхідних дозволів на доступ.

9.4.1. ОСОБИ БЕЗ НАЛЕЖНОГО ДОСТУПУ (MA-5(1))

Впроваджені процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів або не є громадянами України, містять вимогу:.

No: 1
Name: ma_5_1_odp
Type: string
Default: nil

визначені альтернативні заходи захисту, які мають бути розроблені та впроваджені на випадок, якщо компонент системи не може бути очищений, вилучений або відключений від системи;

No: 2
Name: ma_5_1_a
Type: string
Default: nil

впроваджені процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів або не є громадянами України, містять вимогу:

No: 3
Name: ma_5_1_a_01
Type: string
Default: nil

обслуговуючий персонал, що не має необхідних прав доступу, рівня допуску, повинен супроводжуватися та бути під наглядом уповноваженого організацією персоналу з необхідним рівнем допуску та технічною кваліфікацією;

No: 4
Name: ma_5_1_a_02
Type: string
Default: nil

перед тим, як розпочати технічне обслуговування або діагностику персоналом без допуску, упевнитися, що всі компоненти енергонезалежного зберігання інформації в системі очищуються, а всі енергонезалежні носії видаляються або фізично відключаються від системи.

No: 5
Name: ma_5_1_b
Type: string
Default: nil

<MA-05(01)_ODP альтернативні заходи захисту> розробляються і впроваджуються у випадку, якщо систему неможливо очистити, вилучити або відключити від систе328 ми.

9.4.2. ОФОРМЛЕННЯ ДОПУСКУ ДЛЯ СИСТЕМ, ЩО ОБРОБЛЯЮТЬ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ (MA-5(2))

Переконатися, що персонал, який виконує технічне обслуговування та діагностику в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має рівень допуску та офіційне схвалення на доступ для найвищого рівня секретності та для всієї інформації в системі.

No: 1
Name: ma_5_2_1
Type: string
Default: nil

персонал, який виконує роботи з технічного обслуговування та діагностики в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має відповідний рівень допуску;

No: 2
Name: ma_5_2_2
Type: string
Default: nil

персонал, який виконує роботи з технічного обслуговування та діагностики в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має офіційне схвалення на допуск;

9.4.3. ВИМОГИ ДО ГРОМАДЯНСТВА (MA-5(3))

Переконатися, що працівники, які виконують технічне обслуговування та діагностичні заходи з обробки, зберігання або передачі таємної інформації, є громадянами України.

No: 1
Name: ma_5_3_01
Type: string
Default: nil

працівники, які виконують технічне обслуговування та діагностичні заходи з обробки, зберігання або передачі інформації з обмеженим доступом, є громадянами України.

9.4.4. ІНОЗЕМНІ ГРОМАДЯНИ (MA-5(4))

Переконайтеся, що:
(a) іноземні громадяни з відповідним рівнем допуску залучаються для проведення технічного обслуговування та діагностичних робіт у системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли ці системи спільно належать і експлуатуються урядами України та закордонних союзників, або належать та експлуатуються виключно іноземними союзними урядами;
(b) схвалення, згоди та додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.

No: 1
Name: ma_5_4_a
Type: string
Default: nil

іноземні громадяни з відповідним рівнем допуску залучаються для проведення технічного обслуговування та діагностичних робіт у системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли ці системи спільно належать і експлуатуються урядами України та закордонних союзників, або належать та е ксплуатуються виключно іноземними союзними урядами;

No: 2
Name: ma_5_4_b_1
Type: string
Default: nil

схвалення, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.

No: 3
Name: ma_5_4_b_2
Type: string
Default: nil

згоди, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.

No: 4
Name: ma_5_4_b_3
Type: string
Default: nil

додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументова ні в Меморандумі про угоду.

9.4.5. НЕСИСТЕМНЕ ОБСЛУГОВУВАННЯ (MA-5(5))

Переконатися, що персонал, який не супроводжується та здійснює ремонтні роботи, не пов'язаний безпосередньо із системою, але перебуває фізично близько від системи, має необхідні дозволи на доступ.

No: 1
Name: ma_5_5_01
Type: string
Default: nil

персонал, який не супроводжується, що здійснює ремонтні роботи, не пов'язаний безпосередньо з системою, але знаходиться фізично близько від системи, має необхідні дозволи на доступ.

9.5. СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ (MA-6)

Отримати технічну підтримку та/або запасні частини для [Призначення: визначених організацією компонентів системи] в межах [Призначення: визначеного організацією періоду часу] у разі відмови.

No: 1
Name: ma_6_odp_1
Type: string
Default: nil

визначено компоненти системи, для яких отримується технічна підтримка та/або запасні частини;

No: 2
Name: ma_6_odp_2
Type: string
Default: nil

визначено період часу, протягом якого можна отримати технічну підтримку та/або запасні частини у разі відмови;

No: 3
Name: ma_6_01
Type: string
Default: nil

технічна підтримка та/або запасні частини отримуються для

9.5.1. ПРОФІЛАКТИЧНЕ ОБСЛУГОВУВАННЯ (MA-6(1))

Здійснюється профілактичне обслуговування <MA06(01)_ODP[01] компонентів системи> у <MA06(01)_ODP[02] часові інтервали>.

No: 1
Name: ma_6_1_odp_1
Type: string
Default: nil

визначено компоненти системи яким необхідно здійснювати профілактичне обслуговування;

No: 2
Name: ma_6_1_odp_2
Type: string
Default: nil

визначено часові інтервали з якими необхідно здійснювати профілактичне обслуговування визначеним компонентам системи;

No: 3
Name: ma_6_1_01
Type: string
Default: nil

здійснюється профілактичне обслуговування <MA06(01)_ODP[01] компонентів системи> у <MA06(01)_ODP[02] часові інтервали>.

9.5.2. ПЛАНОВЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA-6(2))

Здійснювати планове технічне обслуговування [Призначення: визначених організацією компонентів системи] у [Призначення: визначені організацією часові інтервали].

No: 1
Name: ma_6_2_odp_1
Type: string
Default: nil

визначено компоненти системи яким необхідно здійснювати планове технічне обслуговування;

No: 2
Name: ma_6_2_odp_2
Type: string
Default: nil

визначено часові інтервали з якими необхідно здійснювати планове технічне обслуговування;

No: 3
Name: ma_6_2_01
Type: string
Default: nil

здійснюється планове технічне обслуговування <MA06(02)_ODP[01] компонентів системи> у <MA06(02)_ODP[02] часові інтервали>.

9.5.3. АВТОМАТИЗОВАНА ПІДТРИМКА ПЛАНОВОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ (MA-6(3))

Використовувати автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням [Призначення: автоматизовані засоби визначені організацією].

No: 1
Name: ma_6_3_odp
Type: string
Default: nil

визначено автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням;

No: 2
Name: ma_6_3_01
Type: string
Default: nil

використовуються <MA-06(03)_ODP автоматизовані механізми> для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням.

9.6. ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ В ПОЛЬОВИХ УМОВАХ (MA-7)

Технічне обслуговування в польових умовах < MA-07_ODP[01] систем або компонентів системи > обмежене або заборонене.

No: 1
Name: ma_7_odp_1
Type: string
Default: nil

визначені системи або компоненти системи, на яких технічне обслуговування в польових умовах обмежене або заборонене

No: 2
Name: ma_7_odp_2
Type: string
Default: nil

визначено довірені засоби технічного обслуговуваннятехнічного обслуговування

No: 3
Name: ma_7_01

Type: string
Default: nil

технічне обслуговування в польових умовах < MA-07_ODP[01] систем або компонентів системи > обмежене або заборонене

10. MP

Клас заходів захисту MP — ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ

Опис Цей клас спрямований на безпечне зберігання, транспортування, використання та знищення як цифрових, так і паперових носіїв інформації.

Перелік заходів захисту Політика та процедури щодо захисту носіїв інформації (MP-1); Доступ до носіїв інформації (MP-2); Автоматизований обмеженний доступ (MP-2(1)) [Вилучено]; Криптографічний захист (MP-2(2)) [Вилучено]; Маркування носіїв інформації (MP-3); Зберігання носіїв інформації (MP-4); Криптографічний захист (MP-4(1)) [Вилучено]; Автоматизований обмежений доступ (MP-4(2)); Транспортування носіїв інформації (MP-5); Захист поза контрольованими зонами (MP-5(1)) [Вилучено]; Документування дій (MP-5(2)) [Вилучено]; Зберігачі (MP-5(3)); Криптографічний захист (MP-5(4)) [Вилучено]; Знищення інформації на носіях інформації (MP-6); Переглядати, затвердження, відстеження, документування та перевірка (MP-6(1)); Перевірка обладнання (MP-6(2)); Неруйнівні методи (MP-6(3)); Керована несекретна інформація (MP-6(4)) [Вилучено]; Секретна інформація (MP-6(5)) [Вилучено]; Знищення носіїв інформації (MP-6(6)) [Вилучено]; Подвійна авторизація (MP-6(7)); Віддалене очищення або стирання інформації (MP-6(8)); Використання носіїв інформації (MP-7); Заборона використання без визначеного власника (MP-7(1)) [Вилучено]; Заборона використання (MP-7(2)); Зниження категорії безпеки носіїв інформації (MP-8); Документування процесу (MP-8(1)); Перевірка обладнання (MP-8(2)); Критична інформація (MP-8(3)); Таємна інформація (MP-8(4)).

10.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ЩОДО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ (MP-1)

a. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посад]:
1. 2. політику захисту носіїв інформації, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; процедури, які сприяють здійсненню політики та заходів захисту носіїв інформації.
b. Призначити [Призначення: визначену організацією посадову особу] для управління розробкою, документування, та розповсюдження політики та процедурами захисту носіїв інформації.
c. Переглядати та оновлювати чинну систему захисту носіїв інформації:
1. поточну політику захисту носіїв інформації [Призначення: з визначеною організацією частотою];
2. поточні процедури захисту носіїв інформації [Призначення: з визначеною організацією частотою].

No: 1
Name: mp_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, серед яких має бути поширена політика захисту носіїв інформації;

No: 2
Name: mp_1_odp_2
Type: string
Default: nil

визначено персонал або ролі, серед яких мають бути поширені процедури захисту носіїв інформації;

No: 3
Name: mp_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};

No: 4
Name: mp_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка керуватиме політикою та процедурами захисту носіїв інформації;

No: 5
Name: mp_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика захисту носіїв інформації;

No: 6
Name: mp_1_odp_6
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення чинної політики захисту носіїв інформації;

No: 7
Name: mp_1_odp_7
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються чинні процедури захисту носіїв інформації;

No: 8
Name: mp_1_odp_8
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення процедур захисту носіїв інформації;

No: 9
Name: mp_1_a_1
Type: string
Default: nil

розроблено та задокументовано політику захисту носіїв інформації;

No: 10
Name: mp_1_a_2
Type: string
Default: nil

політика захисту носіїв інформації поширюється на <MP01_ODP[01] персонал або ролі>;

No: 11
Name: mp_1_a_3
Type: string
Default: nil

розроблено та задокументовано процедури захисту носіїв інформації, що сприятимуть реалізації політики захисту носіїв інформації та заходів захисту носіїв інформації;

No: 12
Name: mp_1_a_4
Type: string
Default: nil

процедури захисту носіїв інформації поширюються на <MP01_ODP[02] персонал або ролі>;

No: 13
Name: mp_1_a_1_a_1
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить мету;

No: 14
Name: mp_1_a_1_a_2
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить сферу застосування;

No: 15
Name: mp_1_a_1_a_3
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить ролі;

No: 16
Name: mp_1_a_1_a_4
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить обов'язки;

No: 17
Name: mp_1_a_1_a_5
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить відповідальність керівництва;

No: 18
Name: mp_1_a_1_a_6

Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить координацію між підрозділами організації;

No: 19
Name: mp_1_a_1_a_7
Type: string
Default: nil

<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика захисту носіїв інформації містить систему контролю відповідності;

No: 20
Name: mp_1_a_1_b
Type: string
Default: nil

політика захисту носіїв інформації відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;

No: 21
Name: mp_1_b
Type: string
Default: nil

<MP-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур захисту носіїв інформації.

No: 22
Name: mp_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика захисту носіїв

No: 23
Name: mp_1_c_1_2
Type: string
Default: nil

переглядається та оновлюється поточна політика захисту носіїв

No: 24
Name: mp_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури захисту

No: 25
Name: mp_1_c_2_2
Type: string
Default: nil

переглядаються та оновлюються поточні процедури захисту

10.2. ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ (MP-2)

Обмежити доступ до [Призначення: визначених організацією типів цифрових та/або нецифрових носіїв інформації] [Призначення: визначеним організацією персоналом або ролями].

No: 1
Name: mp_2_odp_1
Type: string
Default: nil

визначено типи цифрових носіїв інформації, доступ до яких обмежено;

No: 2
Name: mp_2_odp_2
Type: string
Default: nil

визначено персонал або ролі, уповноважені на доступ до цифрових носіїв інформації;

No: 3
Name: mp_2_odp_3
Type: string
Default: nil

визначено типи нецифрових носіїв інформації, доступ до яких обмежено;

No: 4
Name: mp_2_odp_4
Type: string
Default: nil

визначено персонал або ролі, уповноважені на доступ до нецифрових носіїв інформації;

No: 5
Name: mp_2_1
Type: string
Default: nil

доступ до <MP-02_ODP[01] типів цифрових носіїв інформації> обмежено для <MP-02_ODP[02] персоналу або ролей>;

No: 6
Name: mp_2_2
Type: string
Default: nil

доступ до <MP-02_ODP[03] типів нецифрових носіїв інформації> обмежено для <MP-02_ODP[04] персоналу або ролей>;

10.2.1. АВТОМАТИЗОВАНИЙ ОБМЕЖЕННИЙ ДОСТУП (MP-2(1)) [Вилучено]

[Вилучено: Включено до MP-04(02)]

Немає параметрів для цього контролю.

10.2.2. КРИПТОГРАФІЧНИЙ ЗАХИСТ (MP-2(2)) [Вилучено]

[Вилучено: Включено до SC-28(01)]

Немає параметрів для цього контролю.

10.3. МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-3)

a. Наносити на носії інформації маркування, що вказують на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації.
b. Звільнити [Призначення: визначені організацією типи носіїв системи] від маркування, якщо носії залишаються в межах [Призначення: визначених організацією контрольованих зон].

No: 1
Name: mp_3_odp_1
Type: string
Default: nil

визначено типи носіїв інформації, які звільняються від маркування під час перебування на контрольованих зонах;

No: 2
Name: mp_3_odp_2
Type: string
Default: nil

визначено контрольовані зони, де носії інформації звільняються від маркування;

No: 3
Name: mp_3_a
Type: string
Default: nil

носії інформації маркуються, щоб вказати на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації;

No: 4
Name: mp_3_b
Type: string
Default: nil

<MP-03_ODP[01] типи носіїв інформації> залишаються в

10.4. ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-4)

a. Фізично контролювати та безпечно зберігати [Призначення: визначені організацією типи цифрових та/або нецифрових носіїв інформації] в межах [Призначення: визначених організацією контрольованих зон].
b. Захищати системні носії, які визначені в MP-4 до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.

No: 1
Name: mp_4_odp_1
Type: string
Default: nil

визначено типи цифрових носіїв інформації, які підлягають фізичному контролю (якщо вибрано);

No: 2
Name: mp_4_odp_2
Type: string
Default: nil

визначено типи нецифрових носіїв інформації, які підлягають фізичному контролю (якщо вибрано);

No: 3
Name: mp_4_odp_3
Type: string
Default: nil

визначено типи цифрових носіїв інформації для безпечного зберігання (якщо вибрано);

No: 4
Name: mp_4_odp_4
Type: string
Default: nil

визначено типи нецифрових носіїв інформації для безпечного зберігання (якщо вибрано);

No: 5
Name: mp_4_odp_5
Type: string
Default: nil

визначено контрольовані зони, в яких можна безпечно зберігати цифрові носії інформації;

No: 6
Name: mp_4_odp_6
Type: string
Default: nil

визначено контрольовані зони, в яких можна безпечно зберігати нецифрові носії інформації;

No: 7
Name: mp_4_a_1
Type: string
Default: nil

<MP-04_ODP[01] типи цифрових носіїв> контролюються фізично;

No: 8
Name: mp_4_a_2
Type: string
Default: nil

«MP-04_ODP[02] типи нецифрових носіїв> контролюються фізично;

No: 9
Name: mp_4_a_3
Type: string
Default: nil

<MP-04_ODP[03] типи цифрових носіїв> безпечно зберігаються

No: 10
Name: mp_4_a_4
Type: string
Default: nil

<MP-04_ODP[04] типи нецифрових носіїв> безпечно

No: 11
Name: mp_4_b
Type: string
Default: nil

типи носіїв інформації (визначені в MP -04_ODP[01], MP 04_ODP[02], MP -04_ODP[03], MP -04_ODP[04]) захищені доти, доки носії інформації не будуть знищені або очищені за допомогою визначеного обладнання, методик та процедур.

10.4.1. КРИПТОГРАФІЧНИЙ ЗАХИСТ (MP-4(1)) [Вилучено]

[Вилучено: Включено до SC-28(01)]

Немає параметрів для цього контролю.

10.4.2. АВТОМАТИЗОВАНИЙ ОБМЕЖЕНИЙ ДОСТУП (MP-4(2))

Доступ до зон зберігання носіїв інформації обмежено за.

No: 1
Name: mp_4_2_odp_1
Type: string
Default: nil

визначено автоматизовані механізми обмеження доступу до зон зберігання носіїв інформації;

No: 2
Name: mp_4_2_odp_2
Type: string
Default: nil

визначено автоматизовані механізми реєстрації спроб доступу до зон зберігання носіїв інформації;

No: 3
Name: mp_4_2_odp_3
Type: string
Default: nil

визначено автоматизовані механізми реєстрації доступу, наданого до зон зберігання носіїв інформації;

No: 4
Name: mp_4_2_1
Type: string
Default: nil

доступ до зон зберігання носіїв інформації обмежено за

No: 5
Name: mp_4_2_2
Type: string
Default: nil

спроби доступу до зон зберігання носіїв інфор мації автоматизованих механізмів>;

No: 6
Name: mp_4_2_3
Type: string
Default: nil

доступ, наданий до зон зберігання носіїв, реєструється за

10.5. ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-5)

a. Захищати та контролювати [Призначення: визначені організацією типи носіїв системи] під час транспортування за межами контрольованих зон, використовуючи [Призначення: визначені організацією заходи безпеки].
b. Вести облік носіїв системи інформації під час транспортування за межами контрольованих зон.
c. Документувати дії, пов'язані з транспортуванням носіїв системи.
d. Обмежити діяльність уповноваженого персоналу, пов'язану з транспортуванням носіїв системи.

No: 1
Name: mp_5_odp_1
Type: string
Default: nil

визначено типи носіїв інформації системи для захисту та контролю під час транспортування за межі контрольованих зон;

No: 2
Name: mp_5_odp_2
Type: string
Default: nil

визначено заходи безпеки, що використовуються для захисту носіїв інформації системи поза контрольованими зонами;

No: 3
Name: mp_5_odp_3
Type: string
Default: nil

визначено заходи безпеки, що використовуються для контролю носіїв інформації системи за межами контрольованих зон;

No: 4
Name: mp_5_a_1
Type: string
Default: nil

<MP-05_ODP[01] типи носіїв інформації системи> захищаються під час транспортування за межі контрольованих зон за допомогою

No: 5
Name: mp_5_a_2
Type: string
Default: nil

<MP-05_ODP[01] типи носіїв інформації системи> контролюються під час транспортування за межі контрольованих

No: 6
Name: mp_5_b
Type: string
Default: nil

під час транспортування за межі контрольованих зон ведеться облік носіїв інформації системи;

No: 7
Name: mp_5_c
Type: string
Default: nil

діяльність, пов'язана з транспортуванням носіїв інформації системи, задокументована;

No: 8
Name: mp_5_d_1
Type: string
Default: nil

визначено персонал, уповноважений здійснювати діяльність з транспортування носіїв інформації;

No: 9
Name: mp_5_d_2
Type: string
Default: nil

діяльність, пов'язана з транспортуванням носіїв інформації системи, обмежується визначеним уповноваженим персоналом.

10.5.1. ЗАХИСТ ПОЗА КОНТРОЛЬОВАНИМИ ЗОНАМИ (MP-5(1)) [Вилучено]

[Вилучено: Включено до MP-05]

Немає параметрів для цього контролю.

10.5.2. ДОКУМЕНТУВАННЯ ДІЙ (MP-5(2)) [Вилучено]

[Вилучено: Включено до MP-05]

Немає параметрів для цього контролю.

10.5.3. ЗБЕРІГАЧІ (MP-5(3))

Визначено зберігачів інформації під час транспортування носіїв інформації системи за межі контрольованих зон.

No: 1
Name: mp_5_3_1
Type: string
Default: nil

визначено зберігачів інформації під час транспортування носіїв інформації системи за межі контрольованих зон.

No: 2
Name: mp_5_3_2
Type: string
Default: nil

залучено визначених зберігачів інформації під час транспорту341 вання носіїв інформації системи за межі контрольованих зон.

10.5.4. КРИПТОГРАФІЧНИЙ ЗАХИСТ (MP-5(4)) [Вилучено]

[Вилучено: Включено до SC-28(01)]

Немає параметрів для цього контролю.

10.6. ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ (MP-6)

a. Очищувати [Призначення: визначені організацією системні носії] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [Призначення: методами та процедурами очищення, визначеними організацією].
b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.

No: 1
Name: mp_6_odp_1
Type: string
Default: nil

визначено носії інформації системи, які підлягають очищенню перед утилізацією;

No: 2
Name: mp_6_odp_2
Type: string
Default: nil

визначено носії інформації системи, які підлягають очищенню перед випуском за межі контрольованої зони;

No: 3
Name: mp_6_odp_3
Type: string
Default: nil

визначені носії інформації системи, що підлягають очищенню перед повторним використанням;

No: 4
Name: mp_6_odp_4
Type: string
Default: nil

визначено методи та процедури очищення, які слід використовувати для очищення перед утилізацією;

No: 5
Name: mp_6_odp_5
Type: string
Default: nil

визначено методи та процедури очищення, які слід використовувати для очищення перед вип уском за межі контрольованої зони;

No: 6
Name: mp_6_odp_6
Type: string
Default: nil

визначено методи та процедури очищення, які слід використовувати для очищення перед повторним використанням;

No: 7
Name: mp_6_a_1
Type: string
Default: nil

<MP-06_ODP[01] носії інформації системи> перед утилізацією та процедур очищення>;

No: 8
Name: mp_6_a_2
Type: string
Default: nil

<MP-06_ODP[02] носії інформації системи> очищаються за перед випуском за межі контрольованої зони;

No: 9
Name: mp_6_a_3
Type: string
Default: nil

<MP-06_ODP[03] носії інформації системи> очищуються за перед повторним використанням;

No: 10
Name: mp_6_b
Type: string
Default: nil

застосовуються механізми очищення, надійність і цілісність яких відповідає категорії безпеки або рівню секретності інформації.

10.6.1. ПЕРЕГЛЯДАТИ, ЗАТВЕРДЖЕННЯ, ВІДСТЕЖЕННЯ, ДОКУМЕНТУВАННЯ ТА ПЕРЕВІРКА (MP-6(1))

Переглядаються заходи з очищення та утилізації носіїв інформації;.

No: 1
Name: mp_6_1_1
Type: string
Default: nil

переглядаються заходи з очищення та утилізації носіїв інформації;

No: 2
Name: mp_6_1_2
Type: string
Default: nil

затверджуються заходи з очищення та утилізації носіїв інформації;

No: 3
Name: mp_6_1_3
Type: string
Default: nil

відстежуються заходи з очищення та утилізації носіїв інформації;

No: 4
Name: mp_6_1_4
Type: string
Default: nil

документуються заходи з очищення та утилізації носіїв інформації;

No: 5
Name: mp_6_1_5
Type: string
Default: nil

перевіряються заходи з очищення та утилізації носіїв інформації;

10.6.2. ПЕРЕВІРКА ОБЛАДНАННЯ (MP-6(2))

Обладнання для очищення тестується <MP06(02)_ODP[01] частота> , щоб переконатися в досягненні запланованого очищення;.

No: 1
Name: mp_6_2_odp_1
Type: string
Default: nil

визначена частота, з якою проводиться перевірка обладнання для очищення;

No: 2
Name: mp_6_2_odp_2
Type: string
Default: nil

визначено частоту, з якою потрібно перевіряти процедури очищення;

No: 3
Name: mp_6_2_1
Type: string
Default: nil

обладнання для очищення тестується <MP06(02)_ODP[01] частота> , щоб переконатися в досягненні запланованого очищення;

No: 4
Name: mp_6_2_2
Type: string
Default: nil

процедури санітарної обробки тестуються <MP06(02)_ODP[02] частота> , щоб переконатися в досягненні запланованого очищення.

10.6.3. НЕРУЙНІВНІ МЕТОДИ (MP-6(3))

Застосовуються методи неруйнівного очищення до зовнішніх носіїв інформації перед підключенням таких пристроїв до системи при <MP-06(03)_ODP умовах>, що вимагають очищення зовнішніх носіїв інформації.

No: 1
Name: mp_6_3_odp
Type: string
Default: nil

визначено умови, які вимагають очищення зовнішніх носіїв інформації;

No: 2
Name: mp_6_3_01

Type: string
Default: nil

застосовуються методи неруйнівного очищення до зовнішніх носіїв інформації перед підключенням таких пристроїв до системи при <MP-06(03)_ODP умовах>, що вимагають очищення зовнішніх носіїв інформації.

10.6.4. КЕРОВАНА НЕСЕКРЕТНА ІНФОРМАЦІЯ (MP-6(4)) [Вилучено]

[Вилучено: Включено до MP-06]

Немає параметрів для цього контролю.

10.6.5. СЕКРЕТНА ІНФОРМАЦІЯ (MP-6(5)) [Вилучено]

[Вилучено: Включено до MP-06]

Немає параметрів для цього контролю.

10.6.6. ЗНИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-6(6)) [Вилучено]

[Вилучено: Включено до MP-06]

Немає параметрів для цього контролю.

10.6.7. ПОДВІЙНА АВТОРИЗАЦІЯ (MP-6(7))

Здійснюється подвійна авторизація для очищення <MP06(07)_ODP носії інформації>.

No: 1
Name: mp_6_7_odp
Type: string
Default: nil

визначено носії інформації для яких необхідно здійснювати подвійну авторизацію для очищення;

No: 2
Name: mp_6_7_01
Type: string
Default: nil

здійснюється подвійна авторизація для очищення <MP06(07)_ODP носії інформації>.

10.6.8. ВІДДАЛЕНЕ ОЧИЩЕННЯ АБО СТИРАННЯ ІНФОРМАЦІЇ (MP-6(8))

Передбачено можливість очищення або стирання інформації з <MP-06(08) _ ODP[01] систем або компонентів.

No: 1
Name: mp_6_8_odp_1

Type: string
Default: nil

визначено системи або компоненти системи для очищення або стирання інформації віддалено або за певних умов;

No: 2
Name: mp_6_8_odp_2
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ:

No: 3
Name: mp_6_8_odp_3
Type: string
Default: nil

визначаються умови, за яких інформація підлягає очищенню або стиранню (якщо вибрано);

No: 4
Name: mp_6_8_01
Type: string
Default: nil

передбачено можливість очищення або стирання інформації з <MP-06(08) _ ODP[01] систем або компонентів

10.7. ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-7)

a. [Вибір: обмежити; заборонити] використання [Призначення: визначених організацією типів носіїв системи] на [Призначення: визначені організацією системи або компоненти системи], використовуючи [Призначення: визначені організацією заходи безпеки].
b. Заборонити використання портативних пристроїв зберігання даних в системах організації, якщо такі пристрої не мають визначеного власника.

No: 1
Name: mp_7_b
Type: string
Default: nil

використання зовнішніх носіїв інформації в системах організації заборонено, якщо такі пристрої не мають власника, якого можна ідентифікувати.

10.7.1. ЗАБОРОНА ВИКОРИСТАННЯ БЕЗ ВИЗНАЧЕНОГО ВЛАСНИКА (MP-7(1)) [Вилучено]

[Вилучено: Включено до MP-07]

Немає параметрів для цього контролю.

10.7.2. ЗАБОРОНА ВИКОРИСТАННЯ (MP-7(2))

Ідентифіковано стійкі до очищення носії інформації;.

No: 1
Name: mp_7_2_1
Type: string
Default: nil

ідентифіковано стійкі до очищення носії інформації;

No: 2
Name: mp_7_2_2
Type: string
Default: nil

використання стійких до очищення носіїв інформації в системах організації заборонено.

10.8. ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ (MP-8)

a. сплануйте розташування або ділянку об'єкта, де знаходиться система, враховуючи фізичні та екологічні ризики;
b. для існуючих об'єктів врахуйте фізичні та екологічні ризики в організаційній стратегії управління ризиками.

No: 1
Name: mp_8_odp_1
Type: string
Default: nil

визначено процес зниження категорії безпеки носіїв інформації;

No: 2
Name: mp_8_odp_2
Type: string
Default: nil

визначено носії інформації системи, що вимагають зниження категорії безпеки;

No: 3
Name: mp_8_a_1
Type: string
Default: nil

встановлено <MP-08_ODP[01] процес зниження категорії безпеки носіїв інформаці>;

No: 4
Name: mp_8_a_2
Type: string
Default: nil

<MP-08_ODP[01] процес зниження категорії безпеки носіїв інформаці> охоплює використання механізмів зниження грифа секретності носіїв інформації за стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації;

No: 5
Name: mp_8_b_1
Type: string
Default: nil

здійснюється перевірка того, що процес зниження категорії безпеки носіїв інформації відповідає категорії безпеки та/або рівню секретності інформації, що підлягає видаленню;

No: 6
Name: mp_8_b_2
Type: string
Default: nil

здійснюється перевірка того, що процес зниження категорії безпеки носіїв інформації співмірний з правами доступу потенційних одержувачів пониженої інформації;

No: 7
Name: mp_8_c
Type: string
Default: nil

визначено <MP-08_ODP[02] носії інформації системи, що потребують пониження статусу>;

No: 8
Name: mp_8_d
Type: string
Default: nil

визначений носій інформації понижено у категорії безпеки за безпеки носіїв інформації>.

10.8.1. ДОКУМЕНТУВАННЯ ПРОЦЕСУ (MP-8(1))

Документуються дії зі зниження категорії безпеки носіїв інформації.

No: 1
Name: mp_8_1_01
Type: string
Default: nil

документуються дії зі зниження категорії безпеки носіїв інформації.

10.8.2. ПЕРЕВІРКА ОБЛАДНАННЯ (MP-8(2))

Обладнання для заниження категорії безпеки перевіряється.

No: 1
Name: mp_8_2_odp_1
Type: string
Default: nil

визначено частоту, з якою потрібно перевіряти обладнання для заниження категорії безпеки ;

No: 2
Name: mp_8_2_odp_2
Type: string
Default: nil

визначено частоту, з якою потрібно перевіряти процедури для заниження категорії безпеки ;

No: 3
Name: mp_8_2_1
Type: string
Default: nil

обладнання для заниження категорії безпеки перевіряється

No: 4
Name: mp_8_2_2
Type: string
Default: nil

процедури для заниження категорії безпеки перевіряється

10.8.3. КРИТИЧНА ІНФОРМАЦІЯ (MP-8(3))

Визначено критичну інформацію за наявності якої на носії інформації, знижують категорію безпеки до рівня публічного доступу.

No: 1
Name: mp_8_3_1
Type: string
Default: nil

визначено критичну інформацію за наявності якої на носії інформації, знижують категорію безпеки до рівня публічного доступу.

No: 2
Name: mp_8_3_2
Type: string
Default: nil

знижується категорія безпеки носіїв інформації, що містять визначену критичну інформацію до рівня публічного доступу.

10.8.4. ТАЄМНА ІНФОРМАЦІЯ (MP-8(4))

Забезпечити безпечне зниження категорії безпеки носіїв для таємної інформації.

No: 1
Name: mp_8_4_1
Type: string
Default: nil

ідентифіковано носії інформації, що містять інформацію з обмеженим доступом;

No: 2
Name: mp_8_4_2
Type: string
Default: nil

носії інформації, що містять інформацію з обмеженим доступом, знижуються в класі перед передачею особам, які не мають необхідних дозволів на доступ.

11. PE

Клас заходів захисту PE — ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО

Опис Цей клас охоплює заходи контролю фізичного доступу до об’єктів організації та захисту обладнання від загроз навколишнього середовища.

Перелік заходів захисту Політика та процедури фізичного захисту та захисту робочого середовища (PE-1); Авторизація фізичного доступу (PE-2); Доступ на основі посади або ролі (PE-2(1)); Дві форми ідентифікації (PE-2(2)); Безперервна охорона (PE-3(3)); Шафи з блокуванням (PE-3(4)); Керування фізичним доступом (PE-3); Доступ до системи (PE-3(1)); Межі об'єкту та системи (PE-3(2)); Керування фізичним доступом — захист від злому (PE-3(5)); Тестування на можливість проникнення (PE-3(6)); Фізичні перешкоди (PE-3(7)); КОНТРОЛЬ ДОСТУПУ У ВЕСТИБЮЛІ (ХОЛІ) (PE-3(8)); Ліній електроживлення (PE-4); Контроль доступу в приміщення для відображення інформації (PE-5); Доступ до вихідних даних уповноваженими особами (PE-5(1)) [Вилучено]; Доступ до вихідних даних фізичними особами (PE-5(2)); Маркування пристроїв виведення інформації (PE-5(3)) [Вилучено]; Моніторинг фізичного доступу (PE-6); Охоронна сигналізація та обладнання для спостереження (PE-6(1)); Моніторинг фізичного доступу — автоматичні розпізнавання вторгнень і відповідна реакція (PE-6(2)); Відеоспостереження (PE-6(3)); Моніторинг фізичного доступу до системи (PE-6(4)); Контроль відвідувачів (PE-7); Реєстр доступу відвідувачів (PE-8); Реєстри доступу відвідувачів — обмеження інформації, що ідентифікує особу (PE-8(3)); Енергетичне обладнання та кабелі (PE-9); Резервні кабелі (PE-9(1)); Автоматичне керування напругою (PE-9(2)); Аварійне відключення (PE-10); Випадкова і несанкціонована активація (PE-10(1)) [Вилучено]; Аварійне енергозабезпечення (PE-11); Довгострокове альтернативне джерело живлення - мінімальні експлуатаційні можливості (PE-11(1)); Довгострокове альтернативне джерело живлення – автономне живлення (PE-11(2)); Аварійне освітлення (PE-12); Основні завдання та функції (PE-12(1)); Протипожежний захист (PE-13); Пристрої та системи виявлення (PE-13(1)); Пристрої та системи автоматичного пожежогасіння (PE-13(2)); Автоматичне пожежогасіння (PE-13(3)) [Вилучено]; Перевірки (PE-13(4)); Контроль температури та вологості (PE-14); Автоматичний контроль (PE-14(1)); Моніторинг за допомогою сигналізацій та сповіщень (PE-14(2)); Захист від пошкодження водою (PE-15); Автоматична підтримка (PE-15(1)); Доставка та видалення (PE-16); Альтернативне робоче місце (PE-17); Розташування компонентів системи (PE-18); Місце розміщення об'єкта (PE-18(1)) [Вилучено]; Витік інформації (PE-19); Національні політики та процедури щодо пемв (PE-19(1)); Моніторинг і відстеження активів (PE-20); Захист від електромагнітного імпульсу (PE-21); Маркування компонентів (PE-22); Розташування об'єкта (PE-23).

11.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ФІЗИЧНОГО ЗАХИСТУ ТА ЗАХИСТУ РОБОЧОГО СЕРЕДОВИЩА (PE-1)

Розроблено та задокументо вано політику фізичного захисту та захисту робочого середовища;.

No: 1
Name: pe_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, до яких має бути доведена політика фізичного захисту та захисту робочого середовища;

No: 2
Name: pe_1_odp_2
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури фізичного захисту та захисту робочого середовища;

No: 3
Name: pe_1_odp_3
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};

No: 4
Name: pe_1_odp_4
Type: string
Default: nil

визначено посадову особу, яка керуватиме політикою та процедурами фізичного захисту та захисту робочого середовища;

No: 5
Name: pe_1_odp_5
Type: string
Default: nil

визначено частоту, з якою переглядається та оновлюється поточна політика фізичного захисту та захисту робочого середовища;

No: 6
Name: pe_1_odp_6
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення поточної політики фізичного захисту та захисту робочого середовища;

No: 7
Name: pe_1_odp_7
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються поточні процедури фізичного захисту та захисту робочого середовища;

No: 8
Name: pe_1_odp_8
Type: string
Default: nil

визначено події, які потребують перегляду та оновлення процедур фізичного захисту та захисту робочого середовища;

No: 9
Name: pe_1_a_1
Type: string
Default: nil

розроблено та задокументо вано політику фізичного захисту та захисту робочого середовища;

No: 10
Name: pe_1_a_2
Type: string
Default: nil

політика фізичного захисту та захисту робочого середовища

No: 11
Name: pe_1_a_3

Type: string
Default: nil

розроблені та задокументовані процедури фізичного захисту та захисту робочого середовища, що сприяють впровадженню політики фізичного захисту та захисту робочого середовища, а також пов'язані з ними заходи захисту;

No: 12
Name: pe_1_a_4
Type: string
Default: nil

процедури фізичного захисту та захисту робочого середовища

No: 13
Name: pe_1_a_1_a_1
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить мету;

No: 14
Name: pe_1_a_1_a_2
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить сферу застосування;

No: 15
Name: pe_1_a_1_a_3
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить ролі;

No: 16
Name: pe_1_a_1_a_4
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить обов'язки;

No: 17
Name: pe_1_a_1_a_5
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить відповідальність керівництва;

No: 18
Name: pe_1_a_1_a_6
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить координацію між підрозділами організації;

No: 19
Name: pe_1_a_1_a_7

Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища містить систему контролю відповідності;

No: 20
Name: pe_1_a_1_b
Type: string
Default: nil

<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика фізичного захисту та захисту робочого середовища відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам;

No: 21
Name: pe_1_b
Type: string
Default: nil

<PE-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур фізичного захисту та захисту робочого середовища;

No: 22
Name: pe_1_c_1_1
Type: string
Default: nil

переглядається та оновлюється поточна політика фізичного захисту та захисту робочого середовища <PE-01_ODP[05] частота>;

No: 23
Name: pe_1_c_1_2
Type: string
Default: nil

поточна політика фізичного захисту та захисту робочого середовища переглядається та оновлюється після <PE-01_ODP[06] подій>;

No: 24
Name: pe_1_c_2_1
Type: string
Default: nil

переглядаються та оновлюються поточні процедури фізичного

No: 25
Name: pe_1_c_2_2
Type: string
Default: nil

поточні процедури фізичного та екологічного захисту переглядаються та оновлюються після <PE-01_ODP[08] подій>.

11.2. АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ (PE-2)

Розроблено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;.

No: 1
Name: pe_2_odp
Type: string
Default: nil

визначено періодичність перегляду списку доступу, у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об'єкта;

No: 2
Name: pe_2_a_1
Type: string
Default: nil

розроблено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;

No: 3
Name: pe_2_a_2
Type: string
Default: nil

затверджено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;

No: 4
Name: pe_2_a_3
Type: string
Default: nil

ведеться перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;

No: 5
Name: pe_2_b
Type: string
Default: nil

для доступу до об'єкта надаються повноваження;

No: 6
Name: pe_2_c
Type: string
Default: nil

переглядається список доступу, у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об'єкта <PE-02_ODP частота>;

No: 7
Name: pe_2_d
Type: string
Default: nil

особи видаляються зі списку доступу до об'єкта, коли доступ більше не потрібен.

11.2.1. ДОСТУП НА ОСНОВІ ПОСАДИ АБО РОЛІ (PE-2(1))

Доступ на основі посади або ролі (pe-2(1)).

Немає параметрів для цього контролю.

11.2.2. ДВІ ФОРМИ ІДЕНТИФІКАЦІЇ (PE-2(2))

Вимагається дві форми ідентифікації від <PE-02(02)_ODP списку прийнятних форм ідентифікації> для доступу відвідувачів до об'єкта, де знаходиться система.

No: 1
Name: pe_2_2_odp
Type: string
Default: nil

визначено список прийнятних форм ідентифікації

No: 2
Name: pe_2_2_01
Type: string
Default: nil

вимагається дві форми ідентифікації від <PE-02(02)_ODP списку прийнятних форм ідентифікації> для доступу відвідувачів до об'єкта, де знаходиться система.

11.3. КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ (PE-3)

Авторизація фізичного доступу забезпечується в <PE-03_ODP[01] пунктах входу і виходу> шляхом перевірки індивідуальних дозволів доступу;.

No: 1
Name: pe_3_odp_1
Type: string
Default: nil

визначено точки входу та виходу в об'єкт, в якому знаходиться система;

No: 2
Name: pe_3_odp_2
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРА-

No: 3
Name: pe_3_odp_3
Type: string
Default: nil

визначено фізичні системи або пристрої контролю доступу, що використовуються для контролю входу та виходу на об'єкт (якщо вибрано);

No: 4
Name: pe_3_odp_4
Type: string
Default: nil

визначено точки входу або виходу, для яких ведуться журнали контролю фізичного доступу;

No: 5
Name: pe_3_odp_5

Type: string
Default: nil

визначено заходи захисту для контролю доступу в зони всередині об'єкту, позначені як загальнодоступні;

No: 6
Name: pe_3_odp_6
Type: string
Default: nil

визначено умови, що вимагають супроводу відвідувачів та моніторингу активності відвідувачів;

No: 7
Name: pe_3_odp_7
Type: string
Default: nil

визначені пристрої фізичного доступу, що підлягають інвентаризації;

No: 8
Name: pe_3_odp_8
Type: string
Default: nil

визначено частоту проведення інвентаризації пристроїв фізичного доступу;

No: 9
Name: pe_3_odp_9
Type: string
Default: nil

визначено частоту, з якою потрібно змінювати коди доступу;

No: 10
Name: pe_3_odp_10
Type: string
Default: nil

визначено частоту, з якою потрібно змінювати ключі;

No: 11
Name: pe_3_a_1
Type: string
Default: nil

авторизація фізичного доступу забезпечується в <PE-03_ODP[01] пунктах входу і виходу> шляхом перевірки індивідуальних дозволів доступу;

No: 12
Name: pe_3_a_2
Type: string
Default: nil

авторизація фізичного доступу здійснюється у <PE-03_ODP[01] точках входу та виходу> шляхом управління входом та виходом ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;

No: 13
Name: pe_3_b
Type: string
Default: nil

журнали контролю фізичного доступу ведуться для <PE03_ODP[04] точок входу або виходу>;

No: 14
Name: pe_3_c

Type: string
Default: nil

доступ в зони всередині об'єкту, визначені як загальнодоступні, захисту>;

No: 15
Name: pe_3_d_1
Type: string
Default: nil

відвідувачів супроводжують;

No: 16
Name: pe_3_d_2
Type: string
Default: nil

активність відвідувачів контролюється <PE-03_ODP[06] умови>;

No: 17
Name: pe_3_e_1
Type: string
Default: nil

ключі захищені;

No: 18
Name: pe_3_e_2
Type: string
Default: nil

коди доступу захищені;

No: 19
Name: pe_3_e_3
Type: string
Default: nil

інші пристрої фізичного доступу захищені;

No: 20
Name: pe_3_f
Type: string
Default: nil

<PE-03_ODP[07] пристрої фізичного доступу> інвентаризуються

No: 21
Name: pe_3_g_1
Type: string
Default: nil

коди доступу змінюється <PE-03_ODP[09] частота> , коли код скомпрометовано, або коли особи, які володіють кодом, переводяться або звільняються;

No: 22
Name: pe_3_g_2
Type: string
Default: nil

ключі змінюються <PE-03_ODP[10] частота>, коли ключі втрачено, або коли особи, що володіють ключами, переводяться або звільняються.

11.3.1. ДОСТУП ДО СИСТЕМИ (PE-3(1))

Фізичні авторизації доступу до системи є обов'язковими;.

No: 1
Name: pe_3_1_odp
Type: string
Default: nil

визначено фізичні приміщення, що містять один або декілька компонентів системи;

No: 2
Name: pe_3_1_1
Type: string
Default: nil

фізичні авторизації доступу до системи є обов'язковими;

No: 3
Name: pe_3_1_2
Type: string
Default: nil

для об'єкта застосовуються засоби контролю фізичного доступу в <PE-03(01)_ODP фізичні приміщення>.

11.3.2. МЕЖІ ОБ'ЄКТУ ТА СИСТЕМИ (PE-3(2))

Перевірки безпеки проводяться <PE-03(02)_ODP частота> на фізичному периметрі об'єкта або системи на предмет витоку інформації або вилучення компонентів системи.

No: 1
Name: pe_3_2_odp
Type: string
Default: nil

не визначено частоту проведення перевірок безпеки на фізичній межі об'єкта або системи на предмет витоку інформації або вилучення компонентів системи;

No: 2
Name: pe_3_2_01
Type: string
Default: nil

перевірки безпеки проводяться <PE-03(02)_ODP частота> на фізичному периметрі об'єкта або системи на предмет витоку інформації або вилучення компонентів системи.

11.3.3. БЕЗПЕРЕРВНА ОХОРОНА (PE-3(3))

Доступ без супроводу до приміщення, де знаходиться система, обмежено для персоналу з <PE-02(03)_ODP[01] ВИБРАНИМ ЗНАЧЕННЯМ ПАРАМЕТРА(ів)>.

No: 1
Name: pe_2_3_odp_1
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень допуску для всієї інформації, що міститься в системі; авторизація офіційного доступу до всієї інформації, що міститься в системі; необхідність

No: 2
Name: pe_2_3_odp_2
Type: string
Default: nil

визначено повноваження фізичного доступу для доступу без супроводу до об'єкта, де знаходиться система (якщо вибрано);

No: 3
Name: pe_2_3_01
Type: string
Default: nil

доступ без супроводу до приміщення, де знаходиться система, обмежено для персоналу з <PE-02(03)_ODP[01] ВИБРАНИМ ЗНАЧЕННЯМ ПАРАМЕТРА(ів)>.

11.3.4. ШАФИ З БЛОКУВАННЯМ (PE-3(4))

Шафи з блокуванням (pe-3(4)).

Немає параметрів для цього контролю.

11.3.5. КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ — ЗАХИСТ ВІД ЗЛОМУ (PE-3(5))

<PE-03(05)_ODP[01] заходи захисту> застосовуються для системи.

No: 1
Name: pe_3_5_odp_1
Type: string
Default: nil

визначено заходи захисту від фізичної підробки або підміни;

No: 2
Name: pe_3_5_odp_2
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {виявлення; запобігання};

No: 3
Name: pe_3_5_odp_3
Type: string
Default: nil

визначено апаратні компоненти, які мають бути захищені від фізичної підробки або підміни;

No: 4
Name: pe_3_5_01
Type: string
Default: nil

<PE-03(05)_ODP[01] заходи захисту> застосовуються для системи.

11.3.6. ТЕСТУВАННЯ НА МОЖЛИВІСТЬ ПРОНИКНЕННЯ (PE-3(6))

Тестування на можливість проникнення (pe-3(6)).

Немає параметрів для цього контролю.

11.3.7. ФІЗИЧНІ ПЕРЕШКОДИ (PE-3(7))

Фізичні перешкоди (pe-3(7)).

Немає параметрів для цього контролю.

11.3.8. КОНТРОЛЬ ДОСТУПУ У ВЕСТИБЮЛІ (ХОЛІ) (PE-3(8))

Контроль доступу використовуються в < PE-03(08)_ODP місцях>.

No: 1
Name: pe_3_8_odp
Type: string
Default: nil

визначено місця на об'єкті, де необхідний контроль доступу;

No: 2
Name: pe_3_8_01
Type: string
Default: nil

контроль доступу використовуються в < PE-03(08)_ODP місцях>.

11.4. ЛІНІЙ ЕЛЕКТРОЖИВЛЕННЯ (PE-4)

Фізичний доступ до <PE-04_ODP[01] систем розподілу та постачання живлення> в межах об'єктів організації контролюється.

No: 1
Name: pe_4_odp_1
Type: string
Default: nil

визначені системи розподілу та постачання живлення, які потребують фізичного контролю доступу;

No: 2
Name: pe_4_odp_2
Type: string
Default: nil

визначено заходи захисту, які необхідно впровадити для контролю фізичного доступу до систем розподілу та постачання живлення в межах об'єкту організації;

No: 3
Name: pe_4_01
Type: string
Default: nil

фізичний доступ до <PE-04_ODP[01] систем розподілу та постачання живлення> в межах об'єктів організації контролюється

11.5. КОНТРОЛЬ ДОСТУПУ В ПРИМІЩЕННЯ ДЛЯ ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ (PE-5)

Керування фізичним доступом до вихідних даних здійснюється з <PE-05_ODP пристроїв для виведення інформації >, для запобігання несанкціонованого отримання користувачами вихідних даних.

No: 1
Name: pe_5_odp
Type: string
Default: nil

визначено пристрої для виведення інформації над якими необхідний контроль над фізичним доступом до вихідних даних;

No: 2
Name: pe_5_01
Type: string
Default: nil

керування фізичним доступом до вихідних даних здійснюється з <PE-05_ODP пристроїв для виведення інформації >, для запобігання несанкціонованого отримання користувачами вихідних даних.

11.5.1. ДОСТУП ДО ВИХІДНИХ ДАНИХ УПОВНОВАЖЕНИМИ ОСОБАМИ (PE-5(1)) [Вилучено]

[Вилучено: включено до PE-05].

Немає параметрів для цього контролю.

11.5.2. ДОСТУП ДО ВИХІДНИХ ДАНИХ ФІЗИЧНИМИ ОСОБАМИ (PE-5(2))

пов'язуються дані про цифрову ідентичність з підтвердженням отримання даних від вихідних пристроїв;

No: 1
Name: pe_5_2
Type: string
Default: nil

пов'язуються дані про цифрову ідентичність з підтвердженням отримання даних від вихідних пристроїв;

11.5.3. МАРКУВАННЯ ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ (PE-5(3)) [Вилучено]

[Вилучено: включено до PE-22].

Немає параметрів для цього контролю.

11.6. МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ (PE-6)

Фізичний доступ до об'єкту, де знаходиться система, моніториться з метою виявлення та реагування на інциденти фізичної безпеки;.

No: 1
Name: pe_6_odp_1
Type: string
Default: nil

визначено частоту перегляду журналів фізичного доступу;

No: 2
Name: pe_6_odp_2
Type: string
Default: nil

визначено події або потенційні ознаки подій, що вимагають перегляду журналів фізичного доступу;

No: 3
Name: pe_6_a
Type: string
Default: nil

фізичний доступ до об'єкту, де знаходиться система, моніториться з метою виявлення та реагування на інциденти фізичної безпеки;

No: 4
Name: pe_6_b_1
Type: string
Default: nil

переглядаються журнали фізичного доступу <PE-06_ODP[01] частота>;

No: 5
Name: pe_6_b_2
Type: string
Default: nil

журнали фізичного доступу переглядаються при виникненні <PE06_ODP[02] подій>;

No: 6
Name: pe_6_c_1
Type: string
Default: nil

результати переглядів узгоджуються з можливостями організації щодо реагування на інциденти;

No: 7
Name: pe_6_c_2

Type: string
Default: nil

результати розслідувань узгоджуються з можливостями організації щодо реагування на інциденти;

11.6.1. ОХОРОННА СИГНАЛІЗАЦІЯ ТА ОБЛАДНАННЯ ДЛЯ СПОСТЕРЕЖЕННЯ (PE-6(1))

Охоронна сигналізація та обладнання для спостереження (pe-6(1)).

Немає параметрів для цього контролю.

11.6.2. МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ — АВТОМАТИЧНІ РОЗПІЗНАВАННЯ ВТОРГНЕНЬ І ВІДПОВІДНА РЕАКЦІЯ (PE-6(2))

Розпізнаються <PE-06(02)_ODP[01] класи або типи вторгнень>;.

No: 1
Name: pe_6_2_odp_1
Type: string
Default: nil

визначено класи або типи вторгнень, які мають розпізнаватися автоматизованими механізмами;

No: 2
Name: pe_6_2_odp_2
Type: string
Default: nil

визначено реакції, які мають ініціюватися автоматизованими механізмами при розпізнаванні визначених організацією класів або типів вторгнень;

No: 3
Name: pe_6_2_odp_3
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для розпізнавання класів або типів вторгнень та ініціювання дій реагування (визначені в PE06(02)_ODP);

No: 4
Name: pe_6_2_1
Type: string
Default: nil

розпізнаються <PE-06(02)_ODP[01] класи або типи вторгнень>;

No: 5
Name: pe_6_2_2
Type: string
Default: nil

<PE-06(02)_ODP[02] реакції> ініціюються за допомогою

11.6.3. ВІДЕОСПОСТЕРЕЖЕННЯ (PE-6(3))

ведеться відеоспостереження за <PE-06(03)_ODP[01] зонами>;
відеозаписи переглядаються <PE-06(03)_ODP[02] частота>;
відеозаписи зберігаються протягом <PE-06(03)_ODP[03] періоду часу>.

No: 1
Name: pe_6_3_odp_1
Type: string
Default: nil

визначено зони, де буде застосовуватися відеоспостереження;

No: 2
Name: pe_6_3_odp_2
Type: string
Default: nil

визначено частоту перегляду відеозаписів;

No: 3
Name: pe_6_3_odp_3
Type: string
Default: nil

визначено період часу, протягом якого необхідно зберігати відеозаписи;

No: 4
Name: pe_6_3_a
Type: string
Default: nil

ведеться відеоспостереження за <PE-06(03)_ODP[01] зонами>;

No: 5
Name: pe_6_3_b
Type: string
Default: nil

відеозаписи переглядаються <PE-06(03)_ODP[02] частота>;

No: 6
Name: pe_6_3_c
Type: string
Default: nil

відеозаписи зберігаються протягом <PE-06(03)_ODP[03] періоду часу>.

11.6.4. МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ ДО СИСТЕМИ (PE-6(4))

моніторинг фізичного доступу до системи здійснюється на додаток до моніторингу фізичного доступу до об'єкта в <PE-06(04)_ODP фізичні приміщення>.

No: 1
Name: pe_6_4_odp
Type: string
Default: nil

визначено фізичні приміщення, що містять один або більше компонентів системи;

No: 2
Name: pe_6_4_01
Type: string
Default: nil

моніторинг фізичного доступу до системи здійснюється на додаток до моніторингу фізичного доступу до об'єкта в <PE-06(04)_ODP фізичні приміщення>.

11.7. КОНТРОЛЬ ВІДВІДУВАЧІВ (PE-7)

Контроль відвідувачів.

Немає параметрів для цього контролю.

11.8. РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ (PE-8)

Записи про доступ відвідувачів для об'єкта, на якому знаходиться.

No: 1
Name: pe_8_odp_1
Type: string
Default: nil

визначено період часу, протягом якого зберігатимуться записи про доступ відвідувачів до об'єкта, на якому перебуває система;

No: 2
Name: pe_8_odp_2
Type: string
Default: nil

визначено частоту перегляду записів про доступ відвідувачів;

No: 3
Name: pe_8_odp_3
Type: string
Default: nil

визначено персонал, якому повідомляється про порушення записів про доступ відвідувачів;

No: 4
Name: pe_8_a
Type: string
Default: nil

записи про доступ відвідувачів для об'єкта, на якому знаходиться

No: 5
Name: pe_8_b
Type: string
Default: nil

переглядаються записи про доступ відвідувачів <PE-08_ODP[02] частота>;

No: 6
Name: pe_8_c
Type: string
Default: nil

про порушення записів про доступ відвідувачів повідомляється

11.8.1. РЕЄСТРИ ДОСТУПУ ВІДВІДУВАЧІВ — ОБМЕЖЕННЯ ІНФОРМАЦІЇ, ЩО ІДЕНТИФІКУЄ ОСОБУ (PE-8(3))

Інформація, що ідентифікує особу, яка міститься в реєстрах доступу відвідувачів, обмежується < PE-08(03)_ODP елементи>, визначеними в оцінці ризиків для конфіденційності.

No: 1
Name: pe_8_3_odp
Type: string
Default: nil

в оцінці ризиків для конфіденційності визначено елементи, що обмежуються в реєстрі відвідувачів

No: 2
Name: pe_8_3_01
Type: string
Default: nil

інформація, що ідентифікує особу, яка міститься в реєстрах доступу відвідувачів, обмежується < PE-08(03)_ODP елементи>, визначеними в оцінці ризиків для конфіденційності.

11.9. ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ (PE-9)

Енергетичне обладнання та кабелі.

Немає параметрів для цього контролю.

11.9.1. РЕЗЕРВНІ КАБЕЛІ (PE-9(1))

використовувати резервні силові кабельні системи, які фізично відокремлені на <PE-09(01)_ODP відстань>.

No: 1
Name: pe_9_1_odp
Type: string
Default: nil

визначено відстань, на яку повинні бути відокремлені резервні силові кабельні системи;

No: 2
Name: pe_9_1_01
Type: string
Default: nil

використовувати резервні силові кабельні системи, які фізично відокремлені на <PE-09(01)_ODP відстань>.

11.9.2. АВТОМАТИЧНЕ КЕРУВАННЯ НАПРУГОЮ (PE-9(2))

впроваджено механізми автоматичного керування напругою для <PE-09(02)_ODP критичних компонентів системи>.

No: 1
Name: pe_9_2_odp
Type: string
Default: nil

визначено критичні компоненти системи для яких необхідно впровадити механізми автоматичного керування напругою;

No: 2
Name: pe_9_2_01
Type: string
Default: nil

впроваджено механізми автоматичного керування напругою для <PE-09(02)_ODP критичних компонентів системи>.

11.10. АВАРІЙНЕ ВІДКЛЮЧЕННЯ (PE-10)

Передбачена можливість відключення живлення <PE-10_ODP[01] системи або окремих компонентів системи> в надзвичайних ситуаціях;.

No: 1
Name: pe_10_odp_1
Type: string
Default: nil

визначено систему або окремі компоненти системи, які потребують можливості вимкнення живлення в надзвичайних ситуаціях;

No: 2
Name: pe_10_odp_2
Type: string
Default: nil

визначено розташування перемикачів або пристроїв аварійного вимкнення в системі або компоненті системи;

No: 3
Name: pe_10_a
Type: string
Default: nil

передбачена можливість відключення живлення <PE-10_ODP[01] системи або окремих компонентів системи> в надзвичайних ситуаціях;

No: 4
Name: pe_10_b
Type: string
Default: nil

аварійні перемикачі або пристрої вимкнення розміщені в <PE10_ODP[02] розташування>, щоб забезпечити доступ для персоналу;

No: 5
Name: pe_10_c
Type: string
Default: nil

можливість аварійного вимкнення живлення захищена від несанкціонованої активації.

11.10.1. ВИПАДКОВА І НЕСАНКЦІОНОВАНА АКТИВАЦІЯ (PE-10(1)) [Вилучено]

[Виключено: включено до PE-10].

Немає параметрів для цього контролю.

11.11. АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ (PE-11)

Передбачено джерело безперебійного живлення для полегшення <PE-11_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> у випадку втрати основного джерела живлення.

No: 1
Name: pe_11_odp
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {впорядковане виключення системи; перехід системи на довгострокову альтернативну систему живлення};):

No: 2
Name: pe_11_01
Type: string
Default: nil

передбачено джерело безперебійного живлення для полегшення <PE-11_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> у випадку втрати основного джерела живлення.

No: 3
Name: pe_11_a
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, є автономним;

No: 4
Name: pe_11_b
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, не залежить від зовнішнього постачання енергії;

No: 5
Name: pe_11_c
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, здатне підтримувати <PE-11(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> у разі тривалої втрати основного джерела живлення.

11.11.1. ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ - МІНІМАЛЬНІ ЕКСПЛУАТАЦІЙНІ МОЖЛИВОСТІ (PE-11(1))

активується альтернативне джерело живлення, передбачене для системи <PE-11(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
альтернативне джерело живлення, передбачене для системи, може підтримувати мінімально необхідну працездатність у разі тривалої втрати основного джерела живлення.

No: 1
Name: pe_11_1_odp
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {вручну; автоматично};

No: 2
Name: pe_11_1_01
Type: string
Default: nil

активується альтернативне джерело живлення, передбачене для системи <PE-11(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 3
Name: pe_11_1_02
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, може підтримувати мінімально необхідну працездатність у разі тривалої втрати основного джерела живлення.

11.11.2. ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ – АВТОНОМНЕ ЖИВЛЕННЯ (PE-11(2))

активується альтернативне джерело живлення, передбачене для системи <PE-11(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
альтернативне джерело живлення, передбачене для системи, є автономним;
альтернативне джерело живлення, передбачене для системи, не залежить від зовнішнього постачання енергії;
альтернативне джерело живлення, передбачене для системи, здатне підтримувати <PE-11(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> у разі тривалої втрати основного джерела живлення.

No: 1
Name: pe_11_2_odp_1
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {вручну; автоматично};

No: 2
Name: pe_11_2_odp_2
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {мінімально необхідні операційні можливості; повна експлуатаційна здатність};

No: 3
Name: pe_11_2_01
Type: string
Default: nil

активується альтернативне джерело живлення, передбачене для системи <PE-11(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 4
Name: pe_11_2_a
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, є автономним;

No: 5
Name: pe_11_2_b
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, не залежить від зовнішнього постачання енергії;

No: 6
Name: pe_11_2_c
Type: string
Default: nil

альтернативне джерело живлення, передбачене для системи, здатне підтримувати <PE-11(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> у разі тривалої втрати основного джерела живлення.

11.12. АВАРІЙНЕ ОСВІТЛЕННЯ (PE-12)

Автоматичне аварійне освітлення, яке вмикається в разі відключення або збою в електропостачанні;.

No: 1
Name: pe_12_1
Type: string
Default: nil

автоматичне аварійне освітлення, яке вмикається в разі відключення або збою в електропостачанні;

No: 2
Name: pe_12_2
Type: string
Default: nil

підтримується автоматичне аварійне освітлення, яке вмикається в разі відключення або збою в електропостачанні;

No: 3
Name: pe_12_3
Type: string
Default: nil

автоматичне аварійне освітлення системи освітлює евакуаційні виходи в межах об'єкта;

No: 4
Name: pe_12_4

Type: string
Default: nil

автоматичне аварійне освітлення системи освітлює шляхи евакуації в межах об'єкта;

11.12.1. ОСНОВНІ ЗАВДАННЯ ТА ФУНКЦІЇ (PE-12(1))

аварійне освітлення передбачено для всіх зон, що підтримують виконання основних завдань і функцій.

No: 1
Name: pe_12_1
Type: string
Default: nil

аварійне освітлення передбачено для всіх зон, що підтримують виконання основних завдань і функцій.

11.13. ПРОТИПОЖЕЖНИЙ ЗАХИСТ (PE-13)

застосовуються системи пожежної сигналізації;
системи пожежної сигналізації підтримуються незалежним джерелом енергії;
підтримуються в робочому стані системи пожежної сигналізації;
застосовуються системи пожежогасіння;
системи пожежогасіння підтримуються незалежним джерелом енергії;
підтримуються в робочому стані системи пожежогасіння.

No: 1
Name: pe_13_01
Type: string
Default: nil

застосовуються системи пожежної сигналізації;

No: 2
Name: pe_13_02
Type: string
Default: nil

системи пожежної сигналізації підтримуються незалежним джерелом енергії;

No: 3
Name: pe_13_03
Type: string
Default: nil

підтримуються в робочому стані системи пожежної сигналізації;

No: 4
Name: pe_13_04
Type: string
Default: nil

застосовуються системи пожежогасіння;

No: 5
Name: pe_13_05
Type: string
Default: nil

системи пожежогасіння підтримуються незалежним джерелом енергії;

No: 6
Name: pe_13_06
Type: string
Default: nil

підтримуються в робочому стані системи пожежогасіння.

11.13.1. ПРИСТРОЇ ТА СИСТЕМИ ВИЯВЛЕННЯ (PE-13(1))

використовуються системи пожежної сигналізації, які автоматично спрацьовують у разі пожежі;
використовуються системи виявлення пожежі, які автоматично сповіщають персонал або ролі у разі виникнення пожежі;
використовуються системи виявлення пожежі, які автоматично сповіщають аварійні команди у разі виникнення пожежі.

No: 1
Name: pe_13_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, які мають бути повідомлені у випадку пожежі;

No: 2
Name: pe_13_1_odp_2
Type: string
Default: nil

визначено аварійні команди, які мають бути сповіщені у випадку пожежі;

No: 3
Name: pe_13_1_01
Type: string
Default: nil

використовуються системи пожежної сигналізації, які автоматично спрацьовують у разі пожежі;

No: 4
Name: pe_13_1_02
Type: string
Default: nil

використовуються системи виявлення пожежі, які автоматично сповіщають <PE-13(01)_ODP[01] персонал або ролі> у разі виникнення пожежі;

No: 5
Name: pe_13_1_03
Type: string
Default: nil

використовуються системи виявлення пожежі, які автоматично сповіщають <PE-13(01)_ODP[02] аварійні команди> у разі виникнення пожежі.

11.13.2. ПРИСТРОЇ ТА СИСТЕМИ АВТОМАТИЧНОГО ПОЖЕЖОГАСІННЯ (PE-13(2))

застосовуються системи пожежогасіння, які активуються автоматично;
використовуються системи пожежогасіння, які автоматично сповіщають персонал або ролі;
використовуються системи пожежогасіння, які автоматично сповіщають аварійні команди;

використовується автоматична система пожежогасіння, коли об'єкт не укомплектований відповідним персоналом на постійній основі.

No: 1
Name: pe_13_2_odp_1
Type: string
Default: nil

визначено персонал або ролі, які мають бути сповіщені у випадку пожежі;

No: 2
Name: pe_13_2_odp_2
Type: string
Default: nil

визначені аварійні команди, які повинні бути сповіщені в разі пожежі;

No: 3
Name: pe_13_2_a_01
Type: string
Default: nil

застосовуються системи пожежогасіння, які активуються автоматично;

No: 4
Name: pe_13_2_a_02
Type: string
Default: nil

використовуються системи пожежогасіння, які автоматично сповіщають <PE-13(02)_ODP[01] персонал або ролі>;

No: 5
Name: pe_13_2_a_03
Type: string
Default: nil

використовуються системи пожежогасіння, які автоматично сповіщають <PE-13(02)_ODP[02] аварійні команди>;

No: 6
Name: pe_13_2_b
Type: string
Default: nil

використовується автоматична система пожежогасіння, коли об'єкт не укомплектований відповідним персоналом на постійній основі.

11.13.3. АВТОМАТИЧНЕ ПОЖЕЖОГАСІННЯ (PE-13(3)) [Вилучено]

[Виключено: включено до PE-13(02)].

Немає параметрів для цього контролю.

11.13.4. ПЕРЕВІРКИ (PE-13(4))

об'єкт проходить перевірки пожежної безпеки уповноваженими та кваліфікованими інспекторами;

виявлені недоліки за результатами перевірок пожежної безпеки усуваються у визначений термін.

No: 1
Name: pe_13_4_odp_1
Type: string
Default: nil

визначено частоту проведення перевірок пожежної безпеки на об'єкті;

No: 2
Name: pe_13_4_odp_2
Type: string
Default: nil

визначено термін для усунення недоліків, виявлених перевірками пожежного нагляду;

No: 3
Name: pe_13_4_01
Type: string
Default: nil

об'єкт проходить перевірки пожежної безпеки <PE-13(04)_ODP[01] частота> уповноваженими та кваліфікованими інспекторами;

No: 4
Name: pe_13_4_02
Type: string
Default: nil

виявлені недоліки за результатами перевірок пожежної безпеки усуваються у <PE-13(04)_ODP[02] термін>.

11.14. КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ (PE-14)

Температура та вологость підтримуються на <PE-14_ODP[01] рівні> у приміщенні, де знаходиться система;.

No: 1
Name: pe_14_odp_1
Type: string
Default: nil

визначено прийнятні рівні для температури та вологості;

No: 2
Name: pe_14_odp_2
Type: string
Default: nil

визначено частоту моніторингу рівнів температури та вологості;

No: 3
Name: pe_14_a
Type: string
Default: nil

температура та вологость підтримуються на <PE-14_ODP[01] рівні> у приміщенні, де знаходиться система;

No: 4
Name: pe_14_b
Type: string
Default: nil

контролюються рівні температури та вологості <PE-14_ODP[02] частота>.

11.14.1. АВТОМАТИЧНИЙ КОНТРОЛЬ (PE-14(1))

впроваджено <PE-14(01)_ODP механізми> на об'єкті для запобігання потенційно шкідливим для системи коливанням.

No: 1
Name: pe_14_1_odp
Type: string
Default: nil

визначено механізми автоматичного регулювання температури та вологості;

No: 2
Name: pe_14_1_01
Type: string
Default: nil

впроваджено <PE-14(01)_ODP механізми> на об'єкті для запобігання потенційно шкідливим для системи коливанням.

11.14.2. МОНІТОРИНГ ЗА ДОПОМОГОЮ СИГНАЛІЗАЦІЙ ТА СПОВІЩЕНЬ (PE-14(2))

застосовується моніторинг температури та вологості;
функція моніторингу температури та вологості надає сигнал тривоги або повідомлення <PE-14(02)_ODP персоналу або ролям>, коли зміни є потенційно шкідливими для персоналу або обладнання.

No: 1
Name: pe_14_2_odp
Type: string
Default: nil

визначено персонал або ролі, які необхідно повідомляти в рамках моніторингу температури та вологості, коли зміни температури та вологості є потенційно шкідливими для персоналу або обладнання;

No: 2
Name: pe_14_2_01
Type: string
Default: nil

застосовується моніторинг температури та вологості;

No: 3
Name: pe_14_2_02
Type: string
Default: nil

функція моніторингу температури та вологості надає сигнал тривоги або повідомлення <PE-14(02)_ODP персоналу або ролям>, коли зміни є потенційно шкідливими для персоналу або обладнання.

11.15. ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ (PE-15)

Захист від пошкодження водою.

Немає параметрів для цього контролю.

11.15.1. АВТОМАТИЧНА ПІДТРИМКА (PE-15(1))

наявність води поблизу системи можна виявити автоматично;
<PE-15(01)_ODP[01] персонал або ролі> оповіщаються за допомогою <PE-15(01)_ODP[02] автоматизованих механізмів>.

No: 1
Name: pe_15_1_odp_1
Type: string
Default: nil

визначено персонал або ролі, які слід сповіщати, коли біля системи виявлено присутність води;

No: 2
Name: pe_15_1_odp_2
Type: string
Default: nil

визначено автоматизовані механізми, що використовуються для виявлення присутності води поблизу системи;

No: 3
Name: pe_15_1_01
Type: string
Default: nil

наявність води поблизу системи можна виявити автоматично;

No: 4
Name: pe_15_1_02
Type: string
Default: nil

<PE-15(01)_ODP[01] персонал або ролі> оповіщаються за допомогою <PE-15(01)_ODP[02] автоматизованих механізмів>.

11.16. ДОСТАВКА ТА ВИДАЛЕННЯ (PE-16)

<PE-16_ODP[01] типи компонентів системи> авторизуються при вході на об’єкт;.

No: 1
Name: pe_16_odp_1
Type: string
Default: nil

визначено типи компонентів системи, які підлягають авторизації та контролю при вході на об’єкт;

No: 2
Name: pe_16_odp_2
Type: string
Default: nil

визначено типи компонентів системи, які підлягають авторизації та контролю при виході з об'єкта;

No: 3
Name: pe_16_a_1
Type: string
Default: nil

<PE-16_ODP[01] типи компонентів системи> авторизуються при вході на об'єкт;

No: 4
Name: pe_16_a_2
Type: string
Default: nil

<PE-16_ODP[01] типи компонентів системи> контролюються при вході на об'єкт;

No: 5
Name: pe_16_a_3
Type: string
Default: nil

<PE-16_ODP[02] типи компонентів системи> авторизуються при виході з об'єкта;

No: 6
Name: pe_16_a_4
Type: string
Default: nil

<PE-16_ODP[02] типи компонентів системи> контролюються при виході з об'єкта;

No: 7
Name: pe_16_b
Type: string
Default: nil

ведеться облік компонентів системи, зазначених вище

11.17. АЛЬТЕРНАТИВНЕ РОБОЧЕ МІСЦЕ (PE-17)

Альтернативне робоче місце.

No: 1
Name: pe_17_odp_1
Type: string
Default: nil

визначені альтернативні робочі місця, дозволені для використання працівниками;

No: 2
Name: pe_17_odp_2
Type: string
Default: nil

визначаються заходи захисту, які будуть застосовуватися на альтернативних робочих місцях; PE-17(c) оцінюється ефективність заходів захисту на альтернативних робочих місцях; PE-17(d) працівникам надаються засоби

комунікації з персоналом служби інформаційної безпеки на випадок інцидентів.

11.18. РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ (PE-18)

Компоненти системи розміщені в межах об'єкта так, щоб мінімізувати потенційну шкоду від <PE-18_ODP фізичні та екологічні небезпеки> і звести до мінімуму можливість несанкціонованого доступу.

No: 1
Name: pe_18_odp
Type: string
Default: nil

визначено фізичні та екологічні небезпеки, які можуть призвести до потенційного пошкодження компонентів системи на об'єкті;

No: 2
Name: pe_18_01
Type: string
Default: nil

компоненти системи розміщені в межах об'єкта так, щоб мінімізувати потенційну шкоду від <PE-18_ODP фізичні та екологічні небезпеки> і звести до мінімуму можливість несанкціонованого доступу.

11.18.1. МІСЦЕ РОЗМІЩЕННЯ ОБ'ЄКТА (PE-18(1)) [Вилучено]

[Виключено: включено до PE-23].

Немає параметрів для цього контролю.

11.19. ВИТІК ІНФОРМАЦІЇ (PE-19)

Витік інформації.

Немає параметрів для цього контролю.

11.19.1. НАЦІОНАЛЬНІ ПОЛІТИКИ ТА ПРОЦЕДУРИ ЩОДО ПЕМВ (PE-19(1))

компоненти системи захищені відповідно до національних політик і процедур щодо ПЕМВ; передача даних захищається відповідно до національних політик і процедур щодо ПЕМВ; мережі захищені відповідно до національних політик і процедур щодо ПЕМВ.

No: 1
Name: pe_19_1_01
Type: string
Default: nil

компоненти системи захищені відповідно до національних політик і процедур щодо ПЕМВ;

No: 2
Name: pe_19_1_02
Type: string
Default: nil

передача даних захищається відповідно до національних політик і процедур щодо ПЕМВ;

No: 3
Name: pe_19_1_03
Type: string
Default: nil

мережі захищені відповідно до національних політик і процедур щодо ПЕМВ.

11.20. МОНІТОРИНГ І ВІДСТЕЖЕННЯ АКТИВІВ (PE-20)

<PE-20_ODP[01] технології> використовуються для відстеження та моніторингу місцезнаходження і переміщення <PE383 зони>.

No: 1
Name: pe_20_odp_1
Type: string
Default: nil

визначено технології, які будуть використовуватися для відстеження та моніторингу місцезнаходження та переміщення активів;

No: 2
Name: pe_20_odp_2
Type: string
Default: nil

визначено активи, місцезнаходження та переміщення яких необхідно відстежувати та моніторити;

No: 3
Name: pe_20_odp_3
Type: string
Default: nil

визначено контрольовані зони, в межах яких місцезнаходження та переміщення активів підлягають відстеженню та моніторингу;

No: 4
Name: pe_20_01
Type: string
Default: nil

<PE-20_ODP[01] технології> використовуються для відстеження та моніторингу місцезнаходження і переміщення <PE383 зони>.

11.21. ЗАХИСТ ВІД ЕЛЕКТРОМАГНІТНОГО ІМПУЛЬСУ (PE-21)

<PE-21_ODP[01] заходи захисту> застосовуються проти пошкодження електромагнітними імпульсами для <PE-21_ODP[02] системи та компонентів системи>.

No: 1
Name: pe_21_odp_1
Type: string
Default: nil

визначено заходи захисту від пошкодження електромагнітними імпульсами;

No: 2
Name: pe_21_odp_2
Type: string
Default: nil

визначено систему та компоненти системи, що потребують захисту від пошкодження електромагнітними імпульсами;

No: 3
Name: pe_21_01
Type: string
Default: nil

<PE-21_ODP[01] заходи захисту> застосовуються проти пошкодження електромагнітними імпульсами для <PE-21_ODP[02] системи та компонентів системи>.

11.22. МАРКУВАННЯ КОМПОНЕНТІВ (PE-22)

Забезпечити маркування компонентів та обладнання.

No: 1
Name: pe_22_odp
Type: string
Default: nil

визначено апаратні компоненти системи, які підлягають маркуванню із зазначенням рівня впливу або класифікації інформації, яку дозволено обробляти, зберігати або передавати за допомогою апаратного компонента;

No: 2
Name: pe_22_01
Type: string
Default: nil

<PE-22_ODP апаратні компоненти системи> позначаються із зазначенням рівня впливу або класифікації інформації, яку дозволено обробляти, зберігати або передавати за допомогою апаратного компонента.

11.23. РОЗТАШУВАННЯ ОБ'ЄКТА (PE-23)

а. Місце розташування або ділянка об'єкта, де знаходиться система, планується з урахуванням фізичних та екологічних небезпек;

b. Для існуючих об’єктів фізичні та екологічні небезпеки враховуються в стратегії управління ризиками організації.

No: 1
Name: pe_23_a
Type: string
Default: nil

місце розташування або ділянка об’єкта, де знаходиться система, планується з урахуванням фізичних та екологічних небезпек;

No: 2
Name: pe_23_b
Type: string
Default: nil

для існуючих об’єктів фізичні та екологічні небезпеки враховуються в стратегії управління ризиками організації.

12. PL

Клас заходів захисту PL — ПЛАНУВАННЯ БЕЗПЕКИ

Опис Цей клас регламентує розробку, документування та регулярне оновлення планів захисту інформації, архітектури безпеки та приватності.

Перелік заходів захисту Політики та процедури планування безпеки (PL-1); Плани захисту інформації та персональних даних (PL-2); Диверсифікація постачальників (PL-2(1)) [Вилучено]; Функціональна архітектура (PL-2(2)) [Вилучено]; Оновлення планів захисту інформації та персональних даних (PL-3) [Вилучено]; Правила поведінки (PL-4); Обмеження на соціальні медіа та мережу (PL-4(1)); Оцінка впливу на приватність (PL-5) [Вилучено]; Планування діяльності, пов’язаної з безпекою (PL-6) [Вилучено]; Концепція експлуатації (PL-7); Архітектура безпеки та приватності (PL-8); «глибока оборона» (PL-8(1)); Різноманітність постачальників (PL-8(2)); Централізоване управління (PL-9); Вибір базового профілю безпеки (PL-10); Налаштування базового профілю безпеки (PL-11).

12.1. ПОЛІТИКИ ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕКИ (PL-1)

Розроблена та задокументована політика планування безпеки.

No: 1
Name: pl_01_odp_01
Type: string
Default: nil

PL-01_ODP[01] визначено персонал або ролі, до яких має бути доведена політика планування безпеки;

No: 2
Name: pl_01_odp_02
Type: string
Default: nil

PL-01_ODP[02] визначено персонал або ролі, на які поширюватимуться процедури планування безпеки;

No: 3
Name: pl_01_odp_03
Type: string
Default: nil

PL-01_ODP[03] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи};

No: 4
Name: pl_01_odp_04
Type: string
Default: nil

PL-01_ODP[04] визначено посадову особу, яка керуватиме політикою та процедурами планування безпеки;

No: 5
Name: pl_01_odp_05
Type: string
Default: nil

PL-01_ODP[05] визначено періодичність перегляду та оновлення поточної політики планування безпеки;

No: 6
Name: pl_01_odp_06
Type: string
Default: nil

PL-01_ODP[06] є події, які потребують перегляду та оновлення поточної політики планування безпеки;

No: 7
Name: pl_01_odp_07
Type: string
Default: nil

PL-01_ODP[07] визначена частота, з якою переглядаються та оновлюються поточні процедури планування безпеки;

No: 8
Name: pl_01_odp_08
Type: string
Default: nil

PL-01_ODP[08] є події, які потребують перегляду та оновлення процедур планування безпеки;

No: 9
Name: pl_01_a_01
Type: string
Default: nil

PL-01a.[01] розроблена та задокументована політика планування безпеки.

No: 10
Name: pl_01_a_02
Type: string
Default: nil

PL-01a.[02] поширюється політика планування безпеки на <PL-01_ODP[01] персонал або ролі>;

No: 11
Name: pl_01_a_03
Type: string
Default: nil

PL-01a.[03] розроблені та задокументовані процедури планування безпеки, що сприяють впровадженню політики планування та пов'язаних з нею засобів контролю планування;

No: 12
Name: pl_01_a_04
Type: string
Default: nil

PL-01a.[04] поширюються процедури планування безпеки на <PL-01_ODP[02] персонал або ролі>;

No: 13
Name: pl_01_a_01_a_01
Type: string
Default: nil

PL-01a.01(a)[01] відповідає політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> меті;

No: 14
Name: pl_01_a_01_a_02
Type: string
Default: nil

PL-01a.01(a)[02] політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> враховує сферу застосування;

No: 15
Name: pl_01_a_01_a_03
Type: string
Default: nil

PL-01a.01(a)[03] <PL-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика планування звертається до ролей;

No: 16
Name: pl_01_a_01_a_04
Type: string
Default: nil

PL-01a.01(a)[04] політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> стосується обов'язків;

No: 17
Name: pl_01_a_01_a_05
Type: string
Default: nil

PL-01a.01(a)[05] політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> враховує зобов'язання керівництва;

No: 18
Name: pl_01_a_01_a_06
Type: string
Default: nil

PL-01a.01(a)[06] політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> передбачає координацію між організаційними одиницями;

No: 19
Name: pl_01_a_01_a_07
Type: string
Default: nil

PL-01a.01(a)[07] політика планування безпеки <PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> стосується комплаєнсу;

No: 20
Name: pl_01_b
Type: string
Default: nil

PL-01b. призначена <PL-01_ODP[04] посадова особа> для управління розробкою, документуванням та розповсюдженням політики та процедур планування;

No: 21
Name: pl_01_c_01_01
Type: string
Default: nil

PL-01c.01[01] переглядається та оновлюється поточна політика планування безпеки <PL-01_ODP[05] частота>;

No: 22
Name: pl_01_c_01_02
Type: string
Default: nil

PL-01c.01[02] переглядається та оновлюється поточна політика планування після <PL-01_ODP[06] подій>;

No: 23
Name: pl_01_c_02_01
Type: string
Default: nil

PL-01c.02[01] переглядаються та оновлюється поточні процедури планування <PL-01_ODP[07] частота>;

No: 24
Name: pl_01_c_02_02
Type: string
Default: nil

PL-01c.02[02] переглядаються та оновлюється поточні процедури планування безпеки після <PL-01_ODP[08] подій>.

12.2. ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ (PL-2)

Розроблено план захисту інформації, який відповідає архітектурі підприємства організації;.

No: 1
Name: pl-02_odp_01
Type: string
Default: nil

призначені особи або групи, з якими пов'язана діяльність з безпекою та конфіденційністю, що впливає на систему, яка потребує планування та координації;

No: 2
Name: pl-02_odp_02
Type: string
Default: nil

призначено персонал або ролі для отримання розповсюджуваних копій планів захисту інформації та конфіденційності системи;

No: 3
Name: pl-02_odp_03
Type: string
Default: nil

визначено періодичність перегляду планів захисту інформації та конфіденційності системи;

No: 4
Name: pl_02_pm_01
Type: string
Default: nil

розроблено план захисту інформації, який відповідає архітектурі підприємства організації;

No: 5
Name: pl_02_pm_02
Type: string
Default: nil

розроблено план конфіденційності для системи, який відповідає архітектурі підприємства організації;

No: 6
Name: pl_02_pm_03
Type: string
Default: nil

розроблено план захисту інформації, який чітко визначає складові компоненти системи;

No: 7
Name: pl_02_pm_04
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який чітко визначає складові компоненти системи;

No: 8
Name: pl_02_pm_05
Type: string
Default: nil

розроблено план захисту інформації системи, який описує операційний контекст системи з точки зору місії та бізнеспроцесів;

No: 9
Name: pl_02_pm_06
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який описує операційний контекст системи з точки зору місії та бізнес-процесів;

No: 10
Name: pl_02_pm_07
Type: string
Default: nil

розроблено план захисту інформації, який визначає осіб, що виконують системні ролі та обов'язки;

No: 11
Name: pl_02_pm_08

Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який визначає осіб, що виконують ролі та обов'язки в системі;

No: 12
Name: pl_02_pm_09
Type: string
Default: nil

розроблено план захисту інформації, який визначає типи інформації, що обробляється, зберігається та передається системою;

No: 13
Name: pl_02_pm_10
Type: string
Default: nil

розроблено план конфіденційності для системи, який визначає типи інформації, що обробляється, зберігається та передається системою;

No: 14
Name: pl_02_pm_11
Type: string
Default: nil

розроблено план захисту інформації, який передбачає категоризацію безпеки системи, включаючи відповідне обґрунтування;

No: 15
Name: pl_02_pm_12
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який передбачає категоризацію системи за рівнем безпеки, включаючи обґрунтування;

No: 16
Name: pl_02_pm_13
Type: string
Default: nil

розроблено план захисту інформації, який описує будь-які конкретні загрози для системи, що викликають потенційні ризики для рганізації;

No: 17
Name: pl_02_pm_14
Type: string
Default: nil

розроблено план конфіденційності для системи, який описує будь-які конкретні загрози для системи, що викликають потенційні ризики для організації;

No: 18
Name: pl_02_pm_15
Type: string
Default: nil

розроблено план захисту інформації, який містить результати оцінки ризиків конфіденційності для систем, що обробляють інформацію, яка ідентифікує особу;

No: 19
Name: pl_02_pm_16

Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який містить результати оцінки ризиків конфіденційності для систем, що обробляють інформацію, яка ідентифікує особу;

No: 20
Name: pl_02_pm_17
Type: string
Default: nil

розроблено план захисту інформації, який описує операційне середовище системи та будь-які залежності або зв'язки з іншими системами чи компонентами системи;

No: 21
Name: pl_02_pm_18
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який описує робоче середовище системи та будь-які залежності або зв'язки з іншими системами чи компонентами системи;

No: 22
Name: pl_02_pm_19
Type: string
Default: nil

розроблено план захисту інформації, який містить огляд вимог до безпеки системи;

No: 23
Name: pl_02_pm_20
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який містить огляд вимог до конфіденційності системи;

No: 24
Name: pl_02_pm_21
Type: string
Default: nil

розроблено план захисту інформації, який визначає будь-які відповідні базові рівні контролю або обмеження, якщо такі є;

No: 25
Name: pl_02_pm_22
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який визначає будь-які відповідні базові рівні контролю або обмеження, якщо такі є;

No: 26
Name: pl_02_pm_23
Type: string
Default: nil

розроблено план захисту інформації, який описує наявні або заплановані засоби контролю для виконання вимог безпеки, включаючи обґрунтування будь-яких рішень щодо адаптації;

No: 27
Name: pl_02_pm_24

Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який описує наявні або заплановані засоби контролю для виконання вимог щодо конфіденційності, включаючи обґрунтування будь-яких рішень, пов'язаних з адаптацією;

No: 28
Name: pl_02_pm_25
Type: string
Default: nil

розроблено план захисту інформації, який включає визначення ризиків для архітектури безпеки та проектних рішень;

No: 29
Name: pl_02_pm_26
Type: string
Default: nil

розроблено план забезпечення конфіденційності для системи, який включає визначення ризиків для архітектури конфіденційності та проектних рішень;

No: 30
Name: pl_02_pm_27
Type: string
Default: nil

розроблено захисту інформації, який включає діяльність, пов'язану з безпекою, що впливає на систему і потребує планування та координації з <PL-02_ODP[01] окремими особами або групами>;

No: 31
Name: pl_02_pm_28
Type: string
Default: nil

розроблено для системи план забезпечення конфіденційності, який включає діяльність, пов'язану з конфіденційністю, що впливає на систему і потребує планування та координації з <PL-02_ODP[01] окремими особами або групами>;

No: 32
Name: pl_02_pm_29
Type: string
Default: nil

розроблено план захисту інформації, який розглядається та затверджується уповноваженою посадовою особою або призначеним представником до початку реалізації плану;

No: 33
Name: pl_02_pm_30
Type: string
Default: nil

розроблено план забезпечення конфіденційності для системи, який перевіряється та затверджується уповноваженою посадовою особою або призначеним представником перед впровадженням плану.

No: 34
Name: pl_02_pm_31
Type: string
Default: nil

розповсюджуються копії планів серед <PL-02_ODP[02] персонал або ролі>;

No: 35
Name: pl_02_pm_32
Type: string
Default: nil

повідомляються наступні зміни до планів <PL-02_ODP[02] персонал або ролі>;

No: 36
Name: pl_02_pm_33
Type: string
Default: nil

оновлюються плани відповідно до змін у системі та середовищі діяльності;

No: 37
Name: pl_02_pm_34
Type: string
Default: nil

оновлюються плани для вирішення проблем, виявлених під час реалізації плану;

No: 38
Name: pl_02_pm_35
Type: string
Default: nil

оновлюються плани для вирішення проблем, виявлених під час контрольних оцінок;

No: 39
Name: pl_02_pm_36
Type: string
Default: nil

захищені плани від несанкціонованого розголошення;

No: 40
Name: pl_02_pm_37
Type: string
Default: nil

захищені плани від несанкціонованої модифікації.

12.2.1. ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ (PL-2(1)) [Вилучено]

Диверсифікація постачальників (pl-2(1)) [вилучено].

Немає параметрів для цього контролю.

12.2.2. ФУНКЦІОНАЛЬНА АРХІТЕКТУРА (PL-2(2)) [Вилучено]

Функціональна архітектура (pl-2(2)) [вилучено].

Немає параметрів для цього контролю.

12.3. ОНОВЛЕННЯ ПЛАНІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ (PL-3) [Вилучено]

Оновлення планів захисту інформації та персональних даних (pl-3) [вилучено].

Немає параметрів для цього контролю.

12.4. ПРАВИЛА ПОВЕДІНКИ (PL-4)

Встановлені правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності для осіб, яким потрібен доступ до системи;.

No: 1
Name: pl-04_odp_01
Type: string
Default: nil

визначено періодичність перегляду та оновлення правил поведінки;

No: 2
Name: pl-04_odp_02
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА:{<PL-04_ODP[03] частота>; коли правила переглядаються або оновлюються};

No: 3
Name: pl-04_odp_03
Type: string
Default: nil

визначена періодичність перегляду та повторного підтвердження правил поведінки (якщо вибрано);

No: 4
Name: pl-04_pm_01
Type: string
Default: nil

встановлені правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності для осіб, яким потрібен доступ до системи;

No: 5
Name: pl-04_pm_02
Type: string
Default: nil

надаються правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності, особам, які отримують доступ до системи; задокументоване підтвердження від таких осіб про те, що вони прочитали, зрозуміли та згодні дотримуватися правил поведінки; 04_ODP[01] частота>; поведінки, прочитати та повторно визнати <PL-04_ODP[02] ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА(ів)>.

12.4.1. ОБМЕЖЕННЯ НА СОЦІАЛЬНІ МЕДІА ТА МЕРЕЖУ (PL-4(1))

Обмеження на соціальні медіа та мережу (pl-4(1)).

Немає параметрів для цього контролю.

12.5. ОЦІНКА ВПЛИВУ НА ПРИВАТНІСТЬ (PL-5) [Вилучено]

Оцінка впливу на приватність (pl-5) [вилучено].

Немає параметрів для цього контролю.

12.6. ПЛАНУВАННЯ ДІЯЛЬНОСТІ, ПОВ'ЯЗАНОЇ З БЕЗПЕКОЮ (PL-6) [Вилучено]

Планування діяльності, пов'язаної з безпекою (pl-6) [вилучено].

Немає параметрів для цього контролю.

12.7. КОНЦЕПЦІЯ ЕКСПЛУАТАЦІЇ (PL-7)

Концепція експлуатації.

Немає параметрів для цього контролю.

12.8. АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ (PL-8)

Описує архітектура безпеки системи те, як вона інтегрована в архітектуру підприємства та підтримує її;.

No: 1
Name: pl_08_pm_01
Type: string
Default: nil

описує архітектура безпеки системи те, як вона інтегрована в архітектуру підприємства та підтримує її;

No: 2
Name: pl_08_pm_02
Type: string
Default: nil

описує архітектура конфіденційності системи те, як вона інтегрована в архітектуру підприємства та підтримує її;

No: 3
Name: pl_08_pm_03
Type: string
Default: nil

описує архітектура безпеки системи будь-які припущення та залежності від зовнішніх систем та сервісів;

No: 4
Name: pl_08_pm_04
Type: string
Default: nil

описує архітектура конфіденційності системи будь-які припущення та залежності від зовнішніх систем і сервісів; підприємства <PL-08_ODP частота> для відображення змін в архітектурі підприємства;

No: 5
Name: pl_08_pm_05
Type: string
Default: nil

заплановані зміни в архітектурі відображені в плані безпеки;

No: 6
Name: pl_08_pm_06
Type: string
Default: nil

відображені заплановані зміни в архітектурі в плані конфіденційності;

No: 7
Name: pl_08_pm_07
Type: string
Default: nil

заплановані зміни архітектури відображені в Концепції діяльності концепції експлуатації системи;

No: 8
Name: pl_08_pm_08
Type: string
Default: nil

заплановані зміни в архітектурі відображені в аналізі критичності;

No: 9
Name: pl_08_pm_09
Type: string
Default: nil

відображені заплановані зміни архітектури в організаційних процедурах;

No: 10
Name: pl_08_pm_10
Type: string
Default: nil

заплановані зміни в архітектурі відображаються на закупівлях та придбанні.

12.8.1. «ГЛИБОКА ОБОРОНА» (PL-8(1))

Архітектура безпеки системи розроблена з використанням підходу «глибокої оборони», який розподіляє <PL- 08(01)_ODP[01] елементи керування> за <PL- 08(01)_ODP[02] місцями та архітектурними рівнями>;.

No: 1
Name: pl_08_1_pm_01
Type: string
Default: nil

архітектура безпеки системи розроблена з використанням підходу «глибокої оборони», який розподіляє <PL-08(01)_ODP[01] елементи керування> за <PL- 08(01)_ODP[02] місцями та архітектурними рівнями>;

No: 2
Name: pl_08_1_pm_02
Type: string
Default: nil

архітектура конфіденційності системи розроблена з використанням підходу глибокого захисту, який розподіляє <PL-08(01)_ODP[01] елементи керування> за <PL- 08(01)_ODP[02] місцями та архітектурними рівнями>;

No: 3
Name: pl_08_1_pm_03
Type: string
Default: nil

архітектура безпеки системи розроблена з використанням підходу «глибокої оборони», який гарантує, що виділені засоби контролю працюють скоординовано і взаємно підсилюють один одного;

No: 4
Name: pl_08_1_pm_04
Type: string
Default: nil

архітектура конфіденційності системи розроблена з використанням підходу «глибокої оборони», який гарантує, що виділені засоби контролю працюють скоординовано і взаємно підкріплюють один одного.

12.8.2. РІЗНОМАНІТНІСТЬ ПОСТАЧАЛЬНИКІВ (PL-8(2))

Різноманітність постачальників (pl-8(2)).

Немає параметрів для цього контролю.

12.9. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ (PL-9)

Централізоване управління.

Немає параметрів для цього контролю.

12.10. ВИБІР БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ (PL-10)

Вибрано базовий профіль безпеки для системи.

No: 1
Name: pl-10_pm_01
Type: string
Default: nil

вибрано базовий профіль безпеки для системи.

12.11. НАЛАШТУВАННЯ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ (PL-11)

Налаштуватовано вибраний базовий профіль безпеки, застосовуючи вказані дії для налаштування.

No: 1
Name: pl-11_pm_01
Type: list
Default: ["admin", "security_officer"]

налаштуватовано вибраний базовий профіль безпеки, застосовуючи вказані дії для налаштування.

13. PS

Безпека персоналу.

Опис Цей клас встановлює вимоги до перевірки, надання повноважень та звільнення персоналу з метою мінімізації ризиків інсайдерських загроз.

Перелік заходів захисту Політика та процедури кадрової безпеки (PS-1); Визначення посадового ризику (PS-2); Перевірка персоналу (PS-3); Інформація з обмеженим доступом (PS-3(1)); Інструктаж (PS-3(2)); Інформація, що потребує додаткових заходів захисту (PS-3(3)); Вимоги до громадянства (PS-3(4)); Звільнення персоналу (PS-4); Вимоги після закінчення трудової діяльності (PS-4(1)); Автоматизоване сповіщення (PS-4(2)); Переведення персоналу (PS-5); Угоди про доступ (PS-6); Інформація, що вимагає спеціального захисту (PS-6(1)) [Вилучено]; Інформація з обмеженим доступом, що вимагає спеціального захисту (PS-6(2)); Вимоги після закінчення трудової діяльності (PS-6(3)); Безпека зовнішнього персоналу (PS-7); Кадрові санкції (PS-8); Опис позицій (PS-9).

13.1. ПОЛІТИКА ТА ПРОЦЕДУРИ КАДРОВОЇ БЕЗПЕКИ (PS-1)

Розроблена та задокументована політика безпеки персоналу;.

No: 1
Name: ps_1_odp_01
Type: string
Default: nil

визначено персонал або ролі, на які поширюється політика кадрової безпеки;

No: 2
Name: ps_1_odp_02
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури кадрової безпеки;

No: 3
Name: ps_1_odp_03
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи};

No: 4
Name: ps_1_odp_04
Type: string
Default: nil

визначено посадову особу, яка керуватиме політикою та процедурами кадрової безпеки;

No: 5
Name: ps_1_odp_05
Type: string
Default: nil

визначена періодичність перегляду та оновлення поточної політики кадрової безпеки;

No: 6
Name: ps_1_odp_06
Type: string
Default: nil

є події, які вимагають перегляду та оновлення поточної політики кадрової безпеки;

No: 7
Name: ps_1_odp_07
Type: string
Default: nil

визначено періодичність перегляду та оновлення поточних процедур кадрової безпеки;

No: 8
Name: ps_1_odp_08
Type: string
Default: nil

є події, які вимагають перегляду та оновлення процедур безпеки персоналу;

No: 9
Name: ps_1a_01
Type: string
Default: nil

розроблена та задокументована політика безпеки персоналу;

No: 10
Name: ps_1a_02
Type: string
Default: nil

поширюється політика безпеки персоналу на <PS-01_ODP[01] персонал або ролі>;

No: 11
Name: ps_1a_03
Type: string
Default: nil

звертається політика кадрової безпеки до мети;

No: 12
Name: ps_1a_04
Type: string
Default: nil

звертається політика кадрової безпеки до сфери застосування;

No: 13
Name: ps_1a_05
Type: string
Default: nil

звертається політика кадрової безпеки до ролей;

No: 14
Name: ps_1a_06
Type: string
Default: nil

звертається політика кадрової безпеки до обов'язків;

No: 15
Name: ps_1a_07
Type: string
Default: nil

звертається політика кадрової безпеки до зобов'язань керівництва;

No: 16
Name: ps_1a_08
Type: string
Default: nil

звертається політика кадрової безпеки до координації між структурними підрозділами організації;

No: 17
Name: ps_1a_09
Type: string
Default: nil

звертається політика кадрової безпеки до дотримання вимог;

No: 18
Name: ps_1a_10

Type: string
Default: nil

відповідає політика кадрової безпеки <PS-01_ODP[03] ВИБРАНОМУ ЗНАЧЕННЮ(ЯМ) ПАРАМЕТРА>;

No: 19
Name: ps_1a_11
Type: string
Default: nil

відповідає політика кадрової безпеки чинному законодавству, виконавчим наказам, директивам, нормативним актам, політикам, стандартам і керівним принципам;

No: 20
Name: ps_1b_01
Type: string
Default: nil

призначена <PS-01_ODP[04] посадова особа> для управління розробкою, документуванням і розповсюдженням політики і процедур безпеки персоналу;

No: 21
Name: ps_1c_01
Type: string
Default: nil

переглядається і оновлюється поточна політика кадрової безпеки з <PS-01_ODP[05] частотою> і після <PS-01_ODP[06] подій>;

No: 22
Name: ps_1d_01
Type: string
Default: nil

розробляються і документуються процедури кадрової безпеки, що сприяють впровадженню політики кадрової безпеки і пов'язаних з нею засобів контролю кадрової безпеки;

No: 23
Name: ps_1d_02
Type: string
Default: nil

поширюються процедури кадрової безпеки на <PS-01_ODP[02] персонал або ролі>;

No: 24
Name: ps_1e_01
Type: string
Default: nil

переглядаються та оновлюються поточні процедури кадрової безпеки з <PS-01_ODP[07] частотою> та після <PS-01_ODP[08] подій>.

13.2. ВИЗНАЧЕННЯ ПОСАДОВОГО РИЗИКУ (PS-2)

Всім посадам в організації присвоєно ідентифікатор ризику;.

No: 1
Name: ps_2_odp
Type: string
Default: nil

визначено періодичність перегляду та оновлення ідентифікаторів посадових ризиків;

No: 2
Name: ps_2a
Type: string
Default: nil

всім посадам в організації присвоєно ідентифікатор ризику;

No: 3
Name: ps_2b
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};

No: 4
Name: ps_2c
Type: string
Default: nil

встановлені критерії відбору для осіб, які обіймають посади в організації;

13.3. ПЕРЕВІРКА ПЕРСОНАЛУ (PS-3)

Проходять особи перевірку перед тим, як надати їм доступ до системи;.

No: 1
Name: ps_3_odp_01
Type: string
Default: nil

визначені умови, що вимагають повторної перевірки осіб;

No: 2
Name: ps_3_odp_02
Type: string
Default: nil

визначена частота повторної перевірки осіб, для яких це показано;

No: 3
Name: ps_3a
Type: string
Default: nil

проходять особи перевірку перед тим, як надати їм доступ до системи;

No: 4
Name: ps_3b_01
Type: string
Default: nil

проходять особи повторну перевірку відповідно до <PS-03_ODP[01] умови, що вимагають повторної перевірки>;

No: 5
Name: ps_3b_02
Type: string
Default: nil

проводиться повторна перевірка у випадках, коли це зазначено, <PS-03_ODP[02] частота>.

13.3.1. ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ (PS-3(1))

Особи мають допуск та доступ до систем, де обробляється, зберігається або передається інформація з обмеженим доступом;.

No: 1
Name: ps_3_1_01
Type: string
Default: nil

особи мають допуск та доступ до систем, де обробляється, зберігається або передається інформація з обмеженим доступом;

No: 2
Name: ps_3_1_02
Type: string
Default: nil

особи, які мають доступ до системи, де обробляється, зберігається або передається інформація з обмеженим доступом, ознайомлені з найвищим ступенем секретності інформації, до якої вони мають доступ у системі.

13.3.2. ІНСТРУКТАЖ (PS-3(2))

Особи, які мають доступ до системи, де обробляється, зберігається або передається інформація з обмеженим доступом, пройшли відповідний офіційний інструктаж про всі відповідні типи інформації, до якої вони отримають доступ в системі.

No: 1
Name: ps_3_2
Type: string
Default: nil

особи, які мають доступ до системи, де обробляється, зберігається або передається інформація з обмеженим доступом, пройшли відповідний офіційний інструктаж про всі відповідні типи інформації, до якої вони отримають доступ в системі.

13.3.3. ІНФОРМАЦІЯ, ЩО ПОТРЕБУЄ ДОДАТКОВИХ ЗАХОДІВ ЗАХИСТУ (PS-3(3))

Мають особи, які отримують доступ до системи, що обробляє, зберігає або передає інформацію, яка потребує додаткових заходів захисту, чинний дозвіл на доступ;.

No: 1
Name: ps_3_3_odp
Type: string
Default: nil

визначені додаткові критерії перевірки персоналу, яким повинні відповідати особи, що мають чинний дозвіл на доступ до системи, яка обробляє, зберігає або передає інформацію, потребує додаткових заходів захисту;

No: 2
Name: ps_3_3a

Type: string
Default: nil

мають особи, які отримують доступ до системи, що обробляє, зберігає або передає інформацію, яка потребує додаткових заходів захисту, чинний дозвіл на доступ;

No: 3
Name: ps_3_3b
Type: string
Default: nil

відповідають особи, які отримують доступ до системи, що обробляє, зберігає або передає інформацію, яка потребує додаткових заходів захисту, <PS-03(03)_ODP додаткові критерії перевірки персоналу>.

13.3.4. ВИМОГИ ДО ГРОМАДЯНСТВА (PS-3(4))

Відповідають особи, які мають доступ до системи, що обробляє, зберігає або передає <PS-03(04)_ODP[01] типи інформації>, <PS-03(04)_ODP[02] вимогам щодо громадянства>.

No: 1
Name: ps_3_4_odp_01
Type: string
Default: nil

доступ осіб до систем відповідає типу інформації, яка обробляється, зберігається або передається системою;

No: 2
Name: ps_3_4_odp_02
Type: string
Default: nil

визначені вимоги щодо громадянства, яким повинні відповідати особи з доступом до системи, де обробляється, зберігається або передається інформація;

No: 3
Name: ps_3_4
Type: string
Default: nil

відповідають особи, які мають доступ до системи, що обробляє, зберігає або передає <PS-03(04)_ODP[01] типи інформації>, <PS-03(04)_ODP[02] вимогам щодо громадянства>.

13.4. ЗВІЛЬНЕННЯ ПЕРСОНАЛУ (PS-4)

При звільненні працівника доступ до системи вимикається протягом <PS-04_ODP[01] часового періоду>;.

No: 1
Name: ps_4_odp_01
Type: string
Default: nil

визначено період часу, протягом якого забороняється доступ до системи;

No: 2
Name: ps_4_odp_02

Type: string
Default: nil

визначені теми інформаційної безпеки для обговорення під час проведення співбесід;

No: 3
Name: ps_4a
Type: string
Default: nil

при звільненні працівника доступ до системи вимикається протягом <PS-04_ODP[01] часового періоду>;

No: 4
Name: ps_4b
Type: string
Default: nil

припиняють дію або анулюють будь-які автентифікатори та облікові дані після припинення трудових відносин з окремими особами;

No: 5
Name: ps_4c
Type: string
Default: nil

проводяться при звільненні окремих працівників співбесіди, які включають обговорення <PS-04_ODP[02] питань інформаційної безпеки>;

No: 6
Name: ps_4d
Type: string
Default: nil

отримується після звільнення особи все майно, пов'язане з безпекою організаційної системи;

No: 7
Name: ps_4e
Type: string
Default: nil

зберігається доступ до організаційної інформації та систем, які раніше перебували під контролем особи, що звільняється, після припинення нею трудових відносин.

13.4.1. ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ (PS-4(1))

Зберігається доступ до інформації організації та в системі, під контролем особи, що звільняється, після припинення з нею трудових відносин;.

No: 1
Name: ps_4_1a
Type: string
Default: nil

зберігається доступ до інформації організації та в системі, під контролем особи, що звільняється, після припинення з нею трудових відносин;

No: 2
Name: ps_4_1b
Type: string
Default: nil

потрібно звільненим особам підписувати підтвердження вимог щодо працевлаштування в рамках процесу припинення діяльності організації.

13.4.2. АВТОМАТИЗОВАНЕ СПОВІЩЕННЯ (PS-4(2))

Використовуються <PS-04(02)_ODP[01] автоматизовані механізми> для <PS-04(02)_ODP[02] ВИБРАНОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

No: 1
Name: ps_4_2_odp_01
Type: string
Default: nil

визначені автоматизовані механізми сповіщення персоналу або ролей про окремі дії з припинення роботи та/або заборони доступу до ресурсів системи;

No: 2
Name: ps_4_2_odp_02
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повідомляти <PS-04(02)_ODP[03] персонал або ролі> про окремі дії завершення; взаборони доступу до системних ресурсів};

No: 3
Name: ps_4_2_odp_03
Type: string
Default: nil

визначено персонал або ролі, про які необхідно повідомляти при звільненні особи (якщо визначено);

No: 4
Name: ps_4_2
Type: string
Default: nil

використовуються <PS-04(02)_ODP[01] автоматизовані механізми> для <PS-04(02)_ODP[02] ВИБРАНОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

13.5. ПЕРЕВЕДЕННЯ ПЕРСОНАЛУ (PS-5)

Переглядаються та підтверджуються поточні потреби в логічних та фізичних дозволах на доступ до систем та об'єктів при перепризначенні або переведенні осіб на інші посади в організації;.

No: 1
Name: ps_5_odp_01
Type: string
Default: nil

визначені дії, які мають бути ініційовані після переведення або перепризначення;

No: 2
Name: ps_5_odp_02
Type: string
Default: nil

визначено період часу, протягом якого мають бути здійснені дії з переведення або перепризначення після переведення або перепризначення;

No: 3
Name: ps_5_odp_03
Type: string
Default: nil

визначено персонал або ролі, про які необхідно повідомляти, коли осіб призначають на інші посади або переводять на інші посади в організації;

No: 4
Name: ps_5_odp_04
Type: string
Default: nil

визначено період часу, протягом якого необхідно повідомляти визначений організацією персонал або ролі, коли осіб перепризначають або переводять на інші посади в межах організації;

No: 5
Name: ps_5a
Type: string
Default: nil

переглядаються та підтверджуються поточні потреби в логічних та фізичних дозволах на доступ до систем та об'єктів при перепризначенні або переведенні осіб на інші посади в організації;

No: 6
Name: ps_5b
Type: string
Default: nil

були ініційовані <PS-05_ODP[01] дії з переведення або перепризначення> протягом <PS-05_ODP[02] періоду часу після формальної дії з переведення>;

No: 7
Name: ps_5c
Type: string
Default: nil

змінюється авторизація доступу за необхідності, щоб відповідати будь-яким змінам в оперативних потребах у зв'язку з перепризначенням або переведенням;

No: 8
Name: ps_5d
Type: string
Default: nil

було повідомлено <PS-05_ODP[03] персонал або ролі> протягом <PS-05_ODP[04] часового періоду>.

13.6. УГОДИ ПРО ДОСТУП (PS-6)

Розроблені та задокументовані угоди про доступ до систем організації;.

No: 1
Name: ps_6_odp_01
Type: string
Default: nil

визначено періодичність перегляду та оновлення угод про доступ;

No: 2
Name: ps_6_odp_02
Type: string
Default: nil

визначена періодичність перепідписання угод про доступ для збереження доступу до інформації організації;

No: 3
Name: ps_6a
Type: string
Default: nil

розроблені та задокументовані угоди про доступ до систем організації;

No: 4
Name: ps_6b
Type: string
Default: nil

переглядаються та оновлюються угоди про доступ <PS-06_ODP[01] частота>;

No: 5
Name: ps_6c_01
Type: string
Default: nil

підписують особи, яким потрібен доступ до інформації та систем організації, відповідні угоди про доступ до того, як їм буде надано доступ;

No: 6
Name: ps_6c_02
Type: string
Default: nil

перепідписують особи, яким потрібен доступ до інформації та систем організації, угоди про доступ для збереження доступу до систем організації, коли угоди про доступ були оновлені чи як <PS-06_ODP[02] частота>.

13.6.1. ІНФОРМАЦІЯ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ (PS-6(1)) [Вилучено]

Інформація, що вимагає спеціального захисту (ps-6(1)) [вилучено].

Немає параметрів для цього контролю.

13.6.2. ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ (PS-6(2))

Надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які мають дійсний дозвіл на доступ, що підтверджується покладеними на них офіційними державними обов'язками;.

No: 1
Name: ps_6_2a
Type: string
Default: nil

надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які мають дійсний дозвіл на доступ, що підтверджується покладеними на них офіційними державними обов'язками;

No: 2
Name: ps_6_2b
Type: string
Default: nil

надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які відповідають відповідним критеріям кадрової безпеки;

No: 3
Name: ps_6_2c
Type: string
Default: nil

надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які прочитали, зрозуміли та підписали угоду про нерозголошення.

13.6.3. ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ (PS-6(3))

Повідомляють людей про застосовні, юридично обов'язкові вимоги щодо захисту інформації організації після закінчення трудової діяльності;.

No: 1
Name: ps_6_3a
Type: string
Default: nil

повідомляють людей про застосовні, юридично обов'язкові вимоги щодо захисту інформації організації після закінчення трудової діяльності;

No: 2
Name: ps_6_3b
Type: string
Default: nil

повинні особи підписувати визнання застосовних, юридично обов'язкових вимог після звільнення як частину надання первинного доступу до інформації з обмеженим доступом.

13.7. БЕЗПЕКА ЗОВНІШНЬОГО ПЕРСОНАЛУ (PS-7)

Встановлені вимоги до безпеки персоналу, включаючи ролі та обов'язки зовнішніх постачальників послуг у сфері безпеки;.

No: 1
Name: ps_7_odp_01
Type: string
Default: nil

визначено персонал або ролі, які мають бути повідомлені про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами, або має системні привілеї;

No: 2
Name: ps_7_odp_02
Type: string
Default: nil

визначено період часу, протягом якого сторонні провайдери повинні повідомляти визначений організацією персонал або ролі про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами або має системні привілеї;

No: 3
Name: ps_7a
Type: string
Default: nil

встановлені вимоги до безпеки персоналу, включаючи ролі та обов'язки зовнішніх постачальників послуг у сфері безпеки;

No: 4
Name: ps_7b
Type: string
Default: nil

зобов'язані зовнішні провайдери дотримуватися політики та процедур кадрової безпеки, встановлених організацією;

No: 5
Name: ps_7c
Type: string
Default: nil

задокументовані вимоги до безпеки персоналу;

No: 6
Name: ps_7d
Type: string
Default: nil

зобов'язані зовнішні провайдери повідомляти <PS-07_ODP[01] персонал або ролі> про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами або має системні привілеї протягом <PS-07_ODP[02] часового періоду>;

No: 7
Name: ps_7e
Type: string
Default: nil

контролюється дотримання провайдером вимог щодо безпеки персоналу.

13.8. КАДРОВІ САНКЦІЇ (PS-8)

Застосовується офіційний процес санкцій до осіб, які не дотримуються встановлених політик і процедур інформаційної безпеки та конфіденційності;.

No: 1
Name: ps_8_odp_01
Type: string
Default: nil

визначено персонал або ролі, про які необхідно повідомляти, коли ініціюється офіційний процес санкцій щодо працівників;

No: 2
Name: ps_8_odp_02
Type: string
Default: nil

визначено період часу, протягом якого визначений організацією персонал або ролі повинні бути повідомлені про початок офіційного процесу застосування санкцій до працівника;

No: 3
Name: ps_8a
Type: string
Default: nil

застосовується офіційний процес санкцій до осіб, які не дотримуються встановлених політик і процедур інформаційної безпеки та конфіденційності;

No: 4
Name: ps_8b
Type: string
Default: nil

було повідомлено <PS-08_ODP[01] персонал або ролі> протягом <PS-08_ODP[02] періоду часу>, коли розпочато офіційний процес застосування санкцій до працівників, із зазначенням особи, до якої застосовано санкції, та причини санкцій.

13.9. ОПИС ПОЗИЦІЙ (PS-9)

Включені функції та обов'язки з безпеки в описи посадових осіб в організації;.

No: 1
Name: ps_9_01
Type: string
Default: nil

включені функції та обов'язки з безпеки в описи посадових осіб в організації;

No: 2
Name: ps_9_02
Type: string
Default: nil

включені ролі та обов'язки щодо конфіденційності в описи посадових осіб в організації.

14. RA

Клас заходів захисту RA — ОЦІНЮВАННЯ РИЗИКУ

Опис Цей клас забезпечує систематичний підхід до виявлення, аналізу та реагування на ризики, пов'язані з обробкою інформації та функціонуванням системи.

Перелік заходів захисту Політика та процедури оцінювання ризику (RA-1); Категоріювання безпеки (RA-2); Категоріювання другого рівня (RA-2(1)); Оцінювання ризику (RA-3); Оцінювання ризику ланцюга постачання (RA-3(1)); Використання інформації з усіх доступних джерел (RA-3(2)); Усвідомлення динамічних загроз (RA-3(3)); Прогностична кібераналітика (RA-3(4)); Оновлення оцінювання ризику (RA-4) [Вилучено]; Сканування вразливостей (RA-5); Можливість оновлення інструментів (RA-5(1)) [Вилучено]; Оновлення за частотою, перед новим скануванням або при ідентифікації (RA-5(2)); Широта та глибина покриття (RA-5(3)); Виявна інформація (RA-5(4)); Привілейований доступ (RA-5(5)); Автоматизований аналіз тенденцій (RA-5(6)); Автоматизоване виявлення та сповіщення про неавторизовані компоненти (RA-5(7)) [Вилучено]; Огляд журналів аудиту за минулі періоди (RA-5(8)); Тестування та аналіз проникнення (RA-5(9)) [Вилучено]; Зіставлення інформації про сканування (RA-5(10)); Програма публічного оприлюднення (RA-5(11)); Заходи протидії технічній розвідці (RA-6); Реагування на ризик (RA-7); Оцінка впливу на приватність (RA-8); Аналіз критичності (RA-9); Активний пошук загроз (RA-10).

14.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ОЦІНЮВАННЯ РИЗИКУ (RA-1)

Поширюється політика оцінки ризиків на <RA-01_ODP[01] персонал або ролі>;.

No: 1
Name: ra_1_odp_01
Type: string
Default: nil

визначено персонал або ролі, на які поширюється політика оцінювання ризику;

No: 2
Name: ra_1_odp_02
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури, що сприяють здійсненню політики оцінювання ризику;

No: 3
Name: ra_1_odp_03
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи};

No: 4
Name: ra_1_odp_04
Type: string
Default: nil

визначена посадова особа, відповідальна за управління політикою та процедурами оцінювання ризику;

No: 5
Name: ra_1_odp_05
Type: string
Default: nil

визначена періодичність перегляду та оновлення поточної політики оцінювання ризику;

No: 6
Name: ra_1_odp_06
Type: string
Default: nil

є події, які вимагають перегляду та оновлення поточної політики оцінювання ризику;

No: 7
Name: ra_1_odp_07
Type: string
Default: nil

визначено періодичність перегляду та оновлення поточних процедур оцінювання ризику;

No: 8
Name: ra_1_odp_08
Type: string
Default: nil

визначені події, які потребують перегляду та оновлення процедур оцінювання ризику;

No: 9
Name: ra_1_a_02
Type: string
Default: nil

RA-01a.[02] поширюється політика оцінки ризиків на <RA-01_ODP[01] персонал або ролі>;

No: 10
Name: ra_1_a_01_a_01
Type: string
Default: nil

RA-01a.01(a)[01] відповідає політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> поставленій меті;

No: 11
Name: ra_1_a_01_a_02
Type: string
Default: nil

RA-01a.01(a)[02] політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> враховує сферу застосування;

No: 12
Name: ra_1_a_01_a_03
Type: string
Default: nil

RA-01a.01(a)[03] політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> враховує ролі;

No: 13
Name: ra_1_a_01_a_04
Type: string
Default: nil

RA-01a.01(a)[04] стосується політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> обов'язків;

No: 14
Name: ra_1_a_01_a_05
Type: string
Default: nil

RA-01a.01(a)[05] враховує політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> зобов'язання керівництва;

No: 15
Name: ra_1_a_01_a_06
Type: string
Default: nil

RA-01a.01(a)[06] політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> передбачає координацію між структурними підрозділами організації;

No: 16
Name: ra_1_a_01_a_07
Type: string
Default: nil

RA-01a.01(a)[07] політика оцінювання ризику <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> враховує комплаєнс;

No: 17
Name: ra_1_a_01_b
Type: string
Default: nil

RA-01a.01(b) відповідає <RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> політика оцінювання ризику чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам і настановам;

No: 18
Name: ra_1_b
Type: string
Default: nil

RA-01b. призначено посадову особу <RA-01_ODP[04] посадову особу> для управління розробкою, документуванням та розповсюдженням політики та процедур оцінювання ризику;

No: 19
Name: ra_1_c_01_01
Type: string
Default: nil

RA-01c.01[01] переглядається та оновлюється поточна політика оцінювання ризику <RA-01_ODP[05] частота>;

No: 20
Name: ra_1_c_01_02
Type: string
Default: nil

RA-01c.01[02] переглядається та оновлюється поточна політика оцінки ризиків після <RA-01_ODP[06] події>;

No: 21
Name: ra_1_c_02_01
Type: string
Default: nil

RA-01c.02[01] переглядається та оновлюються поточні процедури оцінювання ризику <RA-01_ODP[07] частота>;

No: 22
Name: ra_1_c_02_02
Type: string
Default: nil

RA-01c.02[02] переглядаються та оновлюються поточні процедури оцінки ризиків після <RA-01_ODP[08] події>.

No: 23
Name: ra_1_a_01
Type: string
Default: nil

RA-01a.[01] розроблена та задокументована політика оцінювання ризику;

No: 24
Name: ra_1_a_03
Type: string
Default: nil

RA-01a.[03] розроблені та задокументовані процедури оцінки ризиків для сприяння впровадженню політики оцінки ризиків та пов'язаних з нею засобів контролю оцінювання ризику;

14.2. КАТЕГОРІЮВАННЯ БЕЗПЕКИ (RA-2)

Є категоризованою інформація, яку система обробляє, зберігає та передає;.

No: 1
Name: ra_2_01
Type: string
Default: nil

є категоризованою інформація, яку система обробляє, зберігає та передає;

No: 2
Name: ra_2_02
Type: string
Default: nil

результати категоризації безпеки, включно з обґрунтуванням, задокументовані в плані безпеки системи;

14.2.1. КАТЕГОРІЮВАННЯ ДРУГОГО РІВНЯ (RA-2(1))

Категоріювання другого рівня (ra-2(1)).

Немає параметрів для цього контролю.

14.3. ОЦІНЮВАННЯ РИЗИКУ (RA-3)

Частота> або коли відбуваються значні зміни в системі, середовищі її функціонування або інших умовах, які можуть вплинути на стан безпеки або приватності системи.

No: 1
Name: ra_3_odp_01
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та приватності; звіт про оцінювання ризику; <RA-03_ODP[02] документ>};

No: 2
Name: ra_3_odp_02
Type: string
Default: nil

визначено документ, в якому мають бути задокументовані результати оцінювання ризику (якщо вони не задокументовані в планах безпеки та приватності або в звіті про оцінювання ризику) (якщо вибрано);

No: 3
Name: ra_3_odp_03
Type: string
Default: nil

визначено періодичність перегляду результатів оцінювання ризику;

No: 4
Name: ra_3_odp_04
Type: string
Default: nil

визначено персонал або ролі, до яких мають бути доведені результати оцінювання ризику;

No: 5
Name: ra_3_odp_05
Type: string
Default: nil

визначена періодичність оновлення оцінювання ризику;

No: 6
Name: ra_3_c_02
Type: string
Default: nil

частота> або коли відбуваються значні зміни в системі, середовищі її функціонування або інших умовах, які можуть вплинути на стан безпеки або приватності системи.

No: 7
Name: ra_3_01
Type: string
Default: nil

інтегровані результати оцінювання ризику та рішення з управління ризиками з точки зору організації та місії або бізнес-процесів з оцінкою ризиків на системному рівні;

14.3.1. ОЦІНЮВАННЯ РИЗИКУ ЛАНЦЮГА ПОСТАЧАННЯ (RA-3(1))

Оцінювання ризику ланцюга постачання (ra-3(1)).

No: 1
Name: ra_3_1_odp_01
Type: string
Default: nil

визначені системи, компоненти системи та системні послуги для оцінювання ризику ланцюга постачання;

No: 2
Name: ra_3_1_odp_02
Type: string
Default: nil

визначено періодичність оновлення оцінювання ризику ланцюга постачання;

14.3.2. ВИКОРИСТАННЯ ІНФОРМАЦІЇ З УСІХ ДОСТУПНИХ ДЖЕРЕЛ (RA-3(2))

Використання інформації з усіх доступних джерел (ra-3(2)).

Немає параметрів для цього контролю.

14.3.3. УСВІДОМЛЕННЯ ДИНАМІЧНИХ ЗАГРОЗ (RA-3(3))

Усвідомлення динамічних загроз (ra-3(3)).

No: 1
Name: ra_3_3_odp_01
Type: string
Default: nil

є засоби для постійного визначення поточного стану кіберзагроз;

No: 2
Name: ra_3_3_odp_02
Type: string
Default: nil

засоби>.

14.3.4. ПРОГНОСТИЧНА КІБЕРАНАЛІТИКА (RA-3(4))

Розширені можливості автоматизації> для прогнозування та виявлення ризику для <RA-03(04)_ODP[02] систем або компонентів системи>;.

No: 1
Name: ra_3_4_odp_01
Type: string
Default: nil

визначені можливості розширеної автоматизації для прогнозування та виявлення ризику;

No: 2
Name: ra_3_4_odp_02
Type: string
Default: nil

є системи або компоненти системи, в яких повинні бути застосовані розширені можливості автоматизації та аналітики;

No: 3
Name: ra_3_4_odp_03

Type: string
Default: nil

визначені можливості розширеної аналітики для прогнозування та виявлення ризику;

No: 4
Name: ra_3_4_a_01
Type: string
Default: nil

розширені можливості автоматизації> для прогнозування та виявлення ризику для <RA-03(04)_ODP[02] систем або компонентів системи>;

No: 5
Name: ra_3_4_a_02
Type: string
Default: nil

розширені аналітичні можливості> для прогнозування та виявлення ризику для <RA-03(04)_ODP[02] систем або компонентів системи>.

14.4. ОНОВЛЕННЯ ОЦІНЮВАННЯ РИЗИКУ (RA-4) [Вилучено]

Оновлення оцінювання ризику (ra-4) [вилучено].

Немає параметрів для цього контролю.

14.5. СКАНУВАННЯ ВРАЗЛИВОСТЕЙ (RA-5)

Здійснюється моніторинг систем та розміщених застосунків на наявність вразливостей <RA-05_ODP[01] частота та/або випадковість відповідно до визначеного організацією процесу>, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;.

No: 1
Name: ra_5_odp_01
Type: string
Default: nil

визначена необхідність моніторингу систем та розміщених застосунків на наявність вразливостей;

No: 2
Name: ra_5_odp_02
Type: string
Default: nil

визначена періодичність перевірки систем та розміщених на них застосунків на наявність вразливостей;

No: 3
Name: ra_5_odp_03
Type: string
Default: nil

визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;

No: 4
Name: ra_5_odp_04
Type: string
Default: nil

потрібно ділитися інформацією, отриманою в процесі сканування вразливостей та оцінок контролю, з персоналом або ролями, з якими потрібно ділитися;

No: 5
Name: ra_5_a_01
Type: string
Default: nil

RA-05a.[01] здійснюється моніторинг систем та розміщених застосунків на наявність вразливостей <RA-05_ODP[01] частота та/або випадковість відповідно до визначеного організацією процесу>, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;

No: 6
Name: ra_5_a_02
Type: string
Default: nil

RA-05a.[02] перевіряються системи та розміщені застосунки на наявність вразливостей <RA-05_ODP[02] частота та/або випадковим чином відповідно до визначеного організацією процесу>, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;

No: 7
Name: ra_5_b
Type: string
Default: nil

RA-05b. застосовуються інструменти та методи моніторингу вразливостей для забезпечення сумісності між інструментами;

No: 8
Name: ra_5_b_01
Type: string
Default: nil

RA-05b.01 застосовуються інструменти та методи моніторингу вразливостей для автоматизації частини процесу управління вразливостями, використовуючи стандарти для переліку платформ, недоліків програмного забезпечення та неправильних конфігурацій;

No: 9
Name: ra_5_b_02
Type: string
Default: nil

RA-05b.02 застосовуються інструменти та методи моніторингу вразливостей для полегшення взаємодії між інструментами та автоматизації частини процесу управління вразливостями шляхом використання стандартів для формування контрольних списків та процедур тестування;

No: 10
Name: ra_5_b_03
Type: string
Default: nil

RA-05b.03 застосовуються інструменти та методи моніторингу вразливостей для полегшення взаємодії між інструментами та автоматизації частин процесу управління вразливостями шляхом використання стандартів для вимірювання впливу вразливостей;

No: 11
Name: ra_5_c
Type: string
Default: nil

RA-05c. аналізуються звіти про сканування вразливостей та результати моніторингу вразливостей;

No: 12
Name: ra_5_d
Type: string
Default: nil

RA-05d. усуваються легітимні вразливості <RA-05_ODP[03] час реагування> відповідно до організаційної оцінки ризиків;

No: 13
Name: ra_5_e
Type: string
Default: nil

RA-05e. надається інформація, отримана в процесі моніторингу вразливостей та оцінки контролю, <RA-05_ODP[04] персонал або ролі>, щоб допомогти усунути подібні вразливості в інших системах;

No: 14
Name: ra_5_f
Type: string
Default: nil

RA-05f. використовуються інструменти моніторингу вразливостей, які передбачають можливість швидкого оновлення вразливостей, що підлягають скануванню.

14.5.1. МОЖЛИВІСТЬ ОНОВЛЕННЯ ІНСТРУМЕНТІВ (RA-5(1)) [Вилучено]

Можливість оновлення інструментів (ra-5(1)) [вилучено].

Немає параметрів для цього контролю.

14.5.2. ОНОВЛЕННЯ ЗА ЧАСТОТОЮ, ПЕРЕД НОВИМ СКАНУВАННЯМ АБО ПРИ ІДЕНТИФІКАЦІЇ (RA-5(2))

Визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;.

No: 1
Name: ra_5_2_odp_01
Type: string
Default: nil

визначена необхідність моніторингу систем та розміщених застосунків на наявність вразливостей;

No: 2
Name: ra_5_2_odp_02
Type: string
Default: nil

визначена періодичність перевірки систем та розміщених на них застосунків на наявність вразливостей;

No: 3
Name: ra_5_2
Type: string
Default: nil

визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;

14.5.3. ШИРОТА ТА ГЛИБИНА ПОКРИТТЯ (RA-5(3))

Визначено ширину та глибину охоплення сканування вразливостей.

No: 1
Name: ra_5_3
Type: string
Default: nil

визначено ширину та глибину охоплення сканування вразливостей.

14.5.4. ВИЯВНА ІНФОРМАЦІЯ (RA-5(4))

Є інформація про систему відкритою;.

No: 1
Name: ra_5_4_odp_01
Type: string
Default: nil

визначені коригувальні дії, які необхідно вжити, якщо інформація про систему буде виявлена;

No: 2
Name: ra_5_4_odp_02
Type: string
Default: nil

коригувальні дії>, коли інформація про систему підтверджується як така, що може бути виявлена.

No: 3
Name: ra_5_4_01
Type: string
Default: nil

є інформація про систему відкритою;

14.5.5. ПРИВІЛЕЙОВАНИЙ ДОСТУП (RA-5(5))

(05)_ODP[01] компоненти системи> для <RAдіяльность зі сканування вразливостей>.

No: 1
Name: ra_5_5_odp_01
Type: string
Default: nil

визначено компоненти системи, до яких дозволено привілейований доступ для вибраних дій зі сканування вразливостей;

No: 2
Name: ra_5_5_odp_02
Type: string
Default: nil

визначені дії сканування вразливостей, обрані для авторизації привілейованого доступу до компонентів системи;

No: 3
Name: ra_5_5_pm
Type: string
Default: nil

05(05)_ODP[01] компоненти системи> для <RAдіяльность зі сканування вразливостей>.

14.5.6. АВТОМАТИЗОВАНИЙ АНАЛІЗ ТЕНДЕНЦІЙ (RA-5(6))

Автоматизований аналіз тенденцій (ra-5(6)).

No: 1
Name: ra_5_6_odp_01
Type: string
Default: nil

визначені автоматизовані механізми для порівняння результатів багаторазового сканування вразливостей;

No: 2
Name: ra_5_6_odp_02
Type: string
Default: nil

автоматизовані механізми>.

14.5.7. АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА СПОВІЩЕННЯ ПРО НЕАВТОРИЗОВАНІ КОМПОНЕНТИ (RA-5(7)) [Вилучено]

Автоматизоване виявлення та сповіщення про неавторизовані компоненти (ra-5(7)) [вилучено].

Немає параметрів для цього контролю.

14.5.8. ОГЛЯД ЖУРНАЛІВ АУДИТУ ЗА МИНУЛІ ПЕРІОДИ (RA-5(8))

Часовий період>.

No: 1
Name: ra_5_8_odp_01
Type: string
Default: nil

визначена система, чиї журнали аудиту за минулі періоди потрібно переглядати;

No: 2
Name: ra_5_8_odp_02

Type: string
Default: nil

визначено часовий проміжок для потенційного попереднього використання системи;

No: 3
Name: ra_5_8_pm
Type: string
Default: nil

часовий період>.

14.5.9. ТЕСТУВАННЯ ТА АНАЛІЗ ПРОНИКНЕННЯ (RA-5(9)) [Вилучено]

Тестування та аналіз проникнення (ra-5(9)) [вилучено].

Немає параметрів для цього контролю.

14.5.10. ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ ПРО СКАНУВАННЯ (RA-5(10))

Зіставлення інформації про сканування (ra-5(10)).

Немає параметрів для цього контролю.

14.5.11. ПРОГРАМА ПУБЛІЧНОГО ОПРИЛЮДНЕННЯ (RA-5(11))

Програма публічного оприлюднення (ra-5(11)).

Немає параметрів для цього контролю.

14.6. ЗАХОДИ ПРОТИДІЇ ТЕХНІЧНІЙ РОЗВІДЦІ (RA-6)

Місцезнаходження> <RA- 06_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

No: 1
Name: ra_6_odp_01
Type: string
Default: nil

визначені місця для використання заходів ПДТР;

No: 2
Name: ra_6_odp_02

Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<RA-06_ODP[03] частота>; коли <RA-06_ODP[04] події або показники>};

No: 3
Name: ra_6_odp_03
Type: string
Default: nil

визначено частоту, з якою слід проводити заходи ПДТР (якщо обрано);

No: 4
Name: ra_6_odp_04
Type: string
Default: nil

визначені події або показники, які, у разі їх виникнення, спричиняють проведення заходів ПДТР (якщо вони були обрані);

No: 5
Name: ra_6_pm
Type: string
Default: nil

місцезнаходження> <RA- 06_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

14.7. РЕАГУВАННЯ НА РИЗИК (RA-7)

Вживаються заходи реагування на результати оцінок безпеки відповідно до організаційної толерантності до ризиків;.

No: 1
Name: ra_7_01
Type: string
Default: nil

вживаються заходи реагування на результати оцінок безпеки відповідно до організаційної толерантності до ризиків;

No: 2
Name: ra_7_02
Type: string
Default: nil

вживаються заходи реагування на результати оцінювання приватності відповідно до організаційної толерантності до ризиків;

No: 3
Name: ra_7_03
Type: string
Default: nil

вживаються заходи реагування на результати моніторингу відповідно до організаційної толерантності до ризиків;

14.8. ОЦІНКА ВПЛИВУ НА ПРИВАТНІСТЬ (RA-8)

Проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед розробкою або придбанням інформаційних технологій, які які становлять ризик приватності;.

No: 1
Name: ra_8_01
Type: string
Default: nil

проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед розробкою або придбанням інформаційних технологій, які які становлять ризик приватності;

No: 2
Name: ra_8_02
Type: string
Default: nil

проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед початком збору інформації, що містить персональні дані, яка буде оброблятися за допомогою інформаційних технологій;

14.9. АНАЛІЗ КРИТИЧНОСТІ (RA-9)

Систем, системних компонентів або системних служб> в <RA-09_ODP[02] точках прийняття рішень в життєвому циклі розробки системи>.

No: 1
Name: ra_9_odp_01
Type: string
Default: nil

визначені системи, компоненти системи або системні сервіси, що підлягають аналізу на предмет критичності;

No: 2
Name: ra_9_odp_02
Type: string
Default: nil

визначені точки прийняття рішень в життєвому циклі розробки системи, коли необхідно проводити аналіз критичності;

No: 3
Name: ra_9_pm
Type: string
Default: nil

систем, системних компонентів або системних служб> в <RA-09_ODP[02] точках прийняття рішень в життєвому циклі розробки системи>.

14.10. АКТИВНИЙ ПОШУК ЗАГРОЗ (RA-10)

Активний пошук загроз.

No: 1
Name: ra_10_odp_01
Type: string
Default: nil

визначена частота, з якою слід використовувати можливість виявлення загроз;

No: 2
Name: ra_10_odp_02
Type: string
Default: nil

частота>.

15. SA

Клас заходів захисту SA — ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ

Опис Цей клас зосереджується на інтеграції вимог безпеки на всіх етапах життєвого циклу розробки та закупівлі IT-продуктів чи послуг.

Перелік заходів захисту Політики та процедури придбання систем та послуг (SA-1); Розподіл ресурсів (SA-2); Життєвий цикл розробки системи (SA-3); Управління середовищем розробки (SA-3(1)); Використання реальних даних (SA-3(2)); Оновлення технологій (SA-3(3)); Процес закупівель (SA-4); Функціональні властивості заходів (SA-4(1)); Розробка та впровадження інформації для заходів (SA-4(2)); Методи, техніки та практики розробки (SA-4(3)); Віднесення компонентів до систем (SA-4(4)); Конфігурації системи, компонента та системної служби (SA-4(5)); Використання засобів захисту інформації (SA-4(6)); Затверджені профілі захищеності (SA-4(7)); План безперервного моніторингу заходів безпеки (SA-4(8)); Функції, порти, протоколи та послуги, що використовуються (SA-4(9)); Функції, порти, протоколи та послуги, що використовуються (SA-4(10)); Процес закупівель – система записів (SA-4(11)); Процес закупівель – право власності на дані (SA-4(12)); Системна документація (SA-5); Функціональні властивості заходів безпеки (SA-5(1)); Зовнішні системні інтерфейси, (SA-5(2)); АРХІТЕКТУРА (ПРОЄКТ) ВИСОКОГО РІВНЯ (SA-5(3)); АРХІТЕКТУРА (ПРОЄКТ) НИЗЬКОГО РІВНЯ (SA-5(4)); Вихідний код (SA-5(5)); Обмеження щодо використання програмного забезпечення (SA-6); Встановлене користувачем програмне забезпечення (SA-7); Безпека та приватність принципів інжинірингу (SA-8); Чітка абстракція (SA-8(1)); Найменш поширений механізм (SA-8(2)); Модульність і багаторівневість (SA-8(3)); Безпека та приватність принципів інжинірингу – частково впорядковані залежності (SA-8(4)); Ефективний опосередкований доступ (SA-8(5)); Мінімізований обмін (SA-8(6)); Знижена складність (SA-8(7)); Еволюція безпеки в системі (SA-8(8)); Довірені компоненти системи (SA-8(9)); Ієрархічна довіра (SA-8(10)); Зворотній поріг модифікації (SA-8(11)); Ієрархічний захист (SA-8(12)); Мінімізація елементів безпеки (SA-8(13)); Найменші привілеї (SA-8(14)); Предикатний дозвіл (SA-8(15)); Самостійна надійність (SA-8(16)); Безпечно розподілена композиція (SA-8(17)); Довірені канали комунікації (SA-8(18)); Постійний захист (SA-8(19)); Безпечне керування метаданими (SA-8(20)); Самоаналіз (SA-8(21)); Звітність і відстежуваність (SA-8(22)); Безпечні параметри за замовчуванням (SA-8(23)); Збої безпеки і відновлення (SA-8(24)); Економічна безпека (SA-8(25)); Безпека продуктивності (SA-8(26)); Людський фактор безпеки (SA-8(27)); Прийнятна безпека (SA-8(28)); Повторювані і документовані процедури (SA-8(29)); Процесуальна строгість (SA-8(30)); Безпечна модифікація системи (SA-8(31)); Достатнє документування (SA-8(32)); Мінімізація (SA-8(33)); Зовнішні послуги для системи (SA-9); Оцінювання ризиків та організаційні погодження (SA-9(1)); Визначення функцій, портів, протоколів та служб (SA-9(2)); Створення та підтримка довірчих відносин з постачальниками (SA-9(3)); Узгодження інтересів споживачів і постачальників (SA-9(4)); Місце обробки, зберігання та обслуговування

(SA-9(5)); Криптографічні ключі, керовані організацією (SA-9(6)); Перевірка цілісності, що контролюється організацією (SA-9(7)); Місце обробки та зберігання – юрисдикція україни (SA-9(8)); Управління конфігурацією розробника (SA-10); Перевірка цілісності програмного забезпечення та мікропрограм (SA-10(1)); Альтернативні процеси керування конфігурацією (SA-10(2)); Перевірка цілісності апаратних засобів (SA-10(3)); Довірче генерування (SA-10(4)); Відображення цілісності для керування версіями (SA-10(5)); Довірене постачання (SA-10(6)); Представники безпеки та приватності (SA-10(7)); Представники безпеки та приватності (SA-11); Аналіз статичного коду (SA-11(1)); Моделювання загроз та аналіз вразливостей (SA-11(2)); Незалежна перевірка планів оцінювання та доказів (SA-11(3)); Ручний аналіз кодів (SA-11(4)); Тестування на проникнення (SA-11(5)); Аналіз поверхні атаки (SA-11(6)); Перевірка обсягу тестування та оцінювання (SA-11(7)); Динамічний аналіз коду (SA-11(8)); Інтерактивне тестування безпеки додатків (SA-11(9)); Керування ризиками ланцюга постачання (SA-12); Довірчість (SA-13); Аналіз критичності (SA-14); Процеси, стандарти та інструменти розробки (SA-15); Показники якості (SA-15(1)); Засоби відстеження (SA-15(2)); Засоби відстеження безпеки та приватності (SA-15(3)); Зменшення поверхні атаки (SA-15(5)); Постійне вдосконалення (SA-15(6)); Автоматизований аналіз вразливостей (SA-15(7)); Повторне використання інформації про загрози та вразливості (SA-15(8)); Використання реальних даних (SA-15(9)); План реагування на інциденти (SA-15(10)); Резервування системи або компоненту (SA-15(11)); Мінімізація використання персональної інформації (SA-15(12)); Навчання, що надається розробниками (SA-16); Проєкт та архітектура безпеки та приватності для розробника (SA-17); Формальна модель політики (SA-17(1)); Компоненти, що необхідні для забезпечення безпеки (SA-17(2)); Формальна відповідність (SA-17(3)); Неформальна відповідність (SA-17(4)); Концептуальний проєкт (SA-17(5)); Структура для тестування (SA-17(6)); Структура для найменшого привілею (SA-17(7)); Оркестровка (SA-17(8)); Різноманітність проектування (SA-17(9)); Захист та виявлення підробки (SA-18); Справжність компонента (SA-19); Індивідуальна розробка критичних компонентів (SA-20); Перевірка розробника (SA-21); Компоненти системи, що не підтримуються (SA-22); Спеціалізація (SA-23).

15.1. ПОЛІТИКИ ТА ПРОЦЕДУРИ ПРИДБАННЯ СИСТЕМ ТА ПОСЛУГ (SA-1)

Політики та процедури придбання систем та послуг.

No: 1
Name: sa-01_odp_01
Type: string
Default: nil

визначено персонал або ролі, на які поширюватиметься політика придбання систем і послуг;

No: 2
Name: sa-01_odp_02
Type: string
Default: nil

визначено персонал або ролі, на які поширюються процедури придбання систем і послуг;

No: 3
Name: sa-01_odp_03
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи};

No: 4
Name: sa-01_odp_04
Type: string
Default: nil

визначено посадову особу, яка керуватиме політикою та процедурами придбання систем і послуг;

No: 5
Name: sa-01_odp_05
Type: string
Default: nil

визначено періодичність перегляду та оновлення поточної політики придбання систем і послуг;

No: 6
Name: sa-01_odp_06
Type: string
Default: nil

є події, які вимагають перегляду та оновлення поточної політики придбання систем і послуг;

No: 7
Name: sa-01_odp_07
Type: string
Default: nil

визначено частоту, з якою переглядаються та оновлюються поточні процедури придбання систем і послуг;

No: 8
Name: sa-01_odp_08
Type: string
Default: nil

є події, які вимагають перегляду та оновлення процедур придбання систем і послуг;

15.2. РОЗПОДІЛ РЕСУРСІВ (SA-2)

Розподіл ресурсів.

Немає параметрів для цього контролю.

15.3. ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ (SA-3)

Життєвий цикл розробки системи.

No: 1
Name: sa-03_odp
Type: string
Default: nil

визначено життєвий цикл розробки системи;

15.3.1. УПРАВЛІННЯ СЕРЕДОВИЩЕМ РОЗРОБКИ (SA-3(1))

ЗАХИЩЕНЕ СЕРЕДОВИЩЕ РОЗРОБКИ СИСТЕМИ, ВІДПОВІДНО ДО РИЗИКІВ ПРОТЯГОМ УСЬОГО ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ ДЛЯ СИСТЕМИ, КОМПОНЕНТІВ СИСТЕМИ АБО СЛУЖБ.. (SA-03-01).

No: 1
Name: sa-3-1
Type: string
Default: nil

ЗАХИЩЕНЕ СЕРЕДОВИЩЕ РОЗРОБКИ СИСТЕМИ, ВІДПОВІДНО ДО РИЗИКІВ ПРОТЯГОМ УСЬОГО ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ ДЛЯ СИСТЕМИ, КОМПОНЕНТІВ СИСТЕМИ АБО СЛУЖБ.. (SA-03-01)

15.3.2. ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ (SA-3(2))

Використання реальних даних (sa-3(2)).

Немає параметрів для цього контролю.

15.3.3. ОНОВЛЕННЯ ТЕХНОЛОГІЙ (SA-3(3))

Оновлення технологій (sa-3(3)).

Немає параметрів для цього контролю.

15.4. ПРОЦЕС ЗАКУПІВЕЛЬ (SA-4)

Процес закупівель.

No: 1
Name: sa-04_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: { стандартні пункти контракту; <SA- 04_ ODP[02] пункт контракту>};

No: 2
Name: sa-04_odp_02
Type: string
Default: nil

визначено пункт контракту (якщо вибрано);

15.4.1. ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ (SA-4(1))

ПЛАНУЄТЬСЯ ОНОВЛЕННЯ ТЕХНОЛОГІЙ ДЛЯ СИСТЕМИ ПРОТЯГОМ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ; (SA-04-01).

No: 1
Name: sa-4-1
Type: string
Default: nil

ПЛАНУЄТЬСЯ ОНОВЛЕННЯ ТЕХНОЛОГІЙ ДЛЯ СИСТЕМИ ПРОТЯГОМ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ; (SA-04-01)

15.4.2. РОЗРОБКА ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЇ ДЛЯ ЗАХОДІВ (SA-4(2))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ ПОСЛУГИ НАДАВАТИ ІНФОРМАЦІЮ ПРО ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЮ ЗАСОБІВ УПРАВЛІННЯ, ЯКА ВКЛЮЧАЄ ВИКОРИСТАННЯ ДЕТАЛІЗАЦІЇ>. (SA-04-02).

No: 1
Name: sa-4-2
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ ПОСЛУГИ НАДАВАТИ ІНФОРМАЦІЮ ПРО ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЮ ЗАСОБІВ УПРАВЛІННЯ, ЯКА ВКЛЮЧАЄ ВИКОРИСТАННЯ ДЕТАЛІЗАЦІЇ>. (SA-04-02)

15.4.3. МЕТОДИ, ТЕХНІКИ ТА ПРАКТИКИ РОЗРОБКИ (SA-4(3))

Повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає <SA- 04(03)_ODP[01] методи системної інженерії>;.

No: 1
Name: sa-04_03__a_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає <SA- 04(03)_ODP[01] методи системної інженерії>;

No: 2
Name: sa-04_03__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає <SA- 04(03)_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>;

No: 3
Name: sa-04_03__c_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає <SA- 04(03)_ODP[05] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>.

15.4.4. ВІДНЕСЕННЯ КОМПОНЕНТІВ ДО СИСТЕМ (SA-4(4))

Віднесення компонентів до систем (sa-4(4)).

Немає параметрів для цього контролю.

15.4.5. КОНФІГУРАЦІЇ СИСТЕМИ, КОМПОНЕНТА ТА СИСТЕМНОЇ СЛУЖБИ (SA-4(5))

Повинен розробник системи, компонента системи або системної служби постачати систему, компонент або службу із впровадженими <SA-04(05)_ODP конфігураціями безпеки>;.

No: 1
Name: sa-04_05__odp
Type: string
Default: nil

визначено конфігурації безпеки для системи, компонента або служби;

No: 2
Name: sa-04_05__a_
Type: string
Default: nil

повинен розробник системи, компонента системи або системної служби постачати систему, компонент або службу із впровадженими <SA-04(05)_ODP конфігураціями безпеки>;

No: 3
Name: sa-04_05__b_
Type: string
Default: nil

будуть конфігурації використовуватися за замовчуванням для будь-якої наступної переінсталяції або оновлення системи, компонента чи служби.

15.4.6. ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ (SA-4(6))

Використовуються лише засоби захисту інформації, які пройшли державну експертизу або сертифікацію, створені для технічного та криптографічного захисту інформації;.

No: 1
Name: sa-04_06__a_
Type: string
Default: nil

використовуються лише засоби захисту інформації, які пройшли державну експертизу або сертифікацію, створені для технічного та криптографічного захисту інформації;

No: 2
Name: sa-04_06__b_
Type: string
Default: nil

були ці засоби захисту мають позитивний експертний висновок або сертифікат відповідності, а також відповідні дозволи для використання для захисту критичної інформації.

15.4.7. ЗАТВЕРДЖЕНІ ПРОФІЛІ ЗАХИЩЕНОСТІ (SA-4(7))

Обмежується використання комерційної готової до використання технічної продукції, створеної для захисту інформації та з функцією підтримки забезпечення безпеки інформації, до тих продуктів, які були успішно оцінені відповідно до профілю захищеності для конкретного типу технології, затвердженого уповноваженим державним органом, якщо такий профіль наявний;.

No: 1
Name: sa-04_07__a_
Type: string
Default: nil

обмежується використання комерційної готової до використання технічної продукції, створеної для захисту інформації та з функцією підтримки забезпечення безпеки інформації, до тих продуктів, які були успішно оцінені відповідно до профілю захищеності для конкретного типу технології, затвердженого уповноваженим державним органом, якщо такий профіль наявний;

No: 2
Name: sa-04_07__b_
Type: string
Default: nil

якщо немає профілю захищеності для певного типу технологій, затвердженого уповноваженим органом, але забезпечення політики безпеки продукту, що надається на комерційній основі, залежить від криптографічних функцій, — вимагати, щоб криптографічний модуль пройшов державну експертизу, мав позитивний експертний висновок і був рекомендований до використання уповноваженим органом.

15.4.8. ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЗАХОДІВ БЕЗПЕКИ (SA-4(8))

РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТВОРИВ ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЕФЕКТИВНОСТІ ЗАХОДІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ, ЯКИЙ УЗГОДЖУЄТЬСЯ З ВІДПОВІДНИМ ПЛАНОМ ПОСТІЙНОГО МОНІТОРИНГУ ОРГАНІЗАЦІЇ. (SA-04-08).

No: 1
Name: sa-4-8
Type: string
Default: nil

РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТВОРИВ ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЕФЕКТИВНОСТІ ЗАХОДІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ, ЯКИЙ УЗГОДЖУЄТЬСЯ З ВІДПОВІДНИМ ПЛАНОМ ПОСТІЙНОГО МОНІТОРИНГУ ОРГАНІЗАЦІЇ. (SA-04-08)

15.4.9. ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ (SA-4(9))

Функції, порти, протоколи та послуги, що використовуються (sa-4(9)).

Немає параметрів для цього контролю.

15.4.10. ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ (SA-4(10))

ВИКОРИСТОВУЄТЬСЯ ЛИШЕ ТА ІНФОРМАЦІЙНО-ТЕХНІЧНА ПРОДУКЦІЯ, ЩО ПЕРЕБУВАЄ В СПИСКУ ПРОДУКТІВ СХВАЛЕНИХ FIPS 201, ЗАТВЕРДЖЕНИХ УПОВНОВАЖЕНИМ ОРГАНОМ, ДЛЯ МОЖЛИВОСТЕЙ ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ (PIV), РЕАЛІЗОВАНИХ В СИСТЕМАХ ОРГАНІЗАЦІЇ. (SA-04-10).

No: 1
Name: sa-4-10
Type: string
Default: nil

ВИКОРИСТОВУЄТЬСЯ ЛИШЕ ТА ІНФОРМАЦІЙНО-ТЕХНІЧНА ПРОДУКЦІЯ, ЩО ПЕРЕБУВАЄ В СПИСКУ ПРОДУКТІВ СХВАЛЕНИХ FIPS 201, ЗАТВЕРДЖЕНИХ УПОВНОВАЖЕНИМ ОРГАНОМ, ДЛЯ МОЖЛИВОСТЕЙ ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ (PIV), РЕАЛІЗОВАНИХ В СИСТЕМАХ ОРГАНІЗАЦІЇ. (SA-04-10)

15.4.11. ПРОЦЕС ЗАКУПІВЕЛЬ – СИСТЕМА ЗАПИСІВ (SA-4(11))

ВИЗНАЧЕНІ В ДОГОВОРІ ПРО ЗАКУПІВЛЮ <SA-04(11)_ODP ВИМОГИ ЗАКОНУ ПРО КОНФІДЕНЦІЙНІСТЬ> ДЛЯ ЕКСПЛУАТАЦІЇ СИСТЕМИ ЗАПИСІВ ВІД ІМЕНІ ОРГАНІЗАЦІЇ З МЕТОЮ ВИКОНАННЯ ОРГАНІЗАЦІЙНОЇ МІСІЇ АБО ФУНКЦІЇ. (SA-04-11).

No: 1
Name: sa-04_11__odp
Type: string
Default: nil

визначені вимоги Закону про конфіденційність до функціонування записів системи;

No: 2
Name: sa-4-11
Type: string
Default: nil

ВИЗНАЧЕНІ В ДОГОВОРІ ПРО ЗАКУПІВЛЮ <SA-04(11)_ODP ВИМОГИ ЗАКОНУ ПРО КОНФІДЕНЦІЙНІСТЬ> ДЛЯ ЕКСПЛУАТАЦІЇ СИСТЕМИ ЗАПИСІВ ВІД ІМЕНІ ОРГАНІЗАЦІЇ З МЕТОЮ ВИКОНАННЯ ОРГАНІЗАЦІЙНОЇ МІСІЇ АБО ФУНКЦІЇ. (SA-04-11)

15.4.12. ПРОЦЕС ЗАКУПІВЕЛЬ – ПРАВО ВЛАСНОСТІ НА ДАНІ (SA-4(12))

Включені вимоги щодо права власності на дані організації до договору про придбання;.

No: 1
Name: sa-04_12__odp
Type: string
Default: nil

визначені часові рамки для видалення даних із системи підрядника та повернення їх до організації;

No: 2
Name: sa-04_12__a_
Type: string
Default: nil

включені вимоги щодо права власності на дані організації до договору про придбання;

No: 3
Name: sa-04_12__b_
Type: string
Default: nil

потрібно видаляти всі дані з системи підрядника та повертати їх до організації протягом <SA-04(12)_ODP період часу>.

15.5. СИСТЕМНА ДОКУМЕНТАЦІЯ (SA-5)

Системна документація.

No: 1
Name: sa-05_odp_01
Type: string
Default: nil

визначені дії, яких слід вжити, коли документація на систему, системний компонент або системне обслуговування недоступна або відсутня;

No: 2
Name: sa-05_odp_02
Type: string
Default: nil

визначено персонал або ролі для розповсюдження системної документації;

15.5.1. ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ БЕЗПЕКИ (SA-5(1))

Функціональні властивості заходів безпеки (sa-5(1)).

Немає параметрів для цього контролю.

15.5.2. ЗОВНІШНІ СИСТЕМНІ ІНТЕРФЕЙСИ, (SA-5(2))

Зовнішні системні інтерфейси, (sa-5(2)).

Немає параметрів для цього контролю.

15.5.3. АРХІТЕКТУРА (ПРОЄКТ) ВИСОКОГО РІВНЯ (SA-5(3))

Архітектура (проєкт) високого рівня (sa-5(3)).

Немає параметрів для цього контролю.

15.5.4. АРХІТЕКТУРА (ПРОЄКТ) НИЗЬКОГО РІВНЯ (SA-5(4))

Архітектура (проєкт) низького рівня (sa-5(4)).

Немає параметрів для цього контролю.

15.5.5. ВИХІДНИЙ КОД (SA-5(5))

Вихідний код (sa-5(5)).

Немає параметрів для цього контролю.

15.6. ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (SA-6)

Обмеження щодо використання програмного забезпечення.

Немає параметрів для цього контролю.

15.7. ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ (SA-7)

Встановлене користувачем програмне забезпечення.

Немає параметрів для цього контролю.

15.8. БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ (SA-8)

Безпека та приватність принципів інжинірингу.

No: 1
Name: sa-08_odp_01
Type: string
Default: nil

визначені принципи інжинірингу безпеки систем;

No: 2
Name: sa-08_odp_02
Type: string
Default: nil

визначені принципи інжинірингу конфіденційності системи;

15.8.1. ЧІТКА АБСТРАКЦІЯ (SA-8(1))

РЕАЛІЗОВАНО ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЧІТКИХ АБСТРАКЦІЙ. (SA-08-01).

No: 1
Name: sa-8-1
Type: string
Default: nil

РЕАЛІЗОВАНО ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЧІТКИХ АБСТРАКЦІЙ. (SA-08-01)

15.8.2. НАЙМЕНШ ПОШИРЕНИЙ МЕХАНІЗМ (SA-8(2))

РЕАЛІЗУЮТЬ <SA-08(02)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ НАЙМЕНШ ПОШИРЕНОГО МЕХАНІЗМУ. (SA-08-02).

No: 1
Name: sa-08_02__odp
Type: string
Default: nil

реалізовано принцип проектування безпеки чітких абстракцій.

No: 2
Name: sa-8-2
Type: string
Default: nil

РЕАЛІЗУЮТЬ <SA-08(02)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ НАЙМЕНШ ПОШИРЕНОГО МЕХАНІЗМУ. (SA-08-02)

15.8.3. МОДУЛЬНІСТЬ І БАГАТОРІВНЕВІСТЬ (SA-8(3))

Модульність і багаторівневість (sa-8(3)).

Немає параметрів для цього контролю.

15.8.4. БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ – ЧАСТКОВО ВПОРЯДКОВАНІ ЗАЛЕЖНОСТІ (SA-8(4))

<SA-08(04)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЧАСТКОВО ВПОРЯДКОВАНИХ ЗАЛЕЖНОСТЕЙ. (SA-08-04).

No: 1
Name: sa-08_04__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип проектування безпеки частково впорядкованих залежностей;

No: 2
Name: sa-8-4
Type: string
Default: nil

<SA-08(04)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЧАСТКОВО ВПОРЯДКОВАНИХ ЗАЛЕЖНОСТЕЙ. (SA-08-04)

15.8.5. ЕФЕКТИВНИЙ ОПОСЕРЕДКОВАНИЙ ДОСТУП (SA-8(5))

<SA-08(05)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЕФЕКТИВНОГО ОПОСЕРЕДКОВАНОГО ДОСТУПУ. (SA-08-05).

No: 1
Name: sa-08_05__odp
Type: string
Default: nil

визначені системи або її компоненти, які реалізують принцип проектування безпеки ефективного опосередкованого доступу;

No: 2
Name: sa-8-5
Type: string
Default: nil

<SA-08(05)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЕФЕКТИВНОГО ОПОСЕРЕДКОВАНОГО ДОСТУПУ. (SA-08-05)

15.8.6. МІНІМІЗОВАНИЙ ОБМІН (SA-8(6))

<SA-08(06)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ МІНІМІЗАЦІЇ СПІЛЬНОГО ВИКОРИСТАННЯ. (SA-08-06).

No: 1
Name: sa-08_06__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип проектування безпеки, що полягає в мінімізації спільного використання;

No: 2
Name: sa-8-6
Type: string
Default: nil

<SA-08(06)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ МІНІМІЗАЦІЇ СПІЛЬНОГО ВИКОРИСТАННЯ. (SA-08-06)

15.8.7. ЗНИЖЕНА СКЛАДНІСТЬ (SA-8(7))

<SA-08(07)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗА ПРИНЦИПОМ ЗНИЖЕНОЇ СКЛАДНОСТІ. (SA-08-07).

No: 1
Name: sa-08_07__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип проектування безпеки за принципом зниженої складності;

No: 2
Name: sa-8-7
Type: string
Default: nil

<SA-08(07)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗА ПРИНЦИПОМ ЗНИЖЕНОЇ СКЛАДНОСТІ. (SA-08-07)

15.8.8. ЕВОЛЮЦІЯ БЕЗПЕКИ В СИСТЕМІ (SA-8(8))

<SA-08(08)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОГО ПРОЕКТУВАННЯ БЕЗПЕЧНОЇ ЕВОЛЮЦІЙНОСТІ. (SA-08-08).

No: 1
Name: sa-08_08__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип безпечного проектування безпечної еволюційності;

No: 2
Name: sa-8-8
Type: string
Default: nil

<SA-08(08)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОГО ПРОЕКТУВАННЯ БЕЗПЕЧНОЇ ЕВОЛЮЦІЙНОСТІ. (SA-08-08)

15.8.9. ДОВІРЕНІ КОМПОНЕНТИ СИСТЕМИ (SA-8(9))

<SA-08(09)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ДОВІРЕНИХ КОМПОНЕНТІВ. (SA-08-09).

No: 1
Name: sa-08_09__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип побудови безпеки довірених компонентів;

No: 2
Name: sa-8-9
Type: string
Default: nil

<SA-08(09)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ДОВІРЕНИХ КОМПОНЕНТІВ. (SA-08-09)

15.8.10. ІЄРАРХІЧНА ДОВІРА (SA-8(10))

<SA-08(09)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ІЄРАРХІЧНОЇ ДОВІРИ В ДИЗАЙНІ БЕЗПЕКИ. (SA-08-10).

No: 1
Name: sa-08_10__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип ієрархічної довіри при проектуванні безпеки;

No: 2
Name: sa-8-10
Type: string
Default: nil

<SA-08(09)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ІЄРАРХІЧНОЇ ДОВІРИ В ДИЗАЙНІ БЕЗПЕКИ. (SA-08-10)

15.8.11. ЗВОРОТНІЙ ПОРІГ МОДИФІКАЦІЇ (SA-8(11))

<SA-08(11)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗВОРОТНОГО ПОРОГУ МОДИФІКАЦІЇ. (SA-08-11).

No: 1
Name: sa-08_11__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип ієрархічної довіри при проектуванні безпеки;

No: 2
Name: sa-8-11
Type: string
Default: nil

<SA-08(11)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗВОРОТНОГО ПОРОГУ МОДИФІКАЦІЇ. (SA-08-11)

15.8.12. ІЄРАРХІЧНИЙ ЗАХИСТ (SA-8(12))

<SA-08(12)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ ІЄРАРХІЧНОГО ЗАХИСТУ. (SA-08-12).

No: 1
Name: sa-08_12__odp
Type: string
Default: nil

визначені системи або компоненти системи, які реалізують принцип ієрархічного дизайну безпеки;

No: 2
Name: sa-08_13__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип проектування безпеки за принципом мінімізації елементів безпеки;

No: 3
Name: sa-8-12
Type: string
Default: nil

<SA-08(12)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ ІЄРАРХІЧНОГО ЗАХИСТУ. (SA-08-12)

15.8.13. МІНІМІЗАЦІЯ ЕЛЕМЕНТІВ БЕЗПЕКИ (SA-8(13))

Мінімізація елементів безпеки (sa-8(13)).

Немає параметрів для цього контролю.

15.8.14. НАЙМЕНШІ ПРИВІЛЕЇ (SA-8(14))

<SA-08(14)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ НАЙМЕНШИХ ПРИВІЛЕЇВ. (SA-08-14).

No: 1
Name: sa-08_14__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип побудови безпеки за принципом найменших привілеїв;

No: 2
Name: sa-8-14
Type: string
Default: nil

<SA-08(14)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ЗА ПРИНЦИПОМ НАЙМЕНШИХ ПРИВІЛЕЇВ. (SA-08-14)

15.8.15. ПРЕДИКАТНИЙ ДОЗВІЛ (SA-8(15))

<SA-08(15)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ПОПЕРЕДНЬОГО ДОЗВОЛУ. (SA-08-15).

No: 1
Name: sa-08_15__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип проектування безпеки попереднього дозволу;

No: 2
Name: sa-8-15
Type: string
Default: nil

<SA-08(15)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ПОПЕРЕДНЬОГО ДОЗВОЛУ. (SA-08-15)

15.8.16. САМОСТІЙНА НАДІЙНІСТЬ (SA-8(16))

<SA-08(16)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ САМОДОСТАТНЬОЇ НАДІЙНОСТІ. (SA-08-16).

No: 1
Name: sa-08_16__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип проектування безпеки, що ґрунтується на самодостатній надійності;

No: 2
Name: sa-8-16
Type: string
Default: nil

<SA-08(16)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ САМОДОСТАТНЬОЇ НАДІЙНОСТІ. (SA-08-16)

15.8.17. БЕЗПЕЧНО РОЗПОДІЛЕНА КОМПОЗИЦІЯ (SA-8(17))

<SA-08(17)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗАХИЩЕНОГО РОЗПОДІЛЕНОГО ВМІСТУ. (SA-08-17).

No: 1
Name: sa-08_17__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпечного проектування захищеного розподіленого вмісту;

No: 2
Name: sa-8-17
Type: string
Default: nil

<SA-08(17)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ЗАХИЩЕНОГО РОЗПОДІЛЕНОГО ВМІСТУ. (SA-08-17)

15.8.18. ДОВІРЕНІ КАНАЛИ КОМУНІКАЦІЇ (SA-8(18))

<SA-08(18)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ДОВІРЕНИХ КАНАЛІВ ЗВ'ЯЗКУ. (SA-08-18).

No: 1
Name: sa-08_18__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип побудови безпеки довірених каналів зв'язку;

No: 2
Name: sa-8-18
Type: string
Default: nil

<SA-08(18)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОБУДОВИ БЕЗПЕКИ ДОВІРЕНИХ КАНАЛІВ ЗВ'ЯЗКУ. (SA-08-18)

15.8.19. ПОСТІЙНИЙ ЗАХИСТ (SA-8(19))

<SA-08(19)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ДОВГОТРИВАЛОГО (SA-08-19).

No: 1
Name: sa-08_19__odp
Type: string
Default: nil

визначено системи або компоненти системи, які втілюють принцип проектування безпеки довготривалого захисту.

No: 2
Name: sa-8-19
Type: string
Default: nil

<SA-08(19)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ ДОВГОТРИВАЛОГО (SA-08-19)

15.8.20. БЕЗПЕЧНЕ КЕРУВАННЯ МЕТАДАНИМИ (SA-8(20))

<SA-08(20)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОГО УПРАВЛІННЯ МЕТАДАНИМИ. (SA-08-20).

No: 1
Name: sa-08_20__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпечного управління метаданими.

No: 2
Name: sa-8-20
Type: string
Default: nil

<SA-08(20)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОГО УПРАВЛІННЯ МЕТАДАНИМИ. (SA-08-20)

15.8.21. САМОАНАЛІЗ (SA-8(21))

<SA-08(21)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ НА ОСНОВІ САМОАНАЛІЗУ. (SA-08-21).

No: 1
Name: sa-08_21__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип самоаналізу при проектуванні безпеки;

No: 2
Name: sa-8-21
Type: string
Default: nil

<SA-08(21)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕКИ НА ОСНОВІ САМОАНАЛІЗУ. (SA-08-21)

15.8.22. ЗВІТНІСТЬ І ВІДСТЕЖУВАНІСТЬ (SA-8(22))

Звітність і відстежуваність (sa-8(22)).

Немає параметрів для цього контролю.

15.8.23. БЕЗПЕЧНІ ПАРАМЕТРИ ЗА ЗАМОВЧУВАННЯМ (SA-8(23))

<SA-08(23)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕЧНИХ НАЛАШТУВАНЬ ЗА ЗАМОВЧУВАННЯМ. (SA-08-23).

No: 1
Name: sa-08_23__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпечних налаштувань за замовчуванням;

No: 2
Name: sa-8-23
Type: string
Default: nil

<SA-08(23)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ БЕЗПЕЧНИХ НАЛАШТУВАНЬ ЗА ЗАМОВЧУВАННЯМ. (SA-08-23)

15.8.24. ЗБОЇ БЕЗПЕКИ І ВІДНОВЛЕННЯ (SA-8(24))

Збої безпеки і відновлення (sa-8(24)).

Немає параметрів для цього контролю.

15.8.25. ЕКОНОМІЧНА БЕЗПЕКА (SA-8(25))

<SA-08(25)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ ЕКОНОМІКИ. (SA-08-25).

No: 1
Name: sa-08_25__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпеки економіки;

No: 2
Name: sa-8-25
Type: string
Default: nil

<SA-08(25)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ ЕКОНОМІКИ. (SA-08-25)

15.8.26. БЕЗПЕКА ПРОДУКТИВНОСТІ (SA-8(26))

<SA-08(26)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ ПРОДУКТИВНОСТІ. (SA-08-26).

No: 1
Name: sa-08_26__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпеки продуктивності;

No: 2
Name: sa-8-26
Type: string
Default: nil

<SA-08(26)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ ПРОДУКТИВНОСТІ. (SA-08-26)

15.8.27. ЛЮДСЬКИЙ ФАКТОР БЕЗПЕКИ (SA-8(27))

<SA-08(27)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ З УРАХУВАННЯМ ЛЮДСЬКОГО ФАКТОРУ. (SA-08-27).

No: 1
Name: sa-08_27__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпеки з урахуванням людського

No: 2
Name: sa-8-27
Type: string
Default: nil

<SA-08(27)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕКИ З УРАХУВАННЯМ ЛЮДСЬКОГО ФАКТОРУ. (SA-08-27)

15.8.28. ПРИЙНЯТНА БЕЗПЕКА (SA-8(28))

<SA-08(28)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРИЙНЯТНОГО РІВНЯ БЕЗПЕКИ. (SA-08-28).

No: 1
Name: sa-08_28__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип прийнятного рівня безпеки;

No: 2
Name: sa_08_28_a
Type: string
Default: nil

<SA-08(28)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРИЙНЯТНОГО РІВНЯ БЕЗПЕКИ. (SA-08-28)

No: 3
Name: sa_08_28_b

Type: string
Default: nil

<SA-08(29)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПОВТОРЮВАНИХ ТА ЗАДОКУМЕНТОВАНИХ ПРОЦЕДУР. (SA-08-28)

No: 4
Name: sa_08_28_c
Type: string
Default: nil

<SA-08(30)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ПРОЕКТУВАННЯ ПРИЙНЯТНОЇ БЕЗПЕКИ. (SA-08-28)

15.8.29. ПОВТОРЮВАНІ І ДОКУМЕНТОВАНІ ПРОЦЕДУРИ (SA-8(29))

Повторювані і документовані процедури (sa-8(29)).

No: 1
Name: sa-08_29__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип повторюваних та задокументованих процедур;

15.8.30. ПРОЦЕСУАЛЬНА СТРОГІСТЬ (SA-8(30))

Процесуальна строгість (sa-8(30)).

No: 1
Name: sa-08_30__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип проектування прийнятної безпеки;

15.8.31. БЕЗПЕЧНА МОДИФІКАЦІЯ СИСТЕМИ (SA-8(31))

<SA-08(31)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОЇ МОДИФІКАЦІЇ СИСТЕМ. (SA-08-31).

No: 1
Name: sa-08_31__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип безпечної модифікації систем;

No: 2
Name: sa-8-31
Type: string
Default: nil

<SA-08(31)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП БЕЗПЕЧНОЇ МОДИФІКАЦІЇ СИСТЕМ. (SA-08-31)

15.8.32. ДОСТАТНЄ ДОКУМЕНТУВАННЯ (SA-8(32))

<SA-08(32)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ДОСТАТНЬОЇ ДОПУСКНОЇ ДОКУМЕНТАЦІЇ. (SA-08-32).

No: 1
Name: sa-08_32__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип достатньої допускної документації;

No: 2
Name: sa-8-32
Type: string
Default: nil

<SA-08(32)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП ДОСТАТНЬОЇ ДОПУСКНОЇ ДОКУМЕНТАЦІЇ. (SA-08-32)

15.8.33. МІНІМІЗАЦІЯ (SA-8(33))

<SA-08(33)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП МІНІМІЗАЦІЇ КОНФІДЕНЦІЙНОСТІ. (SA-08-33).

No: 1
Name: sa-08_33__odp
Type: string
Default: nil

визначено системи або компоненти системи, які реалізують принцип мінімізації конфіденційності;

No: 2
Name: sa-8-33
Type: string
Default: nil

<SA-08(33)_ODP СИСТЕМИ АБО КОМПОНЕНТИ СИСТЕМИ> РЕАЛІЗУЮТЬ ПРИНЦИП МІНІМІЗАЦІЇ КОНФІДЕНЦІЙНОСТІ. (SA-08-33)

15.9. ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ (SA-9)

Зовнішні послуги для системи.

No: 1
Name: sa-09_odp_01
Type: string
Default: nil

визначені засоби контролю, які будуть застосовуватися зовнішніми постачальниками системних послуг;

No: 2
Name: sa-09_odp_02
Type: string
Default: nil

визначені процеси, методи та техніки, що застосовуються для моніторингу дотримання вимог контролю зовнішніми постачальниками послуг;

15.9.1. ОЦІНЮВАННЯ РИЗИКІВ ТА ОРГАНІЗАЦІЙНІ ПОГОДЖЕННЯ (SA-9(1))

Проводиться організаційна оцінка ризиків перед придбанням або передачею послуг з інформаційної безпеки;.

No: 1
Name: sa-09_01__odp
Type: string
Default: nil

визначено персонал або ролі, які схвалюють придбання або передачу спеціальних послуг з інформаційної безпеки;

No: 2
Name: sa-09_01__a_
Type: string
Default: nil

проводиться організаційна оцінка ризиків перед придбанням або передачею послуг з інформаційної безпеки;

No: 3
Name: sa-09_01__b_
Type: string
Default: nil

схвалюють <SA-09(01)_ODP персонал або ролі> придбання або передачу спеціальних послуг з інформаційної безпеки.

15.9.2. ВИЗНАЧЕННЯ ФУНКЦІЙ, ПОРТІВ, ПРОТОКОЛІВ ТА СЛУЖБ (SA-9(2))

НЕОБХІДНО ПОСТАЧАЛЬНИКАМ <SA-09(02)_ODP ЗОВНІШНІХ СИСТЕМНИХ ПОСЛУГ> ІДЕНТИФІКУВАТИ ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ІНШІ ПОСЛУГИ, НЕОБХІДНІ ДЛЯ ВИКОРИСТАННЯ ТАКИХ ПОСЛУГ. (SA-09-02).

No: 1
Name: sa-09_02__odp
Type: string
Default: nil

визначені зовнішні системні сервіси, які потребують ідентифікації функцій, портів, протоколів та інших сервісів;

No: 2
Name: sa-9-2
Type: string
Default: nil

НЕОБХІДНО ПОСТАЧАЛЬНИКАМ <SA-09(02)_ODP ЗОВНІШНІХ СИСТЕМНИХ ПОСЛУГ> ІДЕНТИФІКУВАТИ ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ІНШІ ПОСЛУГИ, НЕОБХІДНІ ДЛЯ ВИКОРИСТАННЯ ТАКИХ ПОСЛУГ. (SA-09-02)

15.9.3. СТВОРЕННЯ ТА ПІДТРИМКА ДОВІРЧИХ ВІДНОСИН З ПОСТАЧАЛЬНИКАМИ (SA-9(3))

Створення та підтримка довірчих відносин з постачальниками (sa-9(3)).

Немає параметрів для цього контролю.

15.9.4. УЗГОДЖЕННЯ ІНТЕРЕСІВ СПОЖИВАЧІВ І ПОСТАЧАЛЬНИКІВ (SA-9(4))

ВЖИВАЮТЬСЯ <SA-09(04)_ODP[02] ДІЇ> ДЛЯ ПЕРЕВІРКИ ТОГО, ЩО ПОСЛУГ> УЗГОДЖУЮТЬСЯ З ІНТЕРЕСАМИ ОРГАНІЗАЦІЇ ТА (SA-09-04).

No: 1
Name: sa-9-4
Type: string
Default: nil

ВЖИВАЮТЬСЯ <SA-09(04)_ODP[02] ДІЇ> ДЛЯ ПЕРЕВІРКИ ТОГО, ЩО ПОСЛУГ> УЗГОДЖУЮТЬСЯ З ІНТЕРЕСАМИ ОРГАНІЗАЦІЇ ТА (SA-09-04)

15.9.5. МІСЦЕ ОБРОБКИ, ЗБЕРІГАННЯ ТА ОБСЛУГОВУВАННЯ (SA-9(5))

НА ОСНОВІ ВИМОГ <SA-09(05)_ODP[03]>, <SA-09(05)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> ОБМЕЖЕНЕ(І) (SA-09-05).

No: 1
Name: sa-9-5
Type: string
Default: nil

НА ОСНОВІ ВИМОГ <SA-09(05)_ODP[03]>, <SA-09(05)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)> ОБМЕЖЕНЕ(І) (SA-09-05)

15.9.6. КРИПТОГРАФІЧНІ КЛЮЧІ, КЕРОВАНІ ОРГАНІЗАЦІЄЮ (SA-9(6))

ЗБЕРІГАЄТЬСЯ ЕКСКЛЮЗИВНИЙ КОНТРОЛЬ НАД КРИПТОГРАФІЧНИМИ КЛЮЧАМИ ДЛЯ ЗАШИФРОВАНИХ МАТЕРІАЛІВ, ЩО ЗБЕРІГАЮТЬСЯ АБО ПЕРЕДАЮТЬСЯ ЧЕРЕЗ ЗОВНІШНЮ СИСТЕМУ. (SA-09-06).

No: 1
Name: sa-9-6

Type: string
Default: nil

ЗБЕРІГАЄТЬСЯ ЕКСКЛЮЗИВНИЙ КОНТРОЛЬ НАД КРИПТОГРАФІЧНИМИ КЛЮЧАМИ ДЛЯ ЗАШИФРОВАНИХ МАТЕРІАЛІВ, ЩО ЗБЕРІГАЮТЬСЯ АБО ПЕРЕДАЮТЬСЯ ЧЕРЕЗ ЗОВНІШНЮ СИСТЕМУ. (SA-09-06)

15.9.7. ПЕРЕВІРКА ЦІЛІСНОСТІ, ЩО КОНТРОЛЮЄТЬСЯ ОРГАНІЗАЦІЄЮ (SA-9(7))

ПЕРЕДБАЧЕНА МОЖЛИВІСТЬ ПЕРЕВІРКИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ ПІД ЧАС ЇЇ ПЕРЕБУВАННЯ У ЗОВНІШНІЙ СИСТЕМІ. (SA-09-07).

No: 1
Name: sa-9-7
Type: string
Default: nil

ПЕРЕДБАЧЕНА МОЖЛИВІСТЬ ПЕРЕВІРКИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ ПІД ЧАС ЇЇ ПЕРЕБУВАННЯ У ЗОВНІШНІЙ СИСТЕМІ. (SA-09-07)

15.9.8. МІСЦЕ ОБРОБКИ ТА ЗБЕРІГАННЯ – ЮРИСДИКЦІЯ УКРАЇНИ (SA-9(8))

ОБМЕЖУЄТЬСЯ ГЕОГРАФІЧНЕ РОЗМІЩЕННЯ ОБРОБКИ ІНФОРМАЦІЇ ТА ЗБЕРІГАННЯ ДАНИХ ОБ'ЄКТАМИ, РОЗТАШОВАНИМИ В МЕЖАХ ЮРИДИЧНОЇ ЮРИСДИКЦІЇ УКРАЇНИ (SA-09-08).

No: 1
Name: sa-9-8
Type: string
Default: nil

ОБМЕЖУЄТЬСЯ ГЕОГРАФІЧНЕ РОЗМІЩЕННЯ ОБРОБКИ ІНФОРМАЦІЇ ТА ЗБЕРІГАННЯ ДАНИХ ОБ'ЄКТАМИ, РОЗТАШОВАНИМИ В МЕЖАХ ЮРИДИЧНОЇ ЮРИСДИКЦІЇ УКРАЇНИ (SA-09-08)

15.10. УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА (SA-10)

Управління конфігурацією розробника.

No: 1
Name: sa-10_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {дизайн; розробка; впровадження; експлуатація; утилізація};

No: 2
Name: sa-10_odp_02

Type: string
Default: nil

визначено елементи конфігурації під керуванням;

No: 3
Name: sa-10_odp_03
Type: string
Default: nil

визначено персонал, якому повідомляється про недоліки безпеки та способи їх усунення в системі, компонента або служби;

15.10.1. ПЕРЕВІРКА ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ (SA-10(1))

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОГО СЛУЖБИ ЗАБЕЗПЕЧИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПОНЕНТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. (SA-10-01).

No: 1
Name: sa-10-1
Type: string
Default: nil

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОГО СЛУЖБИ ЗАБЕЗПЕЧИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМПОНЕНТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. (SA-10-01)

15.10.2. АЛЬТЕРНАТИВНІ ПРОЦЕСИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ (SA-10(2))

БУЛО ПЕРЕДБАЧЕНО АЛЬТЕРНАТИВНИЙ ПРОЦЕС КЕРУВАННЯ КОНФІГУРАЦІЄЮ ЗА ДОПОМОГОЮ ОРГАНІЗАЦІЙНОГО ПЕРСОНАЛУ ЗА ВІДСУТНОСТІ СПЕЦІАЛІЗОВАНОЇ КОМАНДИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ (SA-10-02).

No: 1
Name: sa-10-2
Type: string
Default: nil

БУЛО ПЕРЕДБАЧЕНО АЛЬТЕРНАТИВНИЙ ПРОЦЕС КЕРУВАННЯ КОНФІГУРАЦІЄЮ ЗА ДОПОМОГОЮ ОРГАНІЗАЦІЙНОГО ПЕРСОНАЛУ ЗА ВІДСУТНОСТІ СПЕЦІАЛІЗОВАНОЇ КОМАНДИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ (SA-10-02)

15.10.3. ПЕРЕВІРКА ЦІЛІСНОСТІ АПАРАТНИХ ЗАСОБІВ (SA-10(3))

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ УМОЖЛИВИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ АПАРАТНИХ КОМПОНЕНТІВ. (SA-10-03).

No: 1
Name: sa-10-3
Type: string
Default: nil

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ УМОЖЛИВИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ АПАРАТНИХ КОМПОНЕНТІВ. (SA-10-03)

15.10.4. ДОВІРЧЕ ГЕНЕРУВАННЯ (SA-10(4))

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ УМОЖЛИВИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ АПАРАТНИХ КОМПОНЕНТІВ. (SA-10-04).

No: 1
Name: sa_10_04_a
Type: string
Default: nil

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ УМОЖЛИВИТИ ПЕРЕВІРКУ ЦІЛІСНОСТІ АПАРАТНИХ КОМПОНЕНТІВ. (SA-10-04)

No: 2
Name: sa_10_04_b
Type: string
Default: nil

УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЧЕ ГЕНЕРУВАННЯ

15.10.5. ВІДОБРАЖЕННЯ ЦІЛІСНОСТІ ДЛЯ КЕРУВАННЯ ВЕРСІЯМИ (SA-10(5))

ПОВИНЕН РОЗРОБНИКА СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ПІДТРИМУВАТИ ЦІЛІСНІСТЬ ВІДОБРАЖЕННЯ МІЖ ОСНОВНИМИ ДАНИМИ ЗБІРКИ, ЩО ОПИСУЮТЬ ПОТОЧНУ ВЕРСІЮ АПАРАТНОГО, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ, І ЛОКАЛЬНОЮ ГОЛОВНОЮ КОПІЄЮ ДАНИХ ДЛЯ ПОТОЧНИХ ВЕРСІЙ. (SA-10-05).

No: 1
Name: sa-10-5
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИКА СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ПІДТРИМУВАТИ ЦІЛІСНІСТЬ ВІДОБРАЖЕННЯ МІЖ ОСНОВНИМИ ДАНИМИ ЗБІРКИ, ЩО ОПИСУЮТЬ ПОТОЧНУ ВЕРСІЮ АПАРАТНОГО, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ, І ЛОКАЛЬНОЮ ГОЛОВНОЮ КОПІЄЮ ДАНИХ ДЛЯ ПОТОЧНИХ ВЕРСІЙ. (SA-10-05)

15.10.6. ДОВІРЕНЕ ПОСТАЧАННЯ (SA-10(6))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ ПРОЦЕДУРИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ТОГО, ЩОБ АПАРАТНІ ЗАСОБИ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ Й ОНОВЛЕННЯ ПРОШИВКИ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ Й ОНОВЛЮЮТЬСЯ В ОРГАНІЗАЦІЇ, ТОЧНО ВІДПОВІДАЛИ

ОРИГІНАЛЬНИМ КОПІЯМ. (SA-10-06).

No: 1
Name: sa-10-6
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ ПРОЦЕДУРИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ТОГО, ЩОБ АПАРАТНІ ЗАСОБИ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ Й ОНОВЛЕННЯ ПРОШИВКИ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ Й ОНОВЛЮЮТЬСЯ В ОРГАНІЗАЦІЇ, ТОЧНО ВІДПОВІДАЛИ ОРИГІНАЛЬНИМ КОПІЯМ. (SA-10-06)

15.10.7. ПРЕДСТАВНИКИ БЕЗПЕКИ ТА ПРИВАТНОСТІ (SA-10(7))

Представники безпеки та приватності (sa-10(7)).

Немає параметрів для цього контролю.

15.11. УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПРЕДСТАВНИКИ БЕЗПЕКИ ТА ПРИВАТНОСТІ (SA-11)

Представники безпеки та приватності.

No: 1
Name: sa-11_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {одиниця; інтеграція; система; регресія};

No: 2
Name: sa-11_odp_02
Type: string
Default: nil

визначено частоту, з якою слід проводити <SA-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> тестування/оцінювання;

No: 3
Name: sa-11_odp_03
Type: string
Default: nil

визначено глибину та охоплення <SA-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> тестування/оцінювання;

15.11.1. АНАЛІЗ СТАТИЧНОГО КОДУ (SA-11(1))

Аналіз статичного коду (sa-11(1)).

Немає параметрів для цього контролю.

15.11.2. МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ (SA-11(2))

Повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час розробки системи, компонента або сервісу, що використовує <SA-11(02)_ODP[01]_інформацію>;.

No: 1
Name: sa-11_02__a__01
Type: string
Default: nil

повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час розробки системи, компонента або сервісу, що використовує <SA-11(02)_ODP[01]_інформацію>;

No: 2
Name: sa-11_02__a__02
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, які використовують <SA-11(02)_ODP[01]_інформацію>;

No: 3
Name: sa-11_02__a__03
Type: string
Default: nil

повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує <SA- 11(02)_ODP[01]_інформацію>;

No: 4
Name: sa-11_02__a__04
Type: string
Default: nil

повинен розробник системи, системного компонента або системного сервісу виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує <SA- 11(02)_ODP[01]_інформацію>;

No: 5
Name: sa-11_02__b__01
Type: string
Default: nil

повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час розробки системи, компонента або сервісу, що використовує <SA-11(02)_ODP[02] засоби та методи>;

No: 6
Name: sa-11_02__b__02

Type: string
Default: nil

повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує <SA-11(02)_ ODP[02] інструменти та методи>;

No: 7
Name: sa-11_02__b__03
Type: string
Default: nil

повинен розробник системи, компонента системи або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, яка використовує <SA-11(02)_ODP[02] інструменти та методи>;

No: 8
Name: sa-11_02__b__04
Type: string
Default: nil

повинен розробник системи, системного компонента або системного сервісу виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує <SA-11(02)_ ODP[02] інструменти та методи>;

No: 9
Name: sa-11_02__c__01
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби виконувати моделювання загроз на <SA- 11(02)_ODP[03] широті та глибині> під час розробки системи, компонента або сервісу;

No: 10
Name: sa-11_02__c__02
Type: string
Default: nil

зобов'язаний розробник системи, компонента системи або системної служби виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, який проводить моделювання та аналіз на <SA- 11(02)_ODP[04] ширину та глибину>;

No: 11
Name: sa-11_02__d__01
Type: string
Default: nil

повинен розробник системи, компонента системи або системної служби виконувати моделювання загроз під час розробки системи, компонента або сервісу, що дає змогу отримати докази, які відповідають <SA-11(02)_ ODP[05] критеріям прийнятності>;

No: 12
Name: sa-11_02__d__02
Type: string
Default: nil

повинен розробник системи, компонента системи або системної служби виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що дає змогу отримати докази, які відповідають критеріям прийнятності <SA-11(02)_ODP[05]>;

No: 13
Name: sa-11_02__d__03
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, який надає докази,

No: 14
Name: sa-11_02__d__04
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, який надає докази, що відповідають <SA- 11(02)_ODP[06] критеріям прийнятності>.

15.11.3. НЕЗАЛЕЖНА ПЕРЕВІРКА ПЛАНІВ ОЦІНЮВАННЯ ТА ДОКАЗІВ (SA-11(3))

Потрібен незалежний агент, який відповідатиме <SA- 11(03)_ODP критеріям незалежності> для перевірки правильності виконання плану оцінки безпеки розробника та доказів, отриманих під час тестування та оцінки;.

No: 1
Name: sa-11_03__odp
Type: string
Default: nil

визначені критерії незалежності, яким повинен відповідати незалежний агент;

No: 2
Name: sa-11_03__a__01
Type: string
Default: nil

потрібен незалежний агент, який відповідатиме <SA- 11(03)_ODP критеріям незалежності> для перевірки правильності виконання плану оцінки безпеки розробника та доказів, отриманих під час тестування та оцінки;

No: 3
Name: sa-11_03__a__02
Type: string
Default: nil

потрібен незалежний агент, який відповідатиме <SA- 11(03)_ODP критеріям незалежності> для перевірки правильності виконання плану оцінювання конфіденційності розробника та доказів, отриманих під час тестування та оцінювання;

No: 4
Name: sa-11_03__b_
Type: string
Default: nil

надано незалежному агенту достатньо інформації для завершення процесу перевірки, чи надано йому повноваження для отримання такої інформації.

15.11.4. РУЧНИЙ АНАЛІЗ КОДІВ (SA-11(4))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ РУЧНУ ПЕРЕВІРКУ КОДУ <SA- (SA-11-04).

No: 1
Name: sa-11-4
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ РУЧНУ ПЕРЕВІРКУ КОДУ <SA- (SA-11-04)

15.11.5. ТЕСТУВАННЯ НА ПРОНИКНЕННЯ (SA-11(5))

Зобов'язаний розробник системи, системного компонента або системної служби виконувати тестування на проникнення на наступному рівні суворості: <SA-11(05)_ODP[01] ширина>;.

No: 1
Name: sa-11_05__a__01
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби виконувати тестування на проникнення на наступному рівні суворості: <SA-11(05)_ODP[01] ширина>;

No: 2
Name: sa-11_05__a__02
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби виконувати тестування на проникнення на наступному рівні суворості: <SA-11(05)_ODP[02] глибина>;

No: 3
Name: sa-11_05__b_
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби проводити тестування на проникнення в умовах <SA-11(05)_ODP[03]_обмежень>.

15.11.6. АНАЛІЗ ПОВЕРХНІ АТАКИ (SA-11(6))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ АНАЛІЗ ВРАЗЛИВОСТЕЙ. (SA-11-06).

No: 1
Name: sa-11-6
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВИКОНУВАТИ АНАЛІЗ ВРАЗЛИВОСТЕЙ. (SA-11-06)

15.11.7. ПЕРЕВІРКА ОБСЯГУ ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ (SA-11(7))

Перевірка обсягу тестування та оцінювання (sa-11(7)).

Немає параметрів для цього контролю.

15.11.8. ДИНАМІЧНИЙ АНАЛІЗ КОДУ (SA-11(8))

Динамічний аналіз коду (sa-11(8)).

Немає параметрів для цього контролю.

15.11.9. ІНТЕРАКТИВНЕ ТЕСТУВАННЯ БЕЗПЕКИ ДОДАТКІВ (SA-11(9))

Інтерактивне тестування безпеки додатків (sa-11(9)).

Немає параметрів для цього контролю.

15.12. КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SA-12)

Керування ризиками ланцюга постачання.

Немає параметрів для цього контролю.

15.13. ДОВІРЧІСТЬ (SA-13)

Довірчість.

Немає параметрів для цього контролю.

15.14. АНАЛІЗ КРИТИЧНОСТІ (SA-14)

Аналіз критичності.

Немає параметрів для цього контролю.

15.15. ПРОЦЕСИ, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ (SA-15)

Процеси, стандарти та інструменти розробки.

No: 1
Name: sa-15_odp_01
Type: string
Default: nil

визначено періодичність перегляду процесу розробки, стандартів, інструментів, опцій інструментів та конфігурацій інструментів;

No: 2
Name: sa-15_odp_02
Type: string
Default: nil

визначені вимоги до безпеки, яким має відповідати процес, стандарти, інструменти, опції інструментів та

No: 3
Name: sa-15_odp_03
Type: string
Default: nil

визначені вимоги до конфіденційності, яким має відповідати процес, стандарти, інструменти, опції інструментів та конфігурації інструментів;

15.15.1. ПОКАЗНИКИ ЯКОСТІ (SA-15(1))

Повинен розробник системи, системного компонента або системної служби визначати метрики якості на початку процесу розробки;.

No: 1
Name: sa-15_01__a_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби визначати метрики якості на початку процесу розробки;

No: 2
Name: sa-15_01__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби надавати докази відповідності показників якості <SA-15(01)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.

15.15.2. ЗАСОБИ ВІДСТЕЖЕННЯ (SA-15(2))

Повинен розробник системи, системного компонента або визначено глибину аналізу критичності; системної служби обирати та використовувати інструменти 15(03)_ODP[03] відстеження безпеки для використання в процесі розробки.

No: 1
Name: sa-15_02_01
Type: string
Default: nil

повинен розробник системи, системного компонента або визначено глибину аналізу критичності; системної служби обирати та використовувати інструменти 15(03)_ODP[03] відстеження безпеки для використання в процесі розробки.

No: 2
Name: sa-15_02_02
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби обирати та використовувати інструменти відстеження приватності для використання в процесі розробки.

15.15.3. ЗАСОБИ ВІДСТЕЖЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ (SA-15(3))

Засоби відстеження безпеки та приватності (sa-15(3)).

Немає параметрів для цього контролю.

15.15.4. ЗМЕНШЕННЯ ПОВЕРХНІ АТАКИ (SA-15(5))

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ЗМЕНШИТИ ПОВЕРХНЮ АТАКИ ДО <SA- 15(05)_ODP МЕЖІ>. (SA-15-05).

No: 1
Name: sa-15_05_odp
Type: string
Default: nil

визначені порогові значення, до яких необхідно зменшити поверхню атаки;

No: 2
Name: sa-15-5
Type: string
Default: nil

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ЗМЕНШИТИ ПОВЕРХНЮ АТАКИ ДО <SA- 15(05)_ODP МЕЖІ>. (SA-15-05)

15.15.5. ПОСТІЙНЕ ВДОСКОНАЛЕННЯ (SA-15(6))

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВПРОВАДЖУВАТИ ЧІТКИЙ ПРОЦЕС ПОСТІЙНОГО ВДОСКОНАЛЕННЯ ПРОЦЕСУ РОЗРОБКИ. (SA-15-06).

No: 1
Name: sa-15-6

Type: string
Default: nil

ЗОБОВ'ЯЗАНИЙ РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ВПРОВАДЖУВАТИ ЧІТКИЙ ПРОЦЕС ПОСТІЙНОГО ВДОСКОНАЛЕННЯ ПРОЦЕСУ РОЗРОБКИ. (SA-15-06)

15.15.6. АВТОМАТИЗОВАНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ (SA-15(7))

Зобов'язаний розробник системи, системного компонента або системного сервісу виконувати автоматизований аналіз вразливостей <SA-15(07)_ODP[01] частота> з використанням <SA-15(07)_ODP[02] інструментарію>;.

No: 1
Name: sa-15_07__a_
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системного сервісу виконувати автоматизований аналіз вразливостей <SA-15(07)_ODP[01] частота> з використанням <SA-15(07)_ODP[02] інструментарію>;

No: 2
Name: sa-15_07__b_
Type: string
Default: nil

зобов'язаний розробник системи, системного компоненту або системної служби визначати потенціал використання виявлених вразливостей <SA-15(07)_ODP[01] частота>;

No: 3
Name: sa-15_07__c_
Type: string
Default: nil

повинен розробник системи, системного компоненту або системної служби визначати потенційні заходи зменшення ризику <SA-15(07)_ODP[01] частота> для наданих вразливостей;

No: 4
Name: sa-15_07__d_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної послуги надавати вихідні дані інструментів і результати аналізу <SA-15(07)_ODP[01] частота> персоналу або <SA-15(07)_ODP[03] ролям>.

15.15.7. ПОВТОРНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ ТА ВРАЗЛИВОСТІ (SA-15(8))

Повторне використання інформації про загрози та вразливості (sa-15(8)).

Немає параметрів для цього контролю.

15.15.8. ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ (SA-15(9))

Використання реальних даних (sa-15(9)).

Немає параметрів для цього контролю.

15.15.9. ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ (SA-15(10))

План реагування на інциденти (sa-15(10)).

Немає параметрів для цього контролю.

15.15.10. РЕЗЕРВУВАННЯ СИСТЕМИ АБО КОМПОНЕНТУ (SA-15(11))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ АБО КОМПОНЕНТА СИСТЕМИ АРХІВУВАТИ СИСТЕМУ АБО КОМПОНЕНТ, ЩО ВИПУСКАЄТЬСЯ АБО ПОСТАЧАЄТЬСЯ, РАЗОМ З ВІДПОВІДНИМИ ДОКАЗАМИ, ЩО ПІДТВЕРДЖУЮТЬ ОСТАТОЧНУ ПЕРЕВІРКУ БЕЗПЕКИ ТА ПРИВАТНОСТІ.

No: 1
Name: sa-15-11
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ АБО КОМПОНЕНТА СИСТЕМИ АРХІВУВАТИ СИСТЕМУ АБО КОМПОНЕНТ, ЩО ВИПУСКАЄТЬСЯ АБО ПОСТАЧАЄТЬСЯ, РАЗОМ З ВІДПОВІДНИМИ ДОКАЗАМИ, ЩО ПІДТВЕРДЖУЮТЬ ОСТАТОЧНУ ПЕРЕВІРКУ БЕЗПЕКИ ТА ПРИВАТНОСТІ.

15.15.11. МІНІМІЗАЦІЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ (SA-15(12))

Мінімізація використання персональної інформації (sa-15(12)).

Немає параметрів для цього контролю.

15.16. НАВЧАННЯ, ЩО НАДАЄТЬСЯ РОЗРОБНИКАМИ (SA-16)

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ПРОВОДИТИ <SA-16_ODP НАВЧАННЯ> ЩОДО ПРАВИЛЬНОГО ВИКОРИСТАННЯ ТА ЕКСПЛУАТАЦІЇ ВПРОВАДЖЕНИХ ФУНКЦІЙ, ЗАСОБІВ УПРАВЛІННЯ ТА/АБО МЕХАНІЗМІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ.

No: 1
Name: sa-16_odp
Type: string
Default: nil

визначено навчання щодо правильного використання та експлуатації впроваджених функцій безпеки та приватності, засобів контролю та/або механізмів, що надаються розробником системи, системного компонента або системної служби;

No: 2
Name: sa-16
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ ПРОВОДИТИ <SA-16_ODP НАВЧАННЯ> ЩОДО ПРАВИЛЬНОГО ВИКОРИСТАННЯ ТА ЕКСПЛУАТАЦІЇ ВПРОВАДЖЕНИХ ФУНКЦІЙ, ЗАСОБІВ УПРАВЛІННЯ ТА/АБО МЕХАНІЗМІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ.

15.17. ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ ДЛЯ РОЗРОБНИКА (SA-17)

Проєкт та архітектура безпеки та приватності для розробника.

Немає параметрів для цього контролю.

15.17.1. ФОРМАЛЬНА МОДЕЛЬ ПОЛІТИКИ (SA-17(1))

Повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати формальну модель політики, що описує <SA- 17(01)_ ODP[01] організаційну політику безпеки>, яку необхідно впроваджувати;.

No: 1
Name: sa-17_01__a__01
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати формальну модель політики, що описує <SA- 17(01)_ODP[01] організаційну політику безпеки>, яку необхідно впроваджувати;

No: 2
Name: sa-17_01__a__02
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати формальну модель політики, що описує <SA- 17(01)_ODP[02] організаційну політику конфіденційності>, яка підлягає виконанню;

No: 3
Name: sa-17_01__b__01
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби доводити, що формальна модель політики є внутрішньо узгодженою і достатньою для забезпечення дотримання визначених елементів політики безпеки організації при її впровадженні;

No: 4
Name: sa-17_01__b__02
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби доводити, що формальна модель політики є внутрішньо узгодженою і достатньою для забезпечення дотримання визначених елементів організаційної політики приватності при її впровадженні.

15.17.2. КОМПОНЕНТИ, ЩО НЕОБХІДНІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ (SA-17(2))

Зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;.

No: 1
Name: sa-17_02__a__01
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;

No: 2
Name: sa-17_02__a__02
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати програмне забезпечення, що має відношення до безпеки;

No: 3
Name: sa-17_02__a__03
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати мікропрограмне забезпечення, що мають відношення до безпеки;

No: 4
Name: sa-17_02__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби надавати обґрунтування того, що визначення обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки, є повним.

15.17.3. ФОРМАЛЬНА ВІДПОВІДНІСТЬ (SA-17(3))

Зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;.

No: 1
Name: sa-17_03__a__01
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;

No: 2
Name: sa-17_03__a__02
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати програмне забезпечення, що має відношення до безпеки;

No: 3
Name: sa-17_03__a__03
Type: string
Default: nil

зобов'язаний розробник системи, системного компонента або системної служби визначати мікропрограми, що мають відношення до безпеки;

No: 4
Name: sa-17_03__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби надавати обґрунтування того, що визначення обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки, є повним.

No: 5
Name: sa-17_03__c_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби демонструвати за допомогою неформальної демонстрації, що формальна специфікація верхнього рівня повністю охоплює інтерфейси до обладнання, програмного

No: 6
Name: sa-17_03__d_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби доводити, що формальна специфікація верхнього рівня є точним описом впровадженого обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки;

No: 7
Name: sa-17_03__e_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби описувати релевантні для безпеки апаратні, програмні та мікропрограмні механізми, які не розглядаються у формальній специфікації верхнього рівня, але є суто внутрішніми для релевантних для безпеки апаратних, програмних та мікропрограмних засобів.

15.17.4. НЕФОРМАЛЬНА ВІДПОВІДНІСТЬ (SA-17(4))

Повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення з точки зору винятків;.

No: 1
Name: sa-17_04__odp
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {неформальна описова специфікація, переконливий аргумент за допомогою формальних методів як можлива};

No: 2
Name: sa-17_04__a__01
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення з точки зору винятків;

No: 3
Name: sa-17_04__a__02
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення в термінах повідомлень про помилки;

No: 4
Name: sa-17_04__a__03
Type: string
Default: nil

повинен розробник системи, системного компоненту або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки обладнання, програмного забезпечення та мікропрограмного забезпечення з точки зору наслідків;

No: 5
Name: sa-17_04__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби показувати за допомогою <SA-17(04)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>, що описова специфікація верхнього рівня узгоджується з формальною моделлю політики;

No: 6
Name: sa-17_04__c_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби демонструвати за допомогою неформальної демонстрації, що описова специфікація верхнього рівня повністю охоплює інтерфейси до апаратного,

програмного та мікропрограмного забезпечення, що мають відношення до безпеки;

No: 7
Name: sa-17_04__d_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби показувати, що описова специфікація верхнього рівня є точним описом інтерфейсів до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення;

No: 8
Name: sa-17_04__e_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби описувати релевантні для безпеки апаратні, програмні та мікропрограмні механізми, які не розглядаються в описовій специфікації верхнього рівня, але є суто внутрішніми для релевантних для безпеки апаратних, програмних та мікропрограмних засобів.

15.17.5. КОНЦЕПТУАЛЬНИЙ ПРОЄКТ (SA-17(5))

Повинен розробник системи, системного компонента або системної служби проектувати та структурувати апаратне, програмне та мікропрограмне забезпечення, пов'язане з безпекою, таким чином, щоб використовувати повний, концептуально простий механізм захисту з чітко визначеною семантикою;.

No: 1
Name: sa-17_05__a_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби проектувати та структурувати апаратне, програмне та мікропрограмне забезпечення, пов'язане з безпекою, таким чином, щоб використовувати повний, концептуально простий механізм захисту з чітко визначеною семантикою;

No: 2
Name: sa-17_05__b_
Type: string
Default: nil

повинен розробник системи, системного компонента або системної служби внутрішньо структурувати обладнання, програмне забезпечення та вбудоване програмне забезпечення, пов'язане з безпекою, з урахуванням цього механізму.

15.17.6. СТРУКТУРА ДЛЯ ТЕСТУВАННЯ (SA-17(6))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТРУКТУРУВАТИ ОБЛАДНАННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПОВ'ЯЗАНЕ (SA-17-06).

No: 1
Name: sa-17-6
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТРУКТУРУВАТИ ОБЛАДНАННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПОВ'ЯЗАНЕ (SA-17-06)

15.17.7. СТРУКТУРА ДЛЯ НАЙМЕНШОГО ПРИВІЛЕЮ (SA-17(7))

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТРУКТУРУВАТИ АПАРАТНЕ, ПРОГРАМНЕ ТА МІКРОПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, НЕОБХІДНЕ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТАКИМ ЧИНОМ, ЩОБ ПОЛЕГШИТИ КОНТРОЛЬ ДОСТУПУ З НАЙМЕНШИМИ ПРИВІЛЕЯМИ. (SA-17-07).

No: 1
Name: sa-17-7
Type: string
Default: nil

ПОВИНЕН РОЗРОБНИК СИСТЕМИ, СИСТЕМНОГО КОМПОНЕНТА АБО СИСТЕМНОЇ СЛУЖБИ СТРУКТУРУВАТИ АПАРАТНЕ, ПРОГРАМНЕ ТА МІКРОПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, НЕОБХІДНЕ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТАКИМ ЧИНОМ, ЩОБ ПОЛЕГШИТИ КОНТРОЛЬ ДОСТУПУ З НАЙМЕНШИМИ ПРИВІЛЕЯМИ. (SA-17-07)

15.17.8. ОРКЕСТРОВКА (SA-17(8))

РОЗРОБЛЕНІ <SA-17(08) _ODP[01] КРИТИЧНІ СИСТЕМИ> З СПРОМОЖНОСТЕЙ>. (SA-17-08).

No: 1
Name: sa-17-8
Type: string
Default: nil

РОЗРОБЛЕНІ <SA-17(08) _ODP[01] КРИТИЧНІ СИСТЕМИ> З СПРОМОЖНОСТЕЙ>. (SA-17-08)

15.17.9. РІЗНОМАНІТНІСТЬ ПРОЕКТУВАННЯ (SA-17(9))

ВИКОРИСТОВУЮТЬСЯ РІЗНІ КОНСТРУКЦІЇ ДЛЯ <SA-17(09)_ODP КРИТИЧНИХ СИСТЕМ>, ЩОБ ЗАДОВОЛЬНИТИ ЗАГАЛЬНИЙ НАБІР ВИМОГ АБО ЗАБЕЗПЕЧИТИ ЕКВІВАЛЕНТНУ ФУНКЦІОНАЛЬНІСТЬ. (SA-17-09).

No: 1
Name: sa-17_09__odp
Type: string
Default: nil

визначені критичні системи або компоненти системи, які мають бути спроектовані по-іншому;

No: 2
Name: sa-17-9
Type: string
Default: nil

ВИКОРИСТОВУЮТЬСЯ РІЗНІ КОНСТРУКЦІЇ ДЛЯ <SA-17(09)_ODP КРИТИЧНИХ СИСТЕМ>, ЩОБ ЗАДОВОЛЬНИТИ ЗАГАЛЬНИЙ НАБІР ВИМОГ АБО ЗАБЕЗПЕЧИТИ ЕКВІВАЛЕНТНУ ФУНКЦІОНАЛЬ-

НІСТЬ. (SA-17-09)

15.18. ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ (SA-18)

Захист та виявлення підробки.

Немає параметрів для цього контролю.

15.19. СПРАВЖНІСТЬ КОМПОНЕНТА (SA-19)

Справжність компонента.

Немає параметрів для цього контролю.

15.20. ІНДИВІДУАЛЬНА РОЗРОБКА КРИТИЧНИХ КОМПОНЕНТІВ (SA-20)

<SA-20_ODP КРИТИЧНА СИСТЕМА> ПОВТОРНО РЕАЛІЗУВАТИ АБО.

No: 1
Name: sa-20_odp
Type: string
Default: nil

потрібно повторно реалізувати або налаштувати на замовлення критичні компоненти системи;

No: 2
Name: sa-20
Type: string
Default: nil

<SA-20_ODP КРИТИЧНА СИСТЕМА> ПОВТОРНО РЕАЛІЗУВАТИ АБО

15.21. ПЕРЕВІРКА РОЗРОБНИКА (SA-21)

Перевірка розробника.

No: 1
Name: sa-21_odp_01
Type: string
Default: nil

визначена система, компонент системи або системна служба, до яких має доступ розробник;

No: 2
Name: sa-21_odp_02
Type: string
Default: nil

визначені офіційні обов'язки, покладені на розробника;

No: 3
Name: sa-21_odp_03
Type: string
Default: nil

визначені додаткові критерії перевірки персоналу розробників;

15.22. КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ (SA-22)

Компоненти системи, що не підтримуються.

No: 1
Name: sa-22_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {внутрішня підтримка; <SA-22_ODP[02] підтримка від зовнішніх постачальників>};

No: 2
Name: sa-22_odp_02
Type: string
Default: nil

визначена підтримка з боку зовнішніх постачальників (якщо обрано);

15.23. СПЕЦІАЛІЗАЦІЯ (SA-23)

ВИКОРИСТОВУЄТЬСЯ <SA-23_ODP[01] ВИБІРКОВЕ СИСТЕМАХ АБО КОМПОНЕНТАХ СИСТЕМИ>, ЩО ПІДТРИМУЮТЬ ОСНОВНІ ПОСЛУГИ АБО ФУНКЦІЇ, ДЛЯ ПІДВИЩЕННЯ ДОВІРИ ДО ЦИХ СИСТЕМ АБО КОМПОНЕНТІВ.

No: 1
Name: sa-23_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {модифікація дизайну; доповнення; реконфігурація};

No: 2
Name: sa-23_odp_02
Type: string
Default: nil

визначені системи або компоненти системи, що підтримують важливі для місії послуги або функції;

No: 3
Name: sa-23
Type: string
Default: nil

ВИКОРИСТОВУЄТЬСЯ <SA-23_ODP[01] ВИБІРКОВЕ СИСТЕМАХ АБО КОМПОНЕНТАХ СИСТЕМИ>, ЩО ПІДТРИМУЮТЬ ОСНОВНІ ПОСЛУГИ АБО ФУНКЦІЇ, ДЛЯ ПІДВИЩЕННЯ ДОВІРИ ДО ЦИХ СИСТЕМ АБО КОМПОНЕНТІВ.

16. SC

Захист систем та комунікацій.

Опис Цей клас охоплює механізми захисту інформації під час її передачі мережами зв'язку, криптографічний захист та ізоляцію критичних компонентів.

Перелік заходів захисту Політика та процедури захисту системи та комунікацій (SC-1); Розділення функцій (SC-2); Інтерфейси для непривілейованих користувачів (SC-2(1)); Відокремлення (SC-2(2)); Ізоляція функцій безпеки (SC-3); Ізоляція функцій забезпечення (SC-3(1)); Функції управління доступом та потоком (SC-3(2)); Мінімізація функціональності (SC-3(3)); З'єднання модулів зв'язність (SC-3(4)); Багаторівнева структура (SC-3(5)); Інформація в загальних системних ресурсах (SC-4); Рівні безпеки (SC-4(1)) [Вилучено]; Інформація в загальних системних багаторівнева або періодична обробка (SC-4(2)); Захист від атак «відмова в обслуговуванні» (SC-5); Обмеження внутрішніх користувачів (SC-5(1)); Захист від атак «відмова в обслуговуванні» продуктивність, пропускна здатність та надмірність (SC-5(2)); Виявлення та моніторинг (SC-5(3)); Доступність ресурсів (SC-6); Доступність ресурсів (SC-7); Фізично відділені підмережі (SC-7(1)) [Вилучено]; Публічний доступ (SC-7(2)) [Вилучено]; Точки доступу (SC-7(3)); Зовнішні комунікаційні служби (SC-7(4)); Відмова за замовчуванням - дозвіл за винятком (SC-7(5)); Відповідь на розпізнані помилки (SC-7(6)) [Вилучено]; Запобігання поділу тунелювання для віддалених пристроїв (SC-7(7)); Маршрутизація трафіку з автентифікованих проксі-серверів (SC-7(8)); Обмеження трафіку вихідних повідомлень (SC-7(9)); Запобігання ексфільтрації (SC-7(10)); Обмеження трафіку вхідних повідомлень (SC-7(11)); Захист на основі хосту (SC-7(12)); Ізоляція засобів безпеки, механізмів і компонентів підтримки (SC-7(13)); Захист від несанкціонованих фізичних з'єднань (SC-7(14)); Маршрутизація доступу до привілейованої мережі (SC-7(15)); Запобігання виявленню компонентів і пристроїв (SC-7(16)); Автоматичне примусове виконання форматів протоколів (SC-7(17)); Збій у безпеці (SC-7(18)); Блокування комунікації від хостів, що налаштовані поза організацією (SC-7(19)); Динамічна ізоляція та відокремлення (SC-7(20)); Ізоляція системних компонентів (SC-7(21)); Окремі підмережі для підключення до різних доменів безпеки (SC-7(22)); Відключення функції зворотного зв'язку відправника про помилку перевірки протоколу (SC-7(23)); Персональні дані (SC-7(24)); Зєднання з несекретними національними системами безпеки (SC-7(25)); Зєднання з секретними національними системами безпеки (SC-7(26)); Зєднання з секретними не національними системами безпеки (SC-7(27)); Зєднання з загальнодоступними мережами (SC-7(28)); Окремі підмережі для ізоляції функцій (SC-7(29)); Конфіденційність та цілісність передачі (SC-8); Криптографічний захист (SC-8(1)); Попередня і постобробка (SC-8(2)); Криптографічний захист повідомлень (SC-8(3)); Приховування або рандомізація комунікації (SC-8(4)); Система розподілу (SC-8(5)); Конфіденційність передачі (SC-9) [Вилучено]; Відключення мережі (SC-10); Довірений канал зв'язку (SC-11); Логічна ізоляція (SC-11(1)); Встановлення ключами (SC-12); Доступність (SC-12(1)); Симетричні ключі (SC-12(2)); Асиметричні ключі (SC-12(3)); Сертифікати pki (SC-12(4)) [Вилучено]; Сертифікати pki, апаратні токени (SC-12(5)) [Вилучено]; Фізичний контроль ключів (SC-12(6)); Криптографічний захист (SC-13); Стандартна криптографія (SC-13(1)) [Вилучено]; Затверджена уповноваженим

органом криптографія (SC-13(2)) [Вилучено]; Особи без офіційних повноважень (SC-13(3)) [Вилучено]; Цифрові підписи (SC-13(4)) [Вилучено]; Захист громадського доступу (SC-14) [Вилучено]; Спільні обчислювальні пристрої та застосунки (SC-15); Фізичне чи логічне відключення (SC-15(1)); Блокування трафіку вхідних і вихідних повідомлень (SC-15(2)) [Вилучено]; Відключення та видалення в безпечних робочих зонах (SC-15(3)); Чітка ідентифікація поточних учасників (SC-15(4)); Передача атрибутів безпеки та приватності (SC-16); Перевірка цілісності (SC-16(1)); Механізм антиспуфінгу (SC-16(2)); Криптографічна прив'язка (SC-16(3)); Сертифікати інфраструктури відкритих ключів (SC-17); Мобільний код (SC-18); Мобільний код (SC-18(1)); Придбання, розробка та використання (SC-18(2)); Запобігання завантаження та виконання (SC-18(3)); Запобігання автоматичного виконання (SC-18(4)); Дозвіл виконання тільки в обмежених середовищах (SC-18(5)); Інтернет-протокол голосового зв'язку (SC-19) [Вилучено]; БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) (SC-20); Дочірній підпростір (SC-20(1)) [Вилучено]; Джерело даних та цілісність (SC-20(2)); Джерело даних та цілісність (SC-21); Джерело даних та цілісність (SC-21(1)) [Вилучено]; Архітектура та забезпечення служби імен, адрес (SC-22); Автентифікація сесії (SC-23); Анулювання ідентифікатора сеансу зв'язку при виході з системи (SC-23(1)); Ініційовані користувачем виходи та повідомлення (SC-23(2)) [Вилучено]; Унікальні ідентифікатори сеансів з рандомізацією (SC-23(3)); Унікальні ідентифікатори сеансів з рандомізацією (SC-23(4)) [Вилучено]; Унікальні ідентифікатори сеансів з рандомізацією (SC-23(5)); Уведення у відомий стан (SC-24); Тонкі вузли (SC-25); ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (DECOYS) (SC-26); Виявлення шкідливого коду (SC-26(1)) [Вилучено]; Незалежні від платформи застосунки (SC-27); Захист інформації в стані спокою (SC-28); Криптографічний захист (SC-28(1)); Автономне сховище (SC-28(2)); Криптографічні ключі (SC-28(3)); Гетерогенність (SC-29); Методи віртуалізації (SC-29(1)); Маскування та хибний напрям (SC-30); Методи віртуалізації (SC-30(1)) [Вилучено]; Випадковість (SC-30(2)); Зміна місця обробки та зберігання (SC-30(3)); Неправдива інформація (SC-30(4)); Маскування системних компонентів (SC-30(5)); Аналіз прихованого каналу (SC-31); Тестування прихованих каналів для експлуатації (SC-31(1)); Максимальна пропускна здатність (SC-31(2)); Вимірювання пропускну здатність в робочих середовищах (SC-31(3)); Поділ системи на частини (SC-32); Відокремлені фізичні домени для привілейованих функцій (SC-32(1)); Підготовка цілісності передачі (SC-33) [Вилучено]; Незмінювані виконавчі програми (SC-34); Відсутність сховища доступного для запису інформації (SC-34(1)); Захист цілісності на носії, придатному тільки для читання (SC-34(2)); Апаратний захист (SC-34(3)) [Вилучено]; РОЗПІЗНАВАННЯ ПРИМАНОК ДЛЯ ЗЛОВМИСНИКІВ (HONEYCLIENT) (SC-35); Розподілена обробка та зберігання (SC-36); Методи опитування (SC-36(1)); Синхронізація (SC-36(2)); Позасмугові канали (SC-37); Забезпечення доставлення та передачі (SC-37(1)); Безпека операцій (SC-38); Ізоляція процесу (SC-39); Апаратне розділення (SC-39(1)); Ізоляція потоків (SC-39(2)); Захист бездротового з'єднання (SC-40); Електромагнітні перешкоди (SC-40(1)); Зменшення потенціалу виявлення (SC-40(2)); Імітаційний або маніпулятивний обмін повідомленнями (SC-40(3)); Доступ до портів та пристроїв введення, виведення (SC-41); Можливості датчика та дані (SC-42); Звітування перед уповноваженими або посадовими особами (SC-42(1)); Дозволене використання (SC-42(2)); Заборона використання пристроїв (SC-42(3)); Повідомлення про збір (SC-42(4)); Мінімізація збору (SC-42(5)); Заборона використання пристроїв (SC-43); Екрановані камери (SC-44); Синхронізація системи з часом (SC-45); Синхронізація з авторитетним джерелом часу (SC-45(1)); Вторинне авторитетне джерело часу (SC-45(2)); Забезпечення виконання міждоменної політики (SC-46); Альтернативний шлях зв'язку (SC-47); Переміщення датчика (SC-48); Динамічно переміщуються до за (SC-48(1)); Примусове апаратне забезпечення виконання (SC-49); Примусове програмне забезпечення виконання (SC-50); Апаратний захист (SC-51).

16.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ЗАХИСТУ СИСТЕМИ ТА КОМУНІКАЦІЙ (SC-1)

а. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посадових осіб]:

1. 2. Політику захисту системи та комунікацій, яка:
(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);
(b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам. Процедури для сприяння впровадженню політики в області захисту систем і комунікацій, а також пов'язаних з ними систем і засобів захисту зв'язку.
b. Призначити [Призначення: визначена організацією посадову особу] для управління політикою та процедурами захисту системи та комунікацій.
c. Переглядати та оновлювати:
1. поточну політику захисту системи та комунікацій [Призначення: визначена організацією частота];
2. поточні процедури захисту системи та комунікацій [Призначення: визначена організацією частота].

No: 1
Name: sc_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, до яких має бути доведена політика захисту системи та комунікацій

No: 2
Name: sc_1_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюються процедури захисту системи та комунікацій

No: 3
Name: sc_1_odp_03
Type: string
Default: nil

Вибрано жодне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи}

No: 4
Name: sc_1_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено посадову особу, яка керуватиме політикою та процедурами захисту системи та комунікацій

No: 5
Name: sc_1_odp_05
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначена періодичність перегляду та оновлення поточної політики захисту системи та комунікацій

No: 6
Name: sc_1_odp_06
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Є події, які вимагають перегляду та оновлення поточної політики захисту системи та комунікацій

No: 7
Name: sc_1_odp_07
Type: string
Default: "щорічно"

Визначена періодичність перегляду та оновлення поточних процедур захисту системи та засобів зв'язку

16.2. РОЗДІЛЕННЯ ФУНКЦІЙ (SC-2)

Розділяти функціональність користувача, включно зі службами, що призначені для користувача інтерфейсу, від функціональності системного управління.

No: 1
Name: sc_2_01
Type: string
Default: nil

Розділена функціональність користувача, включаючи сервіси користувацького інтерфейсу, від функціональності управління системою.

16.2.1. ІНТЕРФЕЙСИ ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ (SC-2(1))

Запобігається представлення функціональності управління системою в інтерфейсі непривілейованим користувачам.

No: 1
Name: sc_2_1_01
Type: string
Default: nil

Запобігається представлення функціональності управління системою в інтерфейсі непривілейованим користувачам

16.2.2. ВІДОКРЕМЛЕННЯ (SC-2(2))

Зберігається інформація окремо від додатків та програмного забезпечення.

No: 1
Name: sc_2_2_01
Type: string
Default: nil

Зберігається інформація окремо від додатків та програмного забезпечення

16.3. ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ (SC-3)

Ізолювати функції безпеки від інших функцій.

No: 1
Name: sc_3_01
Type: string
Default: nil

Ізольовані функції безпеки від інших функцій

16.3.1. ІЗОЛЯЦІЯ ФУНКЦІЙ ЗАБЕЗПЕЧЕННЯ (SC-3(1))

Застосовуються механізми розділення апаратних засобів для реалізації ізоляції функцій безпеки.

No: 1
Name: sc_3_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються механізми розділення апаратних засобів для реалізації ізоляції функцій безпеки

16.3.2. ФУНКЦІЇ УПРАВЛІННЯ ДОСТУПОМ ТА ПОТОКОМ (SC-3(2))

Ізольовані функції безпеки, що забезпечують управління доступом, які не пов'язані з безпекою.

No: 1
Name: sc_3_2_01
Type: string
Default: nil

Ізольовані функції безпеки, що забезпечують управління доступом, які не пов'язані з безпекою

No: 2
Name: sc_3_2_02
Type: string
Default: nil

Ізольовані функції безпеки, що забезпечують контроль доступу, від інших функцій безпеки

No: 3
Name: sc_3_2_03
Type: string
Default: nil

Ізольовані функції безпеки, які не пов'язані з безпекою забезпечують контроль інформаційних потоків

No: 4
Name: sc_3_2_04
Type: string
Default: nil

Ізольовані функції безпеки, що забезпечують контроль інформаційних потоків, від інших функцій безпеки

16.3.3. МІНІМІЗАЦІЯ ФУНКЦІОНАЛЬНОСТІ (SC-3(3))

Мінімізовано кількість функцій, не пов'язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки.

No: 1
Name: sc_3_3_01
Type: integer
Default: 3

Мінімізовано кількість функцій, не пов'язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки

16.3.4. З'ЄДНАННЯ МОДУЛІВ ЗВ'ЯЗНІСТЬ (SC-3(4))

Реалізовані функції безпеки як значною мірою незалежні модулі, які мінімізують зв'язок між модулями.

No: 1
Name: sc_3_4_02
Type: string
Default: nil

Реалізовані функції безпеки як значною мірою незалежні модулі, які мінімізують зв'язок між модулями

16.3.5. БАГАТОРІВНЕВА СТРУКТУРА (SC-3(5))

Реалізовані функції безпеки як багаторівнева структура, що мінімізує взаємодію між шарами дизайну та уникає будь-якої залежності нижчих шарів від функціональності або коректності вищих шарів.

No: 1
Name: sc_3_5_01
Type: string
Default: nil

Реалізовані функції безпеки як багаторівнева структура, що мінімізує взаємодію між шарами дизайну та уникає будь-якої залежності нижчих шарів від функціональності або коректності вищих шарів

16.4. ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ (SC-4)

Запобігати несанкціонованій та ненавмисній передачі інформації через спільні системні ресурси.

No: 1
Name: sc_4_01
Type: string
Default: nil

Запобігається несанкціонована передача інформації через спільні системні ресурси

No: 2
Name: sc_4_02
Type: string
Default: nil

Запобігається ненавмисна передача інформації через спільні системні ресурси.

16.4.1. РІВНІ БЕЗПЕКИ (SC-4(1)) [Вилучено]

[Вилучено: включено до SC-4]

Немає параметрів для цього контролю.

16.4.2. ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ БАГАТОРІВНЕВА АБО ПЕРІОДИЧНА ОБРОБКА (SC-4(2))

Запобігається несанкціонована передача інформації через спільні ресурси відповідно до процедур, коли системна обробка явно перемикається між різними рівнями класифікації інформації або категоріями безпеки.

No: 1
Name: sc_4_2_01
Type: string
Default: nil

Запобігається несанкціонована передача інформації через спільні ресурси відповідно до процедур, коли системна обробка явно перемикається між різними рівнями класифікації інформації або категоріями безпеки

No: 2
Name: sc_4_2_odp
Type: string
Default: nil

Визначені процедури для запобігання несанкціонованій передачі інформації через спільні ресурси

16.5. ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» (SC-5)

a. [Призначення: захистити від; Обмежити] наслідки наступних типів подій відмови в обслуговуванні (DoS): [Призначення: визначені організацією типи подій відмови в обслуговуванні];
b. Застосувати наступні заходи захисту для досягнення мети відмови обслуговування [Призначення: заходи захисту визначені організацією, за типом події відмови в обслуговуванні].

No: 1
Name: sc_5_odp_01
Type: string
Default: nil

Визначені типи подій відмов в обслуговуванні, від яких потрібно захищати або обмежувати; SC-05_ODP[02] вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {захистити від; обмежити}

16.5.1. ОБМЕЖЕННЯ ВНУТРІШНІХ КОРИСТУВАЧІВ (SC-5(1))

Обмежена можливість окремих осіб здійснювати атаки на відмову в обслуговуванні проти інших систем.

No: 1
Name: sc_5_1_01
Type: string
Default: nil

Обмежена можливість окремих осіб здійснювати атаки на відмову в обслуговуванні проти інших систем

No: 2
Name: sc_5_1_odp

Type: list
Default: ["admin", "security_officer"]

Визначені атаки на відмову в обслуговуванні, для яких необхідно обмежити можливість їх запуску окремими особами

16.5.2. ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» ПРОДУКТИВНІСТЬ, ПРОПУСКНА ЗДАТНІСТЬ ТА НАДМІРНІСТЬ (SC-5(2))

Здійснюється управління ємністю, пропускною здатністю або іншими надлишковими ресурсами для обмеження наслідків інформаційних атак на відмову в обслуговуванні.

No: 1
Name: sc_5_2_01
Type: string
Default: nil

Здійснюється управління ємністю, пропускною здатністю або іншими надлишковими ресурсами для обмеження наслідків інформаційних атак на відмову в обслуговуванні

16.5.3. ВИЯВЛЕННЯ ТА МОНІТОРИНГ (SC-5(3))

Використовуються засоби моніторингу для виявлення ознак атак на відмову в обслуговуванні, спрямованих на систему або запущених з неї.

No: 1
Name: sc_5_3_a
Type: string
Default: "автоматизований засіб моніторингу"

Використовуються засоби моніторингу для виявлення ознак атак на відмову в обслуговуванні, спрямованих на систему або запущених з неї

No: 2
Name: sc_5_3_b
Type: string
Default: nil

Здійснюється моніторинг системних ресурсів для визначення наявності достатніх ресурсів для запобігання ефективним атакам на відмову в обслуговуванні

16.6. ДОСТУПНІСТЬ РЕСУРСІВ (SC-6)

Забезпечити захист доступності ресурсів, виділивши [Призначення: визначені організацією ресурси], по [Вибір (один або кілька); пріоритет; квоти; [Призначення: визначені організацією заходи з безпеки]].

No: 1
Name: sc_6_01
Type: string
Default: nil

Захищено доступність ресурсів шляхом розподілу ресурсів за ВИБІРКОВИМ ЗНАЧЕННЯМ ПАРАМЕТРА(ів)

No: 2
Name: sc_6_odp_01
Type: string
Default: nil

Визначені ресурси, які необхідно виділити для захисту доступності ресурсів

No: 3
Name: sc_6_odp_02
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {priority; quota; controls}

No: 4
Name: sc_6_odp_03
Type: string
Default: "автоматизований засіб моніторингу"

Визначені засоби контролю для захисту доступності ресурсів (якщо вибрано)

16.7. ДОСТУПНІСТЬ РЕСУРСІВ (SC-7)

a. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи.
b. Реалізувати підмережі для загальнодоступних компонентів системи, які є [Вибір: фізично; логічно] відділені від внутрішніх мереж організації.
c. Підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташованих відповідно до архітектури безпеки та приватності організації.

Немає параметрів для цього контролю.

16.7.1. ФІЗИЧНО ВІДДІЛЕНІ ПІДМЕРЕЖІ (SC-7(1)) [Вилучено]

[Вилучено: включено до SC-7]

Немає параметрів для цього контролю.

16.7.2. ПУБЛІЧНИЙ ДОСТУП (SC-7(2)) [Вилучено]

[Вилучено: включено до SC-7]

Немає параметрів для цього контролю.

16.7.3. ТОЧКИ ДОСТУПУ (SC-7(3))

Обмежена кількість зовнішніх мережевих підключень до системи.

No: 1
Name: sc_7_3_01

Type: integer
Default: 3

Обмежена кількість зовнішніх мережевих підключень до системи

16.7.4. ЗОВНІШНІ КОМУНІКАЦІЙНІ СЛУЖБИ (SC-7(4))

Реалізовано керований інтерфейс для кожної зовнішньої телекомунікаційної послуги.

No: 1
Name: sc_7_4_a
Type: string
Default: nil

Реалізовано керований інтерфейс для кожної зовнішньої телекомунікаційної послуги

No: 2
Name: sc_7_4_b
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Встановлена політика потоку трафіку для кожного керованого інтерфейсу

No: 3
Name: sc_7_4_c_01
Type: string
Default: nil

Захищена конфіденційність інформації, що передається через кожен інтерфейс

No: 4
Name: sc_7_4_c_02
Type: string
Default: nil

Захищена цілісність інформації, що передається через кожен інтерфейс

No: 5
Name: sc_7_4_d
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Задокументовано кожен виняток з політики управління трафіком з обґрунтуванням місії або бізнес-потреби, а також тривалості такої потреби

No: 6
Name: sc_7_4_e_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Переглядаються винятки з політики потоку трафіку частота

No: 7
Name: sc_7_4_e_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Потрібно видалити винятки з політики потоку трафіку, які більше не підтримуються чітко визначеною місією або бізнеспотребою

No: 8
Name: sc_7_4_f

Type: string
Default: nil

Запобігається несанкціонований обмін управління із зовнішніми мережами

No: 9
Name: sc_7_4_g
Type: string
Default: nil

Публікується інформація, яка дозволяє віддаленим мережам виявляти несанкціонований трафік площини керування з внутрішніх мереж

No: 10
Name: sc_7_4_h
Type: string
Default: nil

Фільтрується несанкціонований трафік з зовнішніх мереж. трафіком плану

No: 11
Name: sc_7_4_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено періодичність перегляду винятків з політики управління інформаційними потоками

16.7.5. ВІДМОВА ЗА ЗАМОВЧУВАННЯМ - ДОЗВІЛ ЗА ВИНЯТКОМ (SC-7(5))

Відмова за замовчуванням - дозвіл за винятком (sc-7(5)).

Немає параметрів для цього контролю.

16.7.6. ВІДПОВІДЬ НА РОЗПІЗНАНІ ПОМИЛКИ (SC-7(6)) [Вилучено]

[Вилучено: включено до SC-7(18)]

Немає параметрів для цього контролю.

16.7.7. ЗАПОБІГАННЯ ПОДІЛУ ТУНЕЛЮВАННЯ ДЛЯ ВІДДАЛЕНИХ ПРИСТРОЇВ (SC-7(7))

Запобігається розділеному тунелюванню для віддалених пристроїв, що підключаються до систем організації, якщо розділене тунелюванню не захищено за допомогою засоби захисту.

No: 1
Name: sc_7_7_01
Type: string
Default: "автоматизований засіб моніторингу"

Запобігається розділеному тунелюванню для віддалених пристроїв, що підключаються до систем організації, якщо розділене тунелюванню не захищено за допомогою засоби захисту

No: 2
Name: sc_7_7_odp
Type: string
Default: nil

Визначені гарантії безпечного прокладання розділеному тунелюванню

16.7.8. МАРШРУТИЗАЦІЯ ТРАФІКУ З АВТЕНТИФІКОВАНИХ ПРОКСІ-СЕРВЕРІВ (SC-7(8))

(08) _ODP[01] внутрішній комунікаційний трафік> спрямовується до <SC-07(08) _ODP[02] зовнішніх мереж> через автентифіковані проксі-сервери на керованих інтерфейсах.

No: 1
Name: sc_7_8_01
Type: string
Default: nil

SC-07(08) _ODP[01] внутрішній комунікаційний трафік> спрямовується до <SC-07(08) _ODP[02] зовнішніх мереж> через автентифіковані проксі-сервери на керованих інтерфейсах

16.7.9. ОБМЕЖЕННЯ ТРАФІКУ ВИХІДНИХ ПОВІДОМЛЕНЬ (SC-7(9))

Виявлено вихідний комунікаційний трафік, що становить загрозу для зовнішніх систем.

No: 1
Name: sc_7_9_a_01
Type: string
Default: nil

Виявлено вихідний комунікаційний трафік, що становить загрозу для зовнішніх систем

No: 2
Name: sc_7_9_a_02
Type: string
Default: nil

Заборонено вихідний комунікаційний трафік, що становить загрозу для зовнішніх систем

No: 3
Name: sc_7_9_b
Type: string
Default: nil

Перевіряється ідентичність внутрішніх пов'язаних з відмовою у зв'язку. користувачів,

16.7.10. ЗАПОБІГАННЯ ЕКСФІЛЬТРАЦІЇ (SC-7(10))

Запобігання ексфільтрації (sc-7(10)).

No: 1
Name: sc_7_10_odp_01

Type: string
Default: nil

визначена періодичність проведення тестів на ексфільтрацію;

16.7.11. ОБМЕЖЕННЯ ТРАФІКУ ВХІДНИХ ПОВІДОМЛЕНЬ (SC-7(11))

дозволено направляти лише вхідні повідомлення від <SC- 07(11) _ODP[01] авторизованих джерел> до <SC-07(11) _ODP[02] авторизованих пунктів призначення>.;

No: 1
Name: sc_7_11_01
Type: string
Default: nil

дозволено направляти лише вхідні повідомлення від <SC- 07(11) _ODP[01] авторизованих джерел> до <SC-07(11) _ODP[02] авторизованих пунктів призначення>.;

16.7.12. ЗАХИСТ НА ОСНОВІ ХОСТУ (SC-7(12))

реалізовано <SC-07(12) _ODP[01] механізми захисту захисту периметру на основі хосту> на <SC-07(12) _ODP[02] системних компонентах>.;

No: 1
Name: sc_7_12_01
Type: string
Default: nil

реалізовано <SC-07(12) _ODP[01] механізми захисту захисту периметру на основі хосту> на <SC-07(12) _ODP[02] системних компонентах>.;

16.7.13. ІЗОЛЯЦІЯ ЗАСОБІВ БЕЗПЕКИ, МЕХАНІЗМІВ І КОМПОНЕНТІВ ПІДТРИМКИ (SC-7(13))

Ізольовані засоби, механізми та компоненти підтримки інформаційної безпеки від інших внутрішніх компонентів системи шляхом впровадження фізично відокремлених підмереж з керованими інтерфейсами до інших компонентів системи.

No: 1
Name: sc_7_13_01
Type: string
Default: "автоматизований засіб моніторингу"

Ізольовані засоби, механізми та компоненти підтримки інформаційної безпеки від інших внутрішніх компонентів системи шляхом впровадження фізично відокремлених підмереж з керованими інтерфейсами до інших компонентів системи

No: 2
Name: sc_7_13_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначені інструменти, механізми та компоненти підтримки інформаційної безпеки, які мають бути ізольовані від інших внутрішніх компонентів системи

16.7.14. ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ФІЗИЧНИХ З'ЄДНАНЬ (SC-7(14))

захищені <SC-07(14)_ODP керовані інтерфейси> від несанкціонованих фізичних підключень;

No: 1
Name: sc_7_14_odp_01
Type: string
Default: nil

визначено керовані інтерфейси, які потрібно захистити від несанкціонованих фізичних з'єднань; 584;

No: 2
Name: sc_7_14_odp_02
Type: string
Default: nil

керовані інтерфейси> від несанкціонованих фізичних підключень;

No: 3
Name: sc_7_14_01
Type: string
Default: nil

захищені <SC-07(14)_ODP керовані інтерфейси> від несанкціонованих фізичних підключень;

16.7.15. МАРШРУТИЗАЦІЯ ДОСТУПУ ДО ПРИВІЛЕЙОВАНОЇ МЕРЕЖІ (SC-7(15))

мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс з метою контролю доступу;
мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс для цілей аудиту.;

No: 1
Name: sc_7_15_01
Type: string
Default: nil

мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс з метою контролю доступу;

No: 2
Name: sc_7_15_02
Type: string
Default: nil

мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс для цілей аудиту.;

16.7.16. ЗАПОБІГАННЯ ВИЯВЛЕННЮ КОМПОНЕНТІВ І ПРИСТРОЇВ (SC-7(16))

запобігається виявлення певних компонентів системи, які представляють керований інтерфейс.;

No: 1
Name: sc_7_16_01
Type: string
Default: nil

запобігається виявлення певних компонентів системи, які представляють керований інтерфейс.;

16.7.17. АВТОМАТИЧНЕ ПРИМУСОВЕ ВИКОНАННЯ ФОРМАТІВ ПРОТОКОЛІВ (SC-7(17))

дотримуються форматів протоколів.;

No: 1
Name: sc_7_17_01
Type: string
Default: nil

дотримуються форматів протоколів.;

16.7.18. ЗБІЙ У БЕЗПЕЦІ (SC-7(18))

запобігають входу систем у незахищені стани в разі аварійного завершення роботи пристрою захисту периметра.;

No: 1
Name: sc_7_18_01
Type: string
Default: nil

запобігають входу систем у незахищені стани в разі аварійного завершення роботи пристрою захисту периметра.;

16.7.19. БЛОКУВАННЯ КОМУНІКАЦІЇ ВІД ХОСТІВ, ЩО НАЛАШТОВАНІ ПОЗА ОРГАНІЗАЦІЄЮ (SC-7(19))

блокується вхідний комунікаційний трафік між <SC- 07(19)_ODP клієнтами зв'язку>, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг; блокується вихідний комунікаційний трафік між <SC- 07(19)_ODP клієнтами зв'язку>, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг.;

No: 1
Name: sc_7_19_odp_01
Type: string
Default: nil

заборонено системам переходити в небезпечні стани в разі операційної відмови пристрою захисту периметру.;

No: 2
Name: sc_7_19_01
Type: string
Default: nil

блокується вхідний комунікаційний трафік між <SC- 07(19)_ODP клієнтами зв'язку>, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг;

No: 3
Name: sc_7_19_02
Type: string
Default: nil

блокується вихідний комунікаційний трафік між <SC- 07(19)_ODP клієнтами зв'язку>, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг.;

16.7.20. ДИНАМІЧНА ІЗОЛЯЦІЯ ТА ВІДОКРЕМЛЕННЯ (SC-7(20))

передбачено можливість динамічної ізоляції <SC-07(20)_ODP системних компонентів> від інших системних компонентів.;

No: 1
Name: sc_7_20_odp_01
Type: string
Default: nil

визначено компоненти системи, які мають бути динамічно ізольовані від інших компонентів системи;

No: 2
Name: sc_7_20_odp_02
Type: string
Default: nil

системних компонентів> від інших системних компонентів.;

No: 3
Name: sc_7_20_01
Type: string
Default: nil

передбачено можливість динамічної ізоляції <SC-07(20)_ODP системних компонентів> від інших системних компонентів.;

16.7.21. ІЗОЛЯЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ (SC-7(21))

застосовуються механізми захисту кордонів для ізоляції <SC- 07(21)_ODP[01] системних компонентів>, що підтримують <SC-07(21)_ODP[02] місії та/або бізнес-функції>.;

No: 1
Name: sc_7_21_odp_02
Type: string
Default: nil

місії та/або бізнес-функції>.;

No: 2
Name: sc_7_21_01
Type: string
Default: nil

застосовуються механізми захисту кордонів для ізоляції <SC- 07(21)_ODP[01] системних компонентів>, що підтримують <SC-07(21)_ODP[02] місії та/або бізнес-функції>.;

16.7.22. ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ПІДКЛЮЧЕННЯ ДО РІЗНИХ ДОМЕНІВ БЕЗПЕКИ (SC-7(22))

реалізовано окремі мережеві адреси для підключення до систем у різних доменах безпеки.;

No: 1
Name: sc_7_22_01
Type: string
Default: nil

реалізовано окремі мережеві адреси для підключення до систем у різних доменах безпеки.;

16.7.23. ВІДКЛЮЧЕННЯ ФУНКЦІЇ ЗВОРОТНОГО ЗВ'ЯЗКУ ВІДПРАВНИКА ПРО ПОМИЛКУ ПЕРЕВІРКИ ПРОТОКОЛУ (SC-7(23))

вимкнено зворотній зв'язок з відправниками у разі помилки перевірки формату протоколу.;

No: 1
Name: sc_7_23_01
Type: string
Default: nil

вимкнено зворотній зв'язок з відправниками у разі помилки перевірки формату протоколу.;

16.7.24. ПЕРСОНАЛЬНІ ДАНІ (SC-7(24))

застосовуються <SC-07(24)_ODP правила обробки> до персональних даних в системах, які обробляють інформацію, що ідентифікує особу;
здійснюється моніторинг дозволеної обробки на зовнішніх інтерфейсах до систем, які обробляють персональні дані;
здійснюється моніторинг дозволеної обробки на ключових внутрішніх кордонах систем, які обробляють персональні дані;
задокументовано кожен виняток для систем, які обробляють персональні дані;
переглядаються винятки для систем, які обробляють персональні дані;
вилучено винятки для систем, які обробляють персональні дані.;

No: 1
Name: sc_7_24_odp_01
Type: string
Default: nil

визначені правила обробки для систем, які обробляють персональну дані;

No: 2
Name: sc_7_24_odp_02
Type: string
Default: nil

правила обробки> до персональних даних в системах, які обробляють інформацію, що ідентифікує особу;

No: 3
Name: sc_7_24_01
Type: string
Default: nil

застосовуються <SC-07(24)_ODP правила обробки> до персональних даних в системах, які обробляють інформацію, що ідентифікує особу;

No: 4
Name: sc_7_24_02
Type: string
Default: nil

здійснюється моніторинг дозволеної обробки на зовнішніх інтерфейсах до систем, які обробляють персональні дані;

No: 5
Name: sc_7_24_03
Type: string
Default: nil

здійснюється моніторинг дозволеної обробки на ключових внутрішніх кордонах систем, які обробляють персональні дані;

No: 6
Name: sc_7_24_04
Type: string
Default: nil

задокументовано кожен виняток для систем, які обробляють персональні дані;

No: 7
Name: sc_7_24_05
Type: string
Default: nil

переглядаються винятки для систем, які обробляють персональні дані;

No: 8
Name: sc_7_24_06
Type: string
Default: nil

вилучено винятки для систем, які обробляють персональні дані.;

16.7.25. ЗЄДНАННЯ З НЕСЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ (SC-7(25))

підмережі розділені <SC-07(29)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>, щоб ізолювати <SC- 07(29)_ODP[02] критичні компоненти та функції системи>.;

No: 1
Name: sc_7_25_01
Type: string
Default: nil

підмережі розділені <SC-07(29)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>, щоб ізолювати <SC-07(29)_ODP[02] критичні компоненти та функції системи>.;

16.7.26. ЗЄДНАННЯ З СЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ (SC-7(26))

заборонено пряме підключення секретної системи національної безпеки до зовнішньої мережі без використання <SC-07(26)_ODP пристрій захисту периметру>.;

No: 1
Name: sc_7_26_odp_01
Type: string
Default: nil

визначено пристрій граничного захисту, необхідний для прямого підключення до зовнішньої мережі;

No: 2
Name: sc_7_26_odp_02
Type: string
Default: nil

пристрій захисту периметру>.;

No: 3
Name: sc_7_26_01

Type: string
Default: nil

заборонено пряме підключення секретної системи національної безпеки до зовнішньої мережі без використання <SC-07(26)_ODP пристрій захисту периметру>.;

16.7.27. ЗЄДНАННЯ З СЕКРЕТНИМИ НЕ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ (SC-7(27))

заборонено пряме підключення <SC-07(27) _ODP[01] несекретної недержавної системи безпеки> до зовнішньої мережі без використання <SC-07(27) _ODP[02] прикордонного захисного пристрою>.;

No: 1
Name: sc_7_27_01
Type: string
Default: nil

заборонено пряме підключення <SC-07(27) _ODP[01] несекретної недержавної системи безпеки> до зовнішньої мережі без використання <SC-07(27) _ODP[02] прикордонного захисного пристрою>.;

16.7.28. ЗЄДНАННЯ З ЗАГАЛЬНОДОСТУПНИМИ МЕРЕЖАМИ (SC-7(28))

заборонено пряме підключення <SC-07(28)_ODP системи> до загальнодоступної мережі. 592;

No: 1
Name: sc_7_28_odp_01
Type: string
Default: nil

визначено систему, якій заборонено пряме підключення до загальнодоступної мережі;

No: 2
Name: sc_7_28_odp_02
Type: string
Default: nil

системи> до загальнодоступної мережі. 592;

No: 3
Name: sc_7_28_01
Type: string
Default: nil

заборонено пряме підключення <SC-07(28)_ODP системи> до загальнодоступної мережі. 592;

16.7.29. ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ІЗОЛЯЦІЇ ФУНКЦІЙ (SC-7(29))

підмережі розділені <SC-07(29) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> для ізоляції <SC-07(29) _ODP[02] критично важливих компонентів і функцій системи>.;

No: 1
Name: sc_7_29_01
Type: string
Default: nil

підмережі розділені <SC-07(29) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> для ізоляції <SC-07(29) _ ODP[02] критично важливих компонентів і функцій системи>.;

16.8. КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ (SC-8)

Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] інформації, що передається.

Немає параметрів для цього контролю.

16.8.1. КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-8(1))

Забезпечити конфіденційність та цілісність передачі за допомогою криптографічного захисту.

No: 1
Name: sc_8_1_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {запобігти несанкціонованому розголошенню інформації; виявити зміни в інформації}

16.8.2. ПОПЕРЕДНЯ І ПОСТОБРОБКА (SC-8(2))

КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТОБРОБКА МЕТА ОЦІНКИ: Визначити, чи:.

No: 1
Name: sc_8_2_01
Type: string
Default: nil

КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТОБРОБКА МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: sc_8_2_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {конфіденційність; цілісність}

16.8.3. КРИПТОГРАФІЧНИЙ ЗАХИСТ ПОВІДОМЛЕНЬ (SC-8(3))

Впроваджено криптографічні механізми для захисту зовнішніх повідомлень, якщо інше не захищено альтернативні фізичні засоби контролю.

No: 1
Name: sc_8_3_01

Type: string
Default: "AES-256-GCM"

Впроваджено криптографічні механізми для захисту зовнішніх повідомлень, якщо інше не захищено альтернативні фізичні засоби контролю

No: 2
Name: sc_8_3_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено альтернативні фізичні засоби контролю для захисту зовнішніх повідомлень

16.8.4. ПРИХОВУВАННЯ АБО РАНДОМІЗАЦІЯ КОМУНІКАЦІЇ (SC-8(4))

Застосовуються криптографічні механізми для приховування або рандомізації шаблонів комунікації, якщо інше не захищено альтернативні фізичні засоби контролю.

No: 1
Name: sc_8_4_01
Type: string
Default: "AES-256-GCM"

Застосовуються криптографічні механізми для приховування або рандомізації шаблонів комунікації, якщо інше не захищено альтернативні фізичні засоби контролю

No: 2
Name: sc_8_4_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначені альтернативні фізичні засоби контролю для захисту від несанкціонованого розкриття шаблонів комунікації

16.8.5. СИСТЕМА РОЗПОДІЛУ (SC-8(5))

Система розподілу (sc-8(5)).

Немає параметрів для цього контролю.

16.9. КОНФІДЕНЦІЙНІСТЬ ПЕРЕДАЧІ (SC-9) [Вилучено]

[Вилучено: включено до SC-8]

Немає параметрів для цього контролю.

16.10. ВІДКЛЮЧЕННЯ МЕРЕЖІ (SC-10)

Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після [Призначення: визначений організацією період часу] бездіяльності.

No: 1
Name: sc_10_odp
Type: integer
Default: 30

Визначено період бездіяльності, після якого система розриває мережеве з'єднання, пов'язане з сеансом зв'язку; SC08(05)_ODP[02] мережеве з'єднання, пов'язане з сеансом зв'язку, розірвано в кінці сеансу або після період часу бездіяльності

16.11. ДОВІРЕНИЙ КАНАЛ ЗВ'ЯЗКУ (SC-11)

a. Надати [Вибір: фізично; логічно] ізольований надійний канал зв'язку для зв'язку між користувачем і довіреними компонентами системи.
b. Дозволити користувачам запросити довірений канал зв'язку для обміну даними між користувачем і наступними функціями безпеки системи, включно з, як мінімум, автентифікацією та повторною автентифікацією: [Призначення: визначені організацією функції безпеки].

No: 1
Name: sc_11_odp_01
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно}

16.11.1. ЛОГІЧНА ІЗОЛЯЦІЯ (SC-11(1))

надається надійний канал зв'язку, який можна беззаперечно відрізнити від інших каналів зв'язку;
ініційовано довірений канал зв'язку для комунікацій між <SC- 11(01)_ODP функції безпеки> системи та користувачем.;

No: 1
Name: sc_11_1_odp_01
Type: string
Default: nil

визначені функції безпеки системи;

No: 2
Name: sc_11_1_01
Type: string
Default: nil

надається надійний канал зв'язку, який можна беззаперечно відрізнити від інших каналів зв'язку;

No: 3
Name: sc_11_1_02
Type: string
Default: nil

ініційовано довірений канал зв'язку для комунікацій між <SC- 11(01)_ODP функції безпеки> системи та користувачем.;

16.12. ВСТАНОВЛЕННЯ КЛЮЧАМИ (SC-12)

Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [Призначення: визначені організацією вимоги до генерації, поширення, зберігання, доступу та знищення ключів].

No: 1
Name: sc_12_01
Type: string
Default: "AES-256-GCM"

Встановлюються криптографічні ключі, коли в системі використовується криптографія відповідно до < SC-12_ODP вимог >

No: 2
Name: sc_12_02
Type: string
Default: "AES-256-GCM"

Здійснюється управління криптографічними ключами, коли в системі використовується криптографія, відповідно до вимог

No: 3
Name: sc_12_odp
Type: string
Default: nil

Визначені вимоги до генерації, розповсюдження, зберігання, доступу та знищення ключів

16.12.1. ДОСТУПНІСТЬ (SC-12(1))

зберігається доступність інформації у випадку втрати криптографічних ключів користувачами.;

No: 1
Name: sc_12_1_01
Type: string
Default: nil

зберігається доступність інформації у випадку втрати криптографічних ключів користувачами.;

16.12.2. СИМЕТРИЧНІ КЛЮЧІ (SC-12(2))

симетричні криптографічні ключі виробляються з використанням технології та процесів управління ключами <SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
симетричні криптографічні ключі контролюються за допомогою технології та процесів управління ключами <SC- 12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
симетричні криптографічні ключі розподіляються з використанням технології та процесів управління ключами <SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 1
Name: sc_12_2_odp_01
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {підтверджено; схвалено}; 599;

No: 2
Name: sc_12_2_odp_02

Type: string
Default: nil

ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 3
Name: sc_12_2_odp_03
Type: string
Default: nil

ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 4
Name: sc_12_2_01
Type: string
Default: nil

симетричні криптографічні ключі виробляються з використанням технології та процесів управління ключами <SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 5
Name: sc_12_2_02
Type: string
Default: nil

симетричні криптографічні ключі контролюються за допомогою технології та процесів управління ключами <SC- 12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 6
Name: sc_12_2_03
Type: string
Default: nil

симетричні криптографічні ключі розподіляються з використанням технології та процесів управління ключами <SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

16.12.3. АСИМЕТРИЧНІ КЛЮЧІ (SC-12(3))

створюються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
контролюються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;
розподіляються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 1
Name: sc_12_3_odp_01
Type: string
Default: nil

вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {затверджені уповноваженим органом технології та процеси управління ключами; посилені сертифікати відкритого ключа; попередньо визначений «ключовий» матеріал; кваліфіковані сертифікати відкритого ключа та надійні апаратні засоби цифрового підпису (токени), які захищають особистий ключ користувача; сертифікати, видані відповідно до визначених організацією вимо};

No: 2
Name: sc_12_3_odp_02
Type: string
Default: nil

ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 3
Name: sc_12_3_odp_03
Type: string
Default: nil

ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 4
Name: sc_12_3_odp_04
Type: string
Default: nil

ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 5
Name: sc_12_3_01
Type: string
Default: nil

створюються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 6
Name: sc_12_3_02
Type: string
Default: nil

контролюються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>;

No: 7
Name: sc_12_3_03
Type: string
Default: nil

розподіляються асиметричні криптографічні ключі за допомогою <SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

16.12.4. СЕРТИФІКАТИ PKI (SC-12(4)) [Вилучено]

ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI [Вилучено: включено до SC-12 (3)].;

No: 1
Name: sc_12_4_01
Type: string
Default: nil

ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI [Вилучено: включено до SC-12 (3)].;

16.12.5. СЕРТИФІКАТИ PKI, АПАРАТНІ ТОКЕНИ (SC-12(5)) [Вилучено]

ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI, АПАРАТНІ ТОКЕНИ [Вилучено: включено до SC-12 (3)].;

No: 1
Name: sc_12_5_01

Type: string
Default: nil

ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI, АПАРАТНІ ТОКЕНИ [Вилучено: включено до SC-12 (3)].;

16.12.6. ФІЗИЧНИЙ КОНТРОЛЬ КЛЮЧІВ (SC-12(6))

зберігається фізичний контроль над криптографічними ключами, коли інформація, що зберігається, шифрується зовнішніми постачальниками послуг.;

No: 1
Name: sc_12_6_01
Type: string
Default: nil

зберігається фізичний контроль над криптографічними ключами, коли інформація, що зберігається, шифрується зовнішніми постачальниками послуг.;

16.13. КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-13)

a. Визначити [Призначення: використання криптографічних засобів, визначених організацією]; b. Впровадити [Завдання: визначені організацією види криптографії для кожного визначеного криптографічного використання].

No: 1
Name: sc_13_01
Type: string
Default: "AES-256-GCM"

КРИПТОГРАФІЧНИЙ ЗАХИСТ МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: sc_13_odp_01
Type: string
Default: "AES-256-GCM"

Визначено використання криптографічних засобів

No: 3
Name: sc_13_odp_02
Type: string
Default: "AES-256-GCM"

Визначено типи криптографії для кожного вказаного криптографічного використання; SC-13a. ідентифіковано використання>; SC-13b. реалізовано типи криптографії для кожного вказаного криптографічного використання (визначеного в SC-13_ODP[01]). криптографічне <SC-13_ODP[01]

16.13.1. СТАНДАРТНА КРИПТОГРАФІЯ (SC-13(1)) [Вилучено]

КРИПТОГРАФІЧНИЙ ЗАХИСТ - СТАНДАРТНА КРИПТОГРАФІЯ [Вилучено: включено до SC-13].;

No: 1
Name: sc_13_1_01
Type: string
Default: nil

КРИПТОГРАФІЧНИЙ ЗАХИСТ - СТАНДАРТНА КРИПТОГРАФІЯ [Вилучено: включено до SC-13].;

16.13.2. ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ (SC-13(2)) [Вилучено]

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ [Вилучено: включено до SC-13].;

No: 1
Name: sc_13_2_01
Type: string
Default: nil

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ [Вилучено: включено до SC-13].;

16.13.3. ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ (SC-13(3)) [Вилучено]

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ [Вилучено: включено до SC-13].;

No: 1
Name: sc_13_3_01
Type: string
Default: nil

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ [Вилучено: включено до SC-13].;

16.13.4. ЦИФРОВІ ПІДПИСИ (SC-13(4)) [Вилучено]

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЦИФРОВІ ПІДПИСИ [Вилучено: включено до SC-13].;

No: 1
Name: sc_13_4_01
Type: string
Default: nil

КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЦИФРОВІ ПІДПИСИ [Вилучено: включено до SC-13].;

16.14. ЗАХИСТ ГРОМАДСЬКОГО ДОСТУПУ (SC-14) [Вилучено]

[Вилучено: включено до AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10]

Немає параметрів для цього контролю.

16.15. СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ ТА ЗАСТОСУНКИ (SC-15)

a. Заборонити віддалену активацію спільних обчислювальних пристроїв (хмар) та застосунків з такими виключеннями: [Призначення: визначені організацією виключення, у яких дозволена віддалена активація].
b. Надати явну вказівку щодо використання користувачами фізично присутніми пристроями.

Немає параметрів для цього контролю.

16.15.1. ФІЗИЧНЕ ЧИ ЛОГІЧНЕ ВІДКЛЮЧЕННЯ (SC-15(1))

відключення <SC-15(01) _ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> пристроїв для спільних обчислень забезпечується у спосіб, що підтримує простоту використання.;

No: 1
Name: sc_15_1_odp_01
Type: string
Default: nil

вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичний; логічний};

No: 2
Name: sc_15_1_01
Type: string
Default: nil

відключення <SC-15(01) _ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> пристроїв для спільних обчислень забезпечується у спосіб, що підтримує простоту використання.;

16.15.2. БЛОКУВАННЯ ТРАФІКУ ВХІДНИХ І ВИХІДНИХ ПОВІДОМЛЕНЬ (SC-15(2)) [Вилучено]

СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - БЛОКУВАННЯ ТРАФІКУ ВХІДНИХ І ВИХІДНИХ ПОВІДОМЛЕНЬ [Вилучено: включено до SC-7].;

Немає параметрів для цього контролю.

16.15.3. ВІДКЛЮЧЕННЯ ТА ВИДАЛЕННЯ В БЕЗПЕЧНИХ РОБОЧИХ ЗОНАХ (SC-15(3))

пристрої та програми для спільних обчислень відключенні або видаленні з <SC-15(03)_ ODP[01] систем або системних компонентів> в <SC-15(03)_ODP[02] захищених робочих зонах>.;

No: 1
Name: sc_15_3_odp_01
Type: string
Default: nil

систем або системних компонентів> в <SC-15(03)_ODP[02] захищених робочих зонах>.;

No: 2
Name: sc_15_3_01
Type: string
Default: nil

пристрої та програми для спільних обчислень відключенні або видаленні з <SC-15(03)_ODP[01] систем або системних компонентів> в <SC-15(03)_ODP[02] захищених робочих зонах>.;

16.15.4. ЧІТКА ІДЕНТИФІКАЦІЯ ПОТОЧНИХ УЧАСНИКІВ (SC-15(4))

надається явна вказівка на поточних учасників <SC- 15(04)_ODP онлайн-зустрічей і конференцій>. 604;

No: 1
Name: sc_15_4_odp_01
Type: string
Default: nil

є онлайн-зустрічі та конференції, для яких необхідно чітко вказувати поточних учасників, визначеними;

No: 2
Name: sc_15_4_01
Type: string
Default: nil

надається явна вказівка на поточних учасників <SC- 15(04)_ODP онлайн-зустрічей і конференцій>. 604;

16.16. ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ (SC-16)

Пов'язувати [Призначення: визначені організацією атрибути безпеки та приватності] з інформацією, яка передається між системами та компонентами системи.

No: 1
Name: sc_16_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Пов'язані атрибути інформацією, якою обмінюються системи; безпеки з

No: 2
Name: sc_16_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Пов'язані атрибути безпеки інформацією, якою обмінюються компоненти системи; з

No: 3
Name: sc_16_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Пов'язані атрибути приватності інформацією, якою обмінюються системи; з

No: 4
Name: sc_16_04

Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Пов'язані атрибути приватності інформацією, якою обмінюються компоненти системи. з

No: 5
Name: sc_16_odp_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені атрибути безпеки, які будуть пов'язані з інформацією, що обмінюється

No: 6
Name: sc_16_odp_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені атрибути приватності, які будуть пов'язані з інформацією, що обмінюється

16.16.1. ПЕРЕВІРКА ЦІЛІСНОСТІ (SC-16(1))

Перевірка цілісності (sc-16(1)).

Немає параметрів для цього контролю.

16.16.2. МЕХАНІЗМ АНТИСПУФІНГУ (SC-16(2))

впроваджені механізми боротьби зі спуфінгом, щоб не дозволити зловмисникам фальсифікувати атрибути безпеки, які вказують на успішне застосування процесу захисту.;

No: 1
Name: sc_16_2_01
Type: string
Default: nil

впроваджені механізми боротьби зі спуфінгом, щоб не дозволити зловмисникам фальсифікувати атрибути безпеки, які вказують на успішне застосування процесу захисту.;

16.16.3. КРИПТОГРАФІЧНА ПРИВ'ЯЗКА (SC-16(3))

реалізовані <SC-16(03)_ODP механізми або методи> для прив'язки атрибутів безпеки та приватності до інформації, що передається.;

No: 1
Name: sc_16_3_odp_01
Type: string
Default: nil

визначені механізми або методи прив'язки атрибутів безпеки та приватності до інформації, що передається;

No: 2
Name: sc_16_3_odp_02
Type: string
Default: nil

механізми або методи> для прив'язки атрибутів безпеки та приватності до інформації, що передається.;

No: 3
Name: sc_16_3_01
Type: string
Default: nil

реалізовані <SC-16(03)_ODP механізми або методи> для прив'язки атрибутів безпеки та приватності до інформації, що передається.;

16.17. СЕРТИФІКАТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ (SC-17)

a. Випускати сертифікати відкритого ключа відповідно до [Призначення: визначеної організацією політики сертифікації];
b. Отримувати сертифікати відкритого ключа від затвердженого постачальника послуг.

Немає параметрів для цього контролю.

16.18. МОБІЛЬНИЙ КОД (SC-18)

a. Визначати прийнятні та неприйнятні мобільні коди та технології мобільних кодів.
b. Проводити авторизацію, відстежувати та контролювати використання мобільного коду всередині системи.

Немає параметрів для цього контролю.

16.18.1. МОБІЛЬНИЙ КОД (SC-18(1))

ідентифіковано <SC-18(01)_ODP[01] неприйнятний мобільний код>; 608;
вживаються <SC-18(01)_ODP[02] коригувальні дії> у разі виявлення неприйнятного мобільного коду.;

No: 1
Name: sc_18_1_odp_01
Type: string
Default: nil

неприйнятний мобільний код>; 608;

No: 2
Name: sc_18_1_odp_02
Type: string
Default: nil

коригувальні дії> у разі виявлення неприйнятного мобільного коду.;

No: 3
Name: sc_18_1_01
Type: string
Default: nil

ідентифіковано <SC-18(01)_ODP[01] неприйнятний мобільний код>; 608;

No: 4
Name: sc_18_1_02
Type: string
Default: nil

вживаються <SC-18(01)_ODP[02] коригувальні дії> у разі виявлення неприйнятного мобільного коду.;

16.18.2. ПРИДБАННЯ, РОЗРОБКА ТА ВИКОРИСТАННЯ (SC-18(2))

відповідає придбання мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ ODP щодо мобільного коду>;
відповідає розробка мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ ODP вимоги до мобільного коду >;
відповідає використання мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ODP вимоги до мобільного коду >.;

No: 1
Name: sc_18_2_odp_01
Type: string
Default: nil

визначені вимоги до мобільного коду для придбання, розробки та використання мобільного коду для розгортання в системі;

No: 2
Name: sc_18_2_odp_02
Type: string
Default: nil

щодо мобільного коду>;

No: 3
Name: sc_18_2_odp_03
Type: string
Default: nil

вимоги до мобільного коду >;

No: 4
Name: sc_18_2_odp_04
Type: string
Default: nil

вимоги до мобільного коду >.;

No: 5
Name: sc_18_2_01
Type: string
Default: nil

відповідає придбання мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ODP щодо мобільного коду>;

No: 6
Name: sc_18_2_02
Type: string
Default: nil

відповідає розробка мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ODP вимоги до мобільного коду >;

No: 7
Name: sc_18_2_03
Type: string
Default: nil

відповідає використання мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ODP вимоги до мобільного коду >.;

16.18.3. ЗАПОБІГАННЯ ЗАВАНТАЖЕННЯ ТА ВИКОНАННЯ (SC-18(3))

запобігається завантаження <SC-18(03)_ODP неприйнятний мобільний код>;
запобігається виконання <SC-18(03)_ODP неприйнятний мобільний код>.;

No: 1
Name: sc_18_3_odp_01
Type: string
Default: nil

визначено неприйнятний мобільний код, який потрібно запобігти завантаженню та виконанню;

No: 2
Name: sc_18_3_odp_02
Type: string
Default: nil

неприйнятний мобільний код>;

No: 3
Name: sc_18_3_odp_03
Type: string
Default: nil

неприйнятний мобільний код>.;

No: 4
Name: sc_18_3_01
Type: string
Default: nil

запобігається завантаження <SC-18(03)_ODP неприйнятний мобільний код>;

No: 5
Name: sc_18_3_02
Type: string
Default: nil

запобігається виконання <SC-18(03)_ODP неприйнятний мобільний код>.;

16.18.4. ЗАПОБІГАННЯ АВТОМАТИЧНОГО ВИКОНАННЯ (SC-18(4))

запобігається автоматичне виконання мобільного коду в <SC- 18(04)_ODP[01] програмних додатках>;
виконуються <SC-18(04)_ODP[02] дії> перед виконанням мобільного коду.;

No: 1
Name: sc_18_4_odp_02

Type: string
Default: nil

дії> перед виконанням мобільного коду.;

No: 2
Name: sc_18_4_01
Type: string
Default: nil

запобігається автоматичне виконання мобільного коду в <SC- 18(04)_ODP[01] програмних додатках>;

No: 3
Name: sc_18_4_02
Type: string
Default: nil

виконуються <SC-18(04)_ODP[02] дії> перед виконанням мобільного коду.;

16.18.5. ДОЗВІЛ ВИКОНАННЯ ТІЛЬКИ В ОБМЕЖЕНИХ СЕРЕДОВИЩАХ (SC-18(5))

дозволено виконання дозволеного мобільного коду лише в обмеженому середовищі віртуальної машини.;

No: 1
Name: sc_18_5_01
Type: string
Default: nil

дозволено виконання дозволеного мобільного коду лише в обмеженому середовищі віртуальної машини.;

16.19. ІНТЕРНЕТ-ПРОТОКОЛ ГОЛОСОВОГО ЗВ'ЯЗКУ (SC-19) [Вилучено]

[Вилучено: залежить від технології; розглядається як будь-яка інша технологія або протокол]

Немає параметрів для цього контролю.

16.20. БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) (SC-20)

a. Надати додаткові дані автентифікації та перевірки цілісності джерела даних разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен/адрес.
b. Надати засоби для вказання статусу безпеки дочірніх зон і (якщо дочірня зона підтримує служби безпечного дозволу) забезпечити перевірку ланцюга довіри між батьківськими та дочірніми доменами при роботі в складі розподіленого ієрархічного простору імен.

Немає параметрів для цього контролю.

16.20.1. ДОЧІРНІЙ ПІДПРОСТІР (SC-20(1)) [Вилучено]

БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДОЧІРНІЙ ПІДПРОСТІР [Вилучено: включено до SC-20].;

Немає параметрів для цього контролю.

16.20.2. ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ (SC-20(2))

надаються справжні джерела походження запитів внутрішніх імен/адрес;
передбачено артефакти захисту цілісність запитів внутрішніх імен/адрес.;

No: 1
Name: sc_20_2_01
Type: string
Default: nil

надаються справжні джерела походження запитів внутрішніх імен/адрес;

No: 2
Name: sc_20_2_02
Type: string
Default: nil

передбачено артефакти захисту цілісність запитів внутрішніх імен/адрес.;

16.21. БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ (SC-21)

Зробити запит та виконати перевірку автентичності джерела даних і перевірку цілісності даних у відповідях на дозвіл імен/адрес, які система отримує від уповноважених джерел.

No: 1
Name: sc_21_01
Type: string
Default: nil

Реалізується запит перевірки автентичності джерела даних для відповідей на запит дозволу імен/адрес, які система отримує від авторитетних джерел

No: 2
Name: sc_21_02
Type: string
Default: nil

Реалізується запит автентифікація походження даних на основі відповідей з дозволу імен/адрес, які система отримує від авторитетних джерел

No: 3
Name: sc_21_03
Type: string
Default: nil

Реалізується запит перевірки цілісності даних для відповідей на запит дозволу імен/адрес, які система отримує від авторитетних джерел

No: 4
Name: sc_21_04
Type: string
Default: nil

Виконується перевірка цілісності даних для відповідей на запит про дозвіл імен/адрес, які система отримує від авторитетних джерел

16.21.1. ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ (SC-21(1)) [Вилучено]

БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (РЕКУРСИВНИЙ АБО КЕШУВАЛЬНИЙ ПЕРЕТВОРЮВАЧ) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ [Вилучено: включено до SC-21].;

Немає параметрів для цього контролю.

16.22. АРХІТЕКТУРА ТА ЗАБЕЗПЕЧЕННЯ СЛУЖБИ ІМЕН, АДРЕС (SC-22)

Переконатися, що системи, які спільно надають послуги розпізнавання імен/адрес для організації, є відмовостійкими та забезпечують поділ внутрішніх і зовнішніх ролей.

No: 1
Name: sc_22_01
Type: string
Default: nil

Є системи, які спільно надають послуги з визначення імен/адрес для організації, відмовостійкими

No: 2
Name: sc_22_02
Type: string
Default: nil

Реалізовано в системах, які спільно надають послуги з вирішення імен/адрес для організації, внутрішній розподіл ролей

No: 3
Name: sc_22_03
Type: string
Default: nil

Реалізовано в системах, які спільно надають послуги з вирішення імен/адрес для організації, зовнішній розподіл ролей

16.23. АВТЕНТИФІКАЦІЯ СЕСІЇ (SC-23)

Забезпечити автентифікацію сеансів зв'язку.

No: 1
Name: sc_23_01
Type: string
Default: nil

Захищено автентифікацію сеансів зв'язку

16.23.1. АНУЛЮВАННЯ ІДЕНТИФІКАТОРА СЕАНСУ ЗВ'ЯЗКУ ПРИ ВИХОДІ З СИСТЕМИ (SC-23(1))

анулюються ідентифікатори сеансу після виходу користувача або іншого припинення сеансу зв'язку.;

No: 1
Name: sc_23_1_01
Type: string
Default: nil

анулюються ідентифікатори сеансу після виходу користувача або іншого припинення сеансу зв'язку.;

16.23.2. ІНІЦІЙОВАНІ КОРИСТУВАЧЕМ ВИХОДИ ТА ПОВІДОМЛЕННЯ (SC-23(2)) [Вилучено]

АВТЕНТИФІКАЦІЯ СЕСІЇ - ІНІЦІЙОВАНІ КОРИСТУВАЧЕМ ВИХОДИ ТА ПОВІДОМЛЕННЯ [Вилучено: включено до SC-21(1)].;

Немає параметрів для цього контролю.

16.23.3. УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ (SC-23(3))

генерується унікальний ідентифікатор сеансу для кожного сеансу з <SC-23(03)_вимоги до випадковості ODP>;
розпізнаються лише системні ідентифікатори сеансів.;

No: 1
Name: sc_23_3_odp_01
Type: string
Default: nil

визначено вимоги до випадковості для генерації унікального ідентифікатора сеансу для кожного сеансу;

No: 2
Name: sc_23_3_01
Type: string
Default: nil

генерується унікальний ідентифікатор сеансу для кожного сеансу з <SC-23(03)_вимоги до випадковості ODP>;

No: 3
Name: sc_23_3_02
Type: string
Default: nil

розпізнаються лише системні ідентифікатори сеансів.;

16.23.4. УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ (SC-23(4)) [Вилучено]

АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ [Вилучено: включено до SC-23(3)].;

No: 1
Name: sc_21_4_01
Type: string
Default: nil

АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ [Вилучено: включено до SC-23(3)].;

16.23.5. УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ (SC-23(5))

дозволено використовувати лише <SC-23(05)_ODP сертифіковані органи> для перевірки встановлення захищених сеансів.;

No: 1
Name: sc_23_5_odp_01
Type: string
Default: nil

визначено центри сертифікації, які будуть допущені до перевірки встановлення захищених сеансів;

No: 2
Name: sc_23_5_odp_02
Type: string
Default: nil

сертифіковані органи> для перевірки встановлення захищених сеансів.;

No: 3
Name: sc_23_5_01
Type: string
Default: nil

дозволено використовувати лише <SC-23(05)_ODP сертифіковані органи> для перевірки встановлення захищених сеансів.;

16.24. УВЕДЕННЯ У ВІДОМИЙ СТАН (SC-24)

Увести систему в [Призначення: визначений організацією відомий стан системи] у разі [Призначення: визначені організацією типи збоїв системи] зі збереженням [Призначення: визначена організацією інформація про стан системи] при збої.

No: 1
Name: sc_24_01
Type: string
Default: nil

Типи системних збоїв на компонентах системи призводять до відомого стану системи, зберігаючи при цьому інформацію про стан системи у збої

No: 2
Name: sc_24_odp_01
Type: string
Default: nil

Визначені типи відмов системи, за яких компоненти системи переходять до відомого стану

No: 3
Name: sc_24_odp_02
Type: string
Default: nil

Відомий стан системи, до якого переходять компоненти системи у випадку її відмови

No: 4
Name: sc_24_odp_03
Type: string
Default: nil

Потрібно зберігати інформацію про стан системи у випадку її збою

16.25. ТОНКІ ВУЗЛИ (SC-25)

Використовувати [Призначення: визначені організацією системні компоненти] з мінімальною функціональністю та зберіганням інформації.

No: 1
Name: sc_25_01
Type: string
Default: nil

Використовується мінімальна функціональність для компонентів системи

No: 2
Name: sc_25_02
Type: string
Default: nil

Виділено мінімальне сховище інформації на компоненти системи

No: 3
Name: sc_25_odp
Type: string
Default: nil

Потрібно використовувати компоненти системи з мінімальною функціональністю та обсягом зберігання інформації

16.26. ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (DECOYS) (SC-26)

Вносити в систему компоненти, які спеціально призначені як об'єкти атак, з метою виявлення, відбиття й аналізу таких атак.

No: 1
Name: sc_26_01

Type: string
Default: "автоматизований засіб моніторингу"

Є в системах організації компоненти, спеціально розроблені для того, щоб стати мішенню зловмисних атак, і чи є в них засоби для виявлення таких атак

No: 2
Name: sc_26_02
Type: string
Default: "автоматизований засіб моніторингу"

Є в організаційних компонентах системи, спеціально розроблені для того, щоб стати мішенню зловмисних атак, і чи є в них засоби для відбиття таких атак

No: 3
Name: sc_26_03
Type: string
Default: nil

Включені в організаційні компоненти системи, спеціально розроблені для того, щоб бути мішенню зловмисних атак, для аналізу таких атак

16.26.1. ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ (SC-26(1)) [Вилучено]

ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) - ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ [Вилучено: включено до SC-35].;

No: 1
Name: sc_26_1_01
Type: string
Default: nil

ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) - ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ [Вилучено: включено до SC-35].;

16.27. НЕЗАЛЕЖНІ ВІД ПЛАТФОРМИ ЗАСТОСУНКИ (SC-27)

Внести до системи: [Призначення: визначені організацією незалежні від платформи застосунки].

No: 1
Name: sc_27_01
Type: string
Default: nil

Включені незалежні від платформи додатки в системи організації

No: 2
Name: sc_27_odp
Type: string
Default: nil

Визначені незалежні від платформи додатки, які мають бути включені в системи організації

16.28. ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ (SC-28)

Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] [Призначення: визначена організацією інформація] в стані спокою.

No: 1
Name: sc_28_odp
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {конфіденційність; цілісність}

No: 2
Name: sc_28_odp_02
Type: string
Default: nil

Є інформація в стані спокою, яка потребує захисту

16.28.1. КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-28(1))

Забезпечити криптографічний захист інформації в стані спокою.

No: 1
Name: sc_28_1_01
Type: string
Default: "AES-256-GCM"

Реалізовані криптографічні механізми для запобігання несанкціонованому розкриттю інформації, що знаходиться в стані спокою на системних компонентах або носіях

No: 2
Name: sc_28_1_02
Type: string
Default: "AES-256-GCM"

Реалізовані криптографічні механізми для запобігання несанкціонованій модифікації інформації, що знаходиться в стані спокою на системних компонентах або носіях

16.28.2. АВТОНОМНЕ СХОВИЩЕ (SC-28(2))

вилучено <SC-28(02)_ODP інформацію> з онлайн-сховища;
зберігається <SC-28(02)_ODP інформація> в автономному режимі в безпечному місці.;

No: 1
Name: sc_28_2_odp_01
Type: string
Default: nil

потрібно вилучати інформацію з онлайн-сховища та зберігати її в офлайн-сховищі в безпечному місці;

No: 2
Name: sc_28_2_odp_02
Type: string
Default: nil

інформацію> з онлайн-сховища;

No: 3
Name: sc_28_2_odp_03
Type: string
Default: nil

інформація> в автономному режимі в безпечному місці.;

No: 4
Name: sc_28_2_01
Type: string
Default: nil

вилучено <SC-28(02)_ODP інформацію> з онлайн-сховища;

No: 5
Name: sc_28_2_02
Type: string
Default: nil

зберігається <SC-28(02)_ODP інформація> в автономному режимі в безпечному місці.;

16.28.3. КРИПТОГРАФІЧНІ КЛЮЧІ (SC-28(3))

забезпечено захищене зберігання криптографічних ключів за допомогою <SC-28(03)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 1
Name: sc_28_3_odp_02
Type: string
Default: nil

гарантії>; апаратно-захищене сховище ключів};

No: 2
Name: sc_28_3_odp_01
Type: string
Default: nil

ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 3
Name: sc_28_3_01
Type: string
Default: nil

забезпечено захищене зберігання криптографічних ключів за допомогою <SC-28(03)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

16.29. ГЕТЕРОГЕННІСТЬ (SC-29)

Використовувати різноманітний набір інформаційних технологій для [Призначення: визначені організацією системні компоненти] при впровадженні системи.

No: 1
Name: sc_29_01
Type: string
Default: nil

Використовується різноманітний набір інформаційних технологій для компоненти системни при впровадженні системи

No: 2
Name: sc_29_odp
Type: string
Default: nil

Визначені компоненти системи, які потребують різноманітного набору інформаційних технологій, що мають бути використані при впровадженні системи

16.29.1. МЕТОДИ ВІРТУАЛІЗАЦІЇ (SC-29(1))

застосовуються методи віртуалізації для підтримки розгортання різноманітних операційних систем та додатків, які змінюються <SC-29(01)_ODP частота>.;

No: 1
Name: sc_29_1_odp_01
Type: string
Default: nil

визначена частота, з якою потрібно змінювати різноманітність операційних систем і додатків, розгорнутих за допомогою методів віртуалізації;

No: 2
Name: sc_29_1_odp_02
Type: string
Default: nil

частота>.;

No: 3
Name: sc_29_1_01
Type: string
Default: nil

застосовуються методи віртуалізації для підтримки розгортання різноманітних операційних систем та додатків, які змінюються <SC-29(01)_ODP частота>.;

16.30. МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ (SC-30)

Використовувати [Призначення: визначені організацією методи маскування та хибного напряму] для [Призначення: визначені організацією системи] у [Призначення: визначений організацією період часу], щоб заплутати та ввести в оману зловмисників.

No: 1
Name: sc_30_01
Type: integer
Default: 30

Застосовуються методи маскування та хибного напряму для систем протягом періодів часу, щоб заплутати та ввести супротивника в оману. застосування методів

No: 2
Name: sc_30_odp_01
Type: string
Default: nil

Визначені методи маскування та хибного напряму, які будуть застосовані для того, щоб заплутати і ввести в оману супротивників, які потенційно можуть націлитися на системи

No: 3
Name: sc_30_odp_02
Type: string
Default: nil

Визначені системи, для яких повинні застосовуватися методи маскування та хибного напряму

No: 4
Name: sc_30_odp_03
Type: integer
Default: 30

Визначені часові періоди для маскування та хибного напряму

16.30.1. МЕТОДИ ВІРТУАЛІЗАЦІЇ (SC-30(1)) [Вилучено]

МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МЕТОДИ ВІРТУАЛІЗАЦІЇ [Вилучено: включено до SC-29(1)].;

No: 1
Name: sc_30_1_01
Type: string
Default: nil

МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МЕТОДИ ВІРТУАЛІЗАЦІЇ [Вилучено: включено до SC-29(1)].;

16.30.2. ВИПАДКОВІСТЬ (SC-30(2))

застосовуються <SC-30(02)_ODP методи> для внесення випадковості в операції та активи організації.;

No: 1
Name: sc_30_2_odp_01
Type: string
Default: nil

визначені методи, що застосовуються для внесення випадковості в операції та активи організації;

No: 2
Name: sc_30_2_odp_02
Type: string
Default: nil

методи> для внесення випадковості в операції та активи організації.;

No: 3
Name: sc_30_2_01
Type: string
Default: nil

застосовуються <SC-30(02)_ODP методи> для внесення випадковості в операції та активи організації.;

16.30.3. ЗМІНА МІСЦЯ ОБРОБКИ ТА ЗБЕРІГАННЯ (SC-30(3))

змінено місце розташування <SC-30(03) _ODP[01] обробки та/або зберігання> <SC-30(03) _ ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

No: 1
Name: sc_30_3_odp_03
Type: string
Default: nil

часова частота>; випадкові часові інтервали};

No: 2
Name: sc_30_3_01
Type: string
Default: nil

змінено місце розташування <SC-30(03) _ODP[01] обробки та/або зберігання> <SC-30(03) _ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.;

16.30.4. НЕПРАВДИВА ІНФОРМАЦІЯ (SC-30(4))

використовується реалістична, але неправдива інформація про стан безпеки або стан <SC-30(04)_ODP компонентів системи>.;

No: 1
Name: sc_30_4_odp_01
Type: string
Default: nil

визначені компоненти системи, для яких використовується реалістична, але неправдива інформація про стан їхньої безпеки;

No: 2
Name: sc_30_4_odp_02
Type: string
Default: nil

компонентів системи>.;

No: 3
Name: sc_30_4_01
Type: string
Default: nil

використовується реалістична, але неправдива інформація про стан безпеки або стан <SC-30(04)_ODP компонентів системи>.;

16.30.5. МАСКУВАННЯ СИСТЕМНИХ КОМПОНЕНТІВ (SC-30(5))

застосовуються <SC-30(05)_ODP[01] методи> для приховування або маскування <SC-30(05)_ODP[02] компонентів системи>.;

No: 1
Name: sc_30_5_odp_01
Type: string
Default: nil

методи> для приховування або маскування <SC-30(05)_ODP[02] компонентів системи>.;

No: 2
Name: sc_30_5_01
Type: string
Default: nil

застосовуються <SC-30(05)_ODP[01] методи> для приховування або маскування <SC-30(05)_ODP[02] компонентів системи>.;

16.31. АНАЛІЗ ПРИХОВАНОГО КАНАЛУ (SC-31)

a. Проводити аналіз прихованого каналу, щоб визначити ті аспекти комунікацій у системі, які володіють потенційними можливостями для реалізації прихованих каналів [Вибір (один або кілька): зберігання; синхронізації].
b. Оцінювати максимальну пропускну здатність цих каналів.

Немає параметрів для цього контролю.

16.31.1. ТЕСТУВАННЯ ПРИХОВАНИХ КАНАЛІВ ДЛЯ ЕКСПЛУАТАЦІЇ (SC-31(1))

тестується підмножини визначених прихованих каналів, щоб визначити, які канали можна використовувати.;

No: 1
Name: sc_31_1_01
Type: string
Default: nil

тестується підмножини визначених прихованих каналів, щоб визначити, які канали можна використовувати.;

16.31.2. МАКСИМАЛЬНА ПРОПУСКНА ЗДАТНІСТЬ (SC-31(2))

зменшується максимальна пропускна здатність для ідентифікованих прихованих <SC-31(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> каналів до < SC- 31(02)_ODP[02] значень>.;

No: 1
Name: sc_31_2_odp_01
Type: string
Default: nil

ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> каналів до < SC- 31(02)_ODP[02] значень>.;

No: 2
Name: sc_31_2_01
Type: string
Default: nil

зменшується максимальна пропускна здатність для ідентифікованих прихованих <SC-31(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> каналів до < SC- 31(02)_ODP[02] значень>.;

16.31.3. ВИМІРЮВАННЯ ПРОПУСКНУ ЗДАТНІСТЬ В РОБОЧИХ СЕРЕДОВИЩАХ (SC-31(3))

вимірюється пропускна здатність <SC-31(03)_ODP підмножини ідентифікованих прихованих каналів> у операційному середовищі системи.;

No: 1
Name: sc_31_3_odp_01
Type: string
Default: nil

визначена підмножина ідентифікованих прихованих каналів, пропускна здатність яких має бути виміряна в операційному середовищі системи; 626;

No: 2
Name: sc_31_3_odp_02
Type: string
Default: nil

підмножини ідентифікованих прихованих каналів> у операційному середовищі системи.;

No: 3
Name: sc_31_3_01
Type: string
Default: nil

вимірюється пропускна здатність <SC-31(03)_ODP підмножини ідентифікованих прихованих каналів> у операційному середовищі системи.;

16.32. ПОДІЛ СИСТЕМИ НА ЧАСТИНИ (SC-32)

Розділити систему на [Призначення: визначені організацією системні компоненти], що розміщені в окремих фізичних доменах або середовищах на основі [Призначення: визначені організацією умови для фізичного поділу компонентів].

No: 1
Name: sc_32_01
Type: string
Default: nil

Розділена система на компоненти системи, що знаходяться в окремих ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА доменах або середовищах на основі обставин для фізичного або логічного поділу компонентів. фізичного або логічного

No: 2
Name: sc_32_odp_01
Type: string
Default: nil

Повинні компоненти системи перебувати в окремих фізичних або логічних доменах або середовищах, виходячи з обставин фізичного або логічного поділу компонентів

No: 3
Name: sc_32_odp_02
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {фізичний; логічний}

No: 4
Name: sc_32_odp_03
Type: string
Default: nil

Визначені обставини для розділення компонентів

16.32.1. ВІДОКРЕМЛЕНІ ФІЗИЧНІ ДОМЕНИ ДЛЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ (SC-32(1))

розділено привілейовані функції на окремі фізичні домени.;

No: 1
Name: sc_32_1_01
Type: string
Default: nil

розділено привілейовані функції на окремі фізичні домени.;

16.33. ПІДГОТОВКА ЦІЛІСНОСТІ ПЕРЕДАЧІ (SC-33) [Вилучено]

[Вилучено: включено до SC-8]

Немає параметрів для цього контролю.

16.34. НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ (SC-34)

У [Призначення: визначені організацією системні компоненти]:
a. Завантажити та виконати операційне середовище з апаратного носія, що працює в режимі лише для зчитування.
b. Завантажити та виконати [Призначення: визначені організацією застосунки] з апаратного носія, що працює в режимі лише для зчитування.

No: 1
Name: sc_34_odp_01
Type: string
Default: nil

Визначені компоненти системи, для яких операційне середовище та додатки мають завантажуватися та виконуватися з апаратних носіїв, призначених лише для читання

No: 2
Name: sc_34_odp_02
Type: string
Default: nil

Визначено додатки, які мають завантажуватися та виконуватися з апаратних носіїв, призначених лише для читання; SC-34a. завантажується та виконується операційне середовище для системних компонентів з апаратного носія, доступного лише для читання; SC-34b. додатки для компонентів системи завантажуються та виконуються з апаратного носія, доступного лише для читання.

16.34.1. ВІДСУТНІСТЬ СХОВИЩА ДОСТУПНОГО ДЛЯ ЗАПИСУ ІНФОРМАЦІЇ (SC-34(1))

використовуються <SC-34(01)_ODP компоненти системи> без записуваної пам'яті, яка зберігається після перезапуску компонента або увімкнення/вимкнення живлення.;

No: 1
Name: sc_34_1_odp_01
Type: string
Default: nil

визначено компоненти системи, які мають бути використані без можливості запису інформації;

No: 2
Name: sc_34_1_odp_02
Type: string
Default: nil

компоненти системи> без записуваної пам'яті, яка зберігається після перезапуску компонента або увімкнення/вимкнення живлення.;

No: 3
Name: sc_34_1_01
Type: string
Default: nil

використовуються <SC-34(01)_ODP компоненти системи> без записуваної пам'яті, яка зберігається після перезапуску компонента або увімкнення/вимкнення живлення.;

16.34.2. ЗАХИСТ ЦІЛІСНОСТІ НА НОСІЇ, ПРИДАТНОМУ ТІЛЬКИ ДЛЯ ЧИТАННЯ (SC-34(2))

захищена цілісність інформації перед зберіганням на носіях, призначених лише для читання; є носій інформації контрольованим після того, як така інформація була записана на нього;

No: 1
Name: sc_34_2_01
Type: string
Default: nil

захищена цілісність інформації перед зберіганням на носіях, призначених лише для читання;

No: 2
Name: sc_34_2_02
Type: string
Default: nil

є носій інформації контрольованим після того, як така інформація була записана на нього;

16.34.3. АПАРАТНИЙ ЗАХИСТ (SC-34(3)) [Вилучено]

НЕЗМІНЮВАНІ ПРОГРАМИ, ЩО ВИКОНУЮТЬСЯ - АПАРАТНИЙ ЗАХИСТ [Вилучено: перенесено до SC-51].;

No: 1
Name: sc_34_3_01
Type: string
Default: nil

НЕЗМІНЮВАНІ ПРОГРАМИ, ЩО ВИКОНУЮТЬСЯ - АПАРАТНИЙ ЗАХИСТ [Вилучено: перенесено до SC-51].;

16.35. РОЗПІЗНАВАННЯ ПРИМАНОК ДЛЯ ЗЛОВМИСНИКІВ (HONEYCLIENT) (SC-35)

Ввімкнути системні компоненти, які активно намагаються ідентифікувати мережевий шкідливий код та шкідливі вебсайти.

No: 1
Name: sc_35_01
Type: string
Default: nil

Ввімкнуті компоненти системи, які активно намагаються ідентифікувати мережевий шкідливий код та шкідливі вебсайти

16.36. РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ (SC-36)

Розподіліть наведені нижче компоненти обробки та зберігання в кількох [Вибір: фізичні локації; логічні домени]: [Призначення: компоненти обробки та зберігання, визначені організацією].

No: 1
Name: sc_36_odp_01
Type: string
Default: nil

Потрібно розподіляти компоненти обробки між кількома локаціями/доменами

No: 2
Name: sc_36_odp_02
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичні локації; логічні домени}

No: 3
Name: sc_36_odp_03
Type: string
Default: nil

Потрібно розподіляти компоненти сховища між кількома локаціями/доменами

No: 4
Name: sc_36_odp_04
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичні локації; логічні домени}

16.36.1. МЕТОДИ ОПИТУВАННЯ (SC-36(1))

застосовуються методи опитування для виявлення потенційних несправностей, помилок або компрометації <SC- 36(01)_ODP[01] компонентів розподіленої обробки та зберігання даних>; вживаються <SC-36(01)_ODP[02] дії> у відповідь на ідентифіковано несправності, помилки або компрометацію.;

No: 1
Name: sc_36_1_odp_02
Type: string
Default: nil

дії> у відповідь на ідентифіковано несправності, помилки або компрометацію.;

No: 2
Name: sc_36_1_01
Type: string
Default: nil

застосовуються методи опитування для виявлення потенційних несправностей, помилок або компрометації <SC- 36(01)_ODP[01] компонентів розподіленої обробки та зберігання даних>;

No: 3
Name: sc_36_1_02
Type: string
Default: nil

вживаються <SC-36(01)_ODP[02] дії> у відповідь на ідентифіковано несправності, помилки або компрометацію.;

16.36.2. СИНХРОНІЗАЦІЯ (SC-36(2))

синхронізовані <SC-36(02)_ODP дублікати систем або компонентів системи>.;

No: 1
Name: sc_36_2_odp_01
Type: string
Default: nil

визначено дублікати систем або системних компонентів, що підлягають синхронізації;

No: 2
Name: sc_36_2_odp_02
Type: string
Default: nil

дублікати систем або компонентів системи>.;

No: 3
Name: sc_36_2_01
Type: string
Default: nil

синхронізовані <SC-36(02)_ODP дублікати систем або компонентів системи>.;

16.37. ПОЗАСМУГОВІ КАНАЛИ (SC-37)

Використовувати [Призначення: визначені організацією позасмугові канали] для фізичного доставлення або електронної передачі [Призначення: визначена організацією інформація, системні компоненти або пристрої] до [Призначення: визначені організацією особи або системи].

No: 1
Name: sc_37_01
Type: string
Default: nil

Використовуються позасмугові канали для фізичної доставки або електронної передачі інформації, системних компонентів або пристроїв до осіб або систем

No: 2
Name: sc_37_odp_02
Type: string
Default: nil

Визначено інформацію, компоненти системи або пристрої для використання позасмугових каналів для фізичної доставки або електронної передачі

No: 3
Name: sc_37_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначені особи або системи, до яких фізична доставка або електронна передача інформації, системних компонентів або пристроїв має бути досягнута за допомогою використання позасмугових каналів

16.37.1. ЗАБЕЗПЕЧЕННЯ ДОСТАВЛЕННЯ ТА ПЕРЕДАЧІ (SC-37(1))

застосовуються <SC-37(01)_ODP[01] засоби контролю> для забезпечення того, щоб тільки <SC-37(01)_ODP[02] особи або системи> отримували <SC-37(01)_ODP[03] інформацію, компоненти системи або пристрої>.;

No: 1
Name: sc_37_1_odp_01
Type: string
Default: nil

засоби контролю> для забезпечення того, щоб тільки <SC-37(01)_ODP[02] особи або системи> отримували <SC-37(01)_ODP[03] інформацію, компоненти системи або пристрої>.;

No: 2
Name: sc_37_1_01
Type: string
Default: nil

застосовуються <SC-37(01)_ODP[01] засоби контролю> для забезпечення того, щоб тільки <SC-37(01)_ODP[02] особи або системи> отримували <SC-37(01)_ODP[03] інформацію, компоненти системи або пристрої>.;

16.38. БЕЗПЕКА ОПЕРАЦІЙ (SC-38)

Впровадити [Призначення: визначені організацією заходи з безпеки операцій] для захисту ключової організаційної інформації протягом усього життєвого циклу розробки системи.

No: 1
Name: sc_38_01
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються засоби контролю заходів з безпеки операцій для захисту ключової інформації організації протягом життєвого циклу розробки системи

No: 2
Name: sc_38_odp

Type: string
Default: "автоматизований засіб моніторингу"

Визначені засоби контролю заходів з безпеки операцій, які будуть застосовуватися для захисту ключової інформації організації протягом усього життєвого циклу розробки системи

16.39. ІЗОЛЯЦІЯ ПРОЦЕСУ (SC-39)

Підтримувати окремий домен виконання для кожного процесу, що виконується в системі.

No: 1
Name: sc_39_01
Type: string
Default: nil

Підтримується окремий домен виконання для кожного процесу, що виконується в системі

16.39.1. АПАРАТНЕ РОЗДІЛЕННЯ (SC-39(1))

реалізовано апаратне розділення для розділення процесів.;

No: 1
Name: sc_39_1_01
Type: string
Default: nil

реалізовано апаратне розділення для розділення процесів.;

16.39.2. ІЗОЛЯЦІЯ ПОТОКІВ (SC-39(2))

підтримується окремий домен виконання для кожного потоку у <SC-39(02)_ODP багатопотокової обробки>.;

No: 1
Name: sc_39_2_odp_01
Type: string
Default: nil

визначено багатопотокову обробку, для якої потрібно підтримувати окремий домен виконання для кожного потоку;

No: 2
Name: sc_39_2_odp_02
Type: string
Default: nil

багатопотокової обробки>.;

No: 3
Name: sc_39_2_01
Type: string
Default: nil

підтримується окремий домен виконання для кожного потоку у <SC-39(02)_ODP багатопотокової обробки>.;

16.40. ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ (SC-40)

Забезпечити захист зовнішніх і внутрішніх [Призначення: визначені організацією бездротові з'єднання] від [Призначення: визначені організацією типи атак з параметрами сигналів або посилання на джерела для таких атак].

No: 1
Name: sc_40_01
Type: string
Default: nil

Захищені зовнішні бездротові з'єднання від типів атак на параметри сигналу або посилання на джерела таких атак. SC-40[02] захищені внутрішні бездротові з'єднання від типів атак на параметри сигналу або посилання на джерела для таких атак

No: 2
Name: sc_40_odp_01
Type: string
Default: nil

Потрібно захищати зовнішні бездротові з'єднання від певних типів атак на параметри сигналу

No: 3
Name: sc_40_odp_02
Type: string
Default: nil

Визначено типи атак на параметри сигналу або посилання на джерела таких атак, від яких потрібно захищати зовнішні бездротові з'єднання

No: 4
Name: sc_40_odp_03
Type: string
Default: nil

Потрібно захищати внутрішні бездротові з'єднання від певних типів атак на параметри сигналу

No: 5
Name: sc_40_odp_04
Type: string
Default: nil

Визначені типи атак на параметри сигналу або посилання на джерела таких атак, від яких потрібно захищати внутрішні бездротові з'єднання

16.40.1. ЕЛЕКТРОМАГНІТНІ ПЕРЕШКОДИ (SC-40(1))

реалізовані криптографічні механізми, які забезпечують < <SC-40(01)_ODP рівень захисту> від впливу навмисних електромагнітних перешкод.;

No: 1
Name: sc_40_1_odp_01
Type: string
Default: nil

визначено рівень захисту від впливу навмисних електромагнітних перешкод;

No: 2
Name: sc_40_1_odp_02
Type: string
Default: nil

рівень захисту> від впливу навмисних електромагнітних перешкод.;

No: 3
Name: sc_40_1_01
Type: string
Default: nil

реалізовані криптографічні механізми, які забезпечують < <SC-40(01)_ODP рівень захисту> від впливу навмисних електромагнітних перешкод.;

16.40.2. ЗМЕНШЕННЯ ПОТЕНЦІАЛУ ВИЯВЛЕННЯ (SC-40(2))

впроваджено криптографічні механізми для зменшення потенціалу виявлення бездротових з'єднань до <SC- 40(02)_ODP рівня зменшення>.;

No: 1
Name: sc_40_2_odp_01
Type: string
Default: nil

визначено рівень зниження, якого необхідно досягти для зменшення потенціалу виявлення бездротових з'єднань;

No: 2
Name: sc_40_2_01
Type: string
Default: nil

впроваджено криптографічні механізми для зменшення потенціалу виявлення бездротових з'єднань до <SC-40(02)_ODP рівня зменшення>.;

16.40.3. ІМІТАЦІЙНИЙ АБО МАНІПУЛЯТИВНИЙ ОБМІН ПОВІДОМЛЕННЯМИ (SC-40(3))

впроваджені криптографічні механізми для визначення та відхилення бездротових передач, які є навмисними спробами досягти імітаційного або маніпулятивного обміну повідомленнями на основі параметрів сигналу.;

No: 1
Name: sc_40_3_01
Type: string
Default: nil

впроваджені криптографічні механізми для визначення та відхилення бездротових передач, які є навмисними спробами досягти імітаційного або маніпулятивного обміну повідомленнями на основі параметрів сигналу.;

16.41. ДОСТУП ДО ПОРТІВ ТА ПРИСТРОЇВ ВВЕДЕННЯ, ВИВЕДЕННЯ (SC-41)

[Вибір: фізично або логічно] відключити або видалити [Призначення: визначені організацією, порти підключення або пристрої введення/виводу] у [Призначення: визначені організацією

системи або системні компоненти].

No: 1
Name: sc_41_odp_01
Type: string
Default: nil

Визначено порти підключення або пристрої вводу/виводу, які потрібно відключити або видалити

No: 2
Name: sc_41_odp_02
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно}

No: 3
Name: sc_41_odp_03
Type: string
Default: nil

Визначені системи або компоненти системи з портами підключення або пристроями вводу/виводу, які потрібно відключити або видалити

16.42. МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ (SC-42)

a. Заборонити дистанційну активацію можливостей зондування навколишнього середовища в системах організації або компонентах системи за такими виключеннями: [Призначення: визначені організацією виключення, в яких допускається дистанційна активація датчиків].
b. Забезпечити явну вказівку використання датчика для [Призначення: визначений організацією клас користувачів].

No: 1
Name: sc_42_01
Type: string
Default: "автоматизований засіб моніторингу"

Механізми, що перешкоджають МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ

No: 2
Name: sc_42_odp_01
Type: string
Default: nil

Вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {використання пристроїв, що мають <SC-42_ODP[02] можливості зондування довкілля> на об'єктах, територіях або системах}; дистанційна активація можливостей зондування довкілля на організаційних системах або системних компонентах з наступними винятками: <SC-42_ODP[04] винятки, де дозволяється дистанційна активація датчиків}

No: 3
Name: sc_42_odp_02
Type: string
Default: nil

Визначені можливості зондування навколишнього середовища в пристроях (якщо вибрано)

No: 4
Name: sc_42_odp_03

Type: string
Default: nil

Визначені об'єкти, зони або системи, на яких заборонено використання пристроїв, що мають можливості зондування навколишнього середовища (якщо вони були обрані)

No: 5
Name: sc_42_odp_04
Type: string
Default: nil

Визначено винятки, коли дозволено віддалену активацію датчиків (якщо вибрано)

16.42.1. ЗВІТУВАННЯ ПЕРЕД УПОВНОВАЖЕНИМИ АБО ПОСАДОВИМИ ОСОБАМИ (SC-42(1))

налаштована система таким чином, щоб дані або інформація, <SC-42(01)_ODP зібрані датчиками>, повідомлялися лише уповноваженим особам або ролям. 640;

No: 1
Name: sc_42_1_odp_01
Type: string
Default: nil

визначені датчики, які будуть використовуватися для збору даних або інформації;

No: 2
Name: sc_42_1_odp_02
Type: string
Default: nil

зібрані датчиками>, повідомлялися лише уповноваженим особам або ролям. 640;

No: 3
Name: sc_42_1_01
Type: string
Default: nil

налаштована система таким чином, щоб дані або інформація, <SC-42(01)_ODP зібрані датчиками>, повідомлялися лише уповноваженим особам або ролям. 640;

16.42.2. ДОЗВОЛЕНЕ ВИКОРИСТАННЯ (SC-42(2))

застосовуються <SC-42(02)_ODP заходи> таким чином, щоб дані або інформація, зібрані <SC-42(01)_ODP датчиками>, використовувалися лише в дозволених цілях;

No: 1
Name: sc_42_2_odp_01
Type: string
Default: nil

потрібно вживати заходів для того, щоб дані або інформація, зібрані датчиками, використовувалися лише в дозволених цілях;

No: 2
Name: sc_42_2_odp_02
Type: string
Default: nil

заходи> таким чином, щоб дані або інформація, зібрані <SC-42(01)_ODP датчиками>, використовувалися лише в дозволених цілях;

No: 3
Name: sc_42_2_01
Type: string
Default: nil

застосовуються <SC-42(02)_ODP заходи> таким чином, щоб дані або інформація, зібрані <SC-42(01)_ODP датчиками>, використовувалися лише в дозволених цілях;

16.42.3. ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ (SC-42(3))

МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ [Вилучено: перенесено до SC-42].;

No: 1
Name: sc_42_3_01
Type: string
Default: nil

МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ [Вилучено: перенесено до SC-42].;

16.42.4. ПОВІДОМЛЕННЯ ПРО ЗБІР (SC-42(4))

застосовуються <SC-42(04)_ODP[01] заходи> для полегшення усвідомлення особою того, що персональні дані збираються за допомогою <SC-42(04)_ODP[02] датчиків>.;

No: 1
Name: sc_42_4_odp_01
Type: string
Default: nil

заходи> для полегшення усвідомлення особою того, що персональні дані збираються за допомогою <SC-42(04)_ODP[02] датчиків>.;

No: 2
Name: sc_42_4_01
Type: string
Default: nil

застосовуються <SC-42(04)_ODP[01] заходи> для полегшення усвідомлення особою того, що персональні дані збираються за допомогою <SC-42(04)_ODP[02] датчиків>.;

16.42.5. МІНІМІЗАЦІЯ ЗБОРУ (SC-42(5))

використовуються <SC-42(05)_ODP датчики>, налаштовані на мінімізацію збору персональних даних, які не є необхідними. 642;

No: 1
Name: sc_42_5_odp_01
Type: string
Default: nil

визначені датчики, які налаштовані на мінімізацію збору непотрібних персональних даних;

No: 2
Name: sc_42_5_odp_02

Type: string
Default: nil

датчики>, налаштовані на мінімізацію збору персональних даних, які не є необхідними. 642;

No: 3
Name: sc_42_5_01
Type: string
Default: nil

використовуються <SC-42(05)_ODP датчики>, налаштовані на мінімізацію збору персональних даних, які не є необхідними. 642;

16.43. МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ (SC-43)

a. Встановити обмеження на використання та рекомендації щодо впровадження для [Призначення: визначених організацією компонентів системи].
b. Проводити авторизацію, спостереження та контроль використання таких компонентів у системі.

No: 1
Name: sc_43_odp
Type: string
Default: nil

Визначені компоненти, для яких мають бути встановлені обмеження на використання та настанови щодо впровадження; SC-43a. встановлені обмеження на використання та настанови щодо впровадження для компонентів; SC-43b.[01] дозволено системі; SC-43b.[02] здійснюється моніторинг компонентів> в системі; SC-43b.[03] контролюється використання компонентів в системі. використання компонентів використання у <SC-43_ODP

16.44. ЕКРАНОВАНІ КАМЕРИ (SC-44)

Впровадити екрановані камери в [Призначення: визначену організацією систему, компонент системи або місце розташування].

No: 1
Name: sc_44_01
Type: string
Default: nil

Використовується в системі <SC-44_ODP, компоненті або місці розташування> застосування екранованої камери системному можливість

No: 2
Name: sc_44_odp
Type: string
Default: nil

Визначена система, компонент системи або місце, де має бути застосований потенціал екранованої камери

16.45. СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ (SC-45)

Синхронізація системного годинника в системі та компонентах системи і між ними.

No: 1
Name: sc_45_01
Type: integer
Default: 30

Синхронізовані системні годинники всередині системи та між системами і системними компонентами

16.45.1. СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ (SC-45(1))

порівнюються внутрішні системні годинники <SC- 45(01)_ODP[01] частота> з <SC-45(01)_ODP[02] авторитетним джерелом часу>;
синхронізовано внутрішній системний годинник з авторитетним джерелом часу, якщо різниця у часі більша за <SC-45(01)_ODP[03] часовий період>.;

No: 1
Name: sc_45_1_odp_02
Type: string
Default: nil

авторитетним джерелом часу>;

No: 2
Name: sc_45_1_odp_03
Type: string
Default: nil

часовий період>.;

No: 3
Name: sc_45_1_01
Type: string
Default: nil

порівнюються внутрішні системні годинники <SC- 45(01)_ODP[01] частота> з <SC-45(01)_ODP[02] авторитетним джерелом часу>;

No: 4
Name: sc_45_1_02
Type: string
Default: nil

синхронізовано внутрішній системний годинник з авторитетним джерелом часу, якщо різниця у часі більша за <SC-45(01)_ODP[03] часовий період>.;

16.45.2. ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ (SC-45(2))

є вторинне авторитетне джерело часу, яке знаходиться в іншому географічному регіоні, ніж первинне авторитетне джерело часу;
синхронізовано внутрішній системний годинник з вторинним авторитетним джерелом часу, якщо первинне авторитетне джерело часу недоступне.;

No: 1
Name: sc_45_2_01
Type: string
Default: nil

є вторинне авторитетне джерело часу, яке знаходиться в іншому географічному регіоні, ніж первинне авторитетне джерело часу;

No: 2
Name: sc_45_2_02
Type: string
Default: nil

синхронізовано внутрішній системний годинник з вторинним авторитетним джерелом часу, якщо первинне авторитетне джерело часу недоступне.;

16.46. ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ МІЖДОМЕННОЇ ПОЛІТИКИ (SC-46)

Впровадити механізм примусового виконання політики [Вибір: фізично; логічно] між фізичними та/або мережевими інтерфейсами для підключених доменів безпеки.

No: 1
Name: sc_46_odp
Type: string
Default: nil

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно}

16.47. АЛЬТЕРНАТИВНИЙ ШЛЯХ ЗВ'ЯЗКУ (SC-47)

Встановіть [Призначення: альтернативні шляхи зв'язку, визначені організацією] для організаційного управління та контролю операцій системи.

No: 1
Name: sc_47_01
Type: string
Default: nil

Встановлені альтернативні шляхи зв'язку для системних операцій та контролю операцій системи

No: 2
Name: sc_47_odp
Type: string
Default: nil

Визначені альтернативні шляхи зв'язку для системних операцій та контролю операцій системи

16.48. ПЕРЕМІЩЕННЯ ДАТЧИКА (SC-48)

Перенесіть [Призначення: датчики та можливості моніторингу, визначені організацією] до [Призначення: місця, визначені організацією] за таких умов або обставин: [Призначення: умови або обставини, визначені організацією].

No: 1
Name: sc_48_01
Type: string
Default: "автоматизований засіб моніторингу"

Переміщуються датчики і засоби моніторингу до місць розташування за умов або обставин

No: 2
Name: sc_48_odp_01
Type: string
Default: nil

Визначені датчики та можливості необхідно перемістити; моніторингу, які

No: 3
Name: sc_48_odp_02
Type: string
Default: "автоматизований засіб моніторингу"

Визначені місця, куди будуть переміщені датчики та засоби моніторингу

No: 4
Name: sc_48_odp_03
Type: list
Default: []

Визначені умови або обставини для переміщення датчиків і можливостей моніторингу

16.48.1. ДИНАМІЧНО ПЕРЕМІЩУЮТЬСЯ ДО ЗА (SC-48(1))

Датчики та засоби моніторингу динамічно переміщуються до місць розташування за умов або обставин.

No: 1
Name: sc_48_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Датчики та засоби моніторингу динамічно переміщуються до місць розташування за умов або обставин.

16.49. ПРИМУСОВЕ АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ (SC-49)

Впровадити механізми апаратного поділу та застосування політики між [Призначення: домени безпеки, визначені організацією].

No: 1
Name: sc_49_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Впроваджено механізми апаратного розділення та застосування політик між доменами безпеки

No: 2
Name: sc_49_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені домени безпеки, які потребують апаратного розділення та механізмів забезпечення дотримання політики

16.50. ПРИМУСОВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ (SC-50)

Впровадити програмне розділення та механізми застосування політики між [Призначення: домени безпеки, визначені організацією].

No: 1
Name: sc_50_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Впроваджено програмне розділення та механізми застосування політик між доменами безпеки.

No: 2
Name: sc_50_odp
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначені домени безпеки, які потребують програмного розділення та механізмів забезпечення дотримання політик

16.51. АПАРАТНИЙ ЗАХИСТ (SC-51)

a. Перевіряти правильність роботи [Призначення: визначені організацією функції безпеки та приватності].
b. Виконувати перевірку [Вибір (один або кілька): [Призначення: визначені організацією системні перехідні стани]; за командою користувача з відповідними повноваженнями; [Призначення: визначена організацією частота]].
c. Повідомляти [Призначення: визначені організацією персонал або посадові особи] про невдалі перевірки безпеки та приватності.
d. [Вибір (один або кілька): Вимкнути систему; Перезапустити систему; [Призначення: визначені організацією альтернативні дії]], коли виявляються аномалії.

No: 1
Name: sc_51_odp_01
Type: string
Default: nil

Визначено компоненти системної прошивки, потребують апаратного захисту від запису; які

No: 2
Name: sc_51_odp_02
Type: list
Default: ["admin", "security_officer"]

визначені уповноважені особи, які повинні виконувати процедури вимкнення та повторного ввімкнення апаратного захисту від запису;

No: 3
Name: sc_51_a
Type: string
Default: nil

використовується апаратний захист від запису для компонентів мікропрограми системи;

No: 4
Name: sc_51_b_01
Type: string
Default: nil

впроваджено спеціальні процедури для уповноважених осіб для ручного вимкнення апаратного захисту від запису для модифікацій мікропрограми;

No: 5
Name: sc_51_b_02
Type: string
Default: nil

реалізовано спеціальні процедури для уповноважених осіб для повторного увімкнення захисту від запису перед поверненням до робочого режиму.

17. SI

Клас заходів захисту SI — ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ

Опис Цей клас спрямований на захист системи від шкідливого коду, виявлення вразливостей та запобігання несанкціонованим змінам інформації.

Перелік заходів захисту Політика і процедури цілісності інформації (SI-1); Виправлення дефектів (SI-2); Централізоване управління (SI-2(1)) [Вилучено]; Автоматизоване виправлення дефектів (SI-2(2)); Час для усунення дефектів та орієнтири для коригувальних дій (SI-2(3)); Автоматичні засоби управління виправленнями (SI-2(4)); Автоматичне оновлення програмного забезпечення та вбудованого програмного забезпечення (SI-2(5)); Видалення попередніх версій програмного забезпечення та вбудованого програмного забезпечення (SI-2(6)); Захист від шкідливого коду (SI-3); Централізоване управління (SI-3(1)) [Вилучено]; Автоматичні оновлення (SI-3(2)) [Вилучено]; Непривілейовані користувачі (SI-3(3)) [Вилучено]; Оновлення тільки привілейованими користувачами (SI-3(4)); Портативні пристрої зберігання даних (SI-3(5)) [Вилучено]; Тестування та верифікація (SI-3(6)); Виявлення без підпису (SI-3(7)) [Вилучено]; Виявлення неавторизованих команд (SI-3(8)); Автентифікація віддалених команд (SI-3(9)) [Вилучено]; Аналіз шкідливого коду (SI-3(10)); Моніторинг системи (SI-4); ЗАГАЛЬНОСИСТЕМНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS) (SI-4(1)); Автоматизовані засоби та механізми аналізу в реальному часі (SI-4(2)); Автоматизовані засоби та механізми інтеграції (SI-4(3)); Трафік вхідних і вихідних комунікацій (SI-4(4)); Системні сповіщення (SI-4(5)); Заборона для непривілейованих користувачів (SI-4(6)) [Вилучено]; Автоматичне реагування на підозрілі події (SI-4(7)); Захист інформації моніторингу (SI-4(8)) [Вилучено]; Тестування засобів і механізмів моніторингу (SI-4(9)); Видимість зашифрованих комунікацій (SI-4(10)); Аналіз аномалій трафіку комунікацій (SI-4(11)); Створені організацією автоматизовані сповіщення (SI-4(12)); Аналіз трафіку та шаблонів подій (SI-4(13)); Виявлення бездротового вторгнення (SI-4(14)); Перехід від бездротового зв'язку до провідних мереж (SI-4(15)); Зіставлення інформації моніторингу (SI-4(16)); Інтегрована ситуаційна обізнаність (SI-4(17)); Аналіз трафіку та прихованої ексфільтрації (SI-4(18)); Особи, які представляють більший ризик (SI-4(19)); Привілейовані користувачі (SI-4(20)); Випробувальні терміни (SI-4(21)); Несанкціоновані послуги мережі (SI-4(22)); Пристрої на основі хоста (SI-4(23)); Індикатори компрометації (SI-4(24)); Аналіз мережевого трафіку (SI-4(25)); Попередження, рекомендації та директиви з безпеки (SI-5); Автоматичні попередження та рекомендації (SI-5(1)); Перевірка функцій безпеки та приватності (SI-6); Сповіщення про неуспішне проходження тестів з безпеки (SI-6(1)) [Вилучено]; Автоматизована підтримка розподіленого тестування (SI-6(2)); Повідомлення про результати

перевірки (SI-6(3)); Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації (SI-7); Перевірка цілісності (SI-7(1)); Автоматичні сповіщення про порушення цілісності (SI-7(2)); Інструменти цілісності з централізованим управлінням (SI-7(3)); Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації – пакування з індикацією ознак її несанкціонованого розкриття (SI-7(4)); Автоматичні відповіді про порушення цілісності (SI-7(5)); Криптографічний захист (SI-7(6)); Інтеграція виявлення і реагування (SI-7(7)); Аудит важливих подій (SI-7(8)); Перевірка процесу завантаження (SI-7(9)); Захист завантажувального вбудованого програмного забезпечення (SI-7(10)); Обмежене середовище з обмеженими привілеями (SI-7(11)) [Вилучено]; Перевірка цілісності (SI-7(12)); Виконання коду в захищених середовищах (SI-7(13)) [Вилучено]; Двійковий або машинно-виконуваний код (SI-7(14)) [Вилучено]; Автентифікація коду (SI-7(15)); Термін виконання процесу без нагляду (SI-7(16)); Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації – самозахист програм від самовільного виконання (SI-7(17)); Захист від спаму (SI-8); Централізоване управління (SI-8(1)) [Вилучено]; Автоматичні оновлення (SI-8(2)); Безперервне навчання (SI-8(3)); Обмеження на введення інформації (SI-9) [Вилучено]; Перевірка вводу інформації (SI-10); Можливість ручного перевизначення (SI-10(1)); Перегляд та усунення помилок (SI-10(2)); Передбачувана поведінка (SI-10(3)); Часові взаємодії (SI-10(4)); Обмеження вхідних даних довіреними джерелами і затвердженими форматами (SI-10(5)); Профілактика вводу даних (SI-10(6)); Обробка помилок (SI-11); Управління та збереження інформації (SI-12); Обмеження елементів персональних даних (SI-12(1)); Мінімізація використання персональних даних під час тестування, навчання та дослідженні (SI-12(2)); Видалення інформації (SI-12(3)); Передбачуване запобігання збоїв (SI-13); Відповідальність за передачу функцій компонентів (SI-13(1)); Термін виконання процесу без нагляду (SI-13(2)) [Вилучено]; Ручна передача функцій компонентів (SI-13(3)); Встановлення резервних компонентів та оповіщення (SI-13(4)); Можливість аварійного перемикання (SI-13(5)); Нестійкість (SI-14); Оновлення з надійних джерел (SI-14(1)); Нестійка інформація (SI-14(2)); Нестійкі підключення (SI-14(3)); Фільтрація вихідних даних (SI-15); Захист пам'яті (SI-16); Відмовостійкі процедури (SI-17); Операції забезпечення якості даних (SI-18); Автоматична підтримка (SI-18(1)); Тегування даних (SI-18(2)); Збирання (SI-18(3)); Індивідуальні запити (SI-18(4)); Повідомлення про виправлення чи видалення (SI-18(5)); Деідентифікація (SI-19); Збір (SI-19(1)); Архівація (SI-19(2)); Видалення (SI-19(3)); Видалення, маскування, шифрування, хешування або заміна прямих ідентифікаторів (SI-19(4)); Контроль статистичного розкриття (SI-19(5)); Диференційована конфіденційність (SI-19(6)); Перевірене програмне забезпечення (SI-19(7)); Мотивований порушник (SI-19(8)); Псування (SI-20); Оновлення інформації (SI-21); Різновиди інформації (SI-22); Фрагментація інформації (SI-23).

17.1. ПОЛІТИКА І ПРОЦЕДУРИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ (SI-1)

Політика і процедури цілісності інформації.

No: 1
Name: si_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, до яких має бути доведена політика цілісності системи та інформації

No: 2
Name: si_1_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюються процедури цілісності системи та інформації

No: 3
Name: si_1_odp_03
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи}

No: 4
Name: si_1_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено посадову особу, відповідальну за управління системою та політикою і процедурами цілісності інформації

No: 5
Name: si_1_odp_05
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Визначено періодичність перегляду та оновлення поточної політики цілісності системи та інформації

No: 6
Name: si_1_odp_06
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Є події, які вимагають перегляду та оновлення поточної політики цілісності системи та інформації

No: 7
Name: si_1_odp_07
Type: integer
Default: 30

Визначено частоту, з якою переглядаються та оновлюються поточні цілісності системи та інформації

17.2. ВИПРАВЛЕННЯ ДЕФЕКТІВ (SI-2)

Виявлено недоліки системи;.

No: 1
Name: si_2_odp
Type: string
Default: nil

визначено період часу, протягом якого необхідно встановити оновлення програмного забезпечення, пов'язані з безпекою, після виходу оновлень;

No: 2
Name: si_2_a_01
Type: string
Default: nil

виявлено недоліки системи;

No: 3
Name: si_2_a_02
Type: string
Default: nil

повідомляється про недоліки системи;

No: 4
Name: si_2_a_03
Type: string
Default: nil

виправлені недоліки системи;

No: 5
Name: si_2_b_01
Type: string
Default: nil

перевіряються оновлення програмного забезпечення, пов'язані з усуненням недоліків, на ефективність перед встановленням;

No: 6
Name: si_2_b_02
Type: string
Default: nil

перевіряються оновлення програмного забезпечення, пов'язані з виправленням дефектів, на наявність потенційних побічних ефектів перед встановленням;

No: 7
Name: si_2_b_03
Type: string
Default: nil

перевіряються оновлення прошивки, пов'язані з усуненням недоліків, на ефективність перед встановленням;

No: 8
Name: si_2_b_04
Type: string
Default: nil

перевіряються оновлення прошивки, пов'язані з усуненням недоліків, на наявність потенційних побічних ефектів перед встановленням;

No: 9
Name: si_2_c_01
Type: string
Default: nil

встановлено оновлення програмного забезпечення, що стосуються безпеки, протягом <SI-02_ODP часовий проміжок> з моменту випуску оновлень;

No: 10
Name: si_2_c_02
Type: string
Default: nil

встановлено оновлення мікропрограми, що стосуються безпеки, протягом <SI-02_ODP часового періоду> з моменту випуску оновлень;

No: 11
Name: si_2_d
Type: string
Default: nil

включено відновлення порушених прав у процес управління організаційною конфігурацією.

17.2.1. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ (SI-2(1)) [Вилучено]

[Вилучено: перенесено до PL-09]

Немає параметрів для цього контролю.

17.2.2. АВТОМАТИЗОВАНЕ ВИПРАВЛЕННЯ ДЕФЕКТІВ (SI-2(2))

Встановлені на компонентах системи відповідні оновлення програмного забезпечення та мікропрограми, що стосуються безпеки, з частотою за допомогою автоматизованих механізмів.

No: 1
Name: si_2_2_01
Type: integer
Default: 30

Встановлені на компонентах системи відповідні оновлення програмного забезпечення та мікропрограми, що стосуються безпеки, з частотою за допомогою автоматизованих механізмів

17.2.3. ЧАС ДЛЯ УСУНЕННЯ ДЕФЕКТІВ ТА ОРІЄНТИРИ ДЛЯ КОРИГУВАЛЬНИХ ДІЙ (SI-2(3))

Вимірюється час між виявленням дефекту та його усуненням; SI-02(03)(b) були встановлені орієнтири для вжиття коригувальних дій.

No: 1
Name: si_2_3_a
Type: integer
Default: 30

Вимірюється час між виявленням дефекту та його усуненням; SI-02(03)(b) були встановлені орієнтири для вжиття коригувальних дій

No: 2
Name: si_2_3_odp
Type: string
Default: nil

Визначені контрольні коригувальних заходів; показники для вжиття

17.2.4. АВТОМАТИЧНІ ЗАСОБИ УПРАВЛІННЯ ВИПРАВЛЕННЯМИ (SI-2(4))

Автоматичні засоби управління виправленнями (si-2(4)).

No: 1
Name: si_2_4_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначені компоненти системи, які потребують автоматизованих інструментів управління виправленнями для полегшення усунення дефектів; SI-02(04)] застосовуються автоматизовані засоби управління виправленнями для полегшення виправлення недоліків у компонентах

17.2.5. АВТОМАТИЧНЕ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (SI-2(5))

(05) _ODP[01] оновлення програмного забезпечення та мікропрограми, що стосуються безпеки>, встановлено автоматично до <SI-02(05) _ODP[02] компонентів системи>.

No: 1
Name: si_2_5_01
Type: string
Default: nil

SI-02(05) _ODP[01] оновлення програмного забезпечення та мікропрограми, що стосуються безпеки>, встановлено автоматично до <SI-02(05) _ODP[02] компонентів системи>

17.2.6. ВИДАЛЕННЯ ПОПЕРЕДНІХ ВЕРСІЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (SI-2(6))

Видаляються попередні версії програмне забезпечення та компоненти мікропрограми після встановлення оновлених версій.

No: 1
Name: si_2_6_01
Type: string
Default: nil

Видаляються попередні версії програмне забезпечення та компоненти мікропрограми після встановлення оновлених версій

No: 2
Name: si_2_6_odp
Type: string
Default: nil

Потрібно видаляти компоненти програмного забезпечення та мікропрограми після встановлення оновлених версій

17.3. ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ (SI-3)

Захист від шкідливого коду.

No: 1
Name: si_3_odp_01
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {підписаний; непідписаний}

No: 2
Name: si_3_odp_02
Type: integer
Default: 30

Визначено частоту, з якою механізми шкідливого коду виконують сканування

No: 3
Name: si_3_odp_03
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {кінцева точка; точки входу та виходу з мережі}

No: 4
Name: si_3_odp_04
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {block malicious code; quarantitne malicious code; take action}

No: 5
Name: si_3_odp_05
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії, яких слід вжити у відповідь на виявлення шкідливого коду (якщо вибрано)

17.3.1. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ (SI-3(1)) [Вилучено]

[Вилучено: включено до PL-9]

Немає параметрів для цього контролю.

17.3.2. АВТОМАТИЧНІ ОНОВЛЕННЯ (SI-3(2)) [Вилучено]

[Вилучено: включено до SI-03]

Немає параметрів для цього контролю.

17.3.3. НЕПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ (SI-3(3)) [Вилучено]

[Вилучено: включено до AC-6(10)]

Немає параметрів для цього контролю.

17.3.4. ОНОВЛЕННЯ ТІЛЬКИ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ (SI-3(4))

Оновлюються механізми захисту від шкідливого коду лише за вказівкою привілейованого користувача.

No: 1
Name: si_3_4_01
Type: string
Default: "автоматизований засіб моніторингу"

Оновлюються механізми захисту від шкідливого коду лише за вказівкою привілейованого користувача

17.3.5. ПОРТАТИВНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ (SI-3(5)) [Вилучено]

[Вилучено: включено до MP-7]

Немає параметрів для цього контролю.

17.3.6. ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ (SI-3(6))

Перевіряються механізми захисту від шкідливого коду частота шляхом введення в систему відомого доброякісного коду.

No: 1
Name: si_3_6_a
Type: string
Default: "щорічно"

Перевіряються механізми захисту від шкідливого коду частота шляхом введення в систему відомого доброякісного коду

No: 2
Name: si_3_6_b_01
Type: string
Default: nil

Відбувається виявлення (доброякісний тест) коду

No: 3
Name: si_3_6_b_02
Type: string
Default: nil

Відбувається відповідне звітування про інцидент

No: 4
Name: si_3_6_odp
Type: string
Default: "щорічно"

Визначено періодичність тестування механізмів захисту від зловмисного коду

17.3.7. ВИЯВЛЕННЯ БЕЗ ПІДПИСУ (SI-3(7)) [Вилучено]

[Вилучено: включено до SI-3]

Немає параметрів для цього контролю.

17.3.8. ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМАНД (SI-3(8))

Виявлено <SI-03(08) _ODP[01] неавторизовані команди операційної системи> через інтерфейс прикладного програмування ядра на <SI-03(08) _ODP[02] апаратних компонентах системи>.

No: 1
Name: si_3_8_a
Type: string
Default: nil

Виявлено <SI-03(08) _ODP[01] неавторизовані команди операційної системи> через інтерфейс прикладного програмування ядра на <SI-03(08) _ODP[02] апаратних компонентах системи>

17.3.9. АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД (SI-3(9)) [Вилучено]

[Вилучено: включено до AC-17(10)]

Немає параметрів для цього контролю.

17.3.10. АНАЛІЗ ШКІДЛИВОГО КОДУ (SI-3(10))

Використовуються інструменти та методи для аналізу характеристик та поведінки шкідливого коду.

No: 1
Name: si_3_10_a
Type: string
Default: nil

Використовуються інструменти та методи для аналізу характеристик та поведінки шкідливого коду

No: 2
Name: si_3_10_b_01
Type: string
Default: nil

Включені результати аналізу шкідливого коду в організаційні процеси реагування на інциденти

No: 3
Name: si_3_10_b_02
Type: string
Default: nil

Включені результати аналізу шкідливого коду в організаційні процеси виправлення недоліків

No: 4
Name: si_3_10_odp
Type: string
Default: nil

Визначені інструменти та методи, які будуть використовуватися для аналізу характеристик та поведінки шкідливого коду

17.4. МОНІТОРИНГ СИСТЕМИ (SI-4)

Моніторинг системи.

No: 1
Name: si_4_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначені методи та способи, що використовуються для виявлення несанкціонованого використання системи

No: 2
Name: si_4_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначена інформація про моніторинг системи, яка повинна надаватися персоналу або ролям

No: 3
Name: si_4_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким має надаватися інформація про моніторинг системи

No: 4
Name: si_4_odp_05
Type: string
Default: "щорічно"

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {за потребою; частота}

17.4.1. ЗАГАЛЬНОСИСТЕМНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS) (SI-4(1))

Підключені окремі засоби виявлення вторгнень загальносистемної системи виявлення вторгнень; до.

No: 1
Name: si_4_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Підключені окремі засоби виявлення вторгнень загальносистемної системи виявлення вторгнень; до

No: 2
Name: si_4_1_02
Type: string
Default: nil

Об'єднані окремі інструменти виявлення вторгнень загальносистемну систему виявлення вторгнень. у

17.4.2. АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ (SI-4(2))

Автоматизовані засоби та механізми аналізу в реальному часі (si-4(2)).

Немає параметрів для цього контролю.

17.4.3. АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ ІНТЕГРАЦІЇ (SI-4(3))

Використовуються автоматизовані інструменти та механізми для інтеграції інструментів та механізмів виявлення вторгнень у механізми контролю доступу.

No: 1
Name: si_4_3_01
Type: string
Default: "автоматизований засіб моніторингу"

Використовуються автоматизовані інструменти та механізми для інтеграції інструментів та механізмів виявлення вторгнень у механізми контролю доступу

No: 2
Name: si_4_3_02
Type: string
Default: "автоматизований засіб моніторингу"

Використовуються автоматизовані інструменти та механізми для інтеграції інструментів та механізмів виявлення вторгнень у механізми контролю потоків

17.4.4. ТРАФІК ВХІДНИХ І ВИХІДНИХ КОМУНІКАЦІЙ (SI-4(4))

Визначені критерії незвичної або несанкціонованої діяльності або умови для вхідного трафіку зв'язку.

No: 1
Name: si_4_4_a_01
Type: list
Default: []

Визначені критерії незвичної або несанкціонованої діяльності або умови для вхідного трафіку зв'язку

No: 2
Name: si_4_4_a_02
Type: list
Default: []

Визначені критерії незвичайної або несанкціонованої діяльності або умови для вихідного трафіку зв'язку

No: 3
Name: si_4_4_b_01
Type: string
Default: "щорічно"

Здійснюється моніторинг вхідного комунікаційного трафіку частота на предмет незвичних або несанкціонованих дій або умов

No: 4
Name: si_4_4_b_02
Type: string
Default: "щорічно"

Контролюється вихідний трафік зв'язку частота на предмет незвичних або несанкціонованих дій або умов. вихідного виявлення

17.4.5. СИСТЕМНІ СПОВІЩЕННЯ (SI-4(5))

Відбувається оповіщення <SI-04(05) _ODP[01] персоналу або ролей> при виникненні згенерованих системою <SI-04(05) _ODP[02] індикаторів компрометації>.

No: 1
Name: si_4_5_01
Type: list
Default: ["admin", "security_officer"]

Відбувається оповіщення <SI-04(05) _ODP[01] персоналу або ролей> при виникненні згенерованих системою <SI-04(05) _ODP[02] індикаторів компрометації>

17.4.6. ЗАБОРОНА ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ (SI-4(6)) [Вилучено]

[Вилучено: включено до AC-6(10)]

Немає параметрів для цього контролю.

17.4.7. АВТОМАТИЧНЕ РЕАГУВАННЯ НА ПІДОЗРІЛІ ПОДІЇ (SI-4(7))

Повідомляється персонал з реагування на інциденти про виявлені підозрілі події.

No: 1
Name: si_4_7_a
Type: list
Default: ["admin", "security_officer"]

Повідомляється персонал з реагування на інциденти про виявлені підозрілі події

No: 2
Name: si_4_7_b
Type: list
Default: ["login", "logout", "failed_attempt"]

Вживаються найменш руйнівні дії при виявленні підозрілих подій

17.4.8. ЗАХИСТ ІНФОРМАЦІЇ МОНІТОРИНГУ (SI-4(8)) [Вилучено]

[Вилучено: включено до SI-4]

Немає параметрів для цього контролю.

17.4.9. ТЕСТУВАННЯ ЗАСОБІВ І МЕХАНІЗМІВ МОНІТОРИНГУ (SI-4(9))

Тестуються інструменти та механізми моніторингу вторгнень <SI-04(09)_ ODP періодичність>.

No: 1
Name: si_4_9_01
Type: string
Default: "щорічно"

Тестуються інструменти та механізми моніторингу вторгнень <SI-04(09)_ ODP періодичність>

No: 2
Name: si_4_9_odp
Type: string
Default: "щорічно"

Визначена періодичність тестування механізмів моніторингу вторгнень; інструментів і

17.4.10. ВИДИМІСТЬ ЗАШИФРОВАНИХ КОМУНІКАЦІЙ (SI-4(10))

Передбачено, щоб <SI-04(10) _ODP[01] зашифрований трафік зв'язку> був видимим для <SI-04(10) _ODP[02] засобів та механізмів моніторингу системи>.

No: 1
Name: si_4_10_01
Type: string
Default: nil

Передбачено, щоб <SI-04(10) _ODP[01] зашифрований трафік зв'язку> був видимим для <SI-04(10) _ODP[02] засобів та механізмів моніторингу системи>

17.4.11. АНАЛІЗ АНОМАЛІЙ ТРАФІКУ КОМУНІКАЦІЙ (SI-4(11))

Аналізується вихідний комунікаційний трафік на зовнішніх інтерфейсах системи для виявлення аномалій.

No: 1
Name: si_4_11_01
Type: string
Default: nil

Аналізується вихідний комунікаційний трафік на зовнішніх інтерфейсах системи для виявлення аномалій

No: 2
Name: si_4_11_02
Type: string
Default: nil

Аналізується вихідний трафік зв'язку в внутрішніх точках для виявлення аномалій

No: 3
Name: si_4_11_odp

Type: string
Default: nil

Визначені внутрішні точки в системі, в яких необхідно аналізувати комунікаційний трафік

17.4.12. СТВОРЕНІ ОРГАНІЗАЦІЄЮ АВТОМАТИЗОВАНІ СПОВІЩЕННЯ (SI-4(12))

Оповіщається <SI-04(12) _ODP[01] персонал або ролі> за допомогою <SI-04(12) _ODP[02] автоматизованих механізмів>, коли <SI-04(12) _ODP[03] дії, що викликають оповіщення> вказують на невідповідну або незвичну викликають оповіщення персоналу, або діяльність, що має вплив на безпеку або приватне життя.

No: 1
Name: si_4_12_01
Type: list
Default: ["admin", "security_officer"]

Оповіщається <SI-04(12) _ODP[01] персонал або ролі> за допомогою <SI-04(12) _ODP[02] автоматизованих механізмів>, коли <SI-04(12) _ODP[03] дії, що викликають оповіщення> вказують на невідповідну або незвичну викликають оповіщення персоналу, або діяльність, що має вплив на безпеку або приватне життя

17.4.13. АНАЛІЗ ТРАФІКУ ТА ШАБЛОНІВ ПОДІЙ (SI-4(13))

Аналізується трафік для системи.

No: 1
Name: si_4_13_a_01
Type: string
Default: nil

Аналізується трафік для системи

No: 2
Name: si_4_13_a_02
Type: string
Default: nil

Проаналізовано патерни подій для системи

No: 3
Name: si_4_13_b_01
Type: string
Default: nil

Розроблені профілі, що представляють загальний трафік

No: 4
Name: si_4_13_b_02
Type: string
Default: nil

Розроблені профілі, що представляють патерни подій

No: 5
Name: si_4_13_c_01
Type: string
Default: nil

Використовуються профілі трафіку пристроїв системного моніторингу

No: 6
Name: si_4_13_c_02
Type: string
Default: nil

Використовуються профілі подій при налаштуванні пристроїв системного моніторингу при налаштуванні

17.4.14. ВИЯВЛЕННЯ БЕЗДРОТОВОГО ВТОРГНЕННЯ (SI-4(14))

Використовується система виявлення бездротових вторгнень для виявлення несанкціонованих бездротових пристроїв.

No: 1
Name: si_4_14_01
Type: string
Default: nil

Використовується система виявлення бездротових вторгнень для виявлення несанкціонованих бездротових пристроїв

No: 2
Name: si_4_14_02
Type: integer
Default: 3

Використовується бездротова система виявлення вторгнень для виявлення спроб атак на систему

No: 3
Name: si_4_14_03
Type: string
Default: nil

Використовується бездротова система виявлення вторгнень для виявлення потенційних компрометації або порушень в системі

17.4.15. ПЕРЕХІД ВІД БЕЗДРОТОВОГО ЗВ'ЯЗКУ ДО ПРОВІДНИХ МЕРЕЖ (SI-4(15))

Перехід від бездротового зв'язку до провідних мереж (si-4(15)).

Немає параметрів для цього контролю.

17.4.16. ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ МОНІТОРИНГУ (SI-4(16))

Співвідноситься інформація з інструментів моніторингу та механізмів, що застосовуються в системі.

No: 1
Name: si_4_16_01
Type: string
Default: nil

Співвідноситься інформація з інструментів моніторингу та механізмів, що застосовуються в системі

17.4.17. ІНТЕГРОВАНА СИТУАЦІЙНА ОБІЗНАНІСТЬ (SI-4(17))

Співвідноситься інформація, отримана в результаті моніторингу фізичної, кібернетичної діяльності та діяльності ланцюга поставок, з метою досягнення інтегрованої, загальноорганізаційної ситуаційної обізнаності.

No: 1
Name: si_4_17_01
Type: string
Default: nil

Співвідноситься інформація, отримана в результаті моніторингу фізичної, кібернетичної діяльності та діяльності ланцюга поставок, з метою досягнення інтегрованої, загальноорганізаційної ситуаційної обізнаності

17.4.18. АНАЛІЗ ТРАФІКУ ТА ПРИХОВАНОЇ ЕКСФІЛЬТРАЦІЇ (SI-4(18))

Аналізується вихідний комунікаційний трафік на зовнішніх по відношенню до системи інтерфейсах для виявлення прихованого витоку інформації.

No: 1
Name: si_4_18_01
Type: string
Default: nil

Аналізується вихідний комунікаційний трафік на зовнішніх по відношенню до системи інтерфейсах для виявлення прихованого витоку інформації

No: 2
Name: si_4_18_02
Type: string
Default: nil

Аналізується вихідний трафік зв'язку в внутрішніх точках для виявлення прихованого витоку інформації

No: 3
Name: si_4_18_odp
Type: string
Default: nil

Визначені внутрішні точки в системі, в яких необхідно аналізувати комунікаційний трафік

17.4.19. ОСОБИ, ЯКІ ПРЕДСТАВЛЯЮТЬ БІЛЬШИЙ РИЗИК (SI-4(19))

Здійснюється <SI-04(19) _ODP[01] додатковий моніторинг> щодо осіб, які були ідентифіковані джерелами <SI-04(19) _ODP[02] як такі, що становлять підвищений рівень ризику>.

No: 1
Name: si_4_19_01
Type: string
Default: nil

Здійснюється <SI-04(19) _ODP[01] додатковий моніторинг> щодо осіб, які були ідентифіковані джерелами <SI-04(19) _ODP[02] як такі, що становлять підвищений рівень ризику>

17.4.20. ПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ (SI-4(20))

Реалізовано привілейованих користувачів. привілейованих додатковий моніторинг.

No: 1
Name: si_4_20_01
Type: string
Default: nil

Реалізовано привілейованих користувачів. привілейованих додатковий моніторинг

No: 2
Name: si_4_20_odp
Type: string
Default: nil

Визначено додатковий користувачів; моніторинг

17.4.21. ВИПРОБУВАЛЬНІ ТЕРМІНИ (SI-4(21))

Здійснюється <SI-04(21) _ODP[01] додатковий моніторинг> осіб під час <SI-04(21) _ODP[02] випробувального терміну>.

No: 1
Name: si_4_21_01
Type: integer
Default: 30

Здійснюється <SI-04(21) _ODP[01] додатковий моніторинг> осіб під час <SI-04(21) _ODP[02] випробувального терміну>

17.4.22. НЕСАНКЦІОНОВАНІ ПОСЛУГИ МЕРЕЖІ (SI-4(22))

Виявлено послуги мережі, які не було авторизовано або схвалено відповідно до процесів авторизації або схвалення.

No: 1
Name: si_4_22_a
Type: string
Default: nil

Виявлено послуги мережі, які не було авторизовано або схвалено відповідно до процесів авторизації або схвалення

17.4.23. ПРИСТРОЇ НА ОСНОВІ ХОСТА (SI-4(23))

Реалізовано <SI-04(23) _ODP[01] механізми моніторингу на основі хостів> на <SI-04(23) _ODP[02] компоненти системи>.

No: 1
Name: si_4_23_01
Type: string
Default: "автоматизований засіб моніторингу"

Реалізовано <SI-04(23) _ODP[01] механізми моніторингу на основі хостів> на <SI-04(23) _ODP[02] компоненти системи>

17.4.24. ІНДИКАТОРИ КОМПРОМЕТАЦІЇ (SI-4(24))

Виявлено індикатори компрометації, 04(24)_ODP[01] джерелами>.

No: 1
Name: si_4_24_01
Type: string
Default: nil

Виявлено індикатори компрометації, 04(24)_ODP[01] джерелами>

No: 2
Name: si_4_24_02
Type: string
Default: nil

Збираються індикатори компрометації, що надаються джерелами

No: 3
Name: si_4_24_03
Type: list
Default: ["admin", "security_officer"]

Індикатори компрометації, надані <SI-04(24) джерелами>, поширюються на <SI-04(24) персонал або ролі>. надані <SI- _ODP[01] _ODP[02]

17.4.25. АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ (SI-4(25))

Забезпечується видимість мережевого трафіку на зовнішніх системних інтерфейсах для оптимізації ефективності пристроїв моніторингу.

No: 1
Name: si_4_25_01
Type: string
Default: nil

Забезпечується видимість мережевого трафіку на зовнішніх системних інтерфейсах для оптимізації ефективності пристроїв моніторингу

No: 2
Name: si_4_25_02
Type: string
Default: nil

Забезпечено видимість мережевого трафіку на ключових внутрішніх інтерфейсах системи для оптимізації ефективності пристроїв моніторингу

17.5. ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ (SI-5)

Попередження, рекомендації та директиви з безпеки.

No: 1
Name: si_5_odp_01
Type: string
Default: nil

Визначені зовнішні організації, від яких необхідно постійно отримувати оповіщення, поради та директиви щодо безпеки системи

No: 2
Name: si_5_odp_02
Type: list
Default: ["admin", "security_officer"]

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {персонал або ролі; елементи; зовнішні організації}

No: 3
Name: si_5_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, до яких мають бути доведені попередження, поради та директиви з безпеки (якщо визначено)

No: 4
Name: si_5_odp_04
Type: string
Default: nil

Визначені елементи в організації, до яких мають надсилатися оповіщення, поради та директиви з безпеки (якщо вони були обрані)

17.5.1. АВТОМАТИЧНІ ПОПЕРЕДЖЕННЯ ТА РЕКОМЕНДАЦІЇ (SI-5(1))

Використовуються автоматизовані механізми для трансляції попередження та рекомендації інформації з питань безпеки по всій організації.

No: 1
Name: si_5_1_01
Type: string
Default: "автоматизований засіб моніторингу"

Використовуються автоматизовані механізми для трансляції попередження та рекомендації інформації з питань безпеки по всій організації

No: 2
Name: si_5_1_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначені автоматизовані механізми, які використовуються для трансляції попередження та рекомендації інформації про безпеку в організації

17.6. ПЕРЕВІРКА ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ (SI-6)

Перевірка функцій безпеки та приватності.

No: 1
Name: si_6_odp_01
Type: string
Default: nil

Визначені функції безпеки, які необхідно перевірити на коректність роботи

No: 2
Name: si_6_odp_02
Type: string
Default: nil

Визначені функції приватності, які потрібно перевіряти на коректність роботи

No: 3
Name: si_6_odp_03
Type: string
Default: "щорічно"

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {перехідні стани системи; за командою користувача з відповідним привілеєм; частота}

No: 4
Name: si_6_odp_04
Type: string
Default: nil

Визначені перехідні стани системи, що вимагають перевірки функцій безпеки та конфіденційності; (якщо вибрано)

No: 5
Name: si_6_odp_05
Type: string
Default: "щорічно"

Визначена періодичність перевірки правильності роботи функцій безпеки та приватності; (якщо вибрано)

No: 6
Name: si_6_odp_06
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, які мають бути сповіщені про невдалу перевірку безпеки та приватності

No: 7
Name: si_6_odp_07
Type: list
Default: ["login", "logout", "failed_attempt"]

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {вимкнути систему; перезапустити систему; альтернативна дія (дії)}

17.6.1. СПОВІЩЕННЯ ПРО НЕУСПІШНЕ ПРОХОДЖЕННЯ ТЕСТІВ З БЕЗПЕКИ (SI-6(1)) [Вилучено]

[Вилучено: включено до SI-6]

Немає параметрів для цього контролю.

17.6.2. АВТОМАТИЗОВАНА ПІДТРИМКА РОЗПОДІЛЕНОГО ТЕСТУВАННЯ (SI-6(2))

Впроваджені автоматизовані механізми для розподіленого тестуванням функцій безпеки; підтримки.

No: 1
Name: si_6_2_01
Type: string
Default: "автоматизований засіб моніторингу"

Впроваджені автоматизовані механізми для розподіленого тестуванням функцій безпеки; підтримки

No: 2
Name: si_6_2_02
Type: string
Default: "автоматизований засіб моніторингу"

Проваджені автоматизовані механізми для розподіленого тестуванням функцій приватності. підтримки

17.6.3. ПОВІДОМЛЕННЯ ПРО РЕЗУЛЬТАТИ ПЕРЕВІРКИ (SI-6(3))

Повідомляються результати перевірки функцій безпеки персоналу або ролям.

No: 1
Name: si_6_3_01
Type: list
Default: ["admin", "security_officer"]

Повідомляються результати перевірки функцій безпеки персоналу або ролям

No: 2
Name: si_6_3_odp
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, призначені для отримання результатів перевірки функцій безпеки та приватності

17.7. ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ (SI-7)

a. Впровадити механізми захисту від спаму в точках входу та виходу системи, щоб виявляти та протидіяти небажаним повідомленням.
b. Оновлювати механізми захисту від спаму, коли доступні нові механізми відповідно до організаційної політики та процедур управління конфігурацією.

No: 1
Name: si_7_odp_01
Type: string
Default: nil

Визначено програмне забезпечення, яке потребує застосування засобів перевірки цілісності для виявлення несанкціонованих змін

No: 2
Name: si_7_odp_02
Type: string
Default: nil

Визначено прошивку, яка потребує застосування інструментів перевірки цілісності для виявлення несанкціонованих змін

No: 3
Name: si_7_odp_03
Type: string
Default: nil

Визначена інформація, яка потребує застосування засобів перевірки цілісності для виявлення несанкціонованих змін

No: 4
Name: si_7_odp_04
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначені дії, яких слід вжити при виявленні несанкціонованих змін у програмному забезпеченні

No: 5
Name: si_7_odp_05
Type: list
Default: ["login", "logout", "failed_attempt"]

визначені дії, яких слід вжити при виявленні несанкціонованих змін у прошивці;

No: 6
Name: si_7_odp_06
Type: string
Default: nil

визначені дії, яких слід вжити при виявленні несанкціонованих змін до інформації;

No: 7
Name: si_7_a_01
Type: string
Default: nil

використовуються засоби перевірки цілісності для виявлення несанкціонованих змін у програмному забезпеченні;

No: 8
Name: si_7_a_02
Type: string
Default: nil

використовуються засоби перевірки цілісності для виявлення несанкціонованих змін у мікропрограмі;

No: 9
Name: si_7_a_03
Type: string
Default: nil

використовуються засоби перевірки цілісності для виявлення несанкціонованих змін до інформації;

No: 10
Name: si_7_b_01
Type: string
Default: nil

виконуються дії при виявленні несанкціонованих змін у програмному забезпеченні;

No: 11
Name: si_7_b_02
Type: string
Default: nil

виконуються дії при виявленні несанкціонованих змін у прошивці;

No: 12
Name: si_7_b_03
Type: string
Default: nil

виконуються дії при виявленні несанкціонованих змін в інформації.

17.7.1. ПЕРЕВІРКА ЦІЛІСНОСТІ (SI-7(1))

Перевірка цілісності (si-7(1)).

Немає параметрів для цього контролю.

17.7.2. АВТОМАТИЧНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ (SI-7(2))

Застосовуються автоматизовані інструменти, які надають повідомлення персоналу або ролям при виявленні розбіжностей під час перевірки цілісності.

No: 1
Name: si_7_2_01
Type: list
Default: ["admin", "security_officer"]

Застосовуються автоматизовані інструменти, які надають повідомлення персоналу або ролям при виявленні розбіжностей під час перевірки цілісності

No: 2
Name: si_7_2_odp
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким необхідно повідомляти про виявлення розбіжностей під час перевірки цілісності

17.7.3. ІНСТРУМЕНТИ ЦІЛІСНОСТІ З ЦЕНТРАЛІЗОВАНИМ УПРАВЛІННЯМ (SI-7(3))

Застосовуються інструменти цілісності з централізованим управлінням.

No: 1
Name: si_7_3_01
Type: string
Default: nil

Застосовуються інструменти цілісності з централізованим управлінням

17.7.4. ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – ПАКУВАННЯ З ІНДИКАЦІЄЮ ОЗНАК ЇЇ НЕСАНКЦІОНОВАНОГО РОЗКРИТТЯ (SI-7(4))

[Вилучено: включено до SA-12]

Немає параметрів для цього контролю.

17.7.5. АВТОМАТИЧНІ ВІДПОВІДІ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ (SI-7(5))

Автоматичні відповіді про порушення цілісності (si-7(5)).

Немає параметрів для цього контролю.

17.7.6. КРИПТОГРАФІЧНИЙ ЗАХИСТ (SI-7(6))

Впроваджені криптографічні механізми для виявлення несанкціонованих змін у програмному забезпеченні.

No: 1
Name: si_7_6_01
Type: string
Default: "AES-256-GCM"

Впроваджені криптографічні механізми для виявлення несанкціонованих змін у програмному забезпеченні

No: 2
Name: si_7_6_02
Type: string
Default: "AES-256-GCM"

Реалізовані криптографічні механізми несанкціонованих змін у прошивці

No: 3
Name: si_7_6_03
Type: string
Default: "AES-256-GCM"

Впроваджені криптографічні механізми несанкціонованих змін інформації

17.7.7. ІНТЕГРАЦІЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ (SI-7(7))

Виявлення змін включено до можливості організації реагування на інциденти.

No: 1
Name: si_7_7_01
Type: string
Default: nil

Виявлення змін включено до можливості організації реагування на інциденти

No: 2
Name: si_7_7_odp
Type: string
Default: nil

Визначені зміни в системі, що мають відношення до безпеки

17.7.8. АУДИТ ВАЖЛИВИХ ПОДІЙ (SI-7(8))

Передбачена можливість аудиту потенційного порушення цілісності.

No: 1
Name: si_7_8_01
Type: string
Default: nil

Передбачена можливість аудиту потенційного порушення цілісності

17.7.9. ПЕРЕВІРКА ПРОЦЕСУ ЗАВАНТАЖЕННЯ (SI-7(9))

Перевіряється цілісність процесу завантаження 07(09)_ODP системних компонентів>. <SI-.

No: 1
Name: si_7_9_01
Type: string
Default: nil

Перевіряється цілісність процесу завантаження 07(09)_ODP системних компонентів>. <SI-

No: 2
Name: si_7_9_odp

Type: string
Default: nil

Визначено компоненти системи, які потребують перевірки цілісності процесу завантаження

17.7.10. ЗАХИСТ ЗАВАНТАЖУВАЛЬНОГО ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ (SI-7(10))

Реалізовано <SI-07(10) _ODP[01] механізми> для захисту цілісності завантажувальної прошивки у <SI-07(10) _ODP[02] системних компонентах>. компоненти системи, захисту цілісності які потребують завантажувальної.

No: 1
Name: si_7_10_01
Type: string
Default: "автоматизований засіб моніторингу"

Реалізовано <SI-07(10) _ODP[01] механізми> для захисту цілісності завантажувальної прошивки у <SI-07(10) _ODP[02] системних компонентах>. компоненти системи, захисту цілісності які потребують завантажувальної

17.7.11. ОБМЕЖЕНЕ СЕРЕДОВИЩЕ З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ (SI-7(11)) [Вилучено]

[Вилучено: включено до CM-7(6)]

Немає параметрів для цього контролю.

17.7.12. ПЕРЕВІРКА ЦІЛІСНОСТІ (SI-7(12))

Перевіряється забезпечення, виконанням. цілісність програмне встановлене користувачем перед.

No: 1
Name: si_7_12_01
Type: string
Default: nil

Перевіряється забезпечення, виконанням. цілісність програмне встановлене користувачем перед

No: 2
Name: si_7_12_odp
Type: string
Default: nil

Визначено програмне забезпечення, встановлене користувачем, яке потребує перевірки цілісності перед виконанням

17.7.13. ВИКОНАННЯ КОДУ В ЗАХИЩЕНИХ СЕРЕДОВИЩАХ (SI-7(13)) [Вилучено]

[Вилучено: включено до CM-7(7)]

Немає параметрів для цього контролю.

17.7.14. ДВІЙКОВИЙ АБО МАШИННО-ВИКОНУВАНИЙ КОД (SI-7(14)) [Вилучено]

[Вилучено: включено до CM-7(8)]

Немає параметрів для цього контролю.

17.7.15. АВТЕНТИФІКАЦІЯ КОДУ (SI-7(15))

Реалізовано криптографічні механізми для автентифікації програмного забезпечення або компонентів мікропрограми перед інсталяцією.

No: 1
Name: si_7_15_01
Type: string
Default: "AES-256-GCM"

Реалізовано криптографічні механізми для автентифікації програмного забезпечення або компонентів мікропрограми перед інсталяцією

No: 2
Name: si_7_15_odp
Type: string
Default: "AES-256-GCM"

Визначено компоненти програмного забезпечення або мікропрограми, які мають бути автентифіковані за допомогою криптографічних механізмів перед встановленням

17.7.16. ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ (SI-7(16))

Заборонено процесам виконуватися без нагляду довше, ніж часовий період.

No: 1
Name: si_7_16_01
Type: integer
Default: 30

Заборонено процесам виконуватися без нагляду довше, ніж часовий період

No: 2
Name: si_7_16_odp
Type: integer
Default: 30

Визначено максимальний період часу, протягом якого процеси можуть виконуватися без нагляду

17.7.17. ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – САМОЗАХИСТ ПРОГРАМ ВІД САМОВІЛЬНОГО ВИКОНАННЯ (SI-7(17))

Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації – самозахист програм від самовільного виконання (si-7(17)).

No: 1
Name: si_7_17_odp
Type: integer
Default: 30

Визначено елементи керування, які потрібно реалізувати для самозахисту програми під час виконання

17.8. ЗАХИСТ ВІД СПАМУ (SI-8)

Захист від спаму.

Немає параметрів для цього контролю.

17.8.1. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ (SI-8(1)) [Вилучено]

[Вилучено: включено до PL-9]

Немає параметрів для цього контролю.

17.8.2. АВТОМАТИЧНІ ОНОВЛЕННЯ (SI-8(2))

Автоматично оновлюються механізми захисту від спаму частота.

No: 1
Name: si_8_2_01
Type: string
Default: "щорічно"

Автоматично оновлюються механізми захисту від спаму частота

No: 2
Name: si_8_2_odp
Type: string
Default: "щорічно"

Визначено періодичність автоматичного механізмів захисту від спаму; оновлення

17.8.3. БЕЗПЕРЕРВНЕ НАВЧАННЯ (SI-8(3))

Впроваджені механізми захисту від спаму з можливістю навчання для більш ефективного визначення законого комунікаційного трафіку.

No: 1
Name: si_8_3_01
Type: string
Default: "автоматизований засіб моніторингу"

Впроваджені механізми захисту від спаму з можливістю навчання для більш ефективного визначення законого комунікаційного трафіку

17.9. ОБМЕЖЕННЯ НА ВВЕДЕННЯ ІНФОРМАЦІЇ (SI-9) [Вилучено]

Обмеження на введення інформації (si-9) [вилучено].

Немає параметрів для цього контролю.

17.10. ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ (SI-10)

Перевіряти дійсність [Призначення: визначена організацією введена інформація].

No: 1
Name: si_10_01
Type: string
Default: nil

Перевіряється дійсність синтаксису вхідної інформації

No: 2
Name: si_10_odp
Type: string
Default: nil

Визначено вхідні дані до системи, які перевірки достовірності; потребують

17.10.1. МОЖЛИВІСТЬ РУЧНОГО ПЕРЕВИЗНАЧЕННЯ (SI-10(1))

Передбачена можливість ручного перевизначення валідації інформаційних входів.

No: 1
Name: si_10_1_a
Type: string
Default: nil

Передбачена можливість ручного перевизначення валідації інформаційних входів

No: 2
Name: si_10_1_b
Type: list
Default: ["admin", "security_officer"]

Використання можливості ручного перевизначення обмежено лише уповноваженими особами

No: 3
Name: si_10_1_c
Type: string
Default: nil

Проводиться аудит перевизначення. використання можливості для ручного

No: 4
Name: si_10_1_odp
Type: string
Default: nil

Визначено авторизованих осіб, які можуть користуватися можливістю ручного перевизначення

17.10.2. ПЕРЕГЛЯД ТА УСУНЕННЯ ПОМИЛОК (SI-10(2))

Переглядаються помилки валідації вхідних даних протягом часового періоду.

No: 1
Name: si_10_2_01
Type: integer
Default: 30

Переглядаються помилки валідації вхідних даних протягом часового періоду

No: 2
Name: si_10_2_02
Type: integer
Default: 30

Помилки валідації вводу вирішуються 10(02)_ODP[02] часового проміжку>. протягом <SI-

17.10.3. ПЕРЕДБАЧУВАНА ПОВЕДІНКА (SI-10(3))

Система поводиться задокументованим чином при отриманні недійсних вхідних даних.

No: 1
Name: si_10_3_02
Type: string
Default: nil

Система поводиться задокументованим чином при отриманні недійсних вхідних даних

17.10.4. ЧАСОВІ ВЗАЄМОДІЇ (SI-10(4))

Враховується часова взаємодія між компонентами системи при визначенні відповідної реакції на невірні вхідні дані.

No: 1
Name: si_10_4_01
Type: integer
Default: 30

Враховується часова взаємодія між компонентами системи при визначенні відповідної реакції на невірні вхідні дані

17.10.5. ОБМЕЖЕННЯ ВХІДНИХ ДАНИХ ДОВІРЕНИМИ ДЖЕРЕЛАМИ І ЗАТВЕРДЖЕНИМИ ФОРМАТАМИ (SI-10(5))

Обмеження вхідних даних довіреними джерелами і затвердженими форматами (si-10(5)).

Немає параметрів для цього контролю.

17.10.6. ПРОФІЛАКТИКА ВВОДУ ДАНИХ (SI-10(6))

Визначено елементи керування, які потрібно реалізувати для самозахисту програми під час виконання.

No: 1
Name: si_10_6_01
Type: integer
Default: 30

Визначено елементи керування, які потрібно реалізувати для самозахисту програми під час виконання

17.11. ОБРОБКА ПОМИЛОК (SI-11)

a. Створити повідомлення про помилки, які надають інформацію, необхідну для реалізації виправних дій, без виявлення інформації, що може бути використана.
b. Показувати повідомлення про помилки лише [Призначення: визначений організацією персонал або посадові особи].

No: 1
Name: si_11_odp
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, яким слід повідомляти про повідомлення про помилки; SI-11a. генеруються повідомлення про помилки, які надають інформацію, необхідну для коригувальних дій, без розкриття інформації, яка може бути використана; SI-11b. показувати повідомлення про помилки лише для персонал або ролі

17.12. УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ (SI-12)

Управляти та зберігати інформацію всередині системи та виводити інформацію із системи відповідно до чинного законодавства, виконавчих наказів, директив, правил, політик, стандартів, керівних принципів та експлуатаційних вимог.

No: 1
Name: si_12_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Здійснюється управління інформацією в системі відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог

No: 2
Name: si_12_02
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Зберігається інформація в системі відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог

No: 3
Name: si_12_03
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Управління інформацією, що виводиться з системи, здійснюється відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та операційних вимог

No: 4
Name: si_12_04
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Зберігається інформація, що виводиться з системи, відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог

17.12.1. ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ (SI-12(1))

Обмежується обробка персональних даних у життєвому циклі інформації в життєвому циклі інформації, елементами інформації, що ідентифікує особу.

No: 1
Name: si_12_1_01
Type: list
Default: ["admin", "security_officer"]

Обмежується обробка персональних даних у життєвому циклі інформації в життєвому циклі інформації, елементами інформації, що ідентифікує особу

No: 2
Name: si_12_1_odp
Type: list
Default: ["admin", "security_officer"]

Визначені елементи персональних даних у життєвому циклі інформації

17.12.2. МІНІМІЗАЦІЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕННІ (SI-12(2))

Використовуються методи для мінімізації використання персональних даних для досліджень; SI-12(02)[02] використовуються методи для мінімізації використання персональних даних для тестування.

No: 1
Name: si_12_2_01
Type: list
Default: ["admin", "security_officer"]

Використовуються методи для мінімізації використання персональних даних для досліджень; SI-12(02)[02] використовуються методи для мінімізації використання персональних даних для тестування

No: 2
Name: si_12_2_03
Type: list
Default: ["admin", "security_officer"]

Застосовуються методи для мінімізації використання персональних даних для навчання

17.12.3. ВИДАЛЕННЯ ІНФОРМАЦІЇ (SI-12(3))

Використовуються методи для знищення інформації після закінчення терміну зберігання.

No: 1
Name: si_12_3_01
Type: string
Default: nil

Використовуються методи для знищення інформації після закінчення терміну зберігання

No: 2
Name: si_12_3_02
Type: string
Default: nil

Використовуються методи для знищення інформації після закінчення терміну зберігання

No: 3
Name: si_12_3_03
Type: integer
Default: 30

Використовуються методи для стирання інформації після закінчення періоду зберігання

17.13. ПЕРЕДБАЧУВАНЕ ЗАПОБІГАННЯ ЗБОЇВ (SI-13)

a. Визначити середній час до збою (MTTF) для [Призначення: визначені організацією компоненти системи] в певних середовищах роботи.
b. Надати замінні компоненти системи та засоби для заміни активних компонентів резервними компонентами відповідно до [Призначення: визначені організацією критерії заміни].

No: 1
Name: si_13_odp_01
Type: integer
Default: 30

Визначені компоненти системи, для яких необхідно визначити середній час до збою (MTTF)

No: 2
Name: si_13_odp_02

Type: list
Default: []

Визначені критерії заміни за середнім часом напрацювання до збою (MTTF), які будуть використовуватися для заміни активних і резервних компонентів; SI-13a. визначено середній час напрацювання до збою (MTTF) для системних компонентів у конкретних умовах експлуатації; SI-13b. передбачені замінні компоненти системи та засоби заміни активних і резервних компонентів відповідно до критеріїв заміни середнього часу напрацювання на відмову (MTTF)

17.13.1. ВІДПОВІДАЛЬНІСТЬ ЗА ПЕРЕДАЧУ ФУНКЦІЙ КОМПОНЕНТІВ (SI-13(1))

Виводяться компоненти системи з експлуатації шляхом передачі обов'язків компонентів на запасні компоненти не пізніше, ніж частка або відсоток середнього напрацювання на відмову.

No: 1
Name: si_13_1_01
Type: integer
Default: 30

Виводяться компоненти системи з експлуатації шляхом передачі обов'язків компонентів на запасні компоненти не пізніше, ніж частка або відсоток середнього напрацювання на відмову

No: 2
Name: si_13_1_odp
Type: integer
Default: 30

Визначено частку або напрацювання до збою, відсоток середнього часу в межах якого обов'язки компонента системи можуть бути передані компоненту, що замінює його

17.13.2. ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ (SI-13(2)) [Вилучено]

[Вилучено: включено до SI-7 (16)]

Немає параметрів для цього контролю.

17.13.3. РУЧНА ПЕРЕДАЧА ФУНКЦІЙ КОМПОНЕНТІВ (SI-13(3))

Ініціюються вручну передачі між активним та резервним компонентами системи, коли використання активного компонента досягає відсоток від середнього часу напрацювання до збою.

No: 1
Name: si_13_3_01
Type: integer
Default: 30

Ініціюються вручну передачі між активним та резервним компонентами системи, коли використання активного компонента досягає відсоток від середнього часу напрацювання до збою

No: 2
Name: si_13_3_odp

Type: integer
Default: 30

Визначено відсоток середнього часу напрацювання на відмову для передач, які потрібно ініціювати вручну

17.13.4. ВСТАНОВЛЕННЯ РЕЗЕРВНИХ КОМПОНЕНТІВ ТА ОПОВІЩЕННЯ (SI-13(4))

Успішно і прозоро встановлюються резервні компоненти протягом часу, якщо виявлено збої у роботі системних компонентів.

No: 1
Name: si_13_4_a
Type: integer
Default: 30

Успішно і прозоро встановлюються резервні компоненти протягом часу, якщо виявлено збої у роботі системних компонентів

17.13.5. МОЖЛИВІСТЬ АВАРІЙНОГО ПЕРЕМИКАННЯ (SI-13(5))

Можливість аварійного перемикання (si-13(5)).

Немає параметрів для цього контролю.

17.14. НЕСТІЙКІСТЬ (SI-14)

Реалізувати нестійкі [Призначення: визначені організацією компоненти системи та служби], які ініціюються у відомих станах і завершуються [Вибір (один або кілька): після закінчення сеансу використання; періодично з [Призначення: визначена організацією частота]].

No: 1
Name: si_14_01
Type: string
Default: nil

Реалізовано непостійні компоненти системи та сервіси, які ініціюються у відомому стані

No: 2
Name: si_14_odp_01
Type: string
Default: nil

Визначені непостійні компоненти системи та сервіси, які необхідно застосовувати

No: 3
Name: si_14_odp_02
Type: string
Default: "щорічно"

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {по закінченні сеансу використання; частота}

No: 4
Name: si_14_odp_03
Type: integer
Default: 30

Визначено частоту завершення роботи непостійних компонентів і сервісів, які ініціюються у відомому стані (якщо вибрано)

17.14.1. ОНОВЛЕННЯ З НАДІЙНИХ ДЖЕРЕЛ (SI-14(1))

Програмне забезпечення та дані, що використовуються під час оновлення системних компонентів та служб, отримані з довірених джерел.

No: 1
Name: si_14_1_01
Type: integer
Default: 30

Програмне забезпечення та дані, що використовуються під час оновлення системних компонентів та служб, отримані з довірених джерел

No: 2
Name: si_14_1_odp
Type: string
Default: nil

Визначені надійні джерела для отримання програмного забезпечення та даних для оновлення системних компонентів і служб

17.14.2. НЕСТІЙКА ІНФОРМАЦІЯ (SI-14(2))

Видаляється інформація, коли вона більше не потрібна.

No: 1
Name: si_14_2_b
Type: string
Default: nil

Видаляється інформація, коли вона більше не потрібна

17.14.3. НЕСТІЙКІ ПІДКЛЮЧЕННЯ (SI-14(3))

Встановлюються з'єднання з системою на вимогу.

No: 1
Name: si_14_3_01
Type: string
Default: nil

Встановлюються з'єднання з системою на вимогу

No: 2
Name: si_14_3_odp
Type: integer
Default: 30

Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {завершення запиту; період невикористання}

17.15. ФІЛЬТРАЦІЯ ВИХІДНИХ ДАНИХ (SI-15)

Перевіряти інформацію, що виходить з [Призначення: визначені організацією програмні продукти та/або застосунки], щоб переконатися, що інформація відповідає очікуваному змісту.

No: 1
Name: si_15_01
Type: string
Default: nil

Перевіряється інформація, що виводиться з програмне забезпечення та/або додатки, щоб переконатися, що інформація відповідає очікуваному змісту

No: 2
Name: si_15_odp
Type: string
Default: nil

Визначені програми та/або додатки, виведення інформації з яких потребує перевірки

17.16. ЗАХИСТ ПАМ'ЯТІ (SI-16)

Виконати [Призначення: визначені організацією заходи безпеки] для захисту системної пам'яті від несанкціонованого коду, що виконується.

No: 1
Name: si_16_01
Type: string
Default: nil

Реалізовано контроль для захисту системної пам'яті від несанкціонованого виконання коду

No: 2
Name: si_16_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено засоби контролю для захисту системної пам'яті від несанкціонованого виконання коду

17.17. ВІДМОВОСТІЙКІ ПРОЦЕДУРИ (SI-17)

Виконати [Призначення: визначені організацією відмовостійкі процедури], коли настають [Призначення: визначені організацією умови виявлення несправностей].

No: 1
Name: si_17_01
Type: list
Default: []

Реалізовано процедури захисту від збоїв при виникненні перелік умов збою. відмови, що вимагають

No: 2
Name: si_17_odp_01

Type: string
Default: nil

Визначені відмовостійкі процедури, пов'язані з умовами відмови

No: 3
Name: si_17_odp_02
Type: list
Default: []

Визначено перелік умов відмовостійких процедур

17.18. ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ (SI-18)

a. Перевіряти точність, актуальність, своєчасність і повноту персональної інформації протягом її життєвого циклу [Завдання: частота, визначена організацією];
b. Виправляти або видаляти неточну або застарілу персональну інформацію.

No: 1
Name: si_18_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено періодичність перевірки точності персональну інформацію протягом життєвого циклу інформації

No: 2
Name: si_18_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено періодичність перевірки актуальності персональної інформації протягом життєвого циклу інформації

No: 3
Name: si_18_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначено періодичність перевірки актуальності персональної інформації протягом життєвого циклу інформації

No: 4
Name: si_18_odp_04
Type: list
Default: ["admin", "security_officer"]

визначено періодичність перевірки повноти персональної інформації протягом життєвого циклу інформації;

No: 5
Name: si_18_a_01
Type: string
Default: nil

перевіряється точність персональної інформації протягом життєвого циклу інформації <SI-18_ODP[01] частота>;

No: 6
Name: si_18_a_02
Type: string
Default: nil

перевіряється актуальність персональної інформації протягом життєвого циклу інформації <SI-18_ODP[02] частота>;

No: 7
Name: si_18_a_03
Type: string
Default: nil

перевіряється своєчасність персональної інформації протягом життєвого циклу інформації <SI-18_ODP[03] частота>;

No: 8
Name: si_18_a_04
Type: string
Default: nil

перевіряється повнота персональної інформації протягом життєвого циклу інформації <SI-18_ODP[04] частота>;

No: 9
Name: si_18_b
Type: string
Default: nil

потрібно виправити або видалити неточну або застарілу персональну інформацію.

17.18.1. АВТОМАТИЧНА ПІДТРИМКА (SI-18(1))

Використовуються автоматизовані механізми для виправлення або видалення персональної інформації яка є неточною, застарілою, неправильно визначеною щодо впливу або неправильно деідентифікованою.

No: 1
Name: si_18_1_01
Type: list
Default: ["admin", "security_officer"]

Використовуються автоматизовані механізми для виправлення або видалення персональної інформації яка є неточною, застарілою, неправильно визначеною щодо впливу або неправильно деідентифікованою

No: 2
Name: si_18_1_odp
Type: list
Default: ["admin", "security_officer"]

Визначені автоматизовані механізми, які використовуються для виправлення або видалення персональної інформації яка є неточною, застарілою, неправильно визначеною щодо впливу або неправильно деідентифікованою

17.18.2. ТЕГУВАННЯ ДАНИХ (SI-18(2))

Тегування даних (si-18(2)).

Немає параметрів для цього контролю.

17.18.3. ЗБИРАННЯ (SI-18(3))

Збирання (si-18(3)).

Немає параметрів для цього контролю.

17.18.4. ІНДИВІДУАЛЬНІ ЗАПИТИ (SI-18(4))

Виправляється або видаляється персональну інформація на вимогу осіб або їхніх уповноважених представників.

No: 1
Name: si_18_4_01
Type: list
Default: ["admin", "security_officer"]

Виправляється або видаляється персональну інформація на вимогу осіб або їхніх уповноважених представників.

17.18.5. ПОВІДОМЛЕННЯ ПРО ВИПРАВЛЕННЯ ЧИ ВИДАЛЕННЯ (SI-18(5))

Одержувачі та фізичні особи повідомляються про виправлення або видалення персональної інформації.

No: 1
Name: si_18_5_01
Type: list
Default: ["admin", "security_officer"]

Одержувачі та фізичні особи повідомляються про виправлення або видалення персональної інформації

No: 2
Name: si_18_5_odp
Type: list
Default: ["admin", "security_officer"]

Визначені одержувачі персональних даних, які повинні бути повідомлені про виправлення або видалення персональних даних

17.19. ДЕІДЕНТИФІКАЦІЯ (SI-19)

a. Видаліть такі елементи персональних даних з наборів даних: [Призначення: визначені організацією елементи персональних даних];
b. Оцініть [Призначення: деідентифікації. частота, визначена організацією] ефективність

No: 1
Name: si_19_odp_02
Type: string
Default: "щорічно"

Визначено частоту, з якою слід оцінювати ефективність деідентифікації; SI-19a. вилучено елементи з наборів даних; SI-19b. оцінюється ефективність деідентифікації частота

17.19.1. ЗБІР (SI-19(1))

Деідентифікується набір даних після збору шляхом відмови від збору персональної інформації.

No: 1
Name: si_19_1_01
Type: list
Default: ["admin", "security_officer"]

Деідентифікується набір даних після збору шляхом відмови від збору персональної інформації

17.19.2. АРХІВАЦІЯ (SI-19(2))

Заборонено архівування елементів персональної інформації, якщо ці елементи в наборі даних не будуть потрібні після того, як набір даних буде заархівовано.

No: 1
Name: si_19_2_01
Type: list
Default: ["admin", "security_officer"]

Заборонено архівування елементів персональної інформації, якщо ці елементи в наборі даних не будуть потрібні після того, як набір даних буде заархівовано

17.19.3. ВИДАЛЕННЯ (SI-19(3))

Видаляються елементи персональної інформаціїз набору даних перед його оприлюдненням, якщо ці елементи в наборі даних не повинні бути частиною оприлюднення даних.

No: 1
Name: si_19_3_01
Type: list
Default: ["admin", "security_officer"]

Видаляються елементи персональної інформаціїз набору даних перед його оприлюдненням, якщо ці елементи в наборі даних не повинні бути частиною оприлюднення даних

17.19.4. ВИДАЛЕННЯ, МАСКУВАННЯ, ШИФРУВАННЯ, ХЕШУВАННЯ АБО ЗАМІНА ПРЯМИХ ІДЕНТИФІКАТОРІВ (SI-19(4))

Видалення, маскування, шифрування, хешування або заміна прямих ідентифікаторів (si-19(4)).

Немає параметрів для цього контролю.

17.19.5. КОНТРОЛЬ СТАТИСТИЧНОГО РОЗКРИТТЯ (SI-19(5))

Не маніпулюють числовими даними так, щоб у результатах аналізу не можна було ідентифікувати жодну особу чи організацію.

No: 1
Name: si_19_5_01
Type: list
Default: ["admin", "security_officer"]

Не маніпулюють числовими даними так, щоб у результатах аналізу не можна було ідентифікувати жодну особу чи організацію

No: 2
Name: si_19_5_02
Type: list
Default: ["admin", "security_officer"]

Не маніпулюють таблицями непередбачених обставин таким чином, щоб у результатах аналізу не можна було ідентифікувати жодну особу чи організацію

No: 3
Name: si_19_5_03
Type: list
Default: ["admin", "security_officer"]

Не маніпулюють статистичними даними так, щоб за результатами аналізу не можна було ідентифікувати жодну особу чи організацію

17.19.6. ДИФЕРЕНЦІЙОВАНА КОНФІДЕНЦІЙНІСТЬ (SI-19(6))

Запобігає розголошенню персональної інформації, додавання недетермінованого шуму до результатів математичних операцій до того, як результати будуть повідомлені.

No: 1
Name: si_19_6_01
Type: list
Default: ["admin", "security_officer"]

Запобігає розголошенню персональної інформації, додавання недетермінованого шуму до результатів математичних операцій до того, як результати будуть повідомлені

17.19.7. ПЕРЕВІРЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ (SI-19(7))

Виконується деідентифікація за допомогою перевірених алгоритмів.

No: 1
Name: si_19_7_01
Type: string
Default: "AES-256-GCM"

Виконується деідентифікація за допомогою перевірених алгоритмів

No: 2
Name: si_19_7_02
Type: string
Default: "AES-256-GCM"

Виконується деідентифікація за допомогою програмного забезпечення, яке пройшло валідацію для реалізації алгоритмів

17.19.8. МОТИВОВАНИЙ ПОРУШНИК (SI-19(8))

Виконується тест мотивованого зловмисника для деідентифікованого набору даних, щоб визначити, чи залишаються ідентифіковані дані або чи можна повторно ідентифікувати деідентифіковані дані.

No: 1
Name: si_19_8_01
Type: string
Default: nil

Виконується тест мотивованого зловмисника для деідентифікованого набору даних, щоб визначити, чи залишаються ідентифіковані дані або чи можна повторно ідентифікувати деідентифіковані дані

17.20. ПСУВАННЯ (SI-20)

Вбудуйте дані або можливості в такі системи або системні компоненти, щоб визначити, чи дані організації були викрадені або неналежним чином видалені з організації: [Призначення: визначені організацією системи або системні компоненти].

No: 1
Name: si_20_01
Type: string
Default: nil

Вбудовані дані або можливості в системи або компоненти системи, щоб визначити, чи були дані організації викрадені або неналежним чином видалені з організації

No: 2
Name: si_20_odp
Type: string
Default: nil

Визначені системи або компоненти системи з даними або можливостями, що підлягають застосуванню

17.21. ОНОВЛЕННЯ ІНФОРМАЦІЇ (SI-21)

Оновлюйте [Призначення: інформація, визначена організацією] з [Призначення: частота, визначена організацією] або згенеруйте інформацію за запитом і видаліть її, коли в ній більше не буде потреби.

No: 1
Name: si_21_01
Type: string
Default: "щорічно"

Інформація оновлюється частота або генерується на вимогу і видаляється, коли більше не потрібна. з якими потрібно оновлювати

No: 2
Name: si_21_odp_01
Type: string
Default: nil

Визначена інформація, яку потрібно оновити

No: 3
Name: si_21_odp_02
Type: integer
Default: 30

Визначені частоти, інформацію

17.22. РІЗНОВИДИ ІНФОРМАЦІЇ (SI-22)

a. Визначити наступні альтернативні джерела інформації для [Завдання: основні функції та послуги, визначені організацією]: [Завдання: альтернативні, визначені організацією джерела інформації];
b. Використовуйте альтернативне джерело інформації для виконання основних функцій або послуг на [Призначення: визначені організацією системи або системні компоненти], коли основне джерело інформації пошкоджено або недоступне.

No: 1
Name: si_22_odp_01
Type: string
Default: nil

Визначені альтернативні джерела інформації для основних функцій та послуг

No: 2
Name: si_22_odp_02
Type: string
Default: nil

Визначені основні функції та послуги, які потребують альтернативних джерел інформації

No: 3
Name: si_22_odp_03
Type: string
Default: nil

Визначені системи або компоненти системи, які потребують альтернативного джерела інформації для виконання основних функцій або послуг; SI-22a. визначені альтернативні джерела інформації для основних функцій та послуг; SI-22b. використовується альтернативне джерело інформації для виконання основних функцій або послуг у системах або компонентах системи, коли первинне джерело інформації пошкоджене або недоступне

17.23. ФРАГМЕНТАЦІЯ ІНФОРМАЦІЇ (SI-23)

Фрагментація інформації.

No: 1
Name: si_23_odp_01
Type: string
Default: nil

Визначені обставини, інформації; які вимагають фрагментації

No: 2
Name: si_23_odp_02
Type: string
Default: nil

Визначена інформація, яка підлягає фрагментації

No: 3
Name: si_23_odp_03
Type: string
Default: nil

Визначені системи або компоненти системи, між якими має бути розподілена фрагментована інформація; SI-23a. за обставин, інформація є фрагментованою; SI-23b. за обставин фрагментована інформація розподіляється між системами або компонентами системи

18. SR

Клас заходів захисту SR — УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА

Опис Цей клас встановлює вимоги для виявлення та мінімізації загроз, що виникають через зовнішніх постачальників продуктів та послуг.

Перелік заходів захисту Політика та процедури управління ризиками ланцюга постачання (SR-1); План управління ризиками ланцюга постачання (SR-2); Створення команди постачання (SR-2(1)); Контроль ланцюга постачання і процесів (SR-3); Різні бази постачання (SR-3(1)); Обмеження шкоди (SR-3(2)); Перенесення заходів захисту управління ризиками ланцюга постачання до субпідрядників (SR-3(3)); Походження (SR-4); Ідентичність (SR-4(1)); Унікальна ідентифікація (SR-4(2)); Перевірка на справжність і відсутність внесення змін (SR-4(3)); Походження – перевірка ланцюга цілісності (SR-4(4)); Стратегії придбання, інструменти і методи (SR-5); Належне постачання (SR-5(1)); Оцінка перед відбором, прийняття, модифікація чи оновлення (SR-5(2)); Оцінка постачальників (SR-6); Тестування та аналіз (SR-6(1)); Безпека операцій ланцюга постачання (SR-7); Повідомлення про порушення ланцюга постачання (SR-8); Захист від злому та виявлення (SR-9); Етапи чи системи розвитку життєвого циклу (SR-9(1)); Перевірка системи і компонентів системи (SR-10); Автентичність компоненту (SR-11); Автентичність компоненту (SR-11(1)); Утилізація компоненту (SR-12).

18.1. ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR-1)

a. Розробіть, задокументуйте та поширте [Призначення: персонал або ролі, визначені організацією]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика управління ризиками ланцюга постачання, яка: a) Розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність; b) Відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам і вказівкам;
2. Процедури для сприяння впровадженню політики управління ризиками ланцюга постачання та відповідних засобів контролю управління ризиками ланцюга постачання;
b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур управління ризиками ланцюга постачання;
c. Перегляньте та оновіть поточне управління ризиками ланцюга постачання:
1. Політика [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією];
2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події,

визначені організацією].

No: 1
Name: sr_1_odp_1
Type: string
Default: nil

SR-01_ODP[01] визначено персонал або ролі, на які поширюється політика управління ризиками ланцюга постачання,

No: 2
Name: sr_1_odp_2
Type: string
Default: nil

SR-01_ODP[02] визначено персонал або ролі, на які поширюються процедури управління ризиками ланцюга постачання,

No: 3
Name: sr_1_odp_3
Type: string
Default: nil

SR-01_ODP[03] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації, рівень завдань/бізнеспроцесу, рівень системи},

No: 4
Name: sr_1_odp_4
Type: string
Default: nil

SR-01_ODP[04] визначена посадова особа, відповідальна за розробку, документування та розповсюдження політики та процедур управління ризиками ланцюга постачання,

No: 5
Name: sr_1_odp_5
Type: string
Default: nil

SR-01_ODP[05] визначена періодичність перегляду та оновлення поточної політики управління ризиками ланцюга постачання,

No: 6
Name: sr_1_odp_6
Type: string
Default: nil

SR-01_ODP[06] є події, які вимагають перегляду та оновлення поточної політики управління ризиками ланцюга постачання,

No: 7
Name: sr_1_odp_7
Type: string
Default: nil

SR-01_ODP[07] визначена періодичність перегляду та оновлення поточної процедури управління ризиками ланцюга постачання,

No: 8
Name: sr_1_odp_8
Type: string
Default: nil

SR-01_ODP[08] визначені події, які вимагають перегляду та оновлення процедур управління ризиками ланцюга постачання,

18.2. ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR-2)

a. Розробіть план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проектуванням, виробництвом, придбанням, доставкою, інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем, компонентів системи або послуг для системи: [Призначення: системи, визначені організацією, системні компоненти або системні служби];
b. Перегляньте та оновіть план управління ризиками ланцюга постачання [Призначення: частота, визначена організацією] або за потреби для усунення загроз;
c. Захистіть план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.

No: 1
Name: sr_2_odp_1
Type: string
Default: nil

SR-02_ODP[01] визначені системи, компоненти системи або системні послуги, для яких розробляється план управління ризиками ланцюга постачання,

No: 2
Name: sr_2_odp_2
Type: string
Default: nil

SR-02_ODP[02] визначено періодичність перегляду та оновлення плану управління ризиками ланцюга постачання,

18.2.1. СТВОРЕННЯ КОМАНДИ ПОСТАЧАННЯ (SR-2(1))

Створена команда з управління ризиками ланцюга постачання, що складається з персонал, ролі та обов'язки для керівництва та підтримки діяльності з управління ризиками ланцюга постачання.

No: 1
Name: sr_2_1_01
Type: list
Default: ["admin", "security_officer"]

Створена команда з управління ризиками ланцюга постачання, що складається з персонал, ролі та обов'язки для керівництва та підтримки діяльності з управління ризиками ланцюга постачання

18.3. КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ (SR-3)

a. Встановлення процесу або процесів для виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання [Призначення: визначена організацією система або компонент системи] у координації з [Завдання: персонал ланцюга постачання, визначений

організацією];
b. Використовуйте такі заходи захисту, щоб захистити систему, компонент системи або системну службу від ризиків ланцюга постачання та обмежити шкоду чи наслідки від подій, пов'язаних із ланцюгом постачання: [Призначення: заходи захисту ланцюга постачання, визначені організацією];
c. Задокументуйте обрані та впроваджені процеси та заходи захисту ланцюгом постачання у [Вибір: плани безпеки та приватності; план управління ризиками ланцюга постачання; [Призначення: документ, визначений організацією]].

No: 1
Name: sr_3_odp_1
Type: string
Default: nil

SR-03_ODP[01] визначено систему або компонент системи, який потребує процесу або процесів для виявлення та усунення слабких місць або недоліків,

No: 2
Name: sr_3_odp_2
Type: string
Default: nil

SR-03_ODP[02] визначено персонал ланцюга поставок, з яким необхідно координувати процес або процеси виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання,

No: 3
Name: sr_3_odp_3
Type: string
Default: nil

SR-03_ODP[03] визначені засоби контролю ланцюга постачання, що застосовуються для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання,

No: 4
Name: sr_3_odp_4
Type: string
Default: nil

SR-03_ODP[04] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та конфіденційності, план управління ризиками ланцюга постачання, <SR- 03_ODP[05] документ>},

No: 5
Name: sr_3_odp_5
Type: string
Default: nil

SR-03_ODP[05] визначено документ, що ідентифікує обрані та впроваджені процеси та засоби контролю ланцюга постачання (якщо обрано),

18.3.1. РІЗНІ БАЗИ ПОСТАЧАННЯ (SR-3(1))

Різні бази постачання (sr-3(1)).

No: 1
Name: sr_3_1_odp_1
Type: string
Default: nil

SR-03_ODP[01] визначено систему або компонент системи, який потребує процесу або процесів для виявлення та усунення слабких місць або недоліків,

No: 2
Name: sr_3_1_odp_2
Type: string
Default: nil

SR-03_ODP[02] визначено персонал ланцюга постачання, з яким необхідно координувати процес або процеси виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга поставок,

No: 3
Name: sr_3_1_odp_3
Type: string
Default: nil

SR-03_ODP[03] визначені засоби контролю ланцюга постачання, що застосовуються для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання,

No: 4
Name: sr_3_1_odp_4
Type: string
Default: nil

SR-03_ODP[04] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та конфіденційності, план управління ризиками ланцюга постачання, <SR- 03_ODP[05] документ>},

No: 5
Name: sr_3_1_odp_5
Type: string
Default: nil

SR-03_ODP[05] визначено документ, що ідентифікує обрані та впроваджені процеси та засоби контролю ланцюга постачання (якщо обрано),

18.3.2. ОБМЕЖЕННЯ ШКОДИ (SR-3(2))

Обмеження шкоди (sr-3(2)).

No: 1
Name: sr_3_2_odp
Type: string
Default: nil

SR-03(02)_ODP визначені засоби контролю для обмеження шкоди від потенційних супротивників ланцюга постачання,

18.3.3. ПЕРЕНЕСЕННЯ ЗАХОДІВ ЗАХИСТУ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ ДО СУБПІДРЯДНИКІВ (SR-3(3))

Включені засоби контролю, передбачені в контрактах з основними підрядниками, також і в контрактах з субпідрядниками.

No: 1
Name: sr_3_3_01

Type: string
Default: "автоматизований засіб моніторингу"

Включені засоби контролю, передбачені в контрактах з основними підрядниками, також і в контрактах з субпідрядниками

18.4. ПОХОДЖЕННЯ (SR-4)

Документуйте, відстежуйте та підтримуйте справжнє походження таких систем, компонентів системи і пов'язаних даних: [Призначення: системи, визначені організацією, системні компоненти та пов'язані дані].

No: 1
Name: sr_4_odp
Type: string
Default: nil

SR-04_ODP визначені системи, компоненти системи та пов'язані з ними дані, які потребують достовірного походження,

18.4.1. ІДЕНТИЧНІСТЬ (SR-4(1))

Ідентичність (sr-4(1)).

No: 1
Name: sr_4_1_odp
Type: string
Default: nil

SR-04(01)_ODP визначені елементи ланцюга постачання, процеси та персонал, пов'язані з системами та критично важливими компонентами системи, які потребують унікальної ідентифікації,

18.4.2. УНІКАЛЬНА ІДЕНТИФІКАЦІЯ (SR-4(2))

Унікальна ідентифікація (sr-4(2)).

No: 1
Name: sr_4_2_odp
Type: string
Default: nil

SR-04(02)_ODP визначені системи та критичні компоненти системи, які потребують унікальної ідентифікації для відстеження в ланцюгу постачання,

18.4.3. ПЕРЕВІРКА НА СПРАВЖНІСТЬ І ВІДСУТНІСТЬ ВНЕСЕННЯ ЗМІН (SR-4(3))

Застосовуються засоби контролю для перевірки того, що отримана система або компонент системи є справжніми.

No: 1
Name: sr_4_3_01

Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються засоби контролю для перевірки того, що отримана система або компонент системи є справжніми

No: 2
Name: sr_4_3_02
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються засоби контролю для перевірки того, що отриману систему або компонент системи не було змінено

18.4.4. ПОХОДЖЕННЯ – ПЕРЕВІРКА ЛАНЦЮГА ЦІЛІСНОСТІ (SR-4(4))

Застосовуються засоби контролю для забезпечення цілісності системи та її компонентів.

No: 1
Name: sr_4_4_01
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються засоби контролю для забезпечення цілісності системи та її компонентів

No: 2
Name: sr_4_4_02
Type: string
Default: nil

Проводиться метод аналізу для забезпечення цілісності системи та компонентів системи

18.5. СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ (SR-5)

Використовуйте наступні стратегії придбання, контрактні інструменти та методи закупівель, щоб захистити від ризиків ланцюга постачання, визначити та пом'якшити їх: [Призначення: визначені організацією стратегії придбання, контрактні інструменти та методи закупівель].

No: 1
Name: sr_5_odp
Type: string
Default: nil

SR-05_ODP визначені стратегії закупівель, контрактні інструменти та методи закупівель для захисту, виявлення та пом'якшення ризиків ланцюга постачання,

18.5.1. НАЛЕЖНЕ ПОСТАЧАННЯ (SR-5(1))

Застосовуються засоби контролю для забезпечення адекватного постачання критично важливих компонентів системи.

No: 1
Name: sr_5_1_01

Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються засоби контролю для забезпечення адекватного постачання критично важливих компонентів системи

18.5.2. ОЦІНКА ПЕРЕД ВІДБОРОМ, ПРИЙНЯТТЯ, МОДИФІКАЦІЯ ЧИ ОНОВЛЕННЯ (SR-5(2))

Оцінюється система, компонент системи або послуги системи перед відбором.

No: 1
Name: sr_5_2_01
Type: string
Default: nil

Оцінюється система, компонент системи або послуги системи перед відбором

No: 2
Name: sr_5_2_02
Type: string
Default: nil

Оцінюється система, компонент системи або послуги системи перед прийняттям

No: 3
Name: sr_5_2_03
Type: string
Default: nil

Оцінюється система, компонент системи або послуги системи перед модифікацією

No: 4
Name: sr_5_2_04
Type: string
Default: nil

Оцінюється система, компонент системи або послуги системи перед оновленням

18.6. ОЦІНКА ПОСТАЧАЛЬНИКІВ (SR-6)

Оцініть і перегляньте ризики ланцюга постачання, пов'язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають [Призначення: частота, визначена організацією].

No: 1
Name: sr_6_odp
Type: string
Default: nil

SR-06_ODP визначена періодичність оцінки та аналізу ризиків, пов'язаних з ланцюгом постачання, що стосуються постачальників або підрядників, а також систем, компонентів системи або системних послуг, які вони надають,

18.6.1. ТЕСТУВАННЯ ТА АНАЛІЗ (SR-6(1))

Тестування та аналіз (sr-6(1)).

Немає параметрів для цього контролю.

18.7. БЕЗПЕКА ОПЕРАЦІЙ ЛАНЦЮГА ПОСТАЧАННЯ (SR-7)

Використовуйте такі заходи захисту операційної безпеки (OPSEC), щоб захистити інформацію, пов'язану з ланцюгом постачання для системи, системного компонента чи системної служби: [Призначення: визначені організацією заходи захисту операційної безпеки (OPSEC)].

No: 1
Name: sr_7_odp
Type: string
Default: nil

SR-07_ODP визначені заходи захисту операційної безпеки (OPSEC) для захисту інформації, пов'язаної з ланцюжком поставок, для системи, системного компонента або системної служби,

18.8. ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ЛАНЦЮГА ПОСТАЧАННЯ (SR-8)

Затвердити угоди та процедури з суб'єктами, залученими до ланцюга постачання для системи, системного компонента або системної послуги для [Вибір (одного або кількох): повідомлення про порушення ланцюга постачання; результати оцінювання або аудитів; [Призначення: інформація, визначена організацією]].

No: 1
Name: sr_8_odp_1
Type: string
Default: nil

SR-08_ODP[01] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повідомлення про порушення ланцюга постачання, <SR-08_ODP[02] результати оцінок або аудитів>},

No: 2
Name: sr_8_odp_2
Type: string
Default: nil

SR-08_ODP[02] визначена інформація, для якої необхідно встановити угоди та процедури (якщо вибрано),

18.9. ЗАХИСТ ВІД ЗЛОМУ ТА ВИЯВЛЕННЯ (SR-9)

Впровадити програму захисту від несанкціонованого доступу для системи, системного компонента або системної служби.

No: 1
Name: sr_9_01
Type: string
Default: nil

Реалізована програма захисту від несанкціонованого доступу для системи, компонента системи або системної служби

18.9.1. ЕТАПИ ЧИ СИСТЕМИ РОЗВИТКУ ЖИТТЄВОГО ЦИКЛУ (SR-9(1))

Застосовуються технології, інструменти та методи захисту від втручання протягом усього життєвого циклу розробки системи.

No: 1
Name: sr_9_1_01
Type: string
Default: nil

Застосовуються технології, інструменти та методи захисту від втручання протягом усього життєвого циклу розробки системи

18.10. ПЕРЕВІРКА СИСТЕМИ І КОМПОНЕНТІВ СИСТЕМИ (SR-10)

Перевірте наступні системи або системні компоненти [Вибір (один або більше): випадковим чином обраних; на [Призначення: частота, визначена організацією], після [Призначення: визначені організацією ознаки необхідності перевірки]] для виявлення втручання: [Призначення: визначені організацією системи або компоненти системи].

No: 1
Name: sr_10_odp_1
Type: string
Default: nil

SR-10_ODP[01] визначені системи або компоненти системи, які

No: 2
Name: sr_10_odp_2
Type: string
Default: nil

SR-10_ODP[02] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {випадково, з частотою <SR-10_ODP[03], за наявності <SR-10_ODP[04] вказівок на необхідність перевірки>},

No: 3
Name: sr_10_odp_3
Type: string
Default: nil

SR-10_ODP[03] визначена періодичність проведення перевірок систем або компонентів системи (якщо вибрано),

No: 4
Name: sr_10_odp_4
Type: string
Default: nil

SR-10_ODP[04] визначені ознаки необхідності перевірки систем або компонентів системи (якщо вони були обрані),

18.11. АВТЕНТИЧНІСТЬ КОМПОНЕНТУ (SR-11)

a. Розробити та впровадити політику та процедури боротьби з підробками, які включають засоби для виявлення та запобігання потраплянню підроблених компонентів у систему;
b. Повідомляти про підроблені системні компоненти [Вибір (один або кілька): джерело підробленого компонента; [Призначення: зовнішні звітні організації, визначені організацією]; [Призначення: персонал або ролі, визначені організацією]].

No: 1
Name: sr_11_odp_1
Type: string
Default: nil

SR-11_ODP[01] вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {джерело підробленого компонента, <SR- 11_ODP[02] зовнішні підзвітні організації>, <SR- 11_ODP[03] персонал або ролі>},

No: 2
Name: sr_11_odp_2
Type: string
Default: nil

SR-11_ODP[02] визначені зовнішні підзвітні організації, яким слід повідомляти про підроблені компоненти системи (якщо вони були обрані),

No: 3
Name: sr_11_odp_3
Type: string
Default: nil

SR-11_ODP[03] визначено персонал або ролі, яким слід повідомляти про підроблені компоненти системи (якщо визначено),

18.11.1. АВТЕНТИЧНІСТЬ КОМПОНЕНТУ (SR-11(1))

Автентичність компоненту (sr-11(1)).

No: 1
Name: sr_11_1_odp
Type: string
Default: nil

SR-11(01)_ODP визначено персонал або ролі, які потребують підготовки для виявлення підроблених компонентів системи (включаючи апаратне, програмне та мікропрограмне забезпечення),

18.12. УТИЛІЗАЦІЯ КОМПОНЕНТУ (SR-12)

Утилізуйте [Призначення: визначені організацією дані, документація, інструменти або системні компоненти] за допомогою таких прийомів і методів: [Призначення: визначені організацією прийоми та методи].

No: 1
Name: sr_12_odp_1
Type: string
Default: nil

SR-12_ODP[01] визначені дані, документація, інструменти або компоненти системи, які підлягають утилізації,

No: 2
Name: sr_12_odp_2
Type: string
Default: nil

SR-12_ODP[02] визначені методи та способи утилізації даних, документації, інструментів або компонентів системи,

No: 3
Name: sr_12_01
Type: string
Default: nil

SR-12 утилізуються <SR-12_ODP[01] дані, документація, інструменти або компоненти системи> з використанням <SR-12_ODP[02] прийомів і методів>.

19. PM

Клас заходів захисту PM — МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Опис Цей клас визначає загальноорганізаційні заходи для ефективного управління програмами інформаційної безпеки та приватності на рівні всього підприємства.

Перелік заходів захисту Ролі програми інформаційної безпеки (PM-2); Ресурси забезпечення інформаційної безпеки та приватності (PM-3); Інвентаризація системи (PM-5); Архітектура підприємства (PM-7); Розвантаження (PM-7(1)); План захисту критичної інфраструктури (PM-8); Стратегія управління ризиками (PM-9); Процес авторизації (PM-10); Визначення завдань та процесів (PM-11); Програма інсайдерської загрози (PM-12); Безпека та приватність працівників (PM-13); Тестування, навчання та моніторинг (PM-14); Контакти з групами та асоціаціями з питань безпеки інформації та приватності (PM-15); Програма інформування про загрози (PM-16); Програма інформування про загрози (PM-16(1)); Захист публічної інформації у зовнішніх системах (PM-17); ПРОГРАМА (КОНЦЕПЦІЯ) ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ (PM-18); Керівні ролі програми приватності (PM-19); Система записів програми приватності (PM-20); Розширене тестування (PM-20(1)); Облік розкриття персональних даних (PM-21); Управління якістю персональних даних (PM-22); Орган управління персональними даними (PM-23); Орган з питань цілісності даних (PM-24); Мінімізація кількості персональних даних, що використовуються під час тестування, навчання та досліджень (PM-25); Управління скаргами (PM-26); Звітність з питань забезпечення приватності (PM-27); Оцінка ризиків (PM-28); Ролі керівників програми управління ризиками (PM-29); План управління ризиками ланцюга постачання (PM-30); Товарів або товарів, необхідних для виконання місії (PM-30(1)); План безперервного моніторингу (PM-31); Призначення (PM-32).

19.1. РОЛІ ПРОГРАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (PM-2)

Призначити старшу посадову особу служби інформаційної безпеки, яка наділена відповідними завданнями та ресурсами для здійснення координації, розробки, впровадження та підтримки програми (концепції) інформаційної безпеки.

No: 1
Name: pm_2_01
Type: list
Default: ["admin", "security_officer"]

Призначено старшу посадову особу з питань інформаційної безпеки в установі

No: 2
Name: pm_2_02
Type: list
Default: ["admin", "security_officer"]

Надано посадовій особі з інформаційної безпеки відомства повноваження та ресурси для координації загальноорганізаційної програми (концепції) з інформаційної безпеки

No: 3
Name: pm_2_03
Type: list
Default: ["admin", "security_officer"]

Має старша посадова особа з питань інформаційної безпеки відомства місію та ресурси для розробки загальноорганізаційної програми інформаційної безпеки

No: 4
Name: pm_2_04
Type: list
Default: ["admin", "security_officer"]

Забезпечено старшу посадову особу з інформаційної безпеки відомства необхідним та ресурсами для впровадження загальноорганізаційної програми інформаційної безпеки

No: 5
Name: pm_2_05
Type: list
Default: ["admin", "security_officer"]

Забезпечено старшу посадову особу з інформаційної безпеки відомства необхідним та ресурсами для підтримки загальноорганізаційної програми (концепції) з інформаційної безпеки

19.2. РЕСУРСИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРИВАТНОСТІ (PM-3)

Включені ресурси, необхідні для реалізації програми (концепції) з інформаційної безпеки, до капітального планування та інвестиційних запитів, а всі винятки задокументовані.

No: 1
Name: pm_03a_01

Type: string
Default: nil

включені ресурси, необхідні для реалізації програми (концепції) з інформаційної безпеки, до капітального планування та інвестиційних запитів, а всі винятки задокументовані

No: 2
Name: pm_03a_02
Type: string
Default: nil

включені ресурси, необхідні для реалізації програми забезпечення конфіденційності, в капітальне планування та інвестиційні запити, а всі винятки задокументовані

No: 3
Name: pm_03b_01
Type: string
Default: nil

підготовлена документація, необхідна для врахування програми (концепції) з інформаційної безпеки в капітальному плануванні та інвестиційних запитах, відповідно до чинних законів, виконавчих наказів, директив, політик, положень, стандартів

No: 4
Name: pm_03b_02
Type: string
Default: nil

підготовлена документація, необхідна для врахування програми конфіденційності в капітальному плануванні та інвестиційних запитах, відповідно до чинних законів, виконавчих наказів, директиви, політик, нормативних актів, стандартів

No: 5
Name: pm_03c_01
Type: string
Default: nil

виділяються ресурси на інформаційну безпеку відповідно до запланованих витрат

No: 6
Name: pm_03c_02
Type: string
Default: nil

виділяються ресурси на забезпечення конфіденційності відповідно до запланованих витрат

19.3. ІНВЕНТАРИЗАЦІЯ СИСТЕМИ (PM-5)

Розробити, відстежувати та звітувати про результати вимірювань показників продуктивності забезпечення безпеки інформації та приватності.

No: 1
Name: pm_5_01
Type: list
Default: []

Розроблено перелік систем організації

No: 2
Name: pm_5_02

Type: list
Default: []

Оновлюється frequency>. перелік оновлення систем переліку організації систем <PM-05_ODP

No: 3
Name: pm_5_odp
Type: string
Default: "щорічно"

Визначена періодичність організації

19.4. АРХІТЕКТУРА ПІДПРИЄМСТВА (PM-7)

Визначити завдання інформаційної безпеки та приватності при розробці документуванні та оновленні плану захисту критичної інфраструктури та ключових ресурсів.

No: 1
Name: pm_7_01
Type: string
Default: nil

Розроблена архітектура інформаційної безпеки; підприємства з урахуванням

No: 2
Name: pm_7_02
Type: string
Default: nil

Підтримується архітектура інформаційної безпеки; підприємства з урахуванням

No: 3
Name: pm_7_03
Type: string
Default: nil

Розроблена архітектура конфіденційності; підприємства з урахуванням

No: 4
Name: pm_7_04
Type: string
Default: nil

Підтримується архітектура конфіденційності; підприємства з урахуванням

No: 5
Name: pm_7_05
Type: string
Default: nil

Розроблена архітектура підприємства з урахуванням ризиків для діяльності та активів організації, окремих осіб, інших організацій та держави в цілому

No: 6
Name: pm_7_06
Type: string
Default: nil

Підтримується архітектура підприємства з урахуванням ризиків, що виникають в результаті цього для операцій та активів організації, окремих осіб, інших організацій та держави.,

19.4.1. РОЗВАНТАЖЕННЯ (PM-7(1))

<PM-07(01)_ODP несуттєві функції або послуги> вивантажуються на інші системи, компоненти системи або зовнішнього постачальника.

No: 1
Name: pm_07_01_odp
Type: string
Default: nil

визначені несуттєві функції або послуги, які потрібно розвантажити

No: 2
Name: pm_07_01
Type: string
Default: nil

<PM-07(01)_ODP несуттєві функції або послуги> вивантажуються на інші системи, компоненти системи або зовнішнього постачальника.

19.5. ПЛАН ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (PM-8)

Враховані питання інформаційної безпеки при розробці плану захисту критичної інфраструктури та ключових ресурсів.

No: 1
Name: pm_08_01
Type: string
Default: nil

враховані питання інформаційної безпеки при розробці плану захисту критичної інфраструктури та ключових ресурсів

No: 2
Name: pm_08_02
Type: string
Default: nil

розглядаються питання інформаційної безпеки в документації плану захисту критичної інфраструктури та ключових ресурсів

No: 3
Name: pm_08_03
Type: string
Default: nil

враховані питання інформаційної безпеки в оновленому плані захисту критичної інфраструктури та ключових ресурсів

No: 4
Name: pm_08_04
Type: string
Default: nil

враховані питання конфіденційності при розробці плану захисту критичної інфраструктури та ключових ресурсів

No: 5
Name: pm_08_05
Type: string
Default: nil

розглядаються питання конфіденційності в документації плану захисту критичної інфраструктури та ключових ресурсів

No: 6
Name: pm_08_06
Type: string
Default: nil

враховані питання конфіденційності в оновленому плані захисту критичної інфраструктури та ключових ресурсів.

19.6. СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ (PM-9)

a. Розробити комплексну стратегію управління:
1. ризиками безпеки для операцій та активів організації, фізичних осіб, інших організацій і держави, пов'язаних з експлуатацією та використанням систем організації;
2. ризиками приватності для фізичних осіб, які можуть виникати внаслідок збирання, обміну, зберігання, передачі, використання та розпорядження персональними даними;
b. Реалізувати стратегію управління ризиками в масштабах організації.
c. Переглядати й оновлювати стратегію управління ризиками [Призначення: з визначеною організацією частотою] або, якщо потрібно, у разі змін в організації.

No: 1
Name: pm_09_odp
Type: string
Default: nil

визначено періодичність перегляду та оновлення стратегії управління ризиками

No: 2
Name: pm_09a_01
Type: string
Default: nil

розроблена комплексна стратегія управління ризиками безпеки для операцій та активів організації, окремих осіб, інших організацій та держави, пов'язаних з експлуатацією та використанням організаційних систем

No: 3
Name: pm_09a_02
Type: string
Default: nil

розроблена комплексна стратегія управління ризиками для приватності осіб, що виникають внаслідок санкціонованої обробки інформації, що ідентифікує особу

No: 4
Name: pm_09b
Type: string
Default: nil

стратегія управління ризиками послідовно впроваджується в організації

No: 5
Name: pm_09c
Type: string
Default: nil

переглядається та оновлюється стратегія управління ризиками <PM-09_ODP частота> або в міру необхідності у зв'язку з організаційними змінами.

19.7. ПРОЦЕС АВТОРИЗАЦІЇ (PM-10)

a. Управляти станом безпеки та приватності інформаційних систем організації та середовищ, у яких ці інформаційні системи експлуатуються через процедури авторизації
b. Призначити окремих осіб для виконання певних ролей і обов'язків у рамках організаційного процесу управління ризиками.
c. Інтегрувати процеси авторизації в загальноорганізаційну програму управління ризиками.

No: 1
Name: pm_10a_01
Type: string
Default: nil

управляється стан безпеки систем організації і середовищ, в яких ці системи працюють, за допомогою процесів авторизації

No: 2
Name: pm_10a_02
Type: string
Default: nil

управляється стан конфіденційності організаційних систем і середовищ, в яких ці системи працюють, за допомогою процесів авторизації

No: 3
Name: pm_10b
Type: string
Default: nil

призначені особи для виконання конкретних ролей та обов'язків в рамках процесу управління організаційними ризиками

No: 4
Name: pm_10c
Type: string
Default: nil

інтегровані процеси авторизації програму управління ризиками. в загальноорганізаційну

19.8. ВИЗНАЧЕННЯ ЗАВДАНЬ ТА ПРОЦЕСІВ (PM-11)

Створити програму розвитку та вдосконалення спеціалістів з питань безпеки та приватності.

No: 1
Name: pm_11_odp
Type: string
Default: nil

визначено періодичність перегляду завдань та бізнеспроцесів

No: 2
Name: pm_11a_01
Type: string
Default: nil

завдання та бізнес-процеси організації визначені з урахуванням інформаційної безпеки

No: 3
Name: pm_11a_02
Type: string
Default: nil

завдання та бізнес-процеси організації визначені з урахуванням права на приватність

No: 4
Name: pm_11a_03
Type: string
Default: nil

завдання та бізнес-процеси організації визначені з урахуванням ризиків для діяльності організації, її активів, окремих осіб, інших організацій та держави в цілому

No: 5
Name: pm_11b_01
Type: string
Default: nil

визначені потреби в захисті інформації, що випливають з визначених завдань та бізнес-процесів

No: 6
Name: pm_11b_02
Type: string
Default: nil

визначені потреби в обробці персональних випливають з визначеної місії та бізнес-процесів

No: 7
Name: pm_11c
Type: string
Default: nil

переглядаються завдання та бізнес-процеси <PM-11_ODP частота>. даних, що

19.9. ПРОГРАМА ІНСАЙДЕРСЬКОЇ ЗАГРОЗИ (PM-12)

Впроваджено програму інсайдерської (внутрішньої) загрози, яка передбачає наявність команди з обробки інцидентів, пов'язаних з внутрішньою дисципліною.

No: 1
Name: pm_12
Type: string
Default: nil

впроваджено програму інсайдерської (внутрішньої) загрози, яка передбачає наявність команди з обробки інцидентів, пов'язаних з внутрішньою дисципліною.

19.10. БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРАЦІВНИКІВ (PM-13)

Існує програма розвитку та вдосконалення спеціалістів з питань безпеки.

No: 1
Name: pm_13_01
Type: string
Default: nil

існує програма розвитку та вдосконалення спеціалістів з питань безпеки

No: 2
Name: pm_13_02
Type: string
Default: nil

створена програма розвитку та вдосконалення спеціалістів з питань приватності.

19.11. ТЕСТУВАННЯ, НАВЧАННЯ ТА МОНІТОРИНГ (PM-14)

Запровадити програму інформування про загрози, яка містить можливості спільного обміну інформацією між організаціями для аналізу загроз.

No: 1
Name: pm_14a_01_01
Type: string
Default: nil

впроваджено процес, який забезпечує розробку планів організації для проведення тестування, навчання та моніторингу безпеки, пов'язаних з системами організації

No: 2
Name: pm_14a_01_02
Type: string
Default: nil

підтримується впроваджений процес, який гарантує, що плани організації щодо проведення тестування, навчання та моніторингу безпеки, пов'язані з системами організації

No: 3
Name: pm_14a_01_03
Type: string
Default: nil

впроваджено процес, який забезпечує розробку планів організації для проведення тестування, навчання та моніторингу конфіденційності, пов'язаних з системами організації

No: 4
Name: pm_14a_01_04
Type: string
Default: nil

підтримуються впроваджений процес, який гарантує, що плани організації щодо проведення тестування, навчання та моніторингу конфіденційності, пов'язані з системами організації

No: 5
Name: pm_14a_02_01
Type: string
Default: nil

продовжує виконуватися впроваджений процес, який гарантує, що організаційні плани щодо проведення тестування, навчання та моніторингу безпеки, пов'язані з системами організації

No: 6
Name: pm_14a_02_02
Type: string
Default: nil

впроваджено процес, який гарантує, що організаційні плани щодо проведення тестування, навчання та моніторингу конфіденційності, пов'язані з системами організації, продовжують виконуватися

No: 7
Name: pm_14b_01
Type: string
Default: nil

перевіряються плани атестації на відповідність стратегії управління ризиками організації

No: 8
Name: pm_14b_02
Type: string
Default: nil

переглядаються навчальні плани на предмет відповідності стратегії управління ризиками організації

No: 9
Name: pm_14b_03
Type: string
Default: nil

переглядаються плани моніторингу на предмет відповідності стратегії управління ризиками організації

No: 10
Name: pm_14b_04
Type: string
Default: nil

перевіряються плани тестування на відповідність загальноорганізаційним пріоритетам реагування на ризики

No: 11
Name: pm_14b_05
Type: string
Default: nil

переглядаються навчальні плани на предмет відповідності загальноорганізаційним пріоритетам реагування на ризики

No: 12
Name: pm_14b_06
Type: string
Default: nil

переглядаються плани моніторингу на предмет відповідності загальноорганізаційним пріоритетам реагування на ризики.

19.12. КОНТАКТИ З ГРУПАМИ ТА АСОЦІАЦІЯМИ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ПРИВАТНОСТІ (PM-15)

Встановлено та інституціоналізовано контакт з окремими групами та асоціаціями у спільноті безпеки для сприяння постійному навчанню та тренінгам з питань безпеки для персоналу організації.

No: 1
Name: pm_15a_01
Type: string
Default: nil

встановлено та інституціоналізовано контакт з окремими групами та асоціаціями у спільноті безпеки для сприяння постійному навчанню та тренінгам з питань безпеки для персоналу організації

No: 2
Name: pm_15a_02
Type: string
Default: nil

встановлено та інституціоналізовано контакт з окремими групами та асоціаціями в межах спільноти з питань приватності, щоб сприяти постійній освіті та навчанню персоналу організації з питань приватності

No: 3
Name: pm_15b_01
Type: string
Default: nil

встановлені та інституціоналізовані контакти з окремими групами та асоціаціями в рамках спільноти безпеки для підтримання актуальності рекомендованих практик, методів та технологій безпеки

No: 4
Name: pm_15b_02
Type: string
Default: nil

встановлені та інституціоналізовані контакти з окремими групами та асоціаціями в межах спільноти безпеки, щоб бути в курсі рекомендованих практик, методів і технологій забезпечення конфіденційності

No: 5
Name: pm_15c_01
Type: string
Default: nil

встановлені та інституціоналізовані контакти з окремими групами та асоціаціями всередині безпекового співтовариства для обміну поточною інформацією про безпеку, включаючи загрози, вразливості та інциденти

No: 6
Name: pm_15c_02
Type: string
Default: nil

встановлено та інституціоналізовано контакт з окремими групами та асоціаціями в межах спільноти з питань конфіденційності для обміну поточною інформацією про конфіденційність, зокрема про загрози, вразливості та інциденти.

19.13. ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ (PM-16)

Впроваджена програма інформування про загрози, яка передбачає можливість обміну інформацією між організаціями для розвідки загроз.

No: 1
Name: pm_16
Type: string
Default: nil

впроваджена програма інформування про загрози, яка передбачає можливість обміну інформацією між організаціями для розвідки загроз.

19.13.1. ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ (PM-16(1))

Mechanisms are employed to maximize the effectiveness of sharing threat intelligence information.

No: 1
Name: pm_16_01
Type: string
Default: nil

automated mechanisms are employed to maximize the effectiveness of sharing threat intelligence information.

19.14. ЗАХИСТ ПУБЛІЧНОЇ ІНФОРМАЦІЇ У ЗОВНІШНІХ СИСТЕМАХ (PM-17)

a. Розробити політику та процедури для забезпечення того, щоб вимоги до захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається у зовнішніх системах, здійснювалися відповідно до чинного законодавства.
b. Оновлювати політику та процедури [Призначення: з визначеною організацією частотою].

No: 1
Name: pm_17_odp_01
Type: string
Default: nil

визначена періодичність перегляду та оновлення політики

No: 2
Name: pm_17_odp_02
Type: string
Default: nil

визначено періодичність перегляду та оновлення процедур

No: 3
Name: pm_17a_01
Type: string
Default: nil

розроблено політику, яка гарантує, що вимоги щодо захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається в зовнішніх системах, виконуються відповідно до чинних законів, виконавчих наказів, директив, політик, нормативних актів та стандартів

No: 4
Name: pm_17a_02
Type: string
Default: nil

встановлені процедури для забезпечення виконання вимог щодо захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається в зовнішніх системах, відповідно до чинних законів, наказів, директив, політик, нормативно-правових актів та стандартів

No: 5
Name: pm_17b_01
Type: string
Default: nil

переглядається та оновлюється політика <PM-17_ODP[01] частота>

No: 6
Name: pm_17b_02
Type: string
Default: nil

переглядаються та оновлюються процедури <PM-17_ODP[02] частота>.

19.15. ПРОГРАМА (КОНЦЕПЦІЯ) ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ (PM-18)

a.
b. Розробити та поширити загальноорганізаційну програму (концепцію) забезпечення приватності, яка:
1. містить опис структури програми забезпечення приватності та ресурсів, призначених для її реалізації;
2. містить огляд вимог до забезпечення приватності й опис засобів управління програмою забезпечення приватності та загальних заходів захисту, встановлених або запланованих для задоволення цих вимог;
3. визначає обов'язки посадової особи щодо приватності, а також визначає обов'язки інших посадових осіб і персоналу з питань забезпечення приватності;
4. описує зобов'язання керівництва, стратегічні цілі та завдання програми забезпечення приватності;
5. відображає координацію між організаційними структурами, відповідальними за різні аспекти приватності;
6. затверджена високопосадовцем, який є відповідальним (та підзвітним) за: управління ризиками приватності, що виникають при здійсненні операцій організації (включно із завданнями, функціями, іміджем і репутацією); організаційними активами, фізичними особами, іншими організаціями та країнами. Оновлювати програму [Призначення: за визначеною організацією частотою], а також в разі змін законодавства, змін в організації і виявлення проблем в ході реалізації програми або оцінювання заходів приватності.

No: 1
Name: pm_18_odp
Type: string
Default: nil

визначена періодичність (концепції) приватності; оновлення плану програми

No: 2
Name: pm_18a_01
Type: string
Default: nil

розроблено загальноорганізаційний план програми (концепції) приватності, який містить огляд програми приватності організації

No: 3
Name: pm_18a_01_01
Type: string
Default: nil

план програми (концепції) приватності містить опис структури програми конфіденційності

No: 4
Name: pm_18a_01_02
Type: string
Default: nil

план програми (концепції) приватності містить опис ресурсів, призначених для реалізації програми конфіденційності

No: 5
Name: pm_18a_02_01
Type: string
Default: nil

план програми (концепції) приватності містить огляд вимог до програми конфіденційності

No: 6
Name: pm_18a_02_02
Type: string
Default: nil

план програми (концепції) приватності містить опис наявних або запланованих засобів контролю для управління програмою (концепцією) приватності для виконання вимог програми

No: 7
Name: pm_18a_02_03
Type: string
Default: nil

план програми (концепції) приватності містить опис загальних засобів контролю, що діють або заплановані для виконання вимог програми конфіденційності

No: 8
Name: pm_18a_03_01
Type: string
Default: nil

в плані програми (концепції) приватності передбачена роль старшої посадової особи організації з питань приватності

No: 9
Name: pm_18a_03_02
Type: string
Default: nil

план програми (концепції) приватності включає визначення та призначення ролей інших посадових осіб і співробітників, відповідальних за забезпечення приватності, та їхні обов'язки

No: 10
Name: pm_18a_04_01

Type: string
Default: nil

план програми (концепції) приватності описує зобов'язання керівництва

No: 11
Name: pm_18a_04_02
Type: string
Default: nil

в плані програми (концепції) приватності описано дотримання вимог

No: 12
Name: pm_18a_04_03
Type: string
Default: nil

план програми (концепція) приватності описує стратегічні цілі та завдання програми приватності

No: 13
Name: pm_18a_05
Type: string
Default: nil

план програми (концепція) приватності відображає координацію між підрозділами організації, відповідальними за різні аспекти приватності

No: 14
Name: pm_18a_06
Type: string
Default: nil

затверджено план програми (концепцію) приватності вищою посадовою особою, яка несе відповідальність і підзвітність за ризики для приватності, яких зазнають операції організації (включно з місією, функціями, іміджем і репутацією), активи організації, окремі особи, інші організації та держава

No: 15
Name: pm_18a_02
Type: string
Default: nil

поширюється план програми (концепція) приватності

No: 16
Name: pm_18b_01
Type: string
Default: nil

оновлено план програми (концепцію) приватності <PM18_ODP частота>

No: 17
Name: pm_18b_02
Type: string
Default: nil

оновлюється план програми (концепція) приватності відповідно до змін у державному законодавстві та політиці щодо приватності

No: 18
Name: pm_18b_03
Type: string
Default: nil

оновлюється план програми відповідно до змін в організації

No: 19
Name: pm_18b_04
Type: string
Default: nil

оновлюється план програми (концепція) приватності забезпечення приватності для вирішення проблем, виявлених під час реалізації плану або оцінок контролю за дотриманням приватності. (концепція) приватності

19.16. КЕРІВНІ РОЛІ ПРОГРАМИ ПРИВАТНОСТІ (PM-19)

Призначити старшу посадову особу з питань забезпечення приватності з повноваженнями, завданням, підзвітністю і ресурсами для координації, розробки та реалізації відповідних вимог забезпечення приватності й управління ризиками приватності в рамках програми забезпечення приватності всієї організації.

No: 1
Name: pm_19_01
Type: string
Default: nil

визначена періодичність приватності; оновлення плану програми

No: 2
Name: pm_19_02
Type: string
Default: nil

розроблено загальноорганізаційний план програми приватності, який містить огляд програми приватності для організації

No: 3
Name: pm_19_03
Type: string
Default: nil

містить план програми приватності опис структури програми приватності

No: 4
Name: pm_19_04
Type: string
Default: nil

містить план програми приватності опис ресурсів, призначених для реалізації програми приватності

No: 5
Name: pm_19_05
Type: string
Default: nil

містить план програми приватності огляд вимог до програми приватності

19.17. СИСТЕМА ЗАПИСІВ ПРОГРАМИ ПРИВАТНОСТІ (PM-20)

підтримувати центральну вебсторінку ресурсу на головному загальнодоступному вебсайті організації, яка слугує центральним джерелом інформації про програму приватності організації та яка:
a. забезпечує доступ громадськості до інформації про діяльність щодо забезпечення приватності в організації та можливість комунікації з уповноваженою посадовою особою з питань забезпечення приватності;
b. оприлюднює організаційну політику забезпечення приватності на вебсайті організації або іншим чином;
c. використовує публічні адреси електронної пошти та/або телефонні лінії, щоб дати можливість громадськості надавати відгуки та/або направляти запитання щодо програми приватності в організації.

No: 1
Name: pm_20_01
Type: string
Default: nil

ведеться центральна вебсторінка загальнодоступному вебсайті організації; на головному

No: 2
Name: pm_20_02
Type: string
Default: nil

слугує вебсторінка основним джерелом програму приватності організації; інформації про PM-20a.[01] забезпечує вебсторінка доступ громадськості до інформації про діяльність організації, пов'язану із захистом приватності

No: 3
Name: pm_20a_01
Type: string
Default: nil

ззабезпечує вебсторінка доступ громадськості до інформації про діяльність організації, пов'язану із захистом приватності

No: 4
Name: pm_20a_02
Type: string
Default: nil

забезпечує вебсторінка можливість громадськості спілкуватися з вищим посадовцем організації з питань приватності

No: 5
Name: pm_20b_01
Type: string
Default: nil

забезпечує вебсторінка публічний доступ до інформації організації щодо приватності

No: 6
Name: pm_20b_02
Type: string
Default: nil

забезпечує вебсторінка публічний доступ до звітів про приватність організації

No: 7
Name: pm_20c
Type: string
Default: nil

є на веб-сторінці загальнодоступні адреси електронної пошти та/або номери телефонів, щоб громадськість могла надавати зворотній зв'язок та/або направляти запитання до відділів з питань приватності.

19.17.1. РОЗШИРЕНЕ ТЕСТУВАННЯ (PM-20(1))

Розроблені та розміщені політики приватності на всіх зовнішніх веб-сайтах;.

No: 1
Name: pm_20_01_01
Type: string
Default: nil

розроблені та розміщені політики приватності на всіх зовнішніх веб-сайтах;

No: 2
Name: pm_20_01_02
Type: string
Default: nil

розроблені та розміщені політики приватності в усіх мобільних додатках;

No: 3
Name: pm_20_01_03
Type: string
Default: nil

розроблені та розміщені політики приватності на всіх інших цифрових сервісах;

No: 4
Name: pm_20_01_a_01
Type: string
Default: nil

політика приватності написана простою мовою;

No: 5
Name: pm_20_01_a_02
Type: string
Default: nil

політика приватності організована таким чином, щоб її було легко зрозуміти та орієнтуватися в ній;

No: 6
Name: pm_20_01_b_01
Type: string
Default: nil

надає політика приватності інформацію, необхідну громадськості для прийняття поінформованого рішення про те, чи взаємодіяти з організацією;

No: 7
Name: pm_20_01_b_02
Type: string
Default: nil

надає політика приватності інформацію, необхідну громадськості для прийняття поінформованого рішення про те, як взаємодіяти з організацією;

No: 8
Name: pm_20_01_c_01
Type: string
Default: nil

оновлюється політика приватності щоразу, коли організація вносить суттєві зміни в описані в ній практики;

No: 9
Name: pm_20_01_c_02
Type: string
Default: nil

містить політика приватності позначку часу/дати, щоб інформувати громадськість про дату останніх змін.

19.18. ОБЛІК РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ (PM-21)

a. Забезпечити доступ громадськості до інформації із забезпечення приватності в організації та можливість комунікації з уповноваженою посадовою особою з питань забезпечення приватності щодо:
1. дати, характеру та мети кожного розкриття запису;
2. імені та адреси особи або організації, щодо яких було зроблено розкриття даних.
b. Обліковувати та зберігати випадки розкриття персональних даних протягом терміну дії запису або п'яти років після розкриття інформації.
c. Здійснювати облік випадків розкриття персональних даних, доступних особі, зазначеній у записі за запитом.

No: 1
Name: pm_21a
Type: string
Default: nil

розроблений і ведеться персональних даних; точний облік розкриття

No: 2
Name: pm_21a_01_01
Type: string
Default: nil

облік включає дату кожного розкриття інформації

No: 3
Name: pm_21a_01_02
Type: string
Default: nil

облік відображає характер кожного розкриття інформації

No: 4
Name: pm_21a_01_03
Type: string
Default: nil

відображає звітність мету кожного розкриття інформації

No: 5
Name: pm_21a_02_01
Type: string
Default: nil

містить звітність ім'я особи або організації, в якій було зроблено розкриття

No: 6
Name: pm_21a_02_02
Type: string
Default: nil

містить звітність адресу або іншу контактну інформацію особи чи організації, якою було здійснено розкриття

No: 7
Name: pm_21b
Type: string
Default: nil

зберігається облік розкриттів протягом усього періоду зберігання інформації, що ідентифікує особу, або протягом п'яти років після розкриття, залежно від того, який з цих термінів довший

No: 8
Name: pm_21c
Type: string
Default: nil

надається облік розкриття персональних даних особи, якої стосується інформація.

19.19. УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ (PM-22)

Розробити та задокументувати загальноорганізаційну політику та процедури, які довзолять:
a. Проводити огляд точності, актуальності, своєчасності та повноти персональних даних протягом їх життєвого циклу;
b. Коригувати або видаляти неточну або застарілу інформацію;
c. Інформувати осіб або інші відповідні організації про внесення змін або видалення персональної інформації;
d. Оскаржувати відмови на запити щодо коригування чи видалення.

No: 1
Name: pm_22_01
Type: string
Default: nil

розроблені та задокументовані загальноорганізаційні політики управління якістю персональних даних

No: 2
Name: pm_22_02
Type: string
Default: nil

розроблені та задокументовані загальноорганізаційні процедури управління якістю персональних даних

No: 3
Name: pm_22a_01
Type: string
Default: nil

передбачено в політиці перевірку точності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації

No: 4
Name: pm_22a_02

Type: string
Default: nil

передбачено в політиці перегляд актуальності інформації, що ідентифікує особу, протягом життєвого циклу інформації

No: 5
Name: pm_22a_03
Type: string
Default: nil

передбачено в політиці перевірку своєчасності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації

No: 6
Name: pm_22a_04
Type: string
Default: nil

передбачено в політиці перевірку повноти інформації, що ідентифікує особу, протягом життєвого циклу інформації

No: 7
Name: pm_22a_05
Type: string
Default: nil

передбачено в процедурах перевірку точності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації

No: 8
Name: pm_22a_06
Type: string
Default: nil

передбачено в процедурах перегляд актуальності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації

No: 9
Name: pm_22a_07
Type: string
Default: nil

процедури передбачають перевірку своєчасності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації

No: 10
Name: pm_22a_08
Type: string
Default: nil

передбачено в процедурах перевірку повноти інформації, що ідентифікує особу, протягом життєвого циклу інформації

No: 11
Name: pm_22b_01
Type: string
Default: nil

передбачено в політиці виправлення або видалення неточної або застарілої персональної інформації, що ідентифікує особу

No: 12
Name: pm_22b_02

Type: string
Default: nil

передбачено в процедурах виправлення або видалення неточної або застарілої персональної інформації

No: 13
Name: pm_22c_01
Type: string
Default: nil

передбачено в політиці розсилання повідомлень про виправлену або видалену персональну інформацію фізичним особам або іншим відповідним суб'єктам

No: 14
Name: pm_22c_02
Type: string
Default: nil

передбачено в процедурах повідомлення про виправлення або видалення персональних даних фізичним особам або іншим відповідним суб'єктам

No: 15
Name: pm_22d_01
Type: string
Default: nil

передбачено в політиці оскарження негативних рішень щодо запитів на виправлення або видалення

No: 16
Name: pm_22d_02
Type: string
Default: nil

передбачені процедури оскарження негативних рішень щодо запитів на виправлення або видалення.

19.20. ОРГАН УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ ДАНИМИ (PM-23)

створити орган управління персональними даними, на якого покладено [Призначення: визначені організацією функції] та виконання [Призначення: визначені організацією обов'язки].

No: 1
Name: pm_23_odp_01
Type: string
Default: nil

визначені ролі органу управління персональними даними

No: 2
Name: pm_23_odp_02
Type: string
Default: nil

визначені обов'язки органу управління персональними даними

No: 3
Name: pm_23
Type: string
Default: nil

створено орган управління даними, що складається з <PM23_ODP[01] ролей> з <PM-23_ODP[02] обов'язками>.

19.21. ОРГАН З ПИТАНЬ ЦІЛІСНОСТІ ДАНИХ (PM-24)

Створити орган з питань цілісності даних для здійснення:
a. Розгляду пропозицій щодо проведення відповідної програми або участі у ній.
b. Проведення огляду усіх поточних програм, в яких бере участь організація.

No: 1
Name: pm_24
Type: string
Default: nil

створено орган з питань цілісності даних

No: 2
Name: pm_24a
Type: string
Default: nil

розглядає орган з питань цілісності даних пропозиції щодо проведення або участі у відповідній програмі

No: 3
Name: pm_24b
Type: string
Default: nil

проводить орган з питань цілісності даних щорічну перевірку всіх програм співставлення, в яких агентство брало участь.

19.22. МІНІМІЗАЦІЯ КІЛЬКОСТІ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕНЬ (PM-25)

a. Розробити та впровадити політики та процедури, спрямовані на врегулювання питань використання персональних даних для внутрішнього тестування, навчання та досліджень.
b. Вжити заходи щодо обмеження або зведення до мінімуму кількості персональних даних, які використовуються для внутрішнього тестування, навчання та досліджень.
c. Надавати дозвіл на використання персональних даних, коли така інформація вимагається для внутрішнього тестування, навчання і досліджень.
d. Здійснювати огляд та оновлення політик та процедур, спрямованих на врегулювання питань використання персональних даних для внутрішнього тестування, навчання та досліджень [Призначення: з визначеною організацією частотою].

No: 1
Name: pm_25_odp_01
Type: string
Default: nil

визначено періодичність перегляду політик, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень

No: 2
Name: pm_25_odp_02
Type: string
Default: nil

визначено періодичність оновлення політик, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень

No: 3
Name: pm_25_odp_03
Type: string
Default: nil

визначено періодичність перегляду процедур, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень

No: 4
Name: pm_25_odp_04
Type: string
Default: nil

визначено періодичність оновлення процедур, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень

No: 5
Name: pm_25a_01
Type: string
Default: nil

розроблені та задокументовані політики, які регулюють використання персональних даних для внутрішнього тестування

No: 6
Name: pm_25a_02
Type: string
Default: nil

розроблені та задокументовані політики, які стосуються використання персональних даних для внутрішнього навчання

No: 7
Name: pm_25a_03
Type: string
Default: nil

розроблені та задокументовані політики, які регулюють використання персональних даних для внутрішніх досліджень

No: 8
Name: pm_25a_04
Type: string
Default: nil

розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішнього тестування

No: 9
Name: pm_25a_05
Type: string
Default: nil

розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішнього навчання; PM-25a.[06] розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішніх досліджень

No: 10
Name: pm_25a_07
Type: string
Default: nil

впроваджено політику, яка регулює використання персональних даних для внутрішнього тестування

No: 11
Name: pm_25a_08
Type: string
Default: nil

впроваджуються політики, які стосуються використання персональних даних для навчання

No: 12
Name: pm_25a_09
Type: string
Default: nil

впроваджуються політики, які стосуються використання персональної інформації для досліджень

No: 13
Name: pm_25a_10
Type: string
Default: nil

впроваджені процедури, які стосуються використання персональних даних для внутрішнього тестування

No: 14
Name: pm_25a_11
Type: string
Default: nil

впроваджені процедури, які стосуються використання персональної інформації для навчання

No: 15
Name: pm_25a_12
Type: string
Default: nil

впроваджені процедури, які стосуються використання особистої інформації для досліджень

No: 16
Name: pm_25b_01
Type: string
Default: nil

обмежено або зведено до мінімуму кількість персональних даних, що використовуються для цілей внутрішнього тестування

No: 17
Name: pm_25b_02
Type: string
Default: nil

обмежено або зведено до мінімуму обсяг інформації, що ідентифікує особу, яка використовується для внутрішніх навчальних цілей

No: 18
Name: pm_25b_03

Type: string
Default: nil

обмежено або зведено до мінімуму обсяг персональних даних, що використовуються для внутрішніх досліджень

No: 19
Name: pm_25c_01
Type: string
Default: nil

дозволено використання внутрішнього тестування; персональних даних для

No: 20
Name: pm_25c_02
Type: string
Default: nil

дозволено використання внутрішнього навчання; персональних даних для

No: 21
Name: pm_25c_03
Type: string
Default: nil

дозволено необхідне використання персональних даних для внутрішніх досліджень

No: 22
Name: pm_25d_01
Type: string
Default: nil

переглядаються політики <PM-25_ODP[01] частота>

No: 23
Name: pm_25d_02
Type: string
Default: nil

оновлюються політики <PM-25_ODP[02] частота>

No: 24
Name: pm_25d_03
Type: string
Default: nil

переглядаються процедури <PM-25_ODP[03] частота>

No: 25
Name: pm_25d_04
Type: string
Default: nil

оновлюються процедури <PM-25_ODP[04] частота>.

19.23. УПРАВЛІННЯ СКАРГАМИ (PM-26)

Впровадити процес отримання та реагування на скарги, проблеми чи запитання від фізичних осіб щодо організаційної практики забезпечення приватності, який охоплює:
a. механізми, які легко використовувати та які є легкодоступними для громадськості;
b. усю інформацію, необхідну для успішного подання скарг;
c. механізми відстеження, що забезпечують отримання всіх скарг та їх вчасний і належний розгляд протягом [Призначення: визначений організацією період часу];

d. підтвердження отримання скарг, заявлених проблем чи запитань від фізичних осіб протягом [Призначення: визначений організацією період часу];
e. надання відповідей на отримані скарги, заявлені проблеми чи запитання від фізичних осіб протягом [Призначення: визначений організацією період часу].

No: 1
Name: pm_26_odp_01
Type: string
Default: nil

визначено період часу, протягом якого мають бути розглянуті скарги (в тому числі звернення або питання) від фізичних осіб

No: 2
Name: pm_26_odp_02
Type: string
Default: nil

визначено період часу, протягом якого мають бути оброблені скарги (в тому числі звернення або питання) від фізичних осіб

No: 3
Name: pm_26_odp_03
Type: string
Default: nil

визначено часовий отримання скарг

No: 4
Name: pm_26_odp_04
Type: string
Default: nil

визначено термін для відповіді на скарги

No: 5
Name: pm_26_01
Type: string
Default: nil

впроваджено процес отримання скарг, занепокоєнь або запитань від фізичних осіб про безпеку та конфіденційність в організації

No: 6
Name: pm_26_02
Type: string
Default: nil

впроваджено процес реагування на скарги, занепокоєння або запитання від фізичних осіб про безпеку та конфіденційність в організації

No: 7
Name: pm_26a_01
Type: string
Default: nil

включає процес управління скаргами механізми, які є простими у використанні для громадськості

No: 8
Name: pm_26c_02
Type: string
Default: nil

включає процес управління скаргами механізми, які є легкодоступними для громадськості

No: 9
Name: pm_26b
Type: string
Default: nil

містить процес управління скаргами всю інформацію, необхідну для успішного подання скарг

No: 10
Name: pm_26c_01a
Type: string
Default: nil

включає процес управління скаргами механізми відстеження, які гарантують, що всі скарги будуть розглянуті протягом <PM-26_ODP[01] періоду часу>

No: 11
Name: pm_26c_01b
Type: string
Default: nil

включає процес управління скаргами механізми відстеження, щоб гарантувати, що всі скарги розглядаються протягом <PM-26_ODP[02] часового періоду>

No: 12
Name: pm_26d
Type: string
Default: nil

передбачає процес управління скаргами підтвердження отримання скарг, занепокоєнь або запитань від фізичних осіб протягом <PM-26_ODP[03] часового періоду>

No: 13
Name: pm_26e
Type: string
Default: nil

включає процес управління скаргами реагування на скарги, занепокоєння або питання від фізичних осіб протягом <PM-26_ODP[04] часового періоду>

19.24. ЗВІТНІСТЬ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ (PM-27)

a. Визначити та задокументувати:
1. припущення, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків;
2. обмеження, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків;
3. пріоритети та компроміси, які розглядаються організацією для здійснення управління ризиками;
4. стійкість організації до ризиків.
b. Поінформувати [Призначення: визначений організацією персонал] про результати визначення ризиків.
c. Переглядати та оновлювати підходи щодо визначення ризиків [Призначення: з визначеною організацією частотою].

No: 1
Name: pm_27_odp_01

Type: string
Default: nil

визначені звіти з питань забезпечення приватності

No: 2
Name: pm_27_odp_02
Type: string
Default: nil

визначені органи нагляду за дотриманням приватності

No: 3
Name: pm_27_odp_03
Type: string
Default: nil

визначені посадові особи, відповідальні за контроль і дотриманням програми приватності

No: 4
Name: pm_27_odp_04
Type: string
Default: nil

визначена періодичність перегляду та оновлення звітів про приватність

No: 5
Name: pm_27a
Type: string
Default: nil

розроблено <PM-27_ODP[01] звіти з питань приватності>

No: 6
Name: pm_27a_01
Type: string
Default: nil

передаються звіти з питань забезпечення приватності до <PM-27_ODP[02] наглядових органів>, щоб продемонструвати підзвітність законодавчим, регуляторним та політичним мандатам щодо приватності

No: 7
Name: pm_27a_02_01
Type: string
Default: nil

поширюються звіти про конфіденційність серед <PM-27_ODP[03] посадових осіб>

No: 8
Name: pm_27a_02_02
Type: string
Default: nil

поширюються звіти з питань забезпечення приватності серед іншого персоналу, відповідального за контроль за дотриманням програми конфіденційності

No: 9
Name: pm_27b
Type: string
Default: nil

переглядаються та оновлюються звіти з питань забезпечення приватності <PM-27_ODP[04] частота>.

19.25. ОЦІНКА РИЗИКІВ (PM-28)

Визначені та задокументовані припущення, що впливають на оцінку ризиків.

No: 1
Name: pm_28_odp_01
Type: string
Default: nil

визначено персонал, який отримуватиме результати визначення ризиків

No: 2
Name: pm_28_odp_02
Type: string
Default: nil

визначено періодичність перегляду та міркувань щодо структуризації ризиків

No: 3
Name: pm_28a_01_01
Type: string
Default: nil

визначені та задокументовані припущення, що впливають на оцінку ризиків

No: 4
Name: pm_28a_01_02
Type: string
Default: nil

визначені та задокументовані припущення, що впливають на реагування ризиків

No: 5
Name: pm_28a_01_03
Type: string
Default: nil

визначені та задокументовані припущення, що впливають на моніторинг ризиків

No: 6
Name: pm_28a_02_01
Type: string
Default: nil

визначені та задокументовані обмеження, що впливають на оцінку ризиків

No: 7
Name: pm_28a_02_02
Type: string
Default: nil

визначені та задокументовані обмеження, що впливають на реагування на ризики

No: 8
Name: pm_28a_02_03
Type: string
Default: nil

визначені та задокументовані обмеження, що впливають на моніторинг ризиків; оновлення

No: 9
Name: pm_28a_03_01

Type: string
Default: nil

визначені та задокументовані пріоритети, розглядаються організацією для управління ризиками

No: 10
Name: pm_28a_03_02
Type: string
Default: nil

визначені та задокументовані компроміси, розглядаються організацією для управління ризиками

No: 11
Name: pm_28a_04
Type: string
Default: nil

визначена та задокументована організаційна толерантність до ризиків

No: 12
Name: pm_28b
Type: string
Default: nil

поширюються результати діяльності з фреймворкінгу ризиків серед персоналу <PM-28_ODP[01]>

No: 13
Name: pm_28c
Type: string
Default: nil

переглядаються та оновлюються міркування фреймінгу ризиків <PM-28_ODP[02] частота>. щодо

19.26. РОЛІ КЕРІВНИКІВ ПРОГРАМИ УПРАВЛІННЯ РИЗИКАМИ (PM-29)

a. Розробити план управління ризиками ланцюга постачання, пов'язаного з розробкою, придбанням, обслуговуванням та утилізацією систем, компонентів системи та послуг для системи.
b. Реалізувати план управління ризиками ланцюга постачання послідовно та наскрізно по всій організації.
c. Переглядати й оновлювати план управління ризиками ланцюга постачання [Призначення: з визначеною організацією частотою] або, якщо потрібно, у разі змін в організації.

No: 1
Name: pm_29a_01
Type: string
Default: nil

призначено старшу посадову особу, відповідальну за управління ризиками

No: 2
Name: pm_29a_02
Type: string
Default: nil

узгоджує старша посадова особа, відповідальна за управління ризиками, процеси управління інформаційною безпекою та конфіденційністю з процесами стратегічного, операційного та бюджетного планування

No: 3
Name: pm_29b_01

Type: string
Default: nil

створена посада (функція) ризик-менеджера

No: 4
Name: pm_29b_02
Type: string
Default: nil

розглядає та аналізує керівник з управління ризиками (функція) ризики з точки зору всієї організації

No: 5
Name: pm_29b_03
Type: string
Default: nil

забезпечує керівник (функція) з управління ризиками узгоджене управління ризиками в межах всієї організації.

19.27. ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (PM-30)

Узгоджує старша посадова особа, відповідальна за управління ризиками ланцюга постачання, процеси управління інформаційною безпекою та конфіденційністю з процесами стратегічного, операційного та бюджетного планування.

No: 1
Name: pm_30_odp
Type: string
Default: nil

призначено старшу посадову особу, відповідальну за управління ризиками ланцюга постачання

No: 2
Name: pm_30a_01
Type: string
Default: nil

узгоджує старша посадова особа, відповідальна за управління ризиками ланцюга постачання, процеси управління інформаційною безпекою та конфіденційністю з процесами стратегічного, операційного та бюджетного планування

No: 3
Name: pm_30a_02
Type: string
Default: nil

створена посада (функція) ризик-менеджер

No: 4
Name: pm_30a_03
Type: string
Default: nil

розглядає та аналізує керівник з управління ризиками (функція) ризики з точки зору всієї організації

No: 5
Name: pm_30a_04

Type: string
Default: nil

забезпечує керівник (функція) з управління ризиками узгоджене управління ризиками в межах всієї організації.

No: 6
Name: pm_30a_05
Type: string
Default: nil

стратегія управління ризиками ланцюга постачання враховує ризики, пов'язані з придбанням систем

No: 7
Name: pm_30a_06
Type: string
Default: nil

стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з придбанням компонентів системи

No: 8
Name: pm_30a_07
Type: string
Default: nil

стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з придбанням системних послуг

No: 9
Name: pm_30a_08
Type: string
Default: nil

тратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням систем

No: 10
Name: pm_30a_09
Type: string
Default: nil

стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням компонентів системи

No: 11
Name: pm_30a_10
Type: string
Default: nil

стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням системних послуг; PM-30a.[11] враховує стратегія управління ризиками ланцюга постачання ризики, пов'язані з утилізацією систем

No: 12
Name: pm_30a_12
Type: string
Default: nil

враховує стратегія управління ризиками ланцюга постачання ризики, пов'язані з утилізацією компонентів системи

No: 13
Name: pm_30a_13
Type: string
Default: nil

стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з утилізацією системних послуг

No: 14
Name: pm_30b
Type: string
Default: nil

стратегія управління ризиками ланцюга послідовно впроваджується в організації

No: 15
Name: pm_30c
Type: string
Default: nil

переглядається та оновлюється стратегія управління ризиками ланцюга постачання <PM-30_ODP частота> або в міру необхідності у зв'язку з організаційними змінами поставок

19.27.1. ТОВАРІВ АБО ТОВАРІВ, НЕОБХІДНИХ ДЛЯ ВИКОНАННЯ МІСІЇ (PM-30(1))

Визначені постачальники критично важливих технологій, продуктів і послуг, що мають вирішальне значення для виконання завдань;.

No: 1
Name: pm_30_01_01
Type: string
Default: nil

визначені постачальники критично важливих технологій, продуктів і послуг, що мають вирішальне значення для виконання завдань;

No: 2
Name: pm_30_01_02
Type: string
Default: nil

є пріоритетними постачальники критично важливих технологій, продуктів та послуг;

No: 3
Name: pm_30_01_03
Type: string
Default: nil

оцінюються постачальники критично важливих технологій, продуктів та послуг.

19.28. ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ (PM-31)

Розробити план безперервного моніторингу в масштабах всієї організації та впровадити програми безперервного моніторингу, які включають:
a. Встановити відповідні показників для моніторингу в масштабах всієї організації [Призначення: визначені організацією показники];
b. Встановити [Призначення: частота, визначеної організацією] для здійснення моніторингу та [Призначення: періодичність, визначена організацією] проведення оцінки ефективності контролю;
c. Постійний моніторинг визначених організацією показників відповідно до стратегії безперервного моніторингу;
d. Співставлення та аналіз інформації, отриманої в результаті здійснення моніторингу, та

контрольних оцінок;
e. Заходи реагування на результати аналізу оцінок контролю та моніторингових даних;
f. Звітування про стан безпеки та приватності систем організації перед [Призначення: визначеним організацією персоналом чи посадовою особою] [Призначення: з визначеною організацією періодичністю].

No: 1
Name: pm_31_odp_01
Type: string
Default: nil

визначені параметри для безперервного моніторингу в масштабах всієї організації

No: 2
Name: pm_31_odp_02
Type: string
Default: nil

визначено періодичність моніторингу

No: 3
Name: pm_31_odp_03
Type: string
Default: nil

визначена періодичність оцінки ефективності контролю

No: 4
Name: pm_31_odp_04
Type: string
Default: nil

визначено персонал або ролі для звітування про стан безпеки систем організації

No: 5
Name: pm_31_odp_05
Type: string
Default: nil

визначено персонал або ролі для звітування про стан конфіденційності систем організації

No: 6
Name: pm_31_odp_06
Type: string
Default: nil

визначено періодичність звітування про стан безпеки систем організації

No: 7
Name: pm_31_odp_07
Type: string
Default: nil

визначено періодичність звітування конфіденційності систем організації

No: 8
Name: pm_31
Type: string
Default: nil

розроблена загальноорганізаційна стратегія безперервного моніторингу

No: 9
Name: pm_31a

Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які включають встановлення <PM-31_ODP[01] параметрів>, що підлягають моніторингу

No: 10
Name: pm_31b_01
Type: string
Default: nil

впроваджено програми безперервного моніторингу, які встановлюють <PM-31_ODP[02] частоту> для моніторингу

No: 11
Name: pm_31b_02
Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які встановлюють <PM-31_ODP[03] частоту> для оцінки ефективності контролю; про стан

No: 12
Name: pm_31c
Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які включають моніторинг <PM-31_ODP[01] параметрів> на постійній основі відповідно до стратегії безперервного моніторингу

No: 13
Name: pm_31d_01
Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які включають співставлення інформації, отриманої в результаті контрольних оцінок та моніторингу

No: 14
Name: pm_31d_02
Type: string
Default: nil

впроваджуються програми постійного моніторингу, які включають аналіз інформації, отриманої в результаті контрольних оцінок та моніторингу

No: 15
Name: pm_31e_01
Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які передбачають заходи реагування на аналіз інформації, отриманої в результаті оцінки результатів контролю

No: 16
Name: pm_31e_02
Type: string
Default: nil

впроваджуються програми безперервного моніторингу, які передбачають заходи реагування на результати аналізу інформації, отриманої під час моніторингу

No: 17
Name: pm_31f_01

Type: string
Default: nil

впроваджено програми безперервного моніторингу, які передбачають звітування про стан безпеки систем організації перед <PM-31_ODP[04] персонал або ролі> <PM31_ODP[06] частота>

No: 18
Name: pm_31f_02
Type: string
Default: nil

впроваджені програми безперервного моніторингу, які передбачають звітування про стан конфіденційності організаційних систем перед <PM-31_ODP[05] персонал або ролі> <PM-31_ODP[07] частота>.

19.29. ПРИЗНАЧЕННЯ (PM-32)

Включіть ролі й обов'язки з безпеки та приватності в опис посади в організації.

No: 1
Name: pm_32_odp
Type: string
Default: nil

визначені системи або компоненти системи, що підтримують важливі для місії послуги або функції

No: 2
Name: pm_32
Type: string
Default: nil

аналізуються допоміжні послуги або функції, необхідні для виконання місії, для забезпечення того, щоб інформаційні ресурси використовувалися відповідно до їхнього призначення

20. PT

Клас заходів захисту PT — ПОВНОВАЖЕННЯ

Опис Цей клас фокусується на дотриманні законодавства щодо захисту персональних даних, отриманні згоди та забезпеченні прав суб'єктів даних.

Перелік заходів захисту Політика та процедури обробки персональних даних (PT-1); Повноваження на обробку персональних даних (PT-2); Тегування даних (PT-2(1)); Автоматизація (PT-2(2)); Цілі обробки персональних даних (PT-3); Тегування даних (PT-3(1)); Автоматизація (PT-3(2)); Згода на обробку персональних даних (PT-4); Індивідуальна згода на обробку персональних даних (PT-4(1)); Своєчасна згода на обробку персональних даних (PT-4(2)); Відкликання (PT-4(3)); Повідомлення про конфіденційність (PT-5); Своєчасне повідомлення про конфіденційність (PT-5(1)); Заяви про конфіденційність (PT-5(2)); Система записів повідомлень про конфіденційність (PT-6); Звичайне використання (PT-6(1)); Посібники та правила (PT-6(2)); Спеціальні категорії персональних даних (PT-7); Номери соціального страхування (PT-7(1)); Інформація про першу поправку (PT-7(2)); Вимоги до відповідності (PT-8).

20.1. ПОЛІТИКА ТА ПРОЦЕДУРИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ (PT-1)

a. Розробіть, задокументуйте та поширте [Призначення: персонал або ролі, визначені організацією]:
1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи], обробки персональних даних та політики прозорості, який: a) розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність; b) відповідає чинним законам, розпорядженням, директивам, положенням, політикам, стандартам і рекомендаціям.
2. Процедури для реалізації політики обробки та прозорості персональних даних, а також пов'язані засоби контролю;
b. Призначте [Призначення: посадову особу, визначену організацією] для керування розробкою, документуванням і розповсюдженням політики й процедур щодо обробки персональних даних та прозорості;
c. Перегляньте та оновіть поточні процедури обробки та прозорість персональних даних:
1. Політика [Призначення: частота, визначена організацією] і наступні [Призначення: події, визначені організацією];
2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: подія, визначена організацією].

No: 1
Name: pt_1_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюється політика обробки персональних даних та забезпечення прозорості

No: 2
Name: pt_1_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, на які поширюються процедури обробки персональних даних та політики прозорості

No: 3
Name: pt_1_odp_03
Type: string
Default: nil

Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнеспроцесу; рівень системи}

No: 4
Name: pt_1_odp_04
Type: list
Default: ["admin", "security_officer"]

Визначено посадову особу, яка керуватиме політикою та процедурами обробки персональних даних, а також політикою та процедурами прозорості

No: 5
Name: pt_1_odp_05
Type: list
Default: ["admin", "security_officer"]

Визначена періодичність перегляду та оновлення поточної політики обробки та прозорості інформації, що ідентифікує особу

No: 6
Name: pt_1_odp_06
Type: list
Default: ["admin", "security_officer"]

Є події, які вимагають перегляду та оновлення поточної політики обробки персональних даних та прозорості

No: 7
Name: pt_1_odp_07
Type: list
Default: ["admin", "security_officer"]

Визначена частота, з якою переглядаються та оновлюються поточні процедури обробки персональних даних та забезпечення прозорості

20.2. ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT-2)

a. визначити та задокументувати [Призначення: повноваження, визначені організацією], які дозволяють [Призначення: обробку, визначену організацією] персональної інформації;
b. обмежити [Призначення: обробку, визначену організацією] персональної інформації лише таким чином, яким дозволено (тільки до того, що дозволено)

No: 1
Name: pt_2_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначені повноваження щодо надання дозволу на обробку (визначені в PT-02_ODP[02]) персональних даних

No: 2
Name: pt_2_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначено тип обробки персональних даних

No: 3
Name: pt_2_odp_03
Type: list
Default: ["admin", "security_officer"]

Визначено тип обробки підлягають обмеженню; PT-02a. визначено та задокументовано орган, який дозволяє обробку персональних даних; PT-02b. обробка персональних обмежується лише таким чином, яким дозволено. персональних даних, що даних,

20.2.1. ТЕГУВАННЯ ДАНИХ (PT-2(1))

Теги даних, що містять <PT-02(01) _ODP[01] санкціонована обробка>, прикріплені до <PT-02(01) _ODP[02] елементів інформації, що іденти0фікує особу>.

No: 1
Name: pt_2_1_01

Type: list
Default: ["admin", "security_officer"]

Теги даних, що містять <PT-02(01) _ODP[01] санкціонована обробка>, прикріплені до <PT-02(01) _ODP[02] елементів інформації, що іденти0фікує особу>

20.2.2. АВТОМАТИЗАЦІЯ (PT-2(2))

Управління дотриманням санкціонованої обробки персональних даних здійснюється за допомогою <PT02(02)_ODP автоматизовані механізми обробки персональних даних>.

No: 1
Name: pt_2_2_01
Type: list
Default: ["admin", "security_officer"]

Управління дотриманням санкціонованої обробки персональних даних здійснюється за допомогою <PT02(02)_ODP автоматизовані механізми обробки персональних даних>

No: 2
Name: pt_2_2_odp
Type: list
Default: ["admin", "security_officer"]

Визначені автоматизовані механізми, які використовуються для управління дотриманням санкціонованої обробки інформації, що ідентифікує особу

20.3. ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ (PT-3)

a. визначити та задокументувати [Призначення: цілі, визначені організацією] для обробки персональних даних;
b. описати мету (цілі) у публічних повідомленнях про конфіденційність і політиках організації;
c. обмежити [Призначення: обробку, визначену організацією] персональних даних лише тією, яка сумісна з визначеною ціллю(ями);
d. відстежувати зміни в обробці персональних даних та впроваджувати [Завдання: визначені організацією механізми], щоб гарантувати, що будь-які зміни вносяться відповідно до [Завдання: визначені організацією вимоги].

No: 1
Name: pt_3_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено мету (цілі) обробки персональних даних

No: 2
Name: pt_3_odp_02
Type: list
Default: ["admin", "security_officer"]

Визначена обробка персональних даних, яка підлягає обмеженню

No: 3
Name: pt_3_odp_03

Type: list
Default: ["admin", "security_officer"]

Визначені механізми, які мають бути впроваджені для забезпечення того, щоб будь-які зміни в персональних данних, вносилися відповідно до вимог

No: 4
Name: pt_3_odp_04
Type: list
Default: ["admin", "security_officer"]

визначені вимоги до зміни обробки персональних даних;

No: 5
Name: pt_3_a
Type: string
Default: nil

визначено та задокументовано мету (цілі) обробки персональних даних;

No: 6
Name: pt_3_b_01
Type: string
Default: nil

описана мета (цілі) в публічних повідомленнях про конфіденційність організації;

No: 7
Name: pt_3_b_02
Type: string
Default: nil

описана мета (цілі) в політиці організації;

No: 8
Name: pt_3_c
Type: string
Default: nil

обробка персональних даних обмежується лише тим, що є сумісним з визначеною метою (цілями);

No: 9
Name: pt_3_d_01
Type: string
Default: nil

здійснюється моніторинг змін в обробці персональних даних;

No: 10
Name: pt_3_d_02
Type: string
Default: nil

впроваджено механізми для забезпечення того, щоб будь-які зміни вносилися відповідно до вимог.

20.3.1. ТЕГУВАННЯ ДАНИХ (PT-3(1))

Теги даних, що містять <PT-03(01) _ODP[01] цілі обробки>, приєднані до <PT-03(01) _ ODP[02] елементів інформації, що ідентифікує особу>.

No: 1
Name: pt_3_1_01

Type: list
Default: ["admin", "security_officer"]

Теги даних, що містять <PT-03(01) _ODP[01] цілі обробки>, приєднані до <PT-03(01) _ODP[02] елементів інформації, що ідентифікує особу>

20.3.2. АВТОМАТИЗАЦІЯ (PT-3(2))

Відстежуються цілі обробки персональних даних за допомогою автоматизованих механізмів.

No: 1
Name: pt_3_2_01
Type: list
Default: ["admin", "security_officer"]

Відстежуються цілі обробки персональних даних за допомогою автоматизованих механізмів

No: 2
Name: pt_3_2_odp
Type: list
Default: ["admin", "security_officer"]

Визначені автоматизовані механізми відстеження цілей обробки персональних даних

20.4. ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT-4)

Впроваджувати [Призначення: інструменти або механізми, визначені організацією], щоб окремі особи давали згоду на обробку їх персональних даних до її збору, що полегшить прийняття обґрунтованих рішень особами.

No: 1
Name: pt_4_01
Type: list
Default: ["admin", "security_officer"]

Впроваджено інструменти або механізми для надання фізичними особами згоди на обробку їхніх персональних даних до її збору, які сприяють прийняттю фізичними особами поінформованих рішень

No: 2
Name: pt_4_odp
Type: list
Default: ["admin", "security_officer"]

Визначені інструменти або механізми, які мають бути застосовані для надання особами згоди на обробку їхніх персональних даних

20.4.1. ІНДИВІДУАЛЬНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT-4(1))

Індивідуальна згода на обробку персональних даних (pt-4(1)).

No: 1
Name: pt_4_1_odp

Type: list
Default: ["admin", "security_officer"]

Визначені механізми адаптації для обробки окремих елементів дозволів персональних даних; PT-04(01) передбачені механізми, які дозволяють особам пристосовувати дозволи на обробку до вибраних елементів персональних даних

20.4.2. СВОЄЧАСНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT-4(2))

Надаються механізми згоди особам частота та в поєднанні з обробкою персональних даних.

No: 1
Name: pt_4_2_01
Type: list
Default: ["admin", "security_officer"]

Надаються механізми згоди особам частота та в поєднанні з обробкою персональних даних

20.4.3. ВІДКЛИКАННЯ (PT-4(3))

Впроваджено інструменти або механізми, які дозволяють фізичним особам відкликати згоду на обробку їхніх персональних даних.

No: 1
Name: pt_4_3_01
Type: list
Default: ["admin", "security_officer"]

Впроваджено інструменти або механізми, які дозволяють фізичним особам відкликати згоду на обробку їхніх персональних даних

No: 2
Name: pt_4_3_odp
Type: list
Default: ["admin", "security_officer"]

Визначені інструменти або механізми для відкликання згоди на обробку персональних даних

20.5. ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ (PT-5)

Впровадити повідомлення про конфіденційність особам, чиї персональні дані обробляються в системі, які:
a. доступні окремим особам під час першої взаємодії з організацією, та згодом [Призначення: частота, визначена організацією];
b. виражені простою мовою;
c. визначають орган, який надає дозвіл на обробку персональних даних;
d. визначають цілі, для яких мають оброблятися персональні дані;
e. включають [Призначення: інформація, визначена організацією].

No: 1
Name: pt_5_odp_01

Type: list
Default: ["admin", "security_officer"]

Визначена частота, з якою повідомлення надається особам на рівні первинної взаємодії з організацією

No: 2
Name: pt_5_odp_02
Type: list
Default: ["admin", "security_officer"]

визначена інформація, яка повинна бути включена до повідомлення про обробку персональних даних;

No: 3
Name: pt_5_a_01
Type: string
Default: nil

направляється особам повідомлення про обробку персональних даних таким чином, щоб вони могли ознайомитися з ним при першій взаємодії з організацією;

No: 4
Name: pt_5_a_02
Type: string
Default: nil

направляється повідомлення фізичним особам про обробку персональних даних, таким чином, щоб це повідомлення було згодом доступне фізичним особам <PT-05_ODP[01] частота>;

No: 5
Name: pt_5_b
Type: string
Default: nil

направляється фізичним особам повідомлення про обробку персональних даних, яке є чітким, легким для розуміння та містить інформацію про обробку персональних даних простою мовою;

No: 6
Name: pt_5_c
Type: string
Default: nil

направляється фізичним особам повідомлення про обробку персональних даних, яке визначає орган, що надає дозвіл на обробку персональних даних;

No: 7
Name: pt_5_d
Type: string
Default: nil

направляється повідомлення фізичним особам про обробку персональних даних, в якому вказується мета, з якою буде оброблятися персональна інформація;

No: 8
Name: pt_5_e
Type: string
Default: nil

направляється повідомлення фізичним особам про обробку персональних даних, які включають <PT-05_ODP[02] інформацію>.

20.5.1. СВОЄЧАСНЕ ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ (PT-5(1))

Надається повідомлення про обробку персональних даних особам у той час і в тому місці, де особа надає персональні дані, у зв'язку з якою здійснюється дія з даними, або періодичність обробки даних частота.

No: 1
Name: pt_5_1_01
Type: list
Default: ["admin", "security_officer"]

Надається повідомлення про обробку персональних даних особам у той час і в тому місці, де особа надає персональні дані, у зв'язку з якою здійснюється дія з даними, або періодичність обробки даних частота

No: 2
Name: pt_5_1_odp
Type: list
Default: ["admin", "security_officer"]

Визначена періодичність подання обробку персональних даних; повідомлення про

20.5.2. ЗАЯВИ ПРО КОНФІДЕНЦІЙНІСТЬ (PT-5(2))

Включаються повідомлення про конфіденційність у форми, які збирають інформацію, що буде зберігатися в системі записів Закону про конфіденційність, або ж заяви про конфіденційність надаються на окремих формах, які можуть зберігатися у приватних осіб.

No: 1
Name: pt_5_2_01
Type: string
Default: nil

Включаються повідомлення про конфіденційність у форми, які збирають інформацію, що буде зберігатися в системі записів Закону про конфіденційність, або ж заяви про конфіденційність надаються на окремих формах, які можуть зберігатися у приватних осіб

20.6. СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ (PT-6)

для систем, які обробляють інформацію, яка зберігатиметься в системі записів Закону про конфіденційність:
a. розробити проект системи повідомлень про записи відповідно до вказівок OMB і подати нову та суттєво змінену систему повідомлень про записи до OMB та відповідних комітетів Конгресу для попереднього розгляду;
b. опублікувати систему записів повідомлень у Державному реєстрі;
c. зберігайте повідомлення системи записів точними, оновленими та в обсязі відповідно до впровадженої політики.

Немає параметрів для цього контролю.

20.6.1. ЗВИЧАЙНЕ ВИКОРИСТАННЯ (PT-6(1))

Переглядаються всі звичайні види використання, опубліковані в повідомленні системи записів періодичність, для забезпечення постійної точності, а також для забезпечення того, щоб звичайні види використання і надалі були сумісними з метою, для якої була зібрана інформація.

No: 1
Name: pt_6_1_01
Type: string
Default: "щорічно"

Переглядаються всі звичайні види використання, опубліковані в повідомленні системи записів періодичність, для забезпечення постійної точності, а також для забезпечення того, щоб звичайні види використання і надалі були сумісними з метою, для якої була зібрана інформація

No: 2
Name: pt_6_1_odp
Type: string
Default: "щорічно"

Визначено періодичність перегляду всіх звичайних видів використання, опублікованих у системі обліку повідомлень

20.6.2. ПОСІБНИКИ ТА ПРАВИЛА (PT-6(2))

Всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються частота, щоб переконатися, що вони залишаються доречними та необхідними відповідно до закону.

No: 1
Name: pt_6_2_01
Type: string
Default: "щорічно"

Всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються частота, щоб переконатися, що вони залишаються доречними та необхідними відповідно до закону

No: 2
Name: pt_6_2_02
Type: string
Default: "щорічно"

Всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються частота, щоб переконатися, що вони були оприлюднені як нормативні акти

No: 3
Name: pt_6_2_03
Type: string
Default: "щорічно"

Всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються частота, щоб переконатися, що вони точно описані в повідомленні про систему записів

No: 4
Name: pt_6_2_odp
Type: string
Default: "щорічно"

Визначено періодичність перегляду всіх винятків із Закону про конфіденційність, заявлених для системи записів

20.7. СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ (PT-7)

Застосувати [Призначення: умови обробки, визначені організацією] для певних категорій персональних даних.

No: 1
Name: pt_7_01
Type: list
Default: ["admin", "security_officer"]

Застосовуються умови обробки до певних категорій персональних даних

No: 2
Name: pt_7_odp
Type: list
Default: ["admin", "security_officer"]

Визначені умови обробки, що застосовуються до певних категорій персональних даних

20.7.1. НОМЕРИ СОЦІАЛЬНОГО СТРАХУВАННЯ (PT-7(1))

При обробці системою номерів соціального страхування усувається непотрібний збір, зберігання та використання номерів соціального страхування.

No: 1
Name: pt_7_1_a_01
Type: string
Default: nil

При обробці системою номерів соціального страхування усувається непотрібний збір, зберігання та використання номерів соціального страхування

No: 2
Name: pt_7_1_a_02
Type: list
Default: ["admin", "security_officer"]

Вивчаються альтернативи використанню номерів соціального страхування в якості персонального ідентифікатора, коли система обробляє їх

No: 3
Name: pt_7_1_b
Type: list
Default: ["admin", "security_officer"]

Не відмовляється система при обробці номерів соціального страхування в індивідуальних правах, пільгах або привілеях, передбачених законом, через відмову особи розкрити свій номер соціального страхування

No: 4
Name: pt_7_1_c_01
Type: list
Default: ["admin", "security_officer"]

При обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, чи є таке розкриття обов'язковим чи добровільним, яким законодавчим чи іншим органом запитується такий номер, і як він буде використовуватися

No: 5
Name: pt_7_1_c_02
Type: list
Default: ["admin", "security_officer"]

При обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, яким законодавчим чи іншим органом запитується цей номер

No: 6
Name: pt_7_1_c_03
Type: list
Default: ["admin", "security_officer"]

При обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, як він буде використовуватися

20.7.2. ІНФОРМАЦІЯ ПРО ПЕРШУ ПОПРАВКУ (PT-7(2))

Заборонена обробка інформації, що описує, як будь-яка особа реалізує права, гарантовані Першою поправкою, за винятком випадків, коли це прямо дозволено законом або особою, або якщо вона не стосується та входить до сфери санкціонованої діяльності правоохоронних органів.

No: 1
Name: pt_7_2_01
Type: list
Default: ["admin", "security_officer"]

Заборонена обробка інформації, що описує, як будь-яка особа реалізує права, гарантовані Першою поправкою, за винятком випадків, коли це прямо дозволено законом або особою, або якщо вона не стосується та входить до сфери санкціонованої діяльності правоохоронних органів

20.8. ВИМОГИ ДО ВІДПОВІДНОСТІ (PT-8)

Коли система чи організація обробляє інформацію з метою проведення програми відповідності необхідно:
a. отримати схвалення Ради з цілісності даних для проведення програми відповідності;
b. розробити та укласти договір комп'ютерної відповідності;
c. незалежним чином перевіряти інформацію, надану програмою відповідності, перш ніж вживати негативних заходів проти особи;
d. повідомляти осіб і надати їм можливість оскаржити висновки, перш ніж вживати проти них негативних заходів.

Немає параметрів для цього контролю.