Комплексна система захисту інформації

Завдання безпеки для VPN та PKI (20)

Зміст

Зміст

Анотація

Завдання з безпеки для забезпечення безпеки VPN-продуктів та інфраструктури PKI (CA, OCSP, TSP, LDAP).

1. AC

Клас заходів захисту AC — УПРАВЛІННЯ ДОСТУПОМ

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

Перелік заходів захисту: Управління обліковими записами (AC-2); Забезпечення доступу (AC-3); Автоматизований моніторинг та управління (AC-17(1)); Захист конфіденційності та цілісності за допомогою шифрування (AC-17(2)); Відключення або деактивація доступу (AC-17(9)).

1.1. 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_09
Type: integer
Default: 24

Визначено передумови та критерії членства в групах і ролях; визначено атрибути (за необхідності) для кожного облікового запису; визначено персонал або ролі, необхідні для затвердження запитів на створення облікових записів; визначено політику, процедури, передумови та критерії створення, активації, зміни, деактивації та видалення облікових записів; визначено персонал або ролі, які мають бути повідомлені; визначено період часу, протягом якого адміністратори облікових записів повинні бути повідомлені про те, що облікові записи більше не потрібні; визначено термін, протягом якого необхідно повідомляти адміністраторів облікових записів про звільнення або переведення користувачів; визначено період часу, протягом якого необхідно повідомляти адміністраторів облікових записів про зміни у використанні системи або необхідність знати про зміни для окремої особи; визначено атрибути, необхідні для авторизації доступу до системи (за потреби); AC-02_ODP[10] AC-02a.[01] AC-02a.[02] AC-02b AC-02c AC-02d.01 AC-02d.02 AC-02d.03[01] AC-02d.03[02] AC-02e AC-02f.[01] AC-02f.[02] AC-02f.[03] AC-02f.[04] AC-02f.[05] AC-02g AC-02h.01 AC-02h.02 AC-02h.03 AC-02i.01 AC-02i.02 AC-02i.03 визначено періодичність перегляду облікових записів; визначено та задокументовано типи облікових записів, дозволених для використання в системі; визначено та задокументовано типи облікових записів, які заборонено використовувати в системі; призначені менеджери облікових записів; необхідні умови та критерії для членства в групах та ролях; визначено авторизованих користувачів системи; вказано приналежність до групи або ролі; для кожного облікового запису вказуються повноваження доступу (тобто привілеї); атрибути (за необхідності) вказуються для кожного облікового запису; для запитів на створення облікових записів потрібні схвалення від персоналу або ролей; облікові записи створюються відповідно до політики, процедур, передумов та критеріїв; облікові записи активуються відповідно до політики, процедур, передумов та критеріїв;

облікові записи змінюються відповідно до політики, процедур, передумов та критеріїв; облікові записи деактивуються відповідно до політики, процедур, передумов та критеріїв; облікові записи видаляються відповідно до політики, процедур, передумов та критеріїв; контролюється використання облікових записів; адміністратори облікових записів та персонал або ролі отримують повідомлення протягом періоду часу, коли облікові записи більше не потрібні; адміністратори облікових записів та персонал або ролі отримують повідомлення протягом періоду часу, коли користувачі звільнені чи переведені; адміністратори облікових записів та персонал або ролі отримують повідомлення протягом періоду часу, коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань. доступ до системи здійснюється на підставі дійсної авторизації доступу; доступ до системи авторизується на основі передбачуваного використання системи; доступ до системи авторизовано на основі атрибутів (за необхідності); AC-02j AC-02k.[01] AC-02k.[02] AC-02l.[01] AC-02l.[02] облікові записи переглядаються на відповідність вимогам управління обліковими записами частота; створено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи; впроваджено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи; процеси управління обліковими записами узгоджуються з процесами звільнення персоналу; процеси управління обліковими записами узгоджуються з процесами переводу персоналу

1.2. 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

1.2.1. АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ТА УПРАВЛІННЯ (AC-17(1))

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

1.2.2. ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ (AC-17(2))

No: 1
Name: ac_17_2_01
Type: string
Default: "AES-256-GCM"

ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ МЕТА ОЦІНКИ: Визначте, чи інформаційна система криптографічні механізми

1.2.3. ВІДКЛЮЧЕННЯ АБО ДЕАКТИВАЦІЯ ДОСТУПУ (AC-17(9))

No: 1
Name: ac_17_9_01
Type: integer
Default: 30

Передбачена можливість відключення або деактивації віддаленого доступу до системи протягом 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

2. AU

Клас заходів захисту AU — АУДИТ ТА ПІДЗВІТНІСТЬ

Цей клас забезпечує можливість відстеження дій у системі, генерування, захист та аналіз записів аудиту для виявлення порушень політики безпеки.

Перелік заходів захисту: Цифрові підписи (AU-10(5)).

2.0.1. ЦИФРОВІ ПІДПИСИ (AU-10(5))

No: 1
Name: au_10_5_01
Type: string
Default: nil

НЕСПРОСТОВНІСТЬ - ЦИФРОВІ ПІДПИСИ [Вилучено: Включено до SI-07]

3. IA

Клас заходів захисту IA — ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

Цей клас відповідає за однозначне розпізнавання користувачів або пристроїв та підтвердження їхньої справжності перед наданням доступу до системи.

Перелік заходів захисту: Віддалений доступ - окремий пристрій (IA-2(11)); ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12)); Управління ідентифікацією (IA-4); Автентифікація на основі відкритого ключа (IA-5(2)); Автентифікація криптографічного модуля (IA-7).

3.0.1. ВІДДАЛЕНИЙ ДОСТУП - ОКРЕМИЙ ПРИСТРІЙ (IA-2(11))

No: 1
Name: ia_2_11_01
Type: string
Default: nil

ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ВІДДАЛЕНИЙ ДОСТУП - ОКРЕМИЙ ПРИСТРІЙ [Вилучено: Включено до IA-02(06)]

3.0.2. ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) (IA-2(12))

No: 1
Name: ia_2_12_01
Type: list
Default: ["admin", "security_officer"]

Приймаються та електронним шляхом підтверджуються повноваження облікових даних особистої ідентифікації

3.1. УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ (IA-4)

No: 1
Name: ia_4_a
Type: list
Default: ["admin", "security_officer"]

Управління ідентифікаторами здійснюється шляхом отримання дозволу від персоналу або ролей на призначення ідентифікатора особі, групі, ролі або пристрою

No: 2
Name: ia_4_b
Type: list
Default: ["admin", "security_officer"]

Управління ідентифікаторами здійснюється шляхом вибору ідентифікатора, який ідентифікує окрему особу, групу, ролі або пристрій

No: 3
Name: ia_4_c
Type: list
Default: ["admin", "security_officer"]

Управління ідентифікаторами здійснюється шляхом призначення ідентифікатора особі, групі, ролі або пристрою; IA-04(d) ідентифікатори управляються шляхом запобігання повторному використанню ідентифікаторів впродовж період часу

No: 4
Name: ia_4_odp_01
Type: list
Default: ["admin", "security_officer"]

Визначено персонал або ролі, від яких необхідно отримати дозвіл на призначення ідентифікатора

No: 5
Name: ia_4_odp_02
Type: integer
Default: 30

Визначено період часу для запобігання повторному використанню ідентифікаторів

3.1.1. АВТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА (IA-5(2))

Немає параметрів для цього контролю.

3.2. АВТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНОГО МОДУЛЯ (IA-7)

No: 1
Name: ia_7_01
Type: list
Default: ["default_deny_rule", "abac_rule_1"]

Впроваджено механізми автентифікації в криптографічний модуль, який відповідає вимогам чинних законів, виконавчих розпоряджень, директив, політик, правил, стандартів та рекомендацій для такої автентифікації

4. SC

Клас заходів захисту SC — ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА

Цей клас охоплює механізми захисту інформації під час її передачі мережами зв'язку, криптографічний захист та ізоляцію критичних компонентів.

Перелік заходів захисту: Запобігання поділу тунелювання для віддалених пристроїв (SC-7(7)); Конфіденційність та криптографічний захист (SC-8(1)); Відключення мережі (SC-10); Встановлення ключами (SC-12); Сертифікати інфраструктури відкритих ключів (SC-17); Автентифікація сесії (SC-23); ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ | КРИПТОГРАФІЧНИЙ ЗАХИСТ; Примусове апаратне забезпечення виконання (SC-49); Апаратний захист (SC-51).

4.0.1. ЗАПОБІГАННЯ ПОДІЛУ ТУНЕЛЮВАННЯ ДЛЯ ВІДДАЛЕНИХ ПРИСТРОЇВ (SC-7(7))

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

4.0.2. КОНФІДЕНЦІЙНІСТЬ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-8(1))

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}

4.1. 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

4.2. 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

4.3. 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.

4.4. АВТЕНТИФІКАЦІЯ СЕСІЇ (SC-23)

Забезпечити автентифікацію сеансів зв'язку.

No: 1
Name: sc_23_01
Type: string
Default: nil

Захищено автентифікацію сеансів зв'язку

4.4.1. ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ | КРИПТОГРАФІЧНИЙ ЗАХИСТ

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

4.5. 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

4.6. 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; SC-51a. використовується апаратний захист від запису для компонентів мікропрограми системи; SC-51b.[01] впроваджено спеціальні процедури для уповноважених осіб для ручного вимкнення апаратного захисту від запису для модифікацій мікропрограми; SC-51b.[02] реалізовано спеціальні процедури для уповноважених осіб для повторного увімкнення захисту від запису перед поверненням до робочого режиму