Комплексна система захисту інформації

Завдання безпеки для месенджера (30)

Зміст

Зміст

Анотація

Завдання з безпеки для забезпечення конфіденційності, цілісності повідомлень та управління сесіями в месенджері.

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); Мінімізація повноважень (AC-6); Управління паралельною сесією (AC-10); Використання письмових та портативний пристроїв для зберігання даних (AC-19(1)); Повне шифрування пристроїв та сховищ інформації (AC-19(5)).

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

1.3. 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

1.4. 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_01
Type: integer
Default: 30

Кількість одночасних сеансів для кожного облікового запису та/або типів облікових записів обмежена кількість

No: 2
Name: ac_10_odp_02
Type: integer
Default: 30

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

1.4.1. ВИКОРИСТАННЯ ПИСЬМОВИХ ТА ПОРТАТИВНИЙ ПРИСТРОЇВ ДЛЯ ЗБЕРІГАННЯ ДАНИХ (AC-19(1))

No: 1
Name: ac_19_1_01
Type: string
Default: nil

КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПИСЬМОВИХ ТА ПОРТАТИВНИЙ ПРИСТРОЇВ ДЛЯ ЗБЕРІГАННЯ ДАНИХ [Вилучено: Включено в MP-07]

1.4.2. ПОВНЕ ШИФРУВАННЯ ПРИСТРОЇВ ТА СХОВИЩ ІНФОРМАЦІЇ (AC-19(5))

Немає параметрів для цього контролю.

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: Події аудиту (AU-2); Неспростовність (AU-10); Цифрові підписи (AU-10(5)).

2.1. 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

2.2. 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_01
Type: list
Default: ["admin", "security_officer"]

Надаються неспростовні докази того, що особа (або процес, що діє від імені особи) виконала дії

No: 2
Name: au_10_odp
Type: list
Default: ["login", "logout", "failed_attempt"]

Визначено дії, на які поширюється принцип неспростовності

2.2.1. 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. CP

Клас заходів захисту CP — ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

Цей клас описує заходи для відновлення функціонування інформаційної системи та забезпечення її безперебійної роботи у разі надзвичайних ситуацій.

Перелік заходів захисту: Резервне копіювання (CP-9).

3.1. РЕЗЕРВНЕ КОПІЮВАННЯ (CP-9)

No: 1
Name: cp_9_01
Type: string
Default: nil

РЕЗЕРВНЕ КОПІЮВАННЯ МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: cp_9_a
Type: string
Default: "щорічно"

Резервне копіювання інформації користувача, що міститься в компонентах системи, здійснюється частота

No: 3
Name: cp_9_b
Type: string
Default: "щорічно"

Виконується резервне копіювання інформації системи, що міститься в системі частота; CP-09(c) створюються резервні копії документації системи, включаючи документацію, пов'язану з безпекою та конфіденційністю частота

No: 4
Name: cp_9_d_01
Type: string
Default: nil

Конфіденційність резервних копій інформації захищена

No: 5
Name: cp_9_d_02
Type: string
Default: nil

Цілісність резервних копій інформації захищена

No: 6
Name: cp_9_d_03
Type: string
Default: nil

Доступність резервних копій інформації захищена

No: 7
Name: cp_9_odp_01
Type: string
Default: nil

Визначено компоненти системи, для яких необхідно проводити резервне копіювання інформації користувачів

No: 8
Name: cp_9_odp_02
Type: integer
Default: 30

Визначено частоту, з якою слід проводити резервне копіювання інформації користувача відповідно до часу відновлення та цілей відновлення

No: 9
Name: cp_9_odp_03
Type: integer
Default: 30

Визначено частоту проведення резервного копіювання інформації системи, що відповідає завдань відновлення і встановлених цілей відновлення

No: 10
Name: cp_9_odp_04
Type: integer
Default: 30

Визначено частоту, з якою слід проводити резервне копіювання документації системи відповідно до часу відновлення та цілей точки відновлення

4. 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: Ідентифікація та автентифікація користувачів (IA-2); Управління ідентифікацією (IA-4); Ефективність біометричної автентифікації (IA-5(12)); Автентифікація криптографічного модуля (IA-7).

4.1. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ (IA-2)

No: 1
Name: ia_2_01
Type: string
Default: nil

ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) МЕТА ОЦІНКИ: Визначити, чи:

No: 2
Name: ia_2_02
Type: string
Default: nil

Процеси що діють від імені користувачів унікально ідентифіковані та автентифіковані

4.2. 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

4.2.1. ЕФЕКТИВНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ (IA-5(12))

No: 1
Name: ia_5_12_odp
Type: string
Default: "автоматизований засіб моніторингу"

Визначено вимоги до якості біометрії; для біометричної автентифікації використовувати механізми, які задовольняють вимоги

4.3. 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

5. MP

Клас заходів захисту MP — ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ

Цей клас спрямований на безпечне зберігання, транспортування, використання та знищення як цифрових, так і паперових носіїв інформації.

Перелік заходів захисту: Знищення інформації на носіях інформації (MP-6).

5.1. 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_a_01
Type: string
Default: nil

Носії інформації системи перед утилізацією піддаються очищенню за допомогою методів та процедур очищення

No: 2
Name: mp_6_a_02
Type: string
Default: nil

Носії інформації системи очищаються за допомогою методів та процедур очищення перед випуском за межі контрольованої зони

No: 3
Name: mp_6_a_03
Type: string
Default: nil

Носії інформації системи очищуються за допомогою методів і процедур очищення перед повторним використанням

No: 4
Name: mp_6_b
Type: string
Default: "автоматизований засіб моніторингу"

Застосовуються механізми очищення, надійність і цілісність яких відповідає категорії безпеки або рівню секретності інформації

No: 5
Name: mp_6_odp_01
Type: string
Default: nil

Визначено носії інформації системи, які підлягають очищенню перед утилізацією

No: 6
Name: mp_6_odp_02
Type: string
Default: nil

Визначено носії інформації системи, які підлягають очищенню перед випуском за межі контрольованої зони

No: 7
Name: mp_6_odp_03
Type: string
Default: nil

Визначені носії інформації системи, що підлягають очищенню перед повторним використанням

No: 8
Name: mp_6_odp_04
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед утилізацією

No: 9
Name: mp_6_odp_05
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед випуском за межі контрольованої зони

No: 10
Name: mp_6_odp_06
Type: string
Default: nil

Визначено методи та процедури очищення, які слід використовувати для очищення перед повторним використанням

6. 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: Захист від атак «відмова в обслуговуванні» (SC-5); Доступність ресурсів (SC-7); Конфіденційність та криптографічний захист (SC-8(1)); Попередня і постобробка (SC-8(2)); Встановлення ключами (SC-12); Сертифікати інфраструктури відкритих ключів (SC-17); БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) (SC-20); БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ (SC-21); (рекурсивний або джерело даних та (SC-22); Автентифікація сесії (SC-23); Захист інформації в стані спокою (SC-28); ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ

СПОКОЮ | КРИПТОГРАФІЧНИЙ ЗАХИСТ; Примусове апаратне забезпечення виконання (SC-49); Апаратний захист (SC-51).

6.1. 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}

6.2. 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.

6.2.1. 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}

6.2.2. ПОПЕРЕДНЯ І ПОСТОБРОБКА (SC-8(2))

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}

6.3. 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

6.4. 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.

6.5. 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.

6.6. 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

6.7. (РЕКУРСИВНИЙ АБО ДЖЕРЕЛО ДАНИХ ТА (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

6.8. АВТЕНТИФІКАЦІЯ СЕСІЇ (SC-23)

Забезпечити автентифікацію сеансів зв'язку.

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

Захищено автентифікацію сеансів зв'язку

6.9. 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

6.9.1. 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

6.10. 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

6.11. 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

7. SI

Клас заходів захисту SI — ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ

Цей клас спрямований на захист системи від шкідливого коду, виявлення вразливостей та запобігання несанкціонованим змінам інформації.

Перелік заходів захисту: Управління та збереження інформації (SI-12).

7.1. 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