
# ДІЯЛЬНІСТЬ У РАМКАХ РЕФОРМИ ДЕРЖАВНИХ ПІДПРИЄМСТВ УКРАЇНИ (SOERA)

## БАЗОВА ПРОГРАМА НАВЧАНЬ ПО АУДИТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВНУТРІШНІХ АУДИТОРІВ

# Програма навчань

| | |
|---|---|
| Домен I | Основи інформаційної безпеки: *конфіденційність, цілісність, доступність* |
| Домен II | Захист доступу: *реєстрація користувачів, зняття з реєстрації, перегляд прав користувачів, та привілейовані облікові записи* |
| Домен III | Захист інформації та активів організації: *дистанційна робота, політика чистого столу, фізична безпека та безпека комунікацій* |
| Перевірка знань | Питання |

# Застереження

Цей тренінг був розроблений для Департаменту гармонізації державного внутрішнього фінансового контролю Міністерства фінансів України і не призначений для використання будь-якими іншими сторонами. Крім того, цей тренінг ґрунтується на галузевій практиці та чинних законах і нормативно-правових актах станом на 26 червня 2024 року. Така практика, закони та нормативні акти можуть змінюватися, тому учасники цього тренінгу повинні регулярно звертатися за оновленими рекомендаціями щодо змісту цього тренінгу.

# Порядок проведення навчання

Форма проведення – вебінари з перевіркою знань

- Програма складається з розгляду методологічних питань та практичних прикладів; до програми залучено 3 тренера-викладача:
  - ✓ Андрій Гуляєв, SOERA;
  - ✓ Євгеній Олійник, SOERA;
  - ✓ Євген Пащенко, CIA, CISA, CISSP, CISM, SOERA.

- учасники навчання – внутрішні аудитори державних установ України;
- мова навчання - українська;
- форма навчання - онлайн сесії тривалістю ~ 3 год. кожна, протягом 3 сесій\вебінарів;
- Час та дата проведення:
  - -1-й вебінар – 26 червня 2024;
  - -2-й вебінар – буде оголошено додатково;
  - -3-й вебінар – буде оголошено додатково.
- платформа навчання – Zoom / MS Teams.

# Домен I

## Інформаційна безпека в контексті IT Аудиту

### Модуль I. Основи інформаційної безпеки

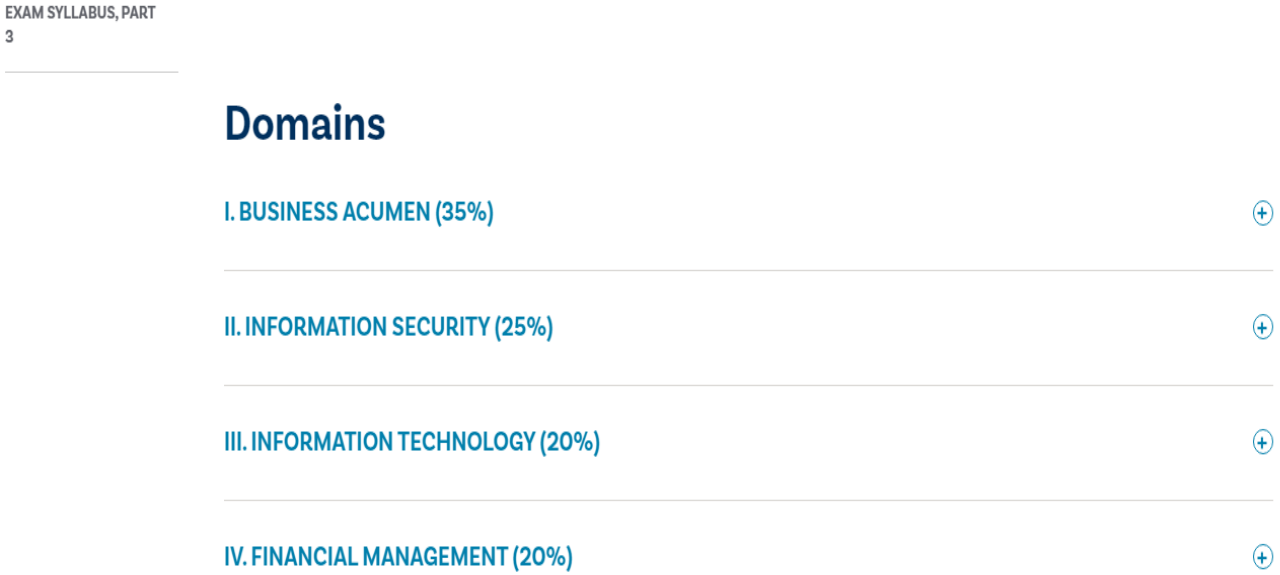
# Чому IT Аудит важливий

- Впровадження нових інформаційних технологій
- Автоматизація бізнес процесів
- Зміна ландшафту IT-ризиків та відповідних кіберзагроз для організації

**The Institute of Internal Auditors (The IIA):**

Аудити інформаційних систем можуть допомогти компаніям у виявленні та запобіганні ризикам у системах інформаційних технологій, які підтримують бізнес.

**Certified Internal Auditor Examination Syllabus Part 3:**

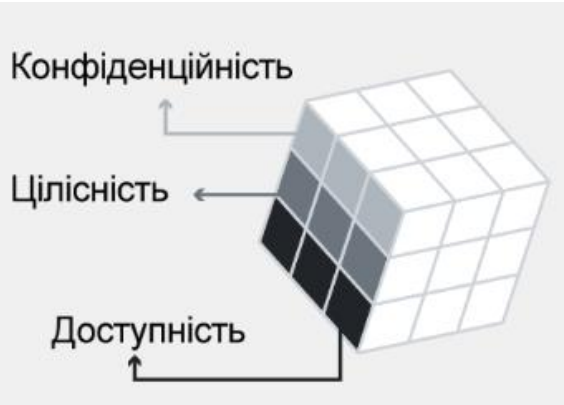



**Джерело: https://www.theiia.org/en/certifications/cia/exam-prep-resources/exam-syllabus/exam-syllabus-part-3**

## Конфіденційність, цілісність, доступність (КЦД)

Модель КЦД поєднує три основних критерії інформаційної безпеки і є базою для забезпечення безпеки, надійності та відмовостійкості.

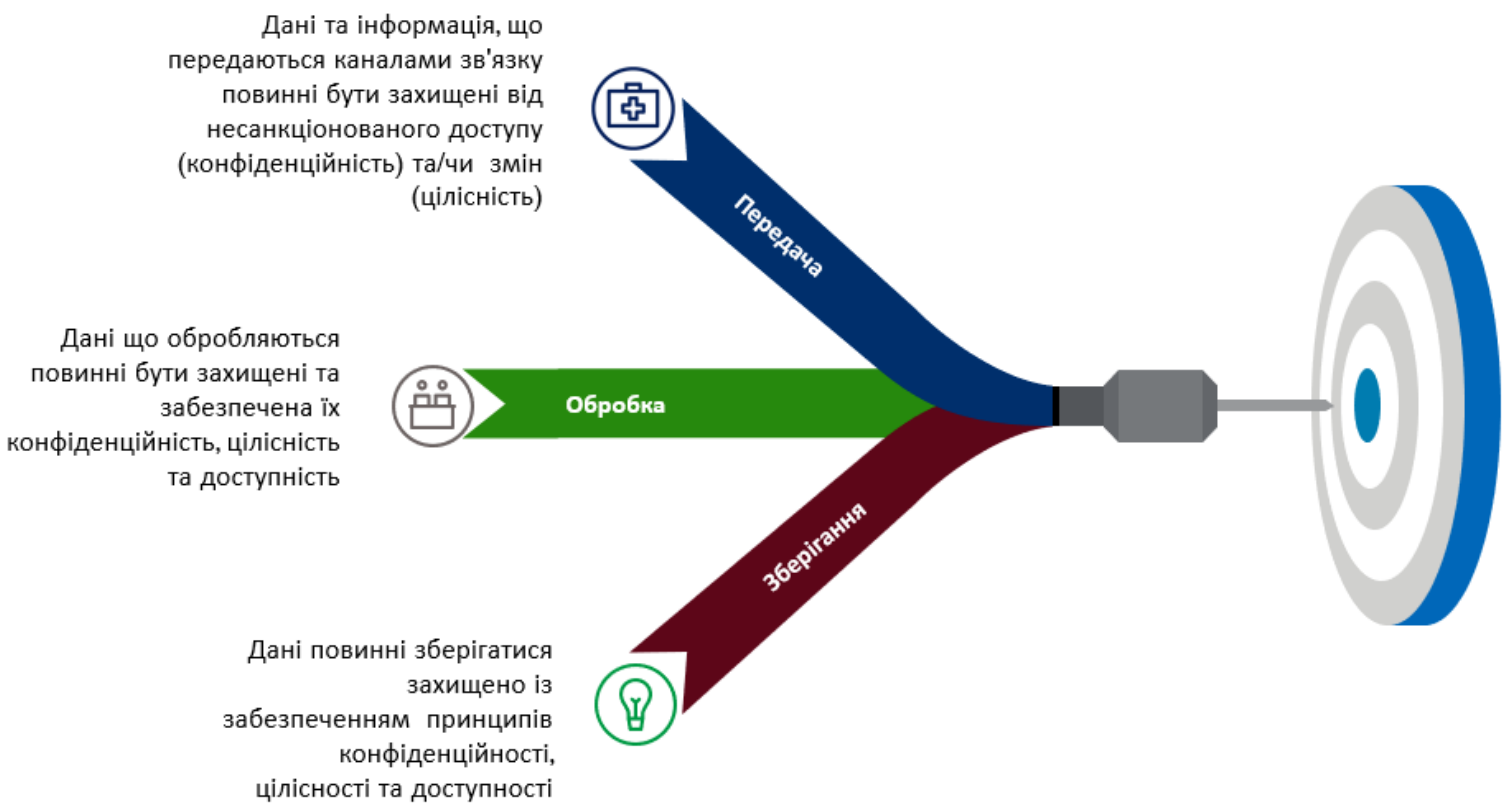
**Конфіденційність** – захист інформації від несанкціонованого доступу або розголошення.

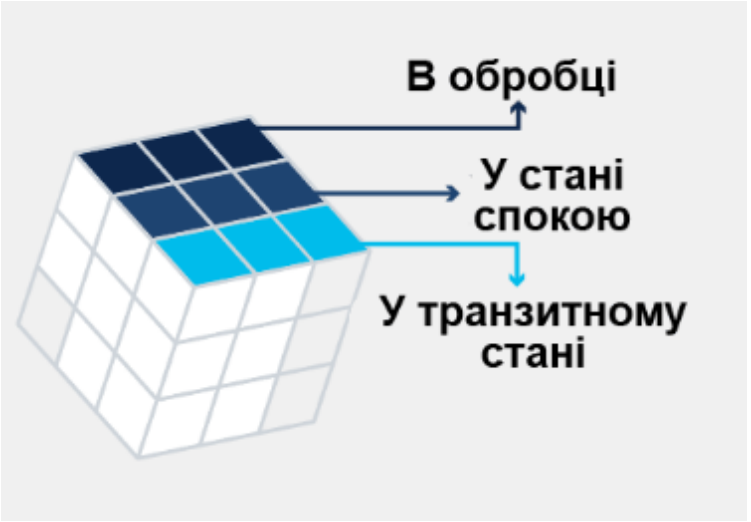




**Цілісність** – точність і повнота інформації відповідно до бізнес-цінностей і очікувань. Неможливість модифікації неавторизованим користувачем.

**Доступність** – можливість доступу до інформації та ресурсів, необхідних для підтримання безперервності бізнес-процесів.

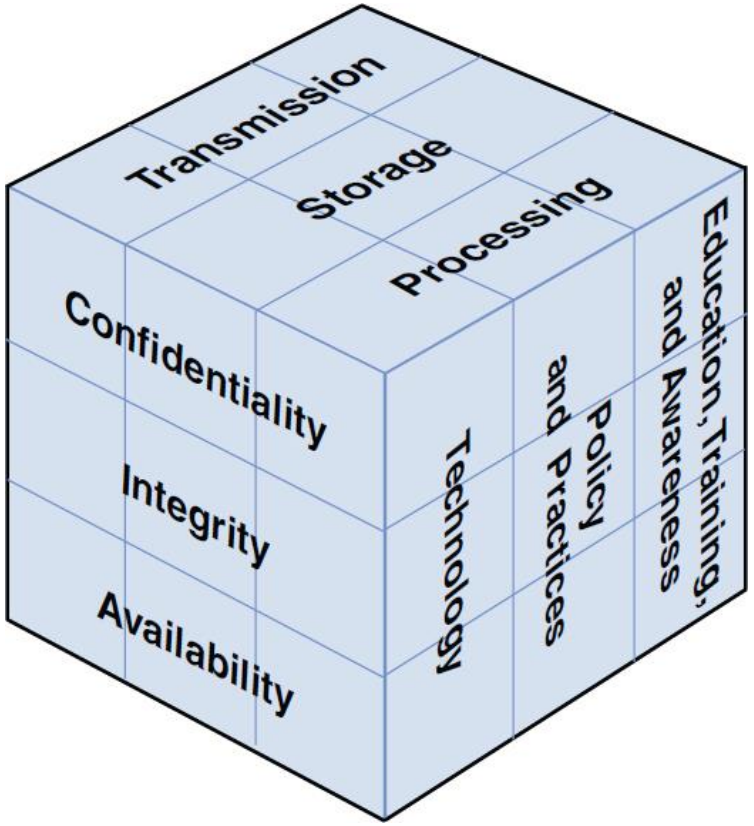
## Спостережність та контрольованість інформаційних систем

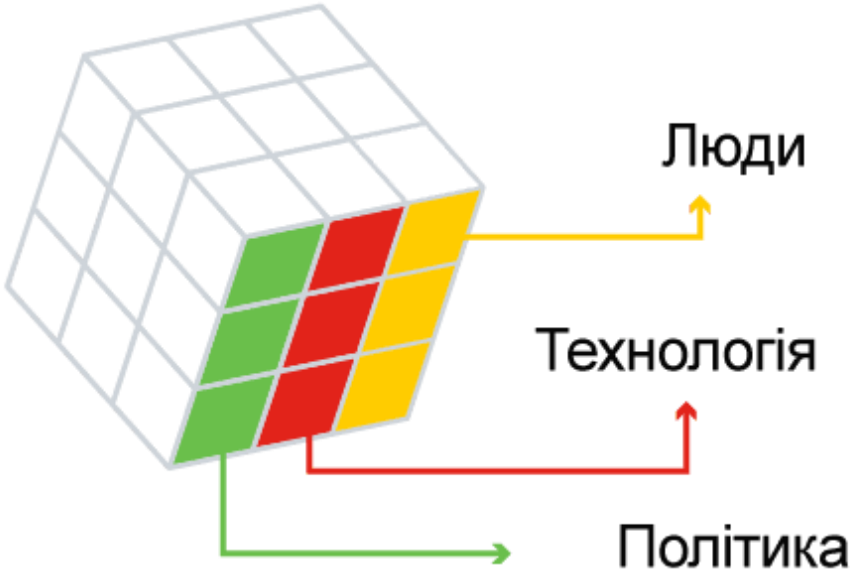


## Куб кібербезпеки та ризикоорієнтовний підхід з управління.

Система управління інформаційною безпекою (СУІБ) є частиною загальної системи Управління організацією, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики. СУІБ призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.



# Фреймворки кібербезпеки та аудиту інформаційних технологій

Стандарти ISO 2700X – серія стандартів, які використовуються для системи управління інформаційною безпекою (СУІБ) та є визначальними з точку зору розробки програм аудиту інформаційних технології:

- ISO/IEC 27000 містить терміни та визначення, які використовуються в серії стандартів ISO 2700X;
- ISO/IEC 27002 надає вказівки щодо впровадження засобів контролю, перелічених у Додатку A до стандарту ISO 27001. Він є дуже корисним, оскільки містить детальну інформацію про те, як запровадити систему контролю СУІБ;
- ISO/IEC 27004 надає рекомендації щодо вимірювання інформаційної безпеки – він добре підходить до ISO 27001, оскільки пояснює, як визначити, чи досягла СУІБ своїх цілей;
- ISO/IEC 27005 містить вимоги з управління ризиками інформаційної безпеки. Цей стандарт доповнює ISO 27001, оскільки дає детальну інформацію про те, як виконувати оцінку ризиків, як обробляти ризики, а також як ними керувати, що, безумовно, є найскладнішим у системі управління інформаційною безпекою;
- Global Technology Audit Guides створені Інститутом Внутрішніх Аудиторів для того, щоб своєчасно адресувати питання, пов'язані з управлінням, контролем і безпекою інформаційних технологій (IT). Серія GTAG служить готовим ресурсом для керівників аудиторських департаментів щодо різних технологічних ризиків і рекомендованих практик. (*Джерело: https://www.theiia.org/en/standards/2024-standards/global-guidance*).

# Фреймворки кібербезпеки та аудиту інформаційних технологій

**ПРАКТИЧНА**
**МЕТОДОЛОГІЯ**
**ІТ-АУДИТУ**

Практична методологія ІТ аудиту розроблена Міністерством фінансів України

# Домен II

## Захист доступу

### Модуль І. Безпека доступу

# Процес: Управління доступом

Рівень: початковий

Зона ризиків IT: Захист доступу

**Управління доступом** – це процес ідентифікації, відстеження, контролю та керування правами доступу користувачів до інформаційних систем та відповідних даних. Будь-який користувач, який запитує доступ до систем, додатків або даних, повинен бути ідентифікований, автентифікований, та авторизований.

Ризик і контроль

Процес управління доступом в організації, з відповідними контролями, **покликаний зменшити (мітигувати) ризик**, того, що користувачі мають привілеї доступу, що виходять за межі необхідних для виконання покладених на них обов'язків, що може призвести до неналежного розподілу обов'язків та зловживання відповідними правами.

Зона ризиків IT: Захист доступу

## Політика управління доступом

- **Політика управління доступом** має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.
  - **Ціль:** Обмежити та контролювати доступ до інформації та засобів оброблення інформації.
  - **Вимоги:** Власники ресурсів організації повинні визначити відповідні ролі щодо контролю доступу, прав доступу та обмеження ролей певних користувачів до ресурсів організації разом з детальними і суворими контролями, що відображають пов’язані ризики інформаційної безпеки.

**! Формалізований документ: Політика управління доступом**

Зона ризиків ІТ: Захист доступу

**Політика управління доступом** визначає:

- вимоги щодо безпеки доступу до окремих прикладних програм бізнесу та відповідних даних;
- політики щодо поширення інформації та відповідальність та методи класифікації інформації;
- несуперечливість прав доступу та політик класифікації інформації з різних систем та мереж;
- контрактні зобов'язання стосовно обмеження доступу до даних чи послуг;
- відокремлення правил контролю доступу, наприклад, запит доступу, санкціонування доступу, адміністрування доступу;
- вимоги щодо офіційного оформлення запитів на доступи та видалення прав доступу;
- вимоги щодо **періодичного перегляду прав доступу**;
- архівація записів усіх значущих подій, пов'язаних з використанням та управлінням ідентифікацією користувачів і таємною інформацією автентифікації;
- ролі з **привілейованими правами доступу**.

Зона ризиків IT: Захист доступу

## Політика управління доступом: додаткові вимоги

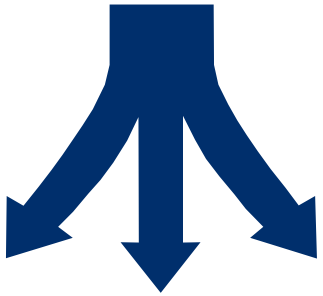
Обмеження доступу мають базуватися на вимогах конкретної прикладної програми бізнесу та відповідати **формалізованій політиці управління доступом**.

- Для підтримки вимог щодо обмеження доступу має бути розглянуто наступне:
  - доступ меню для контролю доступу до функцій прикладних систем;
  - контроль того, які дані можуть бути доступними для конкретного користувача;
  - контроль прав доступу користувачів, наприклад на зчитування, записування, видалення та виконання;
  - контроль прав доступу до інших прикладних програм;
  - обмеження інформації, що міститься у вихідних даних;
  - забезпечення контролю фізичного та логічного доступу для ізоляції чутливих прикладних програм, прикладних даних або систем.

Зона ризиків IT: Захист доступу

Правила контролю доступу потрібно підтримувати **формально визначеними процедурами і відповідальностями**.

**Два принципи, на яких часто основана політика управління доступом:**



**Матриця ролей та повноважень**

**Треба знати:** надано доступ лише до інформації, необхідної для виконання завдань (різні завдання/ролі потребують різну інформацію, до якої потрібно мати доступ, тобто різні профілі доступу).

**Треба використовувати:** надано доступ лише до засобів оброблення інформації (IT-обладнання, прикладних програм, процедур, зон безпеки, тощо), потрібних для виконання завдання/роботи/ролей та обов'язків.

Зона ризиків IT: Захист доступу

## I.I **Реєстрація та зняття з реєстрації користувача**

- **Ціль:** Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.
- **Вимога:** Має бути впроваджено **процес реєстрації** та зняття з реєстрації для того, щоб була можливість управляти правами доступу.

**Реєстрація та зняття з реєстрації користувача** покладається на:

- **отримання дозволу** від власника інформаційної системи чи послуги для використання інформаційної системи чи послуги;
- перевірку, що **рівень доступу наданий відповідно до політик доступу** та погоджений з іншими вимогами, такими як **розділення обов'язків**;
- гарантування, що права доступу не активовані (наприклад, сервіс-провайдером) до того, як процедури авторизації буде завершено;
- підтримки головного журналу прав доступу, наданих ID користувача для доступу до інформаційних систем чи послуг;
- зміна прав доступу користувачам, які змінили ролі чи роботу, та негайне вилучення чи блокування прав доступу користувачам, які звільнилися з організації;
- **періодичний перегляд прав доступу** разом із власниками інформаційних систем або послуг.

Зона ризиків IT: Захист доступу

## I.2 **Реєстрація та зняття з реєстрації користувача**

- Процес управління ідентифікаторами (IDs) користувача має включати:
  - використання унікальних ідентифікаторів (IDs), які дають змогу користувачам підключатися і нести відповідальність за свої дії;
  - використання групових ідентифікаторів (IDs) має бути затверджено та задокументовано і бути дозволено лише там, де це необхідно, з причин, обумовлених бізнесом або функціонуванням;
  - негайне блокування чи видалення прав доступу користувачів, які залишили організацію;
  - періодичну перевірку та видалення чи блокування зайвих ідентифікаторів (IDs) користувачів;
  - гарантування, що зайві ідентифікатори (IDs) користувачів не надають іншим користувачам.

Зона ризиків IT: Захист доступу

**Управління доступом: Базові концепти**

**Ідентифікація, автентифікація, авторизація**

Зона ризиків IT: Захист доступу

**Ідентифікація, автентифікація, авторизація**

- **Ідентифікація** – це процедура розпізнавання суб'єкта. Досягається за допомогою ідентифікатора користувача (наприклад, логін), ідентифікатора процесу тощо.
- **Автентифікація** визначає, що суб’єкт як володіє, так і контролює надані облікові дані (автентифікатори). Деякими прикладами облікових даних, які можна використовувати для підтвердження особи, є паролі, PIN-коди, цифрові підписи, біометричні дані тощо.
- **Авторизація** визначає рівень доступу суб’єкта до об’єкта. Іншими словами, авторизація перевіряє наявність прав для взаємодії з об'єктом.

Зона ризиків IT: Захист доступу

**Управління доступом: Базові концепти**

**Тестування дизайну контролю (1)**

- Як задумано та впроваджено?

**Тестування операційної ефективності контролю (2)**

- Як відпрацьовує?

**Мета тестування:** визначити рівень ефективності політики, а також, процесів та процедур управління доступом до систем та даних організації.

**Ціль:** Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.

Зона ризиків IT: Захист доступу

## I.3 Реєстрація та зняття з реєстрації користувача

**Політика управління доступом**

Відповідний контроль: **Керівництво затверджує характер та обсяг привілеїв доступу для нових користувачів, включаючи стандартні профілі/ролі додатків, критичні операції з фінансовою звітністю та розподіл обов'язків.**

Тестування **дизайну** контролю (1)

Тестування **операційної ефективності** контролю (2)

Зона ризиків IT: Захист доступу

## I.4 Реєстрація та зняття з реєстрації користувача

**Тестування дизайну контролю** 

Чи впроваджено контроль згідно формалізованих вимог?

Основні атрибути дизайну контролю:

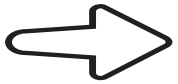
- політики;
- процедури виконання контролю;
- формалізовані вимоги до виконання контролю;
- відповідальні особи за виконання контролю.

**Оцінка дизайну контролю є здебільшого процес якісної оцінки (qualitative assessment process).**

Зона ризиків IT: Захист доступу

## I.5 Реєстрація та зняття з реєстрації користувача

**Тестування операційної ефективності контролю**



Чи відпрацьовує контроль згідно визначених цілей (мітигація\зменшення ризиків)?

Основні атрибути ОЕ контролю:

- розуміння цільової популяції;
- процедури тестування контролю;
- атрибути і критерії тестування контролю;
- результати, винятки та пов’язані ризики.

**Оцінка операційної ефективності контролю є здебільшого процес кількісної оцінки (quantitative assessment process).**

Зона ризиків IT: Захист доступу

## I.6 Реєстрація та зняття з реєстрації користувача

**Тестування ОЕ контролю**

**Дизайн контролю: формалізовані атрибути**

- політики та процедури виконання контролю;
- формалізовані вимоги до виконання контролю;
- відповідальні за виконання контролю особи.

**РЕЗУЛЬТАТ**

**ОЕ контролю: Фактори дизайну контролю**

- Ціль контролю по відношенню до ризику;
- Компетенції виконавців;
- Частота і послідовність;
- Агрегація та передбачуваність;
- Критерії та вимоги до розслідування відхилень.

Зона ризиків IT: Захист доступу

## I.7 Реєстрація та зняття з реєстрації користувача

Дизайн контролю: атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Зверніться до відповідальних осіб/груп, щоб зрозуміти процес, у якому запрошується та затверджується новий доступ чи виконується зміна доступу (модифікація). Зокрема, розгляньте можливість отримати розуміння наступних атрибутів, якщо це доречно: | | |
| Політики та процедури, пов'язані з наданням доступу користувачам. | | |
| Особи або групи, відповідальні за затвердження доступу. | | |
| Окремі особи або групи, відповідальні за адміністрування доступу. | | |
| Як подаються, затверджуються та документуються запити на доступ користувачів? | | |
| Чи використовується інструмент для надання нового доступу та як цей інструмент контролюється? | | |
| Визначте, чи існує розподіл обов'язків між особою, яка затверджує, та особою, яка надає доступ до систем? | | |
| Чи існують різні процеси для надання доступу особам, які не є працівниками (постачальники, підрядники)? | | |
| Наявні процеси, пов'язані з розподілом обов'язків під час надання чи відкликання доступів? | | |

Зона ризиків IT: Захист доступу

## I.8 Реєстрація та зняття з реєстрації користувача

Операційна ефективність контролю: атрибути перевірки

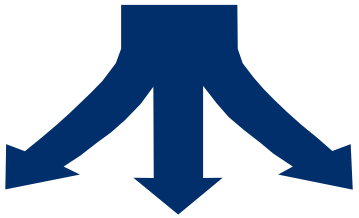
| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Отримайте популяцію нових запитів на доступ і модифікацію доступів існуючих користувачів протягом періоду аудиту. Зробіть вибір нових і змінених користувачів і перевірте наступні атрибути: | | |
| Запит на доступ користувача схвалено відповідними особами? | | |
| Запитуваний доступ узгоджується з доступом, наданим у системі? | | |
| Наданий доступ відповідає обов’язкам, призначеним користувачам, і забезпечує належний розподіл обов’язків? | | |
| Під час перевірки цього атрибута, потрібно враховувати привілеї/повноваження, надані ролі, щоб оцінити, чи роль належним чином забезпечує розподіл обов’язків для виконання критичних повноважень? | | |
| Розподіл обов'язків підтримується між тим, хто затверджує, і особою, яка надає доступ до системи? | | |

Зона ризиків IT: Захист доступу

## 2.1 Зняття з реєстрації користувача

**Політика управління доступом**

Відповідний контроль: **Доступ для звільнених та/або переведених користувачів своєчасно видаляється або змінюється (модифікується).**



Тестування **дизайну** контролю (1)

Тестування **операційної ефективності** контролю (2)

Зона ризиків IT: Захист доступу

## 2.2 Зняття з реєстрації користувача

Дизайн контролю: атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Зверніться до відповідальних осіб/груп, щоб зрозуміти елементи керування, пов'язані з видаленням доступу до програми для звільнених користувачів, або користувачів, чиї права були модифіковані. Зокрема, розгляньте можливість отримати розуміння наступних атрибутів, якщо це доречно: | | |
| Політики або процедури, пов'язані зі зняттям з реєстрації користувачів\відкликанням доступів. | | |
| Механізм інформування IT-менеджменту про відкликання чи зміну прав користувачів. | | |
| Як доступ змінюється або регулюється після припинення або передачі та, чи використовується той самий процес для штатних та нештатних працівників (таких як постачальники, підрядники тощо)? | | |
| Чи процес видалення доступу є ручним чи автоматизованим? | | |
| Чи використовується інструмент для відкликання доступу? | | |
| Спосіб припинення доступу до програм та систем (наприклад, заблокувати або видалити)? | | |
| Хто несе відповідальність за адміністрування безпеки та зміну доступу користувачів у разі звільнення чи переведення (зміни статусу працівника)? | | |
| Якими є очікування щодо своєчасного скасування доступу користувача? | | |

Зона ризиків IT: Захист доступу

## 2.3 Зняття з реєстрації користувача

**Операційна ефективність контролю: атрибути перевірки**

Отримайте від відділу кадрів повний список звільнених (чи переведених) співробітників і підрядників на період аудиторської перевірки. Виходячи з частоти та ризику, пов'язаного з контролем, зробіть вибірку користувачів, доступи яких було припинено (знято з реєстрації). Для кожного вибраного користувача перевірте такі атрибути та надайте висновок щодо ефективності контролю:

- ✓ *Права доступу для припиненого користувача більше не активні в системі. Такий доступ було видалено або заблоковано своєчасно (на основі дати припинення повноважень).*

Зона ризиків IT: Захист доступу

## 2.4 Реєстрація та зняття з реєстрації користувача: привілейовані права

**Ціль:** Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг. Призначення та використання привілейованих прав доступу має бути обмежено та контрольовано.

**Вимога:** Призначення привілейованих прав доступу потрібно контролювати за допомогою формального процесу надання доступів відповідно до визначеної політики контролю доступу.

**Ключові положення:**

- має бути ідентифіковано привілейовані права доступу, пов'язані з кожною системою чи послугою, наприклад, операційною системою, системою управління базами даних і кожною прикладною програмою та користувачами, до яких вони потребують доступу;
- привілейовані права доступу має бути призначено користувачам на основі необхідності використання згідно з політикою контролю доступу, тобто повноваження призначають на рівні мінімальних вимог їх функціональних ролей;
- потрібно підтримувати процеси перегляду всіх призначених привілейованих ролей. Привілейовані права доступу не потрібно надавати до завершення процесу перевірки на надання доступу;
- привілейовані права доступу потрібно призначати ідентифікаторам (IDs) користувача, які відрізняються від тих, що використовуються для регулярної бізнес-діяльності. Регулярна бізнес-діяльність не повинна здійснюватися від імені привілейованих ID.

Зона ризиків IT: Захист доступу

## 2.5 Реєстрація та зняття з реєстрації користувача: привілейовані права

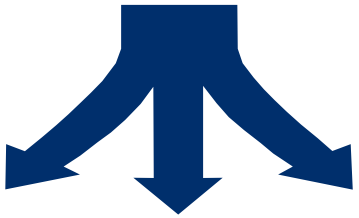
- компетенцію користувачів з привілейованими правами доступу треба регулярно переглядати для впевненості в тому, що вони відповідають своїм обов'язкам;
- має бути розроблено та впроваджено спеціальні процедури для уникнення несанкціонованого використання загальних адміністративних IDs користувача згідно з можливостями конфігурації систем;
- для загальних адміністративних IDs користувача потрібно підтримувати конфіденційність таємної інформації автентифікації під час загального використання (наприклад, часта зміна паролів і одразу, коли привілейований користувач звільняється чи змінює роботу, розповсюджуючи їх між привілейованими користувачами за допомогою відповідних механізмів).

Зона ризиків IT: Захист доступу

## 2.6 Реєстрація користувача: привілейовані права

**Політика управління доступом**

Відповідний контроль: **Доступ привілейованого рівня (наприклад, адміністратори безпеки) авторизований і відповідним чином обмежений.**



Тестування **дизайну** контролю (1)

Тестування **операційної ефективності** контролю (2)

Зона ризиків IT: Захист доступу

## 2.7 Реєстрація користувача: привілейовані права

**Дизайн контролю:** атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Визначте засоби контролю, пов'язані з доступом привілейованого рівня. Зокрема, розгляньте можливість отримати розуміння наступних атрибутів, якщо це доречно: | | |
| Політики, пов'язані з інформаційною безпекою та захистом привілейованого рівня доступу? | | |
| Організаційна структура функції управління безпекою? | | |
| Опис профілів користувачів, яким призначено привілейований рівень доступу? | | |
| Особи, які мають право використовувати привілейований рівень доступу? | | |
| Визначте, що особи, яким призначено привілейований доступ, не мають суперечливих привілеїв, які призводять до конфлікту розподілу обов'язків (тобто привілеї адміністратора безпеки не надано бізнес-користувачам)? | | |
| Профілі зовнішніх користувачів, наприклад профілі постачальників систем, консультантів або профілі «екстрених» користувачів із привілейованим рівнем доступу? | | |
| Перевіте надані матеріали (докази), щоб підтвердити структуру контролю, наприклад, перевірте одного користувача, якому було призначено привілейований доступ, і визначте, що доступ відповідає посадовим обов'язкам користувача. | | |

Зона ризиків IT: Захист доступу

## 2.8 Реєстрація користувача: привілейовані права

**Операційна ефективність контролю:** атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Отримайте повний список користувачів, які мають привілейований рівень доступу (адміністратори). Для кожного ідентифікованого облікового запису перевірте такі атрибути: | | |
| Права доступу відповідають призначеним користувачам обов'язкам? | | |
| Права доступу відповідають призначеним користувачам обов'язкам на основі перевірки посадових обов'язків (включіть посилання на підтверджувальне джерело, наприклад організаційну схему)? | | |
| Загальні облікові записи вимагають доступу на основі потреб бізнесу, і доступ до облікових записів належним чином обмежується та контролюється? | | |

Зона ризиків IT: Захист доступу

## 3.1 Перегляд прав доступу користувачів

- **Ціль:** Забезпечити відповідний доступ користувача і запобігти несанкціонованому доступу до систем та послуг, а також визначити рівень ефективності політики, процесів та процедур управління доступом до систем та даних організації.
- **Вимога:** Має бути впроваджено **формально затверджений процес перегляду прав доступу користувачів** через регулярно встановлені інтервали часу.

Зона ризиків IT: Захист доступу

## 3.2 Перегляд прав доступу користувачів

**Політика управління доступом**

Відповідний контроль: **Доступ користувачів періодично переглядається.**

Тестування **дизайну** контролю (1)

Тестування **операційної ефективності** контролю (2)

Зона ризиків IT: Захист доступу

## 3.3 Перегляд прав доступу користувачів

**Дизайн контролю:** атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Визначте, чи права доступу користувача переглядаються через суворо дотримувані інтервали часу і після будь-яких змін, таких як зміна посади, або припинення найму. | | |
| Права доступу користувача потрібно переглядати та модифікувати у разі переходу з однієї посади на іншу в межах тієї самої організації. | | |
| Санкцію на певні привілейовані права доступу потрібно переглядати через частіші інтервали. | | |
| Призначення привілейованих прав доступу потрібно перевіряти через суворо дотримувані інтервали часу для забезпечення того, щоб не було отримано несанкціонованих привілеїв. | | |
| Зміни до привілейованих облікових записів потрібно реєструвати для періодичного перегляду. | | |

Зона ризиків IT: Захист доступу

## 3.4 Перегляд прав доступу користувачів

**Операційна ефективність контролю:** атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| Виконайте запити до керівництва, відповідального за виконання контролю перегляду доступу користувачів, і отримайте докази того, що керівництво встановило механізм виконання процесу. Механізм виконання процесу може включати повторне виконання та/або перевірку документації по процесу, щоб переконатися в наступному: | | |
| Перегляд доступу користувачів включав повну та точну популяцію користувачів. | | |
| Перегляд було належним чином задокументовано та виконано з відповідним рівнем деталізації, щоб переконатися, що доступ відповідав поточним посадовим обов’язкам кожного користувача. | | |
| Перегляд проводився відповідним управлінським персоналом із належним розподілом обов'язків. | | |
| Доступ до системи було своєчасно належним чином змінено для користувачів, позначених як винятки під час перевірки. | | |

Зона ризиків IT: Захист доступу

**Формалізований документ: Парольні вимоги**

## Управління паролем користувача

Політика паролів – це набір правил і вимог, що регулюють створення, використання та управління паролями в організації з метою забезпечення безпеки інформаційних систем і даних. Політика паролів має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.

**Ціль процесу:**

- **Забезпечення конфіденційності та цілісності даних**: паролі є ключовим механізмом автентифікації, який допомагає захистити дані від доступу неавторизованих користувачів.
- **Мінімізація ризиків безпеки**: належне управління паролями знижує ризик компрометації облікових записів через зламані або викрадені паролі.
- **Забезпечення відповідності нормативним вимогам:** відповідність вимогам законодавства, стандартів і внутрішніх політик щодо інформаційної безпеки.

**Вимоги**:

- **Створення Паролів**: забезпечення стійкості паролів до злому та захисту від несанкціонованого доступу.
- **Використання Паролів**: забезпечення регулярного оновлення паролів та їх захисту від несанкціонованого доступу.
- **Управління Паролями**: встановлення та підтримку політик для забезпечення безпечного використання паролів.

**Опис ризику**: несанкціонований доступ до облікових записів користувачів, що може бути наслідком витоку конфіденційної інформації, поширення шкідливого ПЗ, знищення або маніпуляція з даними.

Зона ризиків IT: Захист доступу

## Управління паролем користувача

- **Політики паролів**: Розробка та впровадження політик, які чітко визначають вимоги до паролів, такі як мінімальна довжина, складність, частота зміни та заборона повторного використання.
- **Засоби створення паролів**: Використання програмного забезпечення для адміністрування та управління паролями користувачів.
- **Захист паролів**: Застосування методів захисту паролів, таких як шифрування та хешування, для запобігання несанкціонованому доступу.
- **Навчання користувачів**: Проведення навчання користувачів щодо важливості сильних паролів та безпечних практик використання паролів.
- **Моніторинг**: Моніторинг систем та облікових записів користувачів на наявність підозрілої активності, пов'язаної з паролями.

Зона ризиків IT: Захист доступу

## Створення паролів

- **Мінімальна довжина пароля:**

Паролі з більшою кількістю символів є більш стійкими до атак методом перебору (brute-force attacks). Кожен додатковий символ значно збільшує кількість можливих комбінацій.

*Відповідно до кращих практик рекомендується використовувати паролі з мінімальною довжиною 8-12 символів. Довші паролі є більш безпечними, але можуть бути менш зручними для користувачів.*

- **Складність пароля:**

Використання різних типів символів (великі і малі літери, цифри, спеціальні символи) значно підвищує складність пароля, роблячи його більш стійким до атак типу "словниковий підбір" (dictionary attacks).

*Відповідно до кращих практик паролі повинні включати в себе комбінації різних типів символів, наприклад, "2O2GhFbBK!" або "A1b2C3d4!%)".*

Зона ризиків IT: Захист доступу

## Створення паролів

- **Унікальність пароля**

Використання унікальних паролів для кожного облікового запису зменшує ризик компрометації інших облікових записів у разі, якщо один пароль буде зламано.

*Відповідно до кращих практик користувачі повинні уникати використання однакових паролів для різних сервісів або облікових записів.*

- **Складновідгадуваність**

Паролі повинні бути такими, що їх складно вгадати, включаючи випадкові або псевдовипадкові символи, а не звичайні слова або фрази.

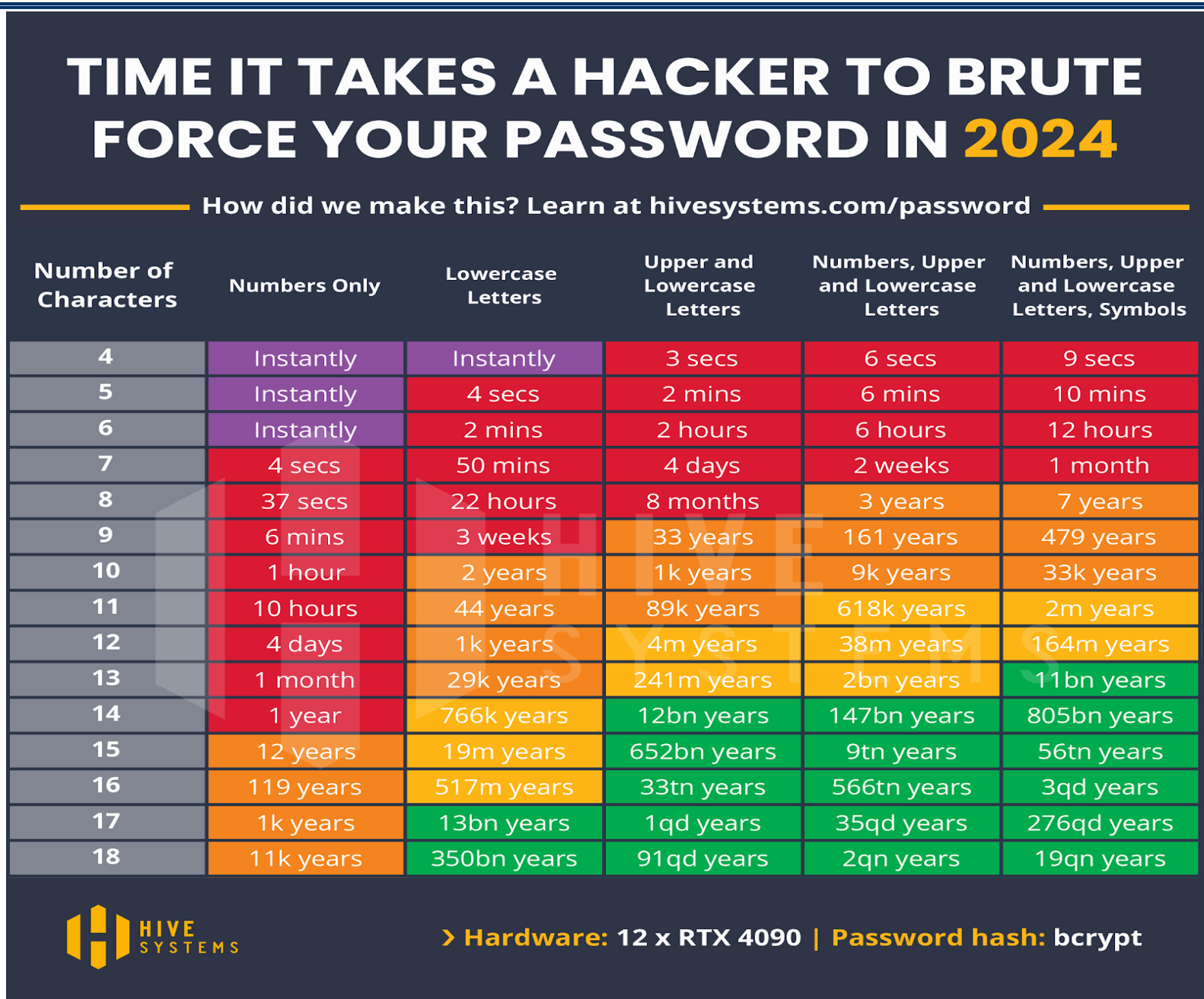
*Відповідно до кращих практик користувачам рекомендується уникати використання загальновідомих слів, імен, дати народження та інших легко передбачуваних даних.*

Для перевірки належного рівня безпеки паролів можна скористатися ресурсом для генерації та оцінки паролів.
Для перевірки факту злому облікового запису можна скористатися ресурсом для перевірки цілісності облікового запису.

Зона ризиків IT: Захист доступу

## Створення паролів

Найбільші міжнародні компанії, що спеціалізуються на кібербезпеці, щорічно проводять дослідження безпеки паролів на основі статистичних даних, що показують мінімальний час, який потрібен хакерам, щоб підібрати пароль.



# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | 3 secs | 6 secs | 9 secs |
| 5 | Instantly | 4 secs | 2 mins | 6 mins | 10 mins |
| 6 | Instantly | 2 mins | 2 hours | 6 hours | 12 hours |
| 7 | 4 secs | 50 mins | 4 days | 2 weeks | 1 month |
| 8 | 37 secs | 22 hours | 8 months | 3 years | 7 years |
| 9 | 6 mins | 3 weeks | 33 years | 161 years | 479 years |
| 10 | 1 hour | 2 years | 1k years | 9k years | 33k years |
| 11 | 10 hours | 44 years | 89k years | 618k years | 2m years |
| 12 | 4 days | 1k years | 4m years | 38m years | 164m years |
| 13 | 1 month | 29k years | 241m years | 2bn years | 11bn years |
| 14 | 1 year | 766k years | 12bn years | 147bn years | 805bn years |
| 15 | 12 years | 19m years | 652bn years | 9tn years | 56tn years |
| 16 | 119 years | 517m years | 33tn years | 566tn years | 3qd years |
| 17 | 1k years | 13bn years | 1qd years | 35qd years | 276qd years |
| 18 | 11k years | 350bn years | 91qd years | 2qn years | 19qn years |

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

Зона ризиків IT: Захист доступу

## Управління паролями

Управління паролями включає встановлення, впровадження та підтримку політик і процедур, що забезпечують надійний захист паролів на всіх етапах їхнього життєвого циклу. Нижче наведені кращі практики управління паролями:

- У випадку коли від користувачів вимагають підтримки їх власних паролів, їм треба спочатку надати безпечний тимчасовий пароль, який їх примушують негайно замінити;
- Встановлення процедур верифікації особи користувача до надання нового, заміненого або тимчасового пароля;
- Тимчасові паролі повинні надаватися користувачам у безпечний спосіб; треба уникати залучення третіх сторін або використання незахищених (відкритий текст) повідомлень електронної пошти;
- Користувачі повинні підтвердити отримання пароля;
- Паролі не повинні ніколи зберігатися в комп'ютерній системі у незахищеному вигляді.

Зона ризиків IT: Захист доступу

## Використання паролів

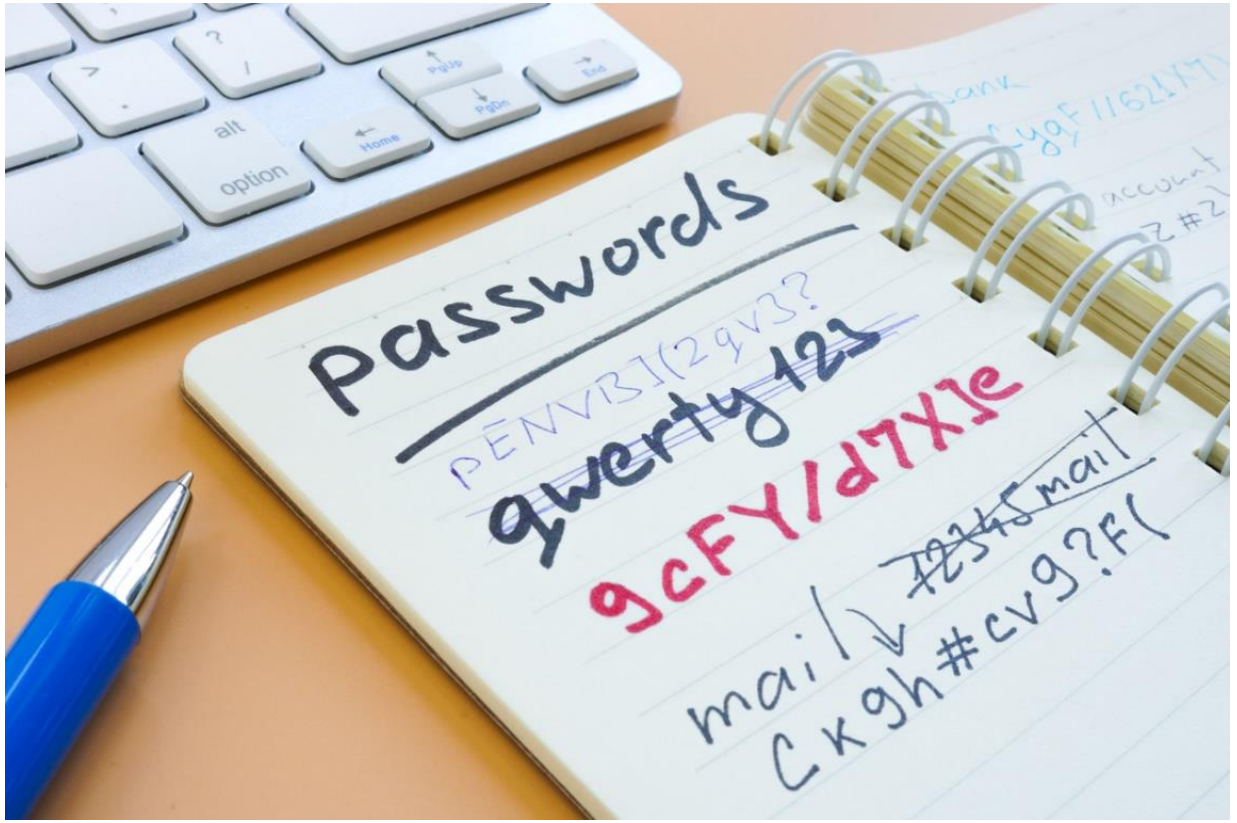
Використання паролів - це процес, що включає створення, зберігання, зміну та управління паролями з метою забезпечення безпеки облікових записів та доступу до систем.

Повинна існувати чітка Політика використання паролів, відповідно до якої усі користувачі повинні бути сповіщені щодо:

1) збереження конфіденційності паролів;

2) уникнення зберігання запису паролів (наприклад, на папері, у файлі програмного забезпечення або у портативному пристрої) доти, доки вони не будуть зберігатися безпечно і спосіб збереження не буде затверджений;

3) зміни паролів кожного разу, коли є якась ознака можливої компрометації системи або пароля;



Зона ризиків ІТ: Захист доступу

**Використання паролів**

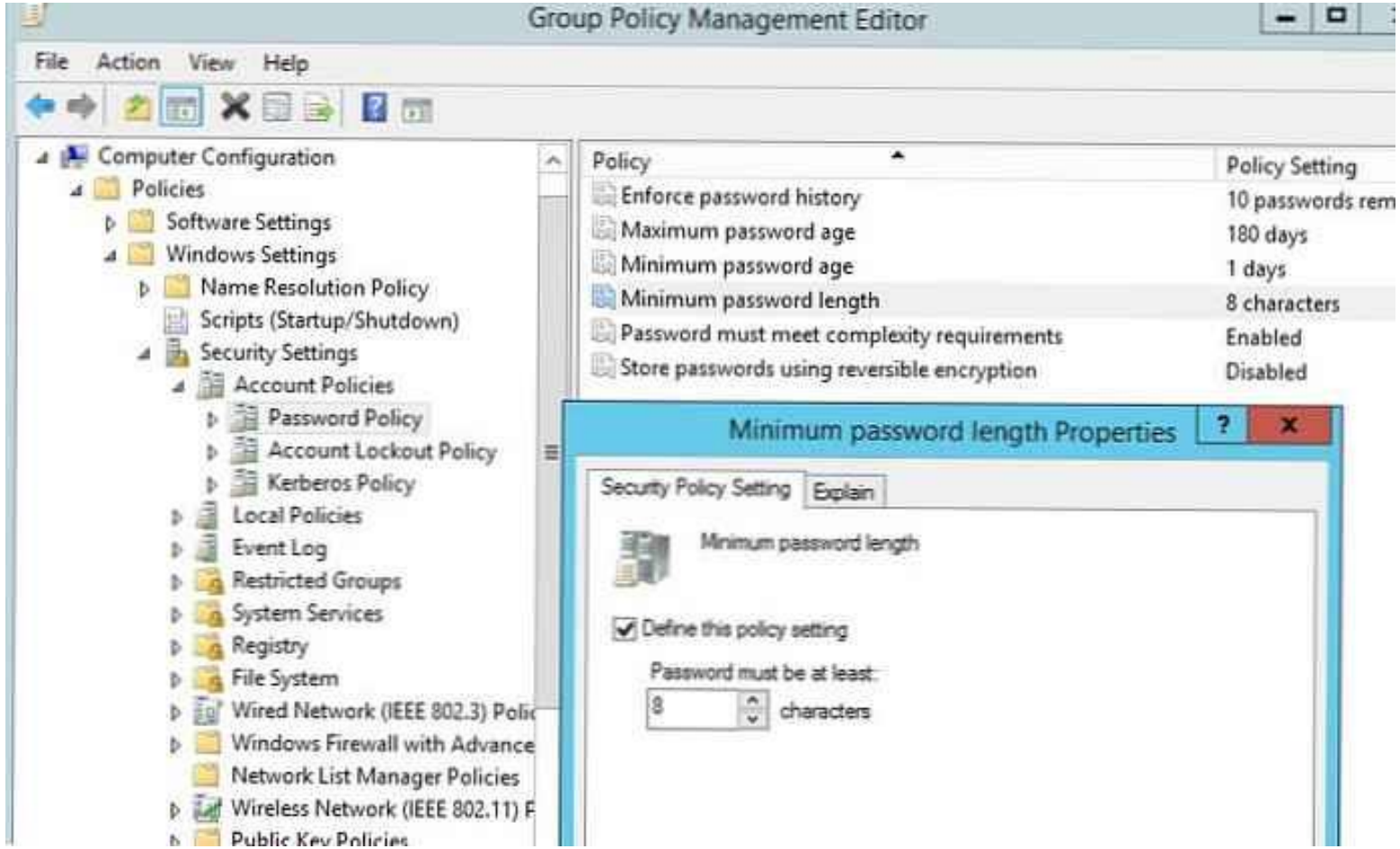
4) вибору якісних паролів з обґрунтовано мінімальною довжиною, які:

- легкі для запам'ятовування;
- не базуються на чомусь, про що будь-хто інший може легко здогадатися або отримати, використовуючи особисту інформацію, наприклад, імена, телефонні номери, дати народження тощо;
- не уразливі до словникових атак (тобто не складаються з слів, що містяться в словниках);
- не мають послідовності однакових тільки цифрових або тільки абеткових символів;
- зміни тимчасових паролів при першій реєстрації;
- зміни паролів через суворо дотримувані інтервали часу та уникнення повторного використання або циклічного використання старих паролів;
- не включення паролів у будь-які автоматизовані процеси реєстрації, наприклад, збережені за допомогою макросу або функціональної клавіші;
- спільно не використовувати індивідуальні паролі користувача;
- не використовувати той самий пароль для бізнес і не бізнес цілей.

Зона ризиків IT: Захист доступу

## Система управління паролями

Користувачі ПК, самі ПК, та й будь-який фізичні ресурси, вимагають суворої ієрархії. Тому, першочергове завдання будь-якого системного адміністратора – це правильна ієрархічна організація мережі всередині компанії. Саме для цих цілей, застосовується технологія компанії Майкрософт Active Directory (AD).



Зона ризиків IT: Захист доступу

## Налаштування Політики паролів в AD

**Застосування історії паролів (Enforce password history)** – визначає кількість старих паролів, які зберігаються в AD, забороняючи користувачеві повторно використовувати один і той самий пароль.

**Максимальний термін дії пароля (Maximum password age)** – визначає термін дії пароля в днях. Після закінчення цього терміну система змусить користувача змінити пароль. Забезпечує регулярність зміни пароля користувачами.

**Мінімальний термін дії пароля (Minimum password age)** – це встановлений період часу, протягом якого користувач не може змінити свій пароль після його останньої зміни. Цей контроль запобігає надмірно частій зміні паролів, що може знижувати їхню ефективність та безпеку.

**Мінімальна довжина паролів (Minimum password length)** – визначає найменшу кількість символів, яка повинна бути в паролі, щоб він вважався безпечним (якщо вказано тут 0 - значить пароль не є обов'язковим).

**Пароль повинен відповідати вимогам складності (Password must meet complexity requirements)** – при включенні цього налаштування користувачеві заборонено використовувати ім'я свого облікового запису в паролі, також в паролі повинні використовуватися 3 типи символів з наступного списку: цифри (0 - 9), символи в верхньому регістрі (A-Z), символи в нижньому регістрі (a-z), спец символи ($, #,%, тощо). Крім того, застосовуються виключення використання простих паролів (зі словника популярних паролів), що повинен оновлюватися на періодичній основі.

**Зберігати паролі, використовуючи оборотне шифрування (Store passwords using reversible encryption)** – паролі користувачів в базі AD зберігаються в зашифрованому вигляді, але в деяких випадках додаткам потрібно надати доступ до паролів в домені. При включенні цієї політики паролі зберігаються в менш захищеному вигляді (по суті відкритому вигляді), що небезпечно.

Зона ризиків IT: Захист доступу

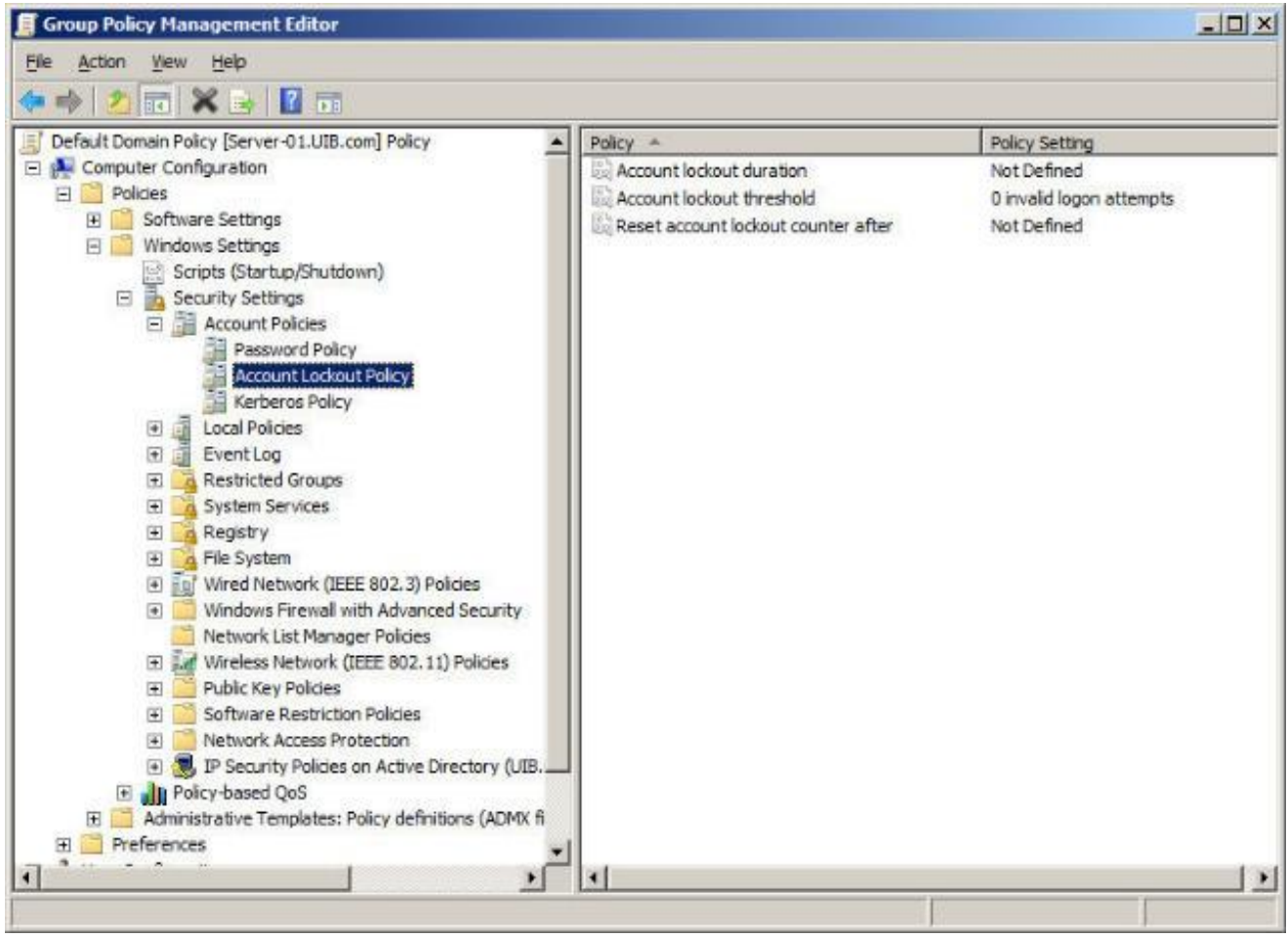
## Налаштування Політики блокування облікового запису в AD

Потрібно окремо виділити налаштування Політики блокування облікового запису (Account Lockout Policy):

**Граничне значення блокування (Account Lockout Threshold)** – кількість спроб введення невірного пароля, які може зробити користувач перед тим, як його обліковий запис буде заблокований. Рекомендоване значення для цього параметру 0, для того щоб облікові записи не були заблоковані при невірно введених паролях.

**Тривалість блокування облікового запису (Account Lockout Duration)** – на який час потрібно блокувати обліковий запис (заборонити вхід), якщо користувач ввів задану кількість разів невірний пароль. Рекомендоване значення 15 хв.

**Час до скидання лічильника блокування (Reset account lockout counter after)** – це період, після якого лічильник невдалих спроб входу обнулиться, якщо користувач не здійснив нових спроб входу протягом цього часу. Рекомендований час до скидання лічильника блокування становить від 5 хвилин до 1 години. Це дає користувачам можливість виправити свої помилки без ризику постійного блокування облікового запису.



Зона ризиків IT: Захист доступу

## Система управління паролем

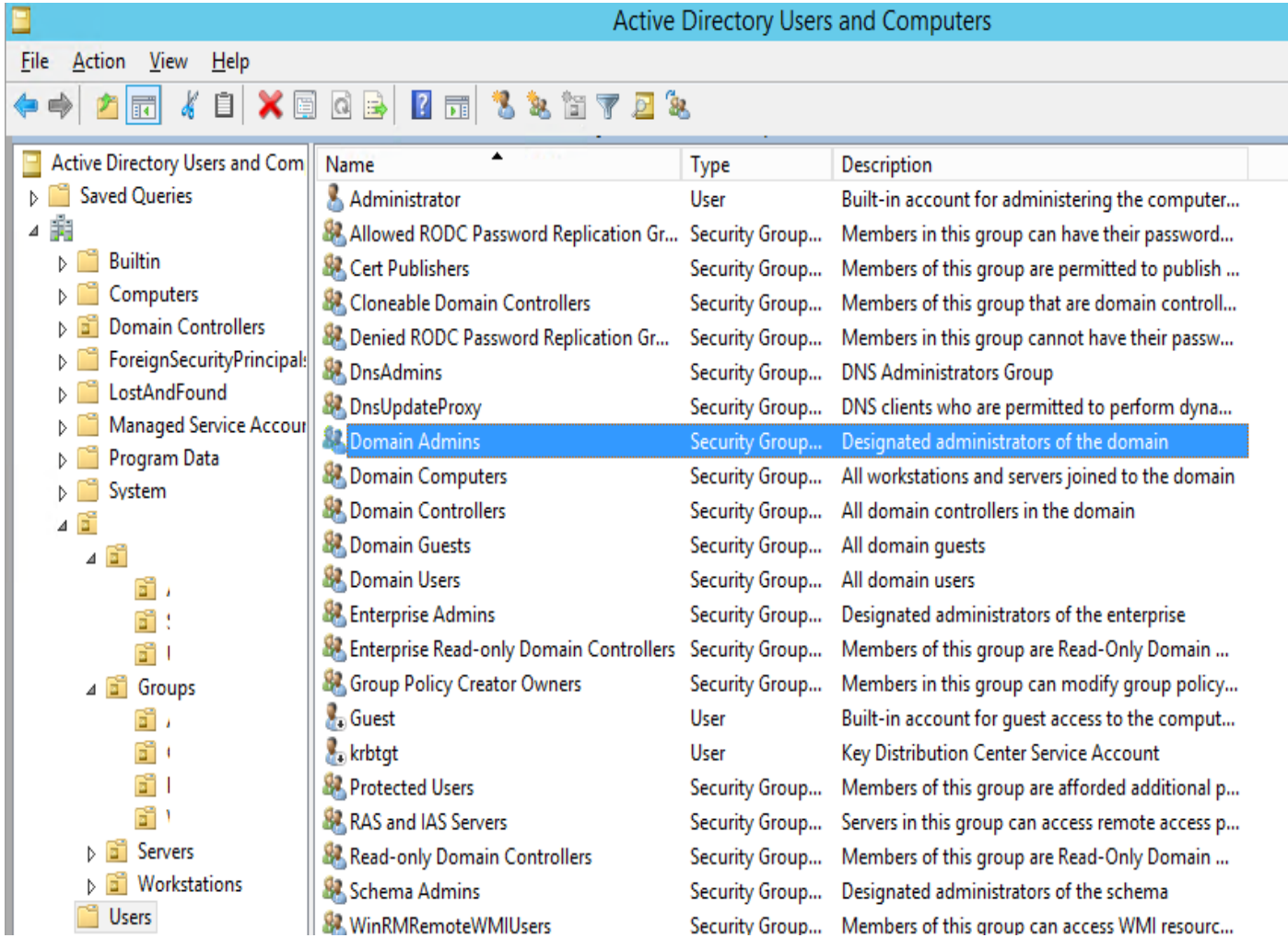
Система управління паролем повинна:

- для підтримки відстежуваності змушувати до використання індивідуальних ідентифікаторів користувача (IDs) та паролів;
- дозволяти користувачам вибирати та змінювати свої власні паролі, а також містити процедуру підтвердження на введення поправок помилкового вводу;
- змушувати вибирати якісні паролі;
- змушувати до зміни паролів;
- примушувати користувачів змінювати тимчасові паролі при першій реєстрації;
- підтримувати запис попередніх паролів користувача і перешкоджати повторному їх використанню;
- не виводити паролі на екран при їх введенні;
- зберігати файли паролів окремо від системних даних прикладних програм;
- зберігати та передавати паролі в захищеній (наприклад, зашифрованій або хешованій) формі.

Зона ризиків IT: Захист доступу

## Ідентифікація, автентифікація, авторизація

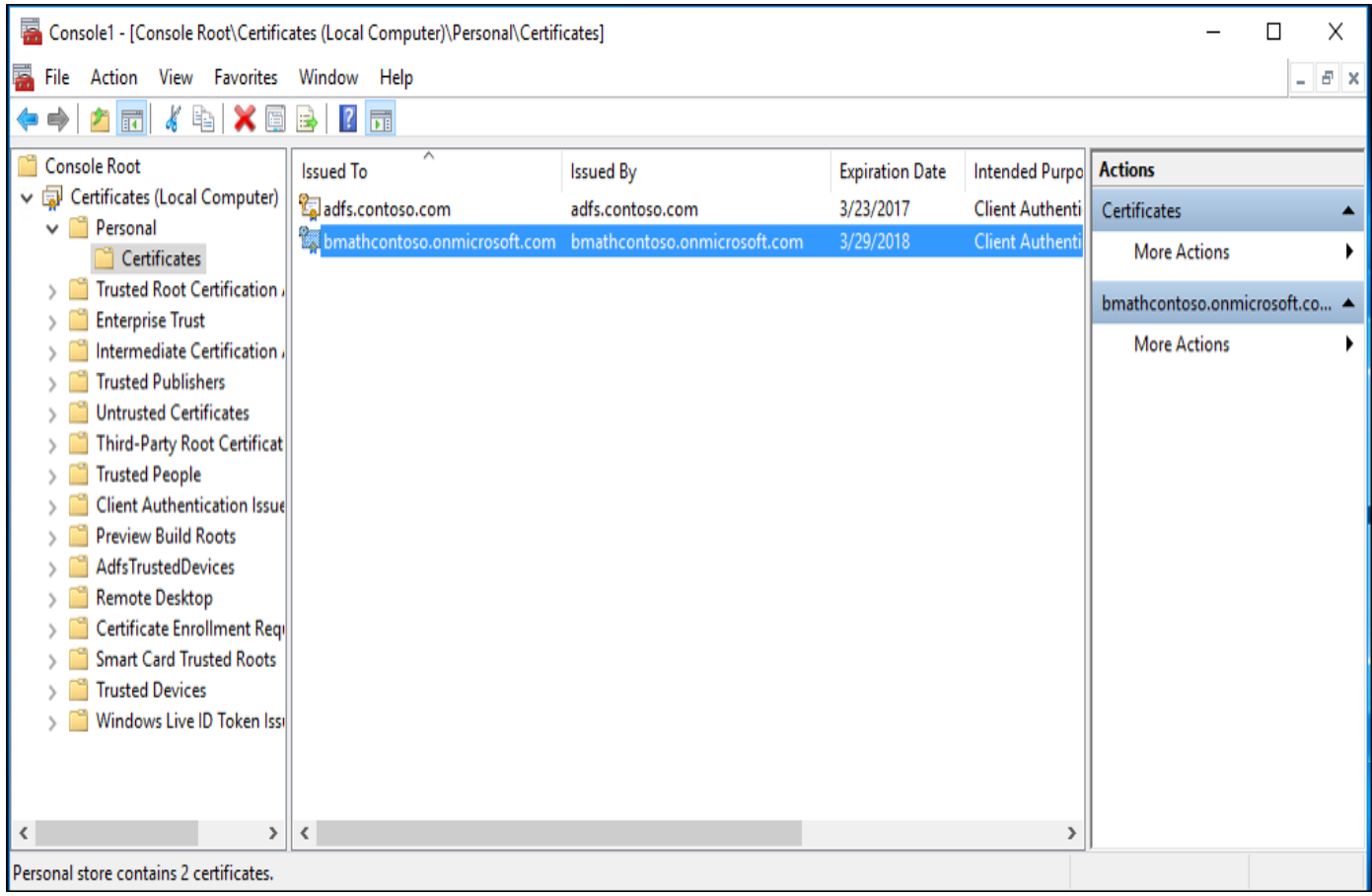
- Всі користувачі повинні мати унікальний ідентифікатор (ID) тільки для свого персонального використання та повинна бути вибрана придатна методика автентифікації для підтвердження заявленої ідентичності користувача. Цей контроль повинен застосовуватися до всіх категорій користувачів (в тому числі персоналу технічного обслуговування, операторів, адміністраторів мережі, системних програмістів і адміністраторів баз даних).
- Звичайна діяльність користувача не повинна здійснюватися з привілейованих облікових записів.
- У надзвичайних випадках, коли від цього є явні переваги, можна застосовувати спільний ідентифікатор користувача (ID) для групи користувачів. У таких випадках повинне бути задокументоване погодження від керівництва.
- Кожна з груп повинна мати опис свого призначення та властивостей.



Зона ризиків IT: Захист доступу

## Ідентифікація, автентифікація, авторизація

- Загальні ідентифікатори для індивідуального використання можуть бути дозволені лише, якщо доступні функції або виконувані за допомогою ідентифікатора дії не потребують відстежування (наприклад, доступ тільки на читання) або якщо застосовано інші контролі (наприклад, пароль для загального ідентифікатора видається одночасно тільки одній особі і це реєструється).
- Там, де потрібна сувора автентифікація та верифікація особи, повинні використовуватися методи, альтернативні паролю, такі як криптографічні засоби, смарт-картки, токени або біометричні засоби (багатофакторна автентифікація MFA).
- Суворість ідентифікації та автентифікації користувача повинна відповідати чутливості інформації, до якої потрібний доступ.



Зона ризиків IT: Захист доступу

## Управління паролем користувача

### Політика управління доступом

Відповідний контроль: **Доступ автентифікується за допомогою унікальних ідентифікаторів користувачів і паролів або інших методів як механізм перевірки того, що користувачі мають право отримати доступ до системи. Параметри пароля відповідають стандартам компанії та/або галузі (наприклад, мінімальна довжина та складність пароля, термін дії, блокування облікового запису).**

**Тестування дизайну контролю**

**Тестування операційної ефективності контролю**

Зона ризиків IT: Захист доступу

## Дизайн контролю: атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| I. Зверніться до керівництва, щоб зрозуміти елементи керування автентифікацією (наприклад, мінімальна довжина пароля, складність, термін дії та блокування облікового запису), що стосуються облікових записів користувачів. Зокрема, розгляньте можливість отримати розуміння наступних атрибутів: | | |
| • Політики, процедури, стандарти та вказівки щодо засобів контролю автентифікації та вимог до паролів. | | |
| • Де розміщується автентифікація (наприклад, чи є окрема програма для входу чи інтегрована з операційною системою)? | | |
| • Чи застосовуються параметри для всіх користувачів (загальносистемне налаштування) чи параметри відрізняються для кожного користувача або типу користувача? | | |
| • Розробка елементів керування автентифікацією для всіх типів облікових записів, визначених у системі (наприклад, облікові записи кінцевих користувачів, системні облікові записи, адміністратори). | | |
| • Конкретні параметри, які застосовуються (довжина, складність, зміна пароля та блокування облікового запису), а також відповідність цих параметрів стандартам та кращим практикам. | | |
| • Ознайомтеся з процесом щодо керування паролями облікових записів за замовчуванням і процесом періодичної зміни цих паролів, а також того, як змінений пароль повідомляється лише тим, хто має обґрунтування необхідності в цьому. | | |

Зона ризиків IT: Захист доступу

## Операційна ефективність контролів: атрибути перевірки (I)

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| 1. Отримайте доступ до всієї нормативної документації щодо засобів контролю автентифікації та вимог до паролів в установі. | | |
| 2. Отримайте доступ до переліку всіх користувачів установи. Зробіть вибірку по параметрам ID користувачів та їх паролів. У відповідності до встановлених вимог складності паролів (довжина, використання цифр, букв верхнього і нижнього регістрів, символів) проведіть аналіз та зазначте ID користувачів, паролі яких не відповідають вимогам. | | |
| 3. Разом із системним адміністратором або працівником IT безпеки перевірте налаштування основних параметрів Політики паролів та їх відповідність кращим практикам в Active Directory: | | |
| • застосування історії паролів; | | |
| • максимальний термін дії паролів; | | |
| • мінімальний термін дії паролів; | | |
| • мінімальна довжина паролів; | | |
| • відповідність вимогам складності паролів; | | |

Зона ризиків IT: Захист доступу

## Операційна ефективність контролів: атрибути перевірки (2)

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| • зберігання паролів, використовуючи оборотне шифрування. | | |
| 4. Разом із системним адміністратором або працівником іт безпеки перевірте налаштування основних параметрів Політики блокування облікових записів та їх відповідність кращим практикам в Active Directory: | | |
| • граничне значення блокування; | | |
| • тривалість блокування облікового запису; | | |
| • час до скидання лічильника блокування. | | |
| 5. Перевірити чи всі працівники мають свій персональний ідентифікатор (ID). | | |
| 6. Зробити вибірку по групах користувачів, яка складатиметься з: назви групи, ID користувачів, що туди входять, короткого опису призначення групи, права групи (читання або внесення змін). Перевірити чи не застосовується спільний ID для всіх членів групи. | | |
| 7. Перевірити наявність встановлення багатофакторної автентифікації для доступу до чутливої інформації. | | |

Зона ризиків IT: Захист доступу

**Формалізований документ: Політика дистанційної роботи**

## Дистанційна робота

**Дистанційна робота** – це форма організації праці, при якій співробітники виконують свої робочі обов'язки поза межами традиційного офісу, зазвичай вдома або в будь-якому іншому місці з доступом до Інтернету.

**Ціль процесу**: полягає в забезпеченні гнучкості та ефективності праці, дозволяючи співробітникам виконувати свої обов'язки поза межами традиційного офісного середовища.

**Вимоги:**

1) **Технологічні:** забезпечення співробітників необхідним обладнанням (комп'ютери, телефони, принтери, тощо), використання захищених каналів зв'язку (VPN, зашифровані електронні листи).
2) **Безпека даних:** захист конфіденційної інформації за допомогою шифрування даних, використання багатофакторної автентифікації (MFA), регулярне оновлення програмного забезпечення та систем безпеки.
3) **Управління доступом:** контроль доступу до корпоративних ресурсів на основі ролей, обмеження доступу до критичних систем та даних.
4) **Політики та процедури:** встановлення політик безпечної роботи з корпоративними даними вдома, навчання співробітників щодо безпечної роботи в дистанційному режимі, визначення чітких вимог до звітності та комунікацій.

**Опис ризику**: втрата або викрадення пристроїв, несанкціонований доступ до інформації і, як результат, її втрата, викрадення або маніпуляції з нею.

Зона ризиків IT: Захист доступу

## Дистанційна робота

Політика дистанційної роботи: основні положення (1)

1) **Умови дистанційної роботи**:

- Дистанційна робота дозволяється лише після отримання відповідного дозволу від керівництва.
- Працівники повинні підписати угоду про дистанційну роботу, яка визначає їх обов'язки та відповідальність щодо дотримання вимог безпеки.

2) **Безпека інформації**:

- Використання VPN: Обов’язкове використання корпоративних VPN для захищеного доступу до внутрішніх ресурсів організації.
- Багатофакторна Автентифікація (MFA): Впровадження MFA для всіх віддалених доступів до критично важливих систем і даних.
- Шифрування: Забезпечення шифрування даних на пристроях, що використовуються для роботи, а також шифрування переданих даних.

Зона ризиків IT: Захист доступу

## Дистанційна робота

Політика дистанційної роботи: основні положення (2)

3) **Використання Обладнання**:

- Корпоративні Пристрої: перевага надається використанню корпоративних пристроїв, які налаштовані і захищені відповідно до стандартів безпеки організації.
- Особисті Пристрої: використання особистих пристроїв дозволяється лише за умови відповідності вимогам безпеки організації, включаючи регулярні оновлення операційних систем і програмного забезпечення.
- Антивірусне Програмне Забезпечення: встановлення і регулярне оновлення антивірусного програмного забезпечення на всіх пристроях, що використовуються для роботи.

4) **Захист Конфіденційної Інформації**:

- Політика Чистого Столу: дотримання політики чистого столу, що включає недопущення залишення конфіденційних документів без нагляду.
- Заборона Роздруківки: заборона роздруківки конфіденційних документів вдома без відповідного дозволу.
- Зашифровані Канали: використання зашифрованих каналів для передавання конфіденційної інформації.

Зона ризиків IT: Захист доступу

## Дистанційна робота

Політика дистанційної роботи: основні положення (3)

**5) Моніторинг та Аудит**:

- Моніторинг Активності: проведення регулярного моніторингу активності працівників для виявлення потенційних загроз безпеці.
- Аудит Безпеки: проведення регулярних аудитів дотримання політики дистанційної роботи.
- Інцидент-Менеджмент: введення механізмів для швидкого реагування на інциденти безпеки.

6) **Навчання та Підтримка**:

- Тренінги: проведення регулярних тренінгів для працівників з питань інформаційної безпеки та безпечної роботи в умовах дистанційної роботи.
- Технічна Підтримка: надання технічної підтримки для вирішення проблем, що виникають під час дистанційної роботи.

Зона ризиків IT: Захист доступу

## Дистанційна робота

Операційна ефективність контролів: атрибути перевірки (1)

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| 1. Отримайте доступ до переліку всіх користувачів установи. Зробіть вибірку з числа тих користувачів, які працюють дистанційно/наполовину дистанційно та перевірте погодження такої роботи з керівництвом. | | |
| 2. Отримайте доступ до реєстру інцидентів в розрізі користувачів, які працюють дистанційно/наполовину дистанційно. Детально дослідіть причини та джерела виникнення інцидентів та якість і швидкість їх усунення. | | |
| 2. Перевірте налаштування доступів облікових записів на предмет обов'язкового використання VPN при доступі до внутрішніх ресурсів організації. | | |
| 3. Перевірте налаштування доступів облікових записів на предмет обов'язкового використання багатофакторної автентифікації всіх віддалених доступів до критично важливих систем і даних. | | |
| 4. Перевірте вимоги до шифрування даних на пристроях, що використовуються для дистанційної роботи. При наявності шифрування визначте його тип, для формування висновків про його надійність. | | |
| 5. Перевірте чи існує реєстр співробітників, що працюють на власному пристрої. Проведіть аналіз відповідностей власних пристроїв стандартам безпеки організації. | | |

Зона ризиків IT: Захист доступу

## Дистанційна робота

Операційна ефективність контролів: атрибути перевірки (2)

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| 6. Перевірте наявність встановленого антивірусного програмного забезпечення, його своєчасне оновлення, наявність ліцензій. | | |
| 7. Перевірте факт підписання угод дистанційної роботи працівниками, що визначають їх обов'язки та відповідальність щодо дотримання вимог безпеки. | | |
| 8. Перевірте факт здійснення моніторингу активності та аудитів дотримання політики дистанційної роботи службою підтримки або іт безпеки. | | |
| 9. Перевірте наявність навчальних матеріалів та фактів проведення тренінгів для працівників установи з дистанційної роботи. | | |

Зона ризиків IT: Захист доступу

**Формалізований документ: Політика чистого столу**

## Політика чистого столу

**Політика чистого столу -** це набір правил і рекомендацій, спрямованих на захист конфіденційної інформації, що знаходиться на робочих місцях.

**Ціль процесу**: мінімізувати ризик несанкціонованого доступу до чутливої інформації.

**Вимоги**: Забезпечення фізичного та програмного захисту інформації, що знаходиться як на цифрових пристроях так і в документальному вигляді на робочому місці працівника.

**Опис ризику**: несанкціонований доступ до інформації і як результат: втрата та маніпуляції над інформацією.

Зона ризиків IT: Захист доступу

## Політика чистого столу

1) **Документація та зберігання паперових документів**:

- Конфіденційність: Всі документи, які містять конфіденційну або особисту інформацію, повинні зберігатися у закритих та безпечних місцях, таких як сейфи або замкнені шухляди.
- Знищення: Документи, які більше не потрібні, повинні бути знищені шляхом подрібнення або іншими безпечними методами.

2) **Обробка та зберігання цифрових даних**:

- Автоматичне блокування: Комп'ютери повинні бути налаштовані на автоматичне блокування після певного періоду бездіяльності.
- Вихід з облікових записів: Користувачі повинні виходити з облікових записів перед тим як покидають робочі місця.
- Шифрування: Всі чутливі дані на цифрових носіях повинні бути зашифровані.

3) **Фізичний доступ до робочого місця:**

- Обмежений доступ: Доступ до робочих місць повинен бути обмежений лише уповноваженим персоналом.
- Ідентифікація: Використання ідентифікаційних карток або інших засобів для контролю доступу до робочих місць.

Зона ризиків IT: Захист доступу

## Політика чистого столу

4) **Робочі поверхні та обладнання:**

- Чистота робочого місця: Робочі столи повинні бути вільними від непотрібних паперів, нотаток та іншого обладнання.
- Зберігання особистих речей: Особисті речі повинні зберігатися у відведених для цього місцях і не повинні залишатися на робочих столах.

5) **Політика використання фізичних носіїв інформації:**

- Контроль доступу: Обмеження доступу до USB-накопичувачів, CD-дисків та інших фізичних носіїв.
- Безпечне зберігання: Зберігання таких носіїв у безпечних місцях, коли вони не використовуються.
- Моніторинг: Відстеження використання фізичних носіїв інформації.

6) **Навчання та підвищення обізнаності:**

- Тренінги: Регулярні тренінги для працівників щодо важливості політики чистого столу та IT-безпеки.
- Ознайомлення з політикою: Всі працівники повинні бути ознайомлені з вимогами політики чистого столу та підтвердити своє розуміння.

Зона ризиків IT: Захист доступу

## Політика чистого столу

Операційна ефективність контролів: атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| 1. Отримати доступ до всіх нормативних документів що стосуються Політики чистого столу. | | |
| 2. Провести вибіркову перевірку належного зберігання та знищення документів працівниками установи. | | |
| 3. Зробити вибірку налаштувань часового інтервалу блокування облікового запису в розрізі користувачів та провести перевірку на відповідність до Політики чистого столу або кращим практикам (у разі її відсутності). | | |
| 4. Перевірити налаштування шифрування даних користувачів, визначити тип шифрування для формування висновків про його надійність. | | |
| 5. Провести перевірку місць зберігання фізичних носіїв (документації, USB накопичувачів, тощо). | | |
| 6. Перевірити журнали тренінгів на предмет наявності проведених навчань персоналу з питань Політики чистого столу. | | |

# Домен III

## Захист інформації та активів організації

### Модуль I. Захист інформаційних та фізичних активів організації

Зона ризиків IT: Безпека комунікацій

**Формалізований документ: Політика фізичної безпеки та безпеки інфраструктури**

## Електронний обмін повідомленнями

- Існує велика кількість типів електронного обміну повідомленнями, таких як електронна пошта, електронний обмін даними, месенджери (Electronic Data Interchange — EDI) та соціальні мережі, які відіграють все більш важливу роль у бізнес-комунікаціях.
- **Ціль:** Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем, даних та послуг.
- **Вимога:** Інформація, яка міститься в електронних повідомленнях, має бути захищена належним чином.
- **Додатково:** Існує велика кількість типів електронного обміну повідомленнями, таких як електронна пошта, електронний обмін даними (Electronic Data Interchange — EDI) та соціальні мережі, які відіграють все більш важливу роль у бізнес-комунікаціях.

Зона ризиків IT: Безпека комунікацій

## Електронний обмін повідомленнями

Міркування безпеки щодо електронного обміну повідомленнями мають включати:

- технічний захист повідомлень від несанкціонованого доступу, модифікації або відмови в обслуговуванні;
- забезпечення коректного адресування та передавання повідомлення;
- загальну надійність і доступність послуги;
- правові вимоги, наприклад вимоги до електронних підписів;
- отримання погодження перед використанням загальнодоступних зовнішніх послуг, таких як засоби оперативного пересилання повідомлень або спільне використання файлів;
- більш жорсткі рівні автентифікації, яка контролює доступ із загальнодоступних мереж.

Зона ризиків IT: Безпека комунікацій

## Електронний обмін повідомленнями: підходи до тестування

- ***Політики та процедури обміну інформацією***
  - Мають бути наявними офіційно оформлені політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів засобів комунікації.
- ***Угоди щодо обміну інформацією***
  - Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо безпечного обміну бізнес-інформацією.
- ***Угоди щодо конфіденційності або нерозголошення***
  - Вимоги до угод щодо конфіденційності або нерозголошення, які відображають потреби організації в захисті інформації, мають бути ідентифіковані, задокументовані та регулярно переглядатися.

Зона ризиків IT: Захист IT активів

**Політика фізичної безпеки та безпеки інфраструктури** має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.

**Ціль**: Запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в її інформацію та засоби оброблення інформації.

**Вимога**: Для захисту зон, що містять конфіденційну або критичну інформацію, чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки.

- **Периметр фізичної безпеки:** Для захисту зон, що містять конфіденційну або критичну інформацію, чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки.
- **Заходи безпеки фізичного прибуття:** Зону безпеки має бути захищено належними заходами безпеки прибуття, щоб забезпечити, що доступ дозволений лише персоналу, який отримав на це право.
- **Убезпечення офісів, кімнат та обладнання:** Має бути розроблено й застосовано фізичну безпеку офісів, кімнат та обладнання.
- **Захист від зовнішніх та інфраструктурних загроз:** Має бути розроблено та застосовано фізичний захист від пошкодження внаслідок природних катаклізмів, акцій громадської непокори та аварій.
- **Робота в зонах безпеки:** Має бути розроблено та застосовано процедури роботи в зонах безпеки.
- **Обладнання:** має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу.

Зона ризиків ІТ: Захист ІТ активів

**Обладнання (ІТ активи) має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу:**

- обладнання має бути розміщено так, щоб мінімізувати непотрібний доступ до робочих зон;
- засоби оброблення інформації, що обробляють конфіденційні дані, мають бути розташовані з осторогою для зниження ризику спостереження інформації особами, які не мають на це санкцій, підчас її використання;
- треба убезпечити засоби зберігання для уникнення несанкціонованого доступу;
- елементи, що потребують спеціального захисту, має бути ізольовано для зменшення загального рівня необхідного захисту;
- має бути узгоджено заходи безпеки для мінімізації ризику потенційних фізичних загроз і загроз навколишнього середовища, наприклад крадіжки, вогню, вибухів, диму, води (або відмови постачання води), пилу, вібрації, хімічних впливів, завад електроживлення, комунікаційних завад, електромагнітного випромінювання та вандалізму;
- має бути розроблено настанови щодо приймання їжі та напоїв, а також паління поблизу засобів оброблення інформації;
- треба здійснювати моніторинг умов довкілля, таких як температура та вологість, які можуть негативно вплинути на функціонування засобів оброблення інформації;
- треба захистити обладнання оброблення конфіденційної інформації для мінімізації ризику витоку інформації внаслідок випромінювання.

Зона ризиків IT: Захист IT активів

**Формалізований документ: Політика використання фізичних носіїв**

## Фізичні носії під час передавання даних

Фізичні носії під час передавання даних - це матеріальні пристрої, такі як USB-флешки, зовнішні жорсткі диски, CD або DVD диски, які використовуються для зберігання та переміщення даних з одного пристрою на інший.

Політика використання фізичних носіїв має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.

**Ціль процесу:** забезпечення безпечного та контрольованого транспортування конфіденційної інформації за допомогою фізичних носіїв.

**Вимоги**: Забезпечення всебічного фізичного та програмного захисту фізичних носіїв під час їх передавання.

**Опис ризиків**:

- Втрата або крадіжка: фізичні носії можуть бути загублені або викрадені під час переміщення або зберігання.
- Несанкціонований доступ: без належного захисту фізичні носії можуть бути доступні для несанкціонованих осіб.
- Пошкодження: фізичні носії можуть бути пошкоджені через фізичні впливи, такі як падіння, волога, екстремальні температури або магнітні поля.
- Несанкціоноване копіювання: Інформація на фізичних носіях може бути скопійована або розголошена.

Зона ризиків IT: Захист IT активів

## Фізичні носії під час передавання даних

Політика використання фізичних носіїв повина описувати наступні тези:

1) **Авторизація і доступ**: встановлення правил щодо того, хто має право передавати фізичні носії, і як це повинно відбуватись. Це може включати внутрішніх співробітників або зовнішніх партнерів, які мають право на обмін інформацією.

2) **Шифрування даних**: Вимоги до шифрування конфіденційної інформації, що зберігається на фізичних носіях, для захисту від несанкціонованого доступу у разі втрати чи крадіжки носія.

3) **Фізичний захист**: Заходи безпеки для захисту фізичних носіїв під час їх транспортування. Це може включати використання сейфів, контейнерів із замками або інших засобів фізичного захисту.

4) **Інвентаризація і відстеження**: Ведення інвентаризації фізичних носіїв, відстеження їх руху та забезпечення обліку. Додатково ведеться окремий облік власних фізичних носіїв працівників, що використовуються для роботи. Це допомагає виявити втрату інформації і забезпечити можливість швидкої реакції у разі виникнення даної проблеми.

Зона ризиків ІТ: Захист ІТ активів

## Фізичні носії під час передавання даних

Політика використання фізичних носіїв (2)

5) **Процедури знищення**: Встановлення процедур для безпечного знищення фізичних носіїв, які вже не потрібні для подальшого використання, щоб запобігти можливому витоку інформації.

6) **Навчання персоналу**: Навчання співробітників правилам безпечного використання і перевезення фізичних носіїв, а також навчання про потенційні загрози та як їх уникнути.

7) **Аудит і відповідальність**: Проведення регулярних аудитів безпеки використання фізичних носіїв і призначення відповідальних осіб за дотримання політики та процедур.

Зона ризиків IT: Захист IT активів

## Фізичні носії під час передавання даних

Операційна ефективність контролів: атрибути перевірки

| Опис процедури | Відповідь | Коментарі |
|---|---|---|
| 1. Отримати доступ до нормативної документації по використанню фізичних носіїв. | | |
| 2. Отримати доступ до реєстру працівників, за якими закріплені фізичні носії. Провести вибіркову перевірку фактичної наявності фізичних носіїв та місця їх зберігання. | | |
| 3. Перевірити вимоги та наявність впровадженого шифрування даних на електронних носіях. Визначити тип шифрування у разі його наявності. | | |
| 4. Перевірити за визначений період результати проведених інвентаризацій фізичних носіїв. Провести аналіз нестач та причини їх виникнення. | | |
| 5. Вибірково перевірити відповідність облікових даних до фактичних фізичних носіїв (назви та модельні номери фізичних носіїв). | | |
| 6. Провести перевірку дотримання процесу знищення фізичних носіїв. | | |
| 7. Перевірити наявність навчальних матеріалів та фактів проведення тренінгів для працівників установи по використанню фізичних носіїв. | | |
| 8. Перевірити факт здійснення аудитів дотримання політики використання фізичних носіїв службою підтримки або іт безпеки. | | |

# Дякуємо!

# Q&A