УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Лекція 8. Управління ризиками та контроль безпеки

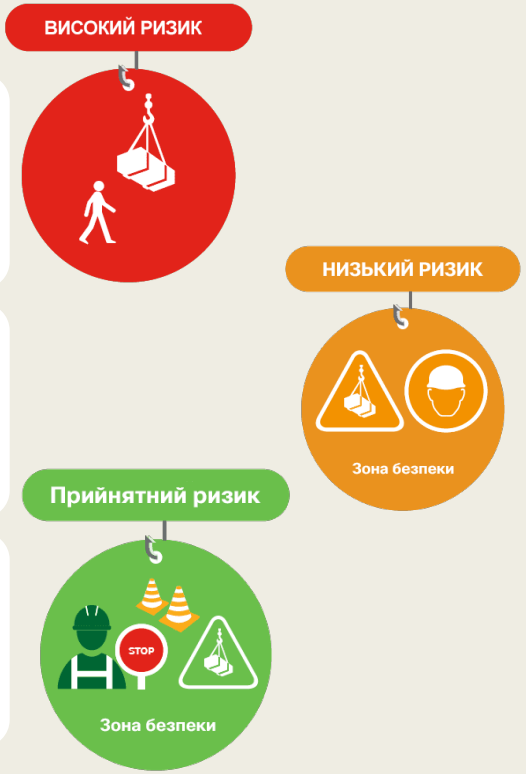
1. Управління ризиками.
2. Оцінювання ризиків.
3. Контроль безпеки.

Управління ризиками

Ризик – це ймовірність втрати через загрозу – зловмисну дію чи несподівану подію – яка завдає шкоди інформаційним системам або активам організації.
Вплив ризику – це пошкодження, завдані подією, яка спричиняє втрату активу(ів) або порушення роботи сервісу(ів).
Мета управління ризиками полягає в тому, щоб зменшити ці загрози до прийнятного рівня та запровадити заходи контролю для підтримки цього рівня.

Рівні загроз можна класифікувати як:

- **Високий ризик** - Недбалість означає, що для зниження ризику не вживаються жодні дії чи не проводиться контроль. Загроза дуже значна, а ціна інциденту може бути катастрофічною
- **Низький ризик** - Дотримання належної обережності може допомогти знизити рівень ризику. Ризик все ще існує, але ці розумні кроки зменшують потенційні збитки.
- **Прийнятний ризик** - Належна обачність передбачає вжиття розумних заходів для усунення ризику. Деякі ризики все ще існують, але для запобігання потенційним збиткам впроваджено декілька заходів контролю.



Типи ризиків

- Ризик може бути внутрішнім, зовнішнім або одночасно і тим і іншим. Його вплив може поширюватися на всю організацію, також впливаючи на інші зовнішні об’єкти.

- Сприяння поінформованості про ризики в організації допомагає співробітникам виробити розуміння, які ризики існують, їх потенційний вплив і як організація може керувати цими ризиками.

Управління ризиками

Процеси ідентифікації та оцінки ризику в організації є безперервними, оскільки типи загроз змінюються і ніколи не зникають повністю. Метою управління ризиками є зниження цих загроз до прийнятного рівня.

Існують різні рівні управління ризиками. Організації повинні належним чином управляти ризиками для захисту інформації та інформаційних систем. Управління ризиками також допомагає запобігти судовим позовам, простоям у діяльності та захищає репутацію організацій.

Процес управління ризиками

- **рівні ризикових дій**
- **концепції управління ризиками**
- **процеси управління ризиками**

Рівні ризикових дій

Управління ризиками – це виявлення, оцінка та визначення пріоритетів ризиків. Організації керують ризиками одним із чотирьох способів. Кожен може бути відповідним вибором, залежно від обставин і типу ризику, про який йде мова:

Уникнення (усунення)

- Уникнення ризику – це повна ліквідація або усунення ризику конкретної загрози. Наприклад, уникнення або усунення загрози, коли користувачі обмінюються паролями або зловживають ними, може включати впровадження системи аутентифікації відбитків пальців на всіх робочих станціях користувачів.

Зниження (зменшення)

- Пом’якшення ризику передбачає впровадження заходів контролю, які дозволяють організації продовжувати виконувати діяльність, використовуючи механізми зниження ризику певної загрози. Організація може також посилити свій технічний контроль і мережний нагляд, щоб зменшити ризик операційних загроз.

Передача

- Організації можуть передавати ризик конкретних загроз третій особі або іншій організації. Фінансовим ризиком загрози можна керувати, придбавши страховий поліс або найнявши підрядника для боротьби з конкретними загрозами.

Прийняття

- Прийняття ризику передбачає визначення загроз, але свідомо не передбачає впровадження процесів зниження ризику. Усвідомлене рішення ґрунтується на аналізі різних компонентів ризику, до його прийняття.

Керування ризиком

Приклади управління ризиками, пов'язаними з конкретними загрозами для інформації чи інформаційних систем організації.

Організація регулярно зобов'язана обробляти конфіденційну інформацію клієнтів. Оприлюднення цієї інформації становить серйозний ризик для організації.

Які кроки може здійснити організація, щоб усунути ризик, пов'язаний із випадковим надсиланням електронною поштою чи передачею цієї інформації?

Впровадити політику, яка забороняє співробітникам надсилати електронні листи або передавати будь-які дані клієнтів.

Заборонити співробітникам доступ до цієї інформації.

Перевіряти та блокувати всі дані, надіслані електронною поштою або передані з мережі організації

Керування ризиком

Приклади управління ризиками, пов’язаними з конкретними загрозами для інформації чи інформаційних систем організації.

Організація мала проблеми з тим, що співробітники обмінюються паролями або використовують слабкі паролі.

Які є способи зниження цього ризику?

Впровадити політику та рекомендації щодо паролів організації,

Посилити використання надійних паролів у всій організаційній системі

Вивчення рівнів ризику

Процес ідентифікації та оцінки ризику в організації є безперервними, оскільки типи загроз змінюються і ніколи не зникають повністю. Метою управління ризиками є зниження цих загроз до прийнятного рівня.

Недбалість — це невиконання особою чи організацією своїх обов'язків через недогляд або відсутність належної уваги до певних ризиків чи завдань. Це може відбуватися через незнання, невміння або небажання виконувати дії, які очікуються для забезпечення безпеки чи успішної діяльності.

Недбалість означає, що для зниження ризику не вживаються жодних дій чи контролю. Загроза дуже значна, а ціна інциденту може бути катастрофічною та призвести до кримінальної відповідальності.

НАСЛІДКИ

Зловживання даними: Якщо організація не забезпечує належний захист персональних даних своїх клієнтів, це може призвести до їх втрати або крадіжки, що спричинить репутаційні та фінансові втрати для компанії.

Недотримання стандартів безпеки: У випадку, коли організація нехтує впровадженням основних заходів безпеки, наприклад, таких як регулярні оновлення систем або встановлення антивірусного програмного забезпечення, це може призвести до атак на інформаційні системи.

Виробничі аварії: Недбалість у дотриманні правил техніки безпеки на виробництві може призвести до аварій, травм або навіть смерті працівників.

Вивчення рівнів ризику

Належний догляд (due care)

- Розумний рівень уваги та дій, які людина або організація має докладати для запобігання виникненню небезпеки чи збитків.
- Означає здійснення необхідних заходів для захисту від потенційних ризиків, виконання своїх зобов'язань належним чином і відповідно до стандартів або норм.
- Стосується активних дій, спрямованих на уникнення шкоди.
- Постійна дія в рамках забезпечення безпеки.
- Ризик все ще існує, але розумні заходи зменшують потенційні збитки.

Належна обачність (due diligence)

- Процес ретельного аналізу та оцінки ризиків перед ухваленням важливого рішення або здійсненням дій.
- Включає збір інформації, аналіз потенційних загроз і оцінку можливих наслідків.
- Зазвичай проводиться перед важливими фінансовими, юридичними або бізнесовими рішеннями, щоб забезпечити прийняття інформованих рішень на основі повної картини ситуації.
- Має разовий або обмежений у часі характер
- Деякі ризики все ще існують, але для запобігання потенційним збиткам впроваджено декілька заходів контролю.

Концепції управління ризиками

Управління ризиками – це метод, який використовується для виявлення та оцінки факторів, які можуть загрожувати інформації та інформаційним системам. Вивчення аналізу ризику включає кілька загальновживаних термінів і понять, у тому числі наступні:

Активи	Будь-яка цінність, яка використовується і необхідна для виконання бізнес завдань. Активи включають як матеріальні, так і нематеріальні об’єкти, такі як обладнання, програмний код, дані, засоби, персонал, ринкова вартість та громадська думка. Управління ризиками – це захист цінних організаційних активів.
Загрози	Зловмисний акт або несподівана подія, що завдає шкоди інформаційним системам або іншим пов’язаним організаційним активам. Це можуть бути навмисні дії, які призводять до втрати або пошкодження активу. Загрози також можуть бути ненавмисними, як-от аварія, стихійне лихо або поломка обладнання.
Вразливість	Будь-який недолік або слабкість, які можуть дозволити загрозі заподіяти шкоду та пошкодити актив. Прикладами можуть бути помилковий код, неправильна конфігурація та недотримання процедур.

Концепції управління ризиками

Вплив	Вплив ризику – це збиток, завданий подією, яка спричиняє втрату активу або порушення роботи сервісу. Цей збиток можна виміряти кількісно або якісно на основі впливу на діяльність організації.
Ризик	ймовірність збитків через загрозу активам організації.
Контрзаходи	це дія, пристрій або техніка, які зменшують загрозу чи вразливість шляхом їх усунення чи запобігання. Прикладом може бути антивірусне програмне забезпечення, брандмауери, політики та навчання.
Оцінка ризику	процес виявлення вразливостей та загроз та оцінки можливих впливів, щоб визначити, де запровадити засоби контролю безпеки.

Оцінка ризику безпеки визначає, прораховує та пріоритизує ризики і вразливості у системі. Оцінка ризику визначає розпізнані загрози та суб’єктів загрози, а також ймовірність того, що ці фактори призведуть до ризику або збитку.

Концепції управління ризиками

Приклад:

Підприємство керує базою даних клієнтів, яка відстежує онлайн-покупки продуктів. Ці покупки здійснюються за допомогою рахунків PayPal або кредитних карток. Сервер баз даних має декілька вразливостей. База даних знаходиться на сервері в серверній кімнаті в штаб-квартирі компанії. Сервер коштує $25000. База даних складається з 40000 клієнтів і понад 1,5 мільйона транзакцій. Сервер записує понад 120 транзакцій на день, генеруючи понад 25 тис. продажів на день. Резервне копіювання бази даних здійснюється щодня о 2 годині ночі. Усі замовлення також відстежуються та реєструються в окремих системах у разі збою сервера. Цей процес може зайняти до 50 людино-годин введення вручну щодня.

Які типи вразливостей мають проаналізувати співробітники відділу кібербезпеки?

Вразливості резервного копіювання та відновлення (недостатня захищеність резервних копій, вразливість до втрати даних між резервними копіями)

Вразливість до втрати даних через людський фактор (кількість ручного введення підвищує ризик помилок та спотворення даних, збільшує час відновлення операцій)

Вразливості мережевої безпеки (відсутність брандмауера, слабка автентифікація, проблеми з конфігурацією мережевих захистів)

Вразливість даних клієнтів і транзакцій (невикористання шифрування даних, недостатній контроль доступу до бази даних)

Фізична вразливість сервера (недостатній контроль доступу до серверної кімнати)

Які є можливі загрози для сервера на основі виявлених вразливостей?

Втрата даних через відсутність частого резервного копіювання:
У разі збою сервера всі дані, що були записані після останнього резервного копіювання, можуть бути втрачені. Це може вплинути на транзакції, замовлення та клієнтські записи, особливо з огляду на великий обсяг щоденних операцій

Ризик людських помилок при відновленні даних:
У разі збою введення даних вручну підвищує ризик помилок, що може призвести до порушення коректності транзакцій та втрати інформації про замовлення, що вплине на бізнес-операції.

Кіберзагрози (хакерські атаки):
Вразливості на сервері можуть бути використані зловмисниками для проведення атак, таких як SQL-ін'єкції, атаки на відмову в обслуговуванні (DDoS) або крадіжка даних клієнтів. Це може призвести до компрометації фінансових і особистих даних клієнтів.

Компрометація фінансових даних:
Якщо дані не шифруються під час зберігання або передачі, зловмисники можуть викрасти фінансову інформацію (дані карток, облікові записи PayPal), що призведе до фінансових втрат для клієнтів і підприємства та значної шкоди репутації компанії.

Несанкціонований фізичний доступ:
Зловмисник може фізично отримати доступ до сервера та викрасти або пошкодити дані. Він також може запустити шкідливе ПЗ або перезавантажити сервер, що призведе до збоїв у роботі.

Який вплив на організацію мають наступні загрози:

Витік даних:

Компрометація особистої інформації клієнтів (імена, адреси, платіжні дані) може призвести до фінансових втрат для клієнтів і юридичних наслідків для компанії через порушення законодавства про захист даних (наприклад, GDPR).

Пошкодження репутації, втрата довіри клієнтів та потенційне скорочення клієнтської бази.

Підвищені витрати на відновлення систем, юридичні послуги та компенсації клієнтам.

Фінансові втрати через штрафи та судові процеси.

Програма-вимагач (Ransomware):

Шифрування критичних даних бази клієнтів та транзакцій, що паралізує роботу компанії на тривалий час.

Вимога значної суми викупу для розблокування даних, що може призвести до фінансових втрат.

Навіть після оплати викупу немає гарантії, що доступ до даних буде відновлено.

Втрата даних, якщо резервне копіювання вразливе або зашифроване разом із основними даними.

Репутаційні втрати через втрату даних та затримку у відновленні роботи.

Відмова обладнання:

У разі збою сервера організація може втратити доступ до баз даних клієнтів і транзакцій, що призведе до зупинки бізнес-операцій.

Втрата даних, якщо не було належних резервних копій, що призведе до додаткових витрат на відновлення та можливих помилок при введенні даних вручну.

Потреба у витратах на ремонт або заміну обладнання.

Невиконання зобов'язань перед клієнтами, що може вплинути на репутацію і довіру до організації.

Шкідливе програмне забезпечення (Malware):

Може пошкодити файли, зібрати конфіденційну інформацію, зруйнувати бази даних або використовувати ресурси сервера для атак на інші системи.

Може призвести до зниження продуктивності системи, втрати даних і навіть її повного блокування.

Довгострокові репутаційні втрати через компрометацію системи безпеки.

Фінансові витрати на очищення системи, відновлення даних і зміцнення захисту від майбутніх атак.

*Які **контрзаходи** можливі для наступних загроз серверу баз даних організації:*

Витік даних:

Шифрування даних як під час зберігання, так і під час передачі, щоб у разі витоку інформація залишалася незрозумілою без ключа шифрування.

Контроль доступу на основі ролей та принципу найменших привілеїв, щоб тільки авторизовані користувачі мали доступ до конфіденційної інформації.

Аудит доступу та регулярний моніторинг активності, щоб відстежувати та реагувати на підозрілу діяльність.

Впровадження **багатофакторної автентифікації (MFA)** для захисту акаунтів користувачів, які мають доступ до бази даних.

Програма-вимагач (Ransomware):

Регулярне резервне копіювання даних із збереженням копій у захищених та відокремлених середовищах (наприклад, у хмарі), щоб забезпечити можливість відновлення без сплати викупу.

Навчання персоналу для підвищення обізнаності про **фішинг** та інші техніки соціальної інженерії, через які зазвичай поширюються програми-вимагачі.

Встановлення **антивірусного програмного забезпечення** та засобів виявлення шкідливих програм, що можуть запобігти запуску програм-вимагачів.

Сегментація мережі, щоб зловмисне програмне забезпечення не могло поширюватися між різними системами та базами даних.

Відмова обладнання:

Регулярна **профілактика та обслуговування** серверного обладнання для мінімізації ризику відмови через апаратні несправності.

Дублювання серверів (кластеризація) та використання **відмовостійких систем**, які автоматично перемикаються на резервні сервери у разі збою основного обладнання.

Хмарне резервне зберігання даних або використання зовнішніх центрів обробки даних для забезпечення доступу до інформації у випадку відмови локального обладнання.

Регулярні **тести на відновлення після збоїв** (Disaster Recovery Tests), щоб переконатися, що система може бути відновлена без втрати даних і тривалої зупинки.

Шкідливе програмне забезпечення (Malware):

Встановлення та регулярне оновлення **антивірусного програмного забезпечення** і **систем виявлення вторгнень (IDS/IPS)** для виявлення та блокування шкідливих програм.

Використання **мережевої сегментації**, щоб ізолювати критичні бази даних від загальних користувацьких систем та мінімізувати ризики зараження.

Оновлення та патчинг програмного забезпечення серверів і систем безпеки, щоб усунути відомі вразливості, через які шкідливе ПЗ може проникати до систем.

Навчання співробітників **основам кібергігієни** (наприклад, не відкривати підозрілі електронні листи, не завантажувати файли з ненадійних джерел).

Процеси управління ризиками

Управління ризиками – це формальний процес, який зменшує вплив загроз і вразливостей. Не можна повністю усунути ризик, але можна управляти ризиком до прийнятного рівня. Управління ризиками вимірює вплив загрози та витрати на впровадження засобів контролю або контрзаходів для зниження загрози. Усі організації беруть на себе певний ризик. Вартість контрзаходу **не** повинна перевищувати вартість активу, який захищається.

Крок 1: Окреслення та оцінка ризику

Визначити загрози в організації, які підвищують ризик. Виявлені загрози включають процеси, продукти, атаки, потенційний збій або порушення роботи сервісів, негативне сприйняття репутації організації, потенційну юридичну відповідальність або втрату інтелектуальної власності.

Після визначення ризику його оцінюють та аналізують, щоб визначити серйозність загрози. Деякі загрози можуть призвести до зупинки всієї організації, тоді як інші загрози є незначними незручностями. Ризику може бути назначений пріоритет за фактичним фінансовим впливом (кількісний аналіз) або масштабованим впливом на діяльність організації (якісний аналіз).

Крок 2: Відповідь на ризик

Розробка плану дій для зменшення загального ризику організації. Керівництво оцінює загрози та визначає їх пріоритети; потім команда визначає, як реагувати на кожну загрозу. Ризик може бути усунутий, знижений, переданий або прийнятий.

Крок 3: Контроль ризиків

Постійно переглядайте зменшення ризику за рахунок дій з його ліквідації, зниження чи передачі. Не всі ризики можна усунути, тому прийняті загрози необхідно уважно відстежувати. Важливо розуміти, що певний ризик завжди присутній і прийнятний. У міру впровадження контрзаходів вплив ризику має зменшуватися. Необхідний постійний моніторинг та перегляд нових контрзаходів.

Типи джерел загроз

Оцінка загроз є основою для оцінки ризику.

Загроза – це потенційна можливість виявлення та використання вразливості, тоді як **вектор загрози** – це шлях, який зловмисник використовує для впливу на ціль.

Джерела загроз можуть бути внутрішніми або зовнішніми та поділяються на наступні категорії.

- **Ворожі**: Загрози від окремих осіб, груп, організацій або націй.
- **Випадкові**: Дії, які відбуваються без зловмисного наміру.
- **Структурні**: Збої в роботі обладнання та програмного забезпечення.
- **Стихійні**: Стихійні лиха, які можуть бути як природними, так і спричиненими людиною, наприклад, пожежі та повені.

Методологія оцінки ризиків

Організації визначають розмір шкоди та перевіряють свої операційні ризики, виконуючи оцінювання ризиків, щоб переконатися, що управління ризиками відповідає всім їхнім бізнес-цілям.

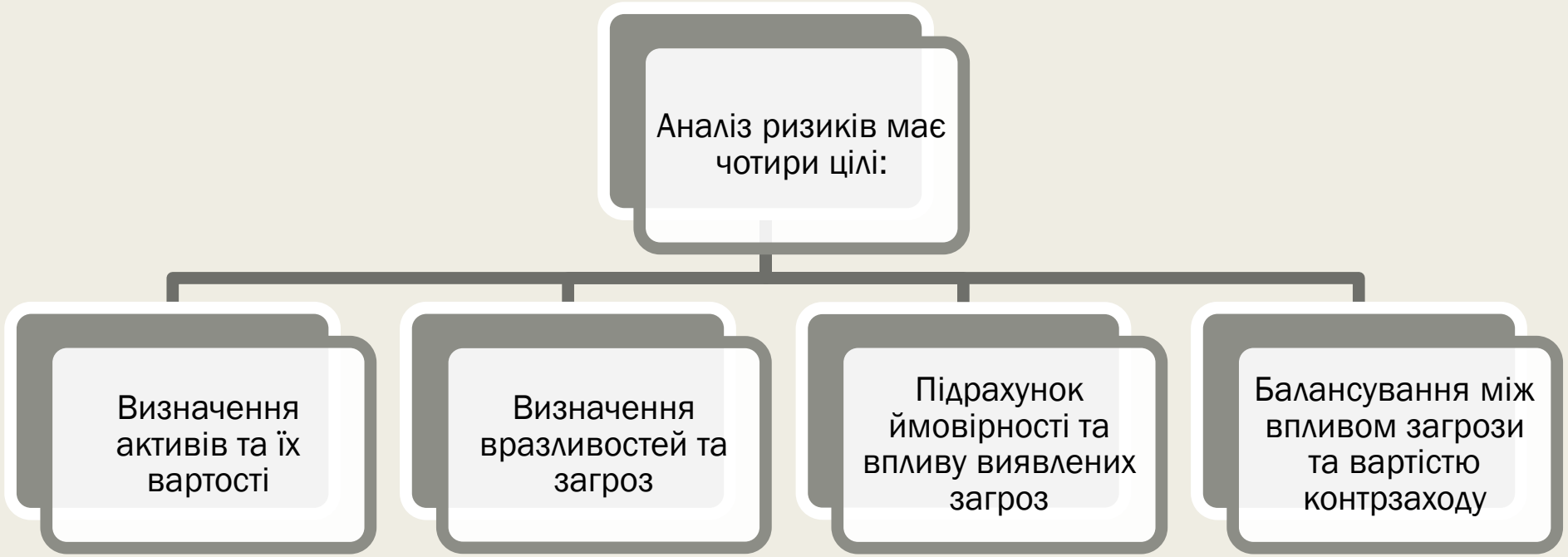
Спроба визначити ймовірність атаки суб'єктом загрози може бути складною і може включати оцінку рівня навичок, мотивів, можливостей та масштабу.

Під час оцінювання вразливості важливу роль відіграють такі фактори як простота виявлення, можливість використання, поінформованість та виявлення вторгнень. Використовуючи комбінацію очікування та ретроспективних даних, можна забезпечити найточнішу ймовірність того, що подія відбудеться.

Після того визначається величина впливу. Проста міра впливу може варіюватися від дуже низького до дуже високого або від незначного до катастрофічного впливу.

Аналіз ризиків

Аналіз ризиків вивчає небезпеку, яку становлять природні та антропогенні події для активів організації. Користувач виконує ідентифікацію активів, щоб визначити, які активи необхідно захистити.



Два підходи до аналізу ризиків:

- Кількісний аналіз ризиків
- Якісний аналіз ризиків

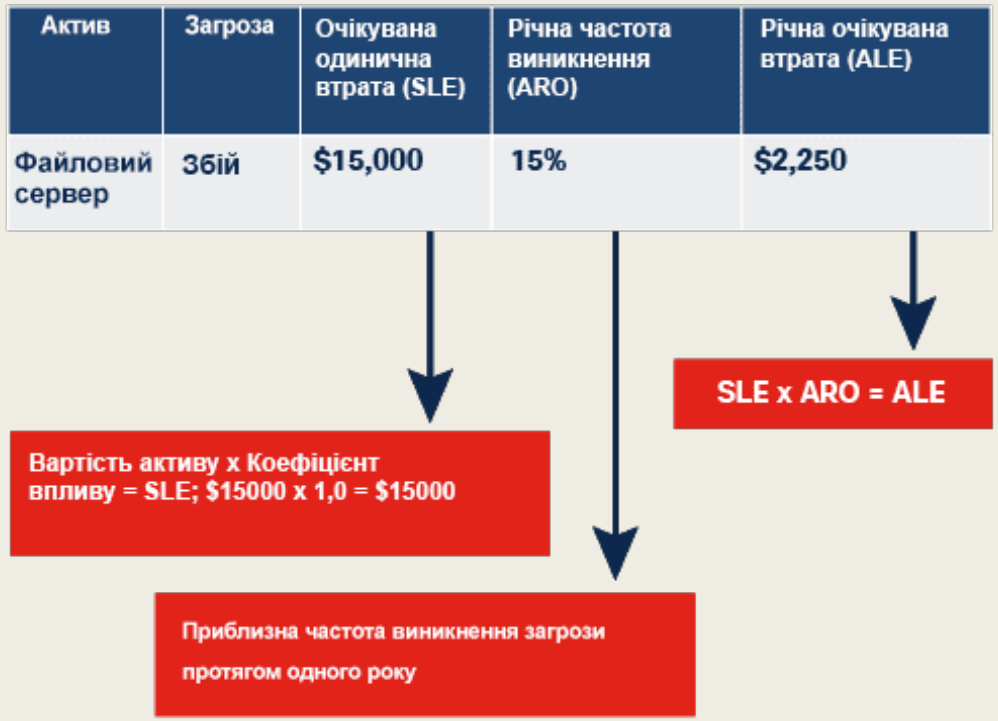
Кількісний аналіз ризиків

Кількісний аналіз ризиків присвоює числа процесу аналізу ризиків. У прикладі, **вартість активу** є вартістю заміни файлового сервера (активу). Вартість активу також може бути виміряна доходами, отриманими за рахунок використання активу.

Коефіцієнт впливу (exposure factor – EF) – це суб'єктивне значення, виражене у відсотках втрати файлового сервера через конкретну загрозу. Якщо відбувається повна втрата, EF дорівнює 1,0 (100%).

Річна частота виникнення (annualized rate of occurrence – ARO) – це ймовірність того, що втрата виникне протягом року. Показник ARO може перевищувати 100%, якщо втрата траплятиметься частіше одного разу на рік.

Розрахунок **щорічної очікуваної втрати (annual loss expectancy – ALE)** дозволяє керівництву визначити витрати організації на захист файлового сервера.



Якісний аналіз ризиків

Якісний аналіз ризику використовує оцінки та сценарії, які відображають відношення ймовірності виникнення загрози до її впливу. У прикладі, збій сервера є ймовірним, але його вплив може бути незначним.

Матриця ризиків – це інструмент, який допомагає визначити пріоритети ризиків, щоб визначити, на які з них організація має розробити відповідь. Результати можна ранжувати та використовувати як керівництво, щоб визначити, чи організація вживає заходів.

Коли елементи матриці ризиків позначені кольором, як показано на рисунку, вона називається *тепловою картою ризику.*

Категорія	Часто - 5	Ймовірно - 4	Зрідка - 3	Рідко - 2	Малоймовірно - 1
Катастрофічний - 4	20	16	12	8	4
Критичний - 3	15	12	9	6	3
Граничний - 2	10	8*	6	4	2
Незначний - 1	5	4	3	2	1

* Збій сервера

Зниження ризиків

Зниження ризику передбачає зменшення ймовірності або серйозності втрат від загроз. Багато засобів технічного контролю знижують ризики, зокрема, системи аутентифікації, дозволи на файли та брандмауери.

Організації повинні розуміти, що зниження ризику може як позитивно, так і негативно впливати на організацію. Достатнє зниження ризику намагається збалансувати негативний вплив контрзаходів, контроль та користь від зменшення ризику.

Найпоширеніші способи зниження ризику

Термін	Опис
Прийняття ризику і періодична його переоцінка	Короткострокова стратегія полягає в тому, щоб прийняти ризик, створивши плани дій на випадок прояву цього ризику. Люди та організації повинні прийняти ризик на щоденній основі.
Знизити ризик шляхом впровадження засобів контролю	Сучасні методології зменшують ризик за рахунок поступової розробки програмного забезпечення та надання регулярних оновлень і виправлень (патчів) для усунення вразливостей і неправильних конфігурацій.
Уникати ризику шляхом повної зміни підходу	Хороший план зниження ризику може включати дві або більше стратегій.
Передати ризик третій стороні	Послуги аутсорсингу, страхування та закупівля контрактів на технічне обслуговування є прикладами передачі ризику. Найм спеціалістів для виконання важливих завдань зі зниження ризику може бути хорошим рішенням і дати кращі результати з меншими довгостроковими інвестиціями.

Визначення пріоритетів активів

Приклад: у організації створили таблицю управління активами, яку, як вони сподіваються, можна використовувати для впорядкування активів від найвищого до найнижчого пріоритету. *На основі інформації в цій таблиці оцініть активи в правильному порядку від 1 (високий пріоритет) до 4 (низький пріоритет)*

Опис актива і загрози	Коефіцієнт впливу (EF) $/%	Річна частота виникнення (ARO)	Річна очікувана втрата (ALE) EF x ARO = ALE
Збій блоку живлення сервера баз даних	$2,500	Раз на 2 роки	$1,250
	10%	50%	
Збій диска сервера бази даних	$5,000	Раз на 5 років	$1,000
	20%	20%	
Хакерська атака на веб-сервер	$200,000	5 разів на рік	$1,000,000
	400%	500%	
Крадіжка ноутбука	$2,000	Раз на 4 роки	$500
	200%	25%	

Збій блоку живлення сервера бази даних — 2

Збій диску сервера бази даних — 3

Хакерська атака веб-сервера — 1

Крадіжка ноутбука — 4

Контроль безпеки. Типи контролю

Ризик, властивий системі, – це ризик, який система створює своїм існуванням – без будь-якого управління людьми, процесами або технологіями.

Контроль безпеки – це засоби захисту або контрзаходи, які організація вживає, щоб уникнути, виявити, протидіяти або мінімізувати ризики безпеки для активів організації.

Існує три види контролю:

Адміністративний контроль складається з процедур і політик, які організація встановлює коли має справу з конфіденційною інформацією. Ці елементи контролю визначають дії людей

Технічний контроль охоплює апаратне та/або програмне забезпечення, впроваджене для управління ризиками та забезпечення захисту.

Фізичний контроль – це механізми, такі як огорожі та замки, що використовуються для захисту систем, об’єктів, персоналу та ресурсів. Фізичний контроль фізично відокремлює людей або інші загрози від систем.

Функціональний контроль безпеки

Функціональне використання конкретного захисного чи протидіючого заходу допоможе визначити причину його вибору та впровадження.

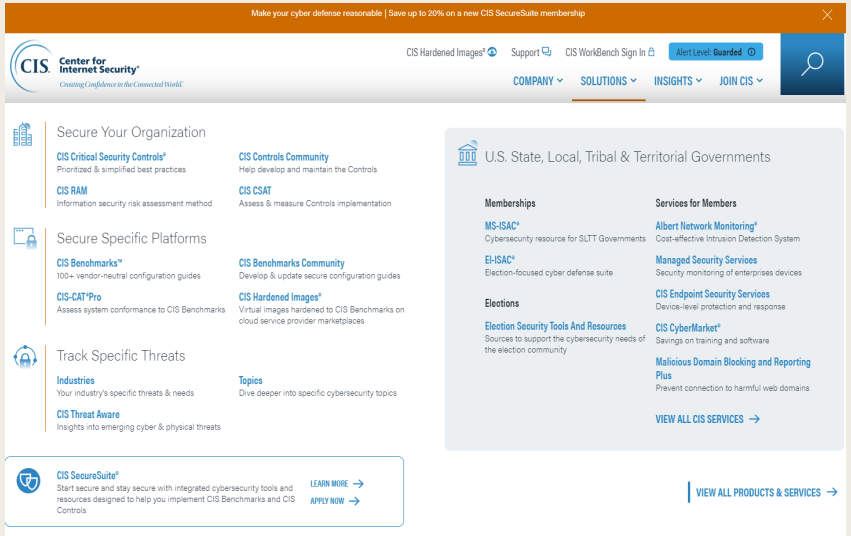
Термін	Опис
Запобіжні заходи	Запобіжні заходи контролю зупиняють небажану і несанкціоновану діяльність або/та застосовують обмеження для авторизованих користувачів.
Стримувальні заходи	Стримувальний фактор має на меті перешкодити події відбутися.
Детективні заходи	Виявлення контролю доступу визначає різні типи несанкціонованої діяльності. Детективні заходи не є запобіжними, натомість орієнтовані на виявлення порушення безпеки після того, як воно сталося.
Коригувальні заходи	Коригувальні заходи протидіють небажаному, відновлюючи систему до стану конфіденційності, цілісності та доступності. Вони також можуть відновити систему до нормального стану після несанкціонованої діяльності.
Заходи з відновлення	Заходи з відновлення поновлюють ресурси, функції та можливості до нормального стану після порушення політики безпеки.
Компенсаційні заходи	Компенсаційні заходи надають варіанти іншим заходам для посилення виконання політики безпеки. Компенсаційні заходи також можуть використовуватися замість заходів, які неможливо використати в даних умовах.

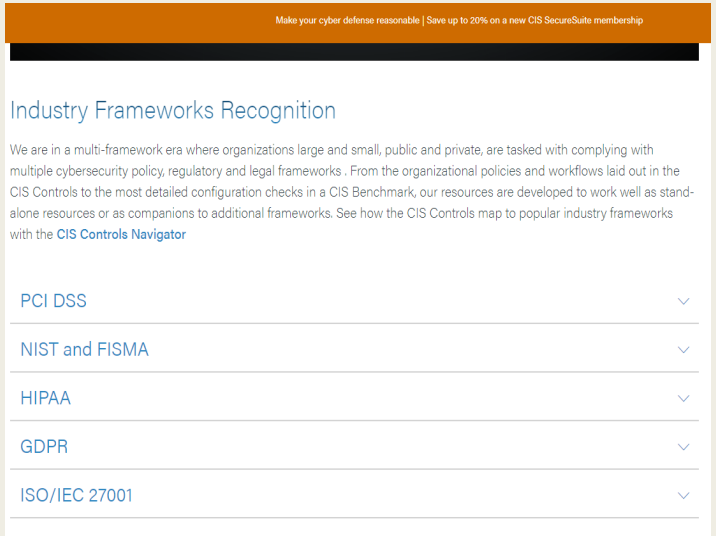
Контроль і відповідність

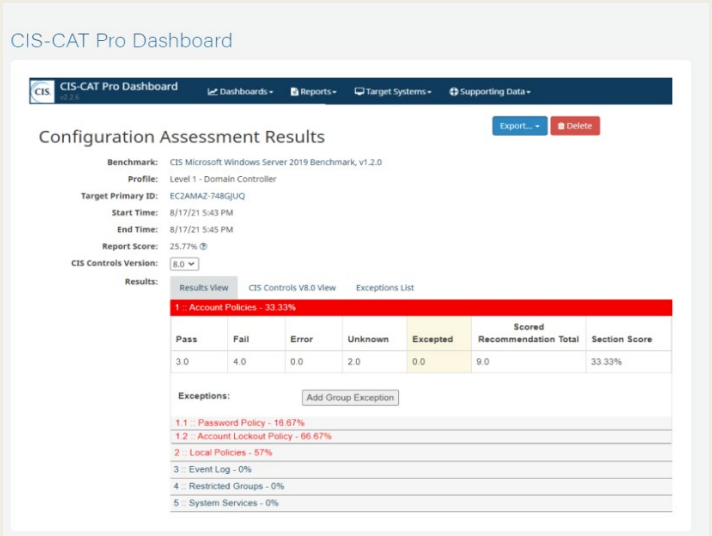
Центр безпеки в Інтернеті (Center for Internet Security – CIS) увідповіднив свої 18 критичних засобів контролю безпеки з деякими загальними фреймворками відповідності. Це увідповіднення надає корисні вказівки спеціалістам із безпеки, які працюють над створенням та підтримкою відповідності з необхідними фреймворками.

Пошук у Google **site:cisecurity.org mapping and compliance** повертає сторінку, на якій CIS надає вказівки щодо контролю безпеки, що стосуються основних галузевих фреймворків відповідності, таких як PCI DSS, NIST Cybersecurity Framework, FISMA, HIPAA, GDPR та ISO/IEC 27001. Там можна знайти корисні посилання та довідкову інформацію щодо того, як заходи контролю CIS забезпечують відповідність різним фреймворкам.

Крім того, члени CIS отримують доступ до керівництва та інструменту оцінки контролю CIS-CAT Pro, який допомагає оцінювати відповідність шляхом зіставлення засобів контролю CIS з окремими фреймворками відповідності.







Приклад: У результаті проведеної оцінки ризику організація збирається впровадити заходи контролю безпеки, перераховані нижче. Якими будуть правильні мітки функціонального контролю до кожного з них?

- **Запобіжні заходи контролю доступу** зупиняють небажану чи несанкціоновану діяльність або застосовують обмеження для авторизованих користувачів.
- **Стримувальні заходи** перешкоджають події відбутися.
- **Детективні заходи** визначають різні види несанкціонованої діяльності.
- **Коригувальні заходи** протидіють небажаному.
- **Заходи з відновлення** відновлюють ресурси, функції та можливості.
- **Компенсаційні заходи**, які також називають альтернативними заходами, є замінниками інших заходів контролю для посилення виконання політики безпеки.

Аналіз потреб організації в безпеці

Шкільна система складається з однієї вищої школи, однієї середньої школи та трьох початкових шкіл. Район налічує близько 2500 учнів, 210 викладачів, 220 осіб адміністративно-допоміжного персоналу та 25 обслуговуючих працівників. Інтернет-точка присутності та центр обробки даних розміщені в середній школі, де також розташовані офіси керівництва. Школи підключені до середньої школи через надлишкову волоконно-оптичну мережу. Центр обробки даних містить усі необхідні сервери в одному місці.

Компанію найняли для аналізу фізичної безпеки та кібербезпеки шкільної системи Грінвілла. Нещодавно стався інцидент, коли старшокласник отримав облікові дані вчителя та увійшов в адміністративну мережу. Учень змінив свої оцінки, відключив камери відеоспостереження та отримав номери телефонів учнів.

Начальник служби безпеки району нещодавно залишила роботу і посада була вільна. За впровадження заходів безпеки відповідала низка консультантів і співробітників, а самі заходи безпеки не були належним чином задокументовані. Головне завдання — запропонувати заходи контролю безпеки, які слід запровадити, і проаналізувати поточну систему, щоб побачити, чи використовує вона ці заходи. Директор та шкільна рада склали перелік проблем безпеки. Необхідно використати наступні пункти як початкову точку для аналізу:

- Велика кількість комп'ютерів із застарілим апаратним і програмним забезпеченням безладно розміщені у всіх відокремлених підрозділах, більшість в класах і навчальних лабораторіях.
- Деякі відокремлені підрозділи на національному рівні зіткнулися із судовими позовами через втрату інформації про батьків через витоки даних.
- Інша шкільна дільниця у штаті була закрита, доки системи не будуть відновлені після атаки програм-вимагачів, які зашифрували дані, що зберігалися на кількох комп’ютерах в районній мережі.
- Академічні записи були доступні та змінені учнями.
- Батько, який не мав права бачитися зі своєю дитиною, отримав доступ до позашкільних заходів на території школи, яку відвідувала дитина.
- Сервер бібліотеки в центрі обробки даних був відключений прибиральником у минулому.
- Інформація про учня була розкрита адміністративним працівником у відповідь на шкідливий електронний лист.

Перегляд заходів контролю безпеки

Контроль безпеки можна розділити на три види:

1. **Контроль фізичної безпеки** – реалізується для контролю фізичного доступу до людей, обладнання, об'єктів та інформації.
2. **Технічний контроль безпеки** – реалізується для захисту апаратних і програмних систем та інформації, яку ці системи передають, обробляють або зберігають.
3. **Адміністративний контроль безпеки** – це політики, процедури, правила та інструкції, яких дотримується персонал для досягнення цілей безпеки організації.

Вважається, що заходи контролю безпеки виконують три функції:

1. **Запобіжну** – запобігають загрозам безпеки
2. **Детективну** – виявляють несанкціоновану діяльність
3. **Коригувальну** – усувають небажану активність шляхом відновлення систем до нормального CIA стану

Таблиця рекомендацій щодо конкретних заходів безпеки

	Запобіжна	Детективна	Коригувальна
Фізичний контроль			
Технічний контроль			
Адміністративний контроль			

	Запобіжна	Детективна	Коригувальна
Фізичний контроль	• Заблокований доступ із сигналізацією до шкільних будівель • Доступ лише адміністратора до центру обробки даних і мережних об’єктів • Спринклерні системи • Сигнали тривожної кнопки • Резервне живлення для критичних систем • Регулярне технічне обслуговування обладнання	• Система відеоспостереження • Сигналізація на дверях та вікнах, датчики руху • Детектори диму • Оцінка вразливості та пентестинг • Зовнішнє освітлення	• Усунення фізичних пошкоджень • Швидка заміна пошкодженого або несправного критичного обладнання • Підтримка запасів запасних частин • Повторна видача втрачених бейджів та карток доступу • Тимчасова оренда приміщення
Технічний контроль	• Мережні брандмауери або IPS • Брандмауери та антивірусне ПЗ на хостах • Багатофакторна аутентифікація для доступу до сховищ конфіденційних даних • Доступ через VPN для роботи вдома • Зміцнення системи мережних пристроїв • Шифрування даних записів про учнів • Контроль мережних додатків • Вичерпні дані та резервне копіювання ОС • Надійне управління виправленнями • Контроль до будівлі на основі карток • DNS-проксі	• Моніторинг доступу та інші журнали • Моніторинг безпеки мережі • Робота IDS • Збір і аналіз журналів з хостів • Пастки для хакерів • AAA або інші системи журналювання • SIEM • Базовий план мережі та аналіз тенденцій	• Управління виправленнями • Стримування та видалення шкідливих програм • Відновлення даних і образу диска з резервної копії
Адмін. контроль	• Бейджі для працівників • Прибирання дата-центру та мережних об’єктів тільки під наглядом • Реєстрація всіх гостей і видача бейджів гостям • Найм спеціального персоналу для охорони • Політика надійності та оновлення пароля • Навчання з питань безпеки для всього персоналу та учнів • Політики та групи контролю доступу на основі ролі • Політика та процедури управління активами	• Аудит оцінок • Перегляд журналу AAA	• Планування безперервності • Планування реагування на інциденти • Тренування реагування на інциденти • Експертиза • Навчання користувачів після інциденту

ВИСНОВКИ

- Ризик – це ймовірність втрати через загрозу, зловмисну дію чи несподівану подію, яка завдає шкоди інформаційним системам або активам організації.
- Вплив ризику – це пошкодження, завдані подією, яка спричиняє втрату активу(ів) або порушення роботи сервісу(ів).
- Мета управління ризиками полягає в тому, щоб зменшити ці загрози до прийнятного рівня та запровадити заходи контролю для підтримки цього рівня. Ризик може бути внутрішнім, зовнішнім або одночасно і тим і іншим.
- Процес управління ризиками вимагає окреслення ризику, оцінки ризику та реакції на ризик.
- Оцінка загроз є основою для оцінки ризику.
- Загроза – це можливість того, що вразливість буде виявлена та використана.
- Вектор загрози – це шлях, який зловмисник використовує для впливу на ціль.
- Джерела загроз поділяються на ворожі, випадкові, структурні та стихійні.
- Організації визначають розмір шкоди та перевіряють свої операційні ризики, виконуючи оцінювання ризиків, щоб переконатися, що управління ризиками відповідає всім їхнім бізнес-цілям.
- Вони визначають, чи є загроза низькою, прийнятною чи значною.
- Кількісний аналіз ризиків присвоює числа процесу аналізу ризиків.
- Якісний аналіз ризику використовує оцінки та сценарії, які відображають відношення ймовірності виникнення загрози до її впливу.

ВИСНОВКИ

- Матриця ризиків – це інструмент, який допомагає визначити пріоритети ризиків, щоб визначити, на які з них організація має розробити відповідь.
- Може розглядатися кілька підходів, включаючи прийняття ризику та періодичну його переоцінку, зниження ризику шляхом впровадження заходів контролю, повне уникнення ризику шляхом зміни підходу, передача ризику третій стороні.
- Контроль безпеки – це засоби захисту або контрзаходи, які організація вживає, щоб уникнути, виявити, протидіяти або мінімізувати ризики безпеки для активів організації.
- Адміністративний контроль складається з процедур і політик, які організація встановлює коли має справу з конфіденційною інформацією.
- Технічний контроль охоплює апаратне та/або програмне забезпечення, впроваджене для управління ризиками та забезпечення захисту.
- Фізичний контроль – це механізми, такі як огорожі та замки, що використовуються для захисту систем, об’єктів, персоналу та ресурсів.
- Функціональний контроль безпеки включає запобіжні, стримувальні, детективні, коригувальні, відновлювальні та компенсаційні заходи.