# Розділ 2. Куб кібербезпеки

Фахівці з кібербезпеки - це експерти, які займаються захистом у кіберпросторі. Джон Мак-Камбер один з перших експертів з кібербезпеки, розробив широко використовувану конструкцію під назвою Куб Мак-Камбера або Куб кібербезпеки. Він використовується як інструмент для захисту мереж, доменів та Інтернету. Куб кібербезпеки чимось нагадує кубик Рубика.

Перший вимір Куба кібербезпеки визначає три принципи інформаційної безпеки. Фахівці з кібербезпеки називають ці три принципи (конфіденційність, цілісність, доступність) КЦД-тріадою (CIA Triad). Другий вимір визначає три стани інформації або даних. Третій вимір куба визначає необхідні дії для забезпечення захисту. Ці виміри часто називають трьома категоріями гарантованої кібербезпеки.

Ця глава також описує модель кібербезпеки ISO. Вона являє собою міжнародну основу стандартизації та керування інформаційними системами.

# Принципи захисту

Перший вимір куба кібербезпеки визначає цілі захисту кіберпростору. Цілі, визначені в першому вимірі, є основоположними принципами. Цими трьома принципами є конфіденційність, цілісність і доступність. Ці принципи забезпечують орієнтир і дозволяють фахівцеві з кібербезпеки визначати пріоритети дій при захисті будь-якої мережної системи

Конфіденційність запобігає розкриттю інформації неавторизованим людям, ресурсам або процесам. Цілісність даних позначає їх точність, узгодженість та достовірність. Нарешті, доступність гарантує, що інформація доступна авторизованими користувачами у разі потреби. Для запам’ятовування цих трьох принципів використовуйте абревіатуру КЦД (англ. CIA).

**Стани даних**

Кіберпростір - це домен, що містить значну кількість критично важливих даних. Тому експерти з кібербезпеки зосереджені на захисті даних. Другий вимір куба кібербезпеки зосереджений на проблемах захисту даних, які знаходяться у кіберпросторі в різних станах. Дані мають три можливі стани:

* Дані в передачі
* Дані в стані спокою або зберігання
* Дані в обробці

Захист кіберпростору вимагає, щоб фахівці в області кібербезпеки гарантували безпеку даних у всіх трьох станах.

# Гарантії кібербезпеки

Третій вимір куба кібербезпеки визначає навички і знання, які фахівець з кібербезпеки може використовувати для захисту у кіберпросторі. Фахівці з кібербезпеки повинні використовувати цілу низку наявних навичок і знань, коли захищають дані в кіберпросторі. Вони повинні це робити залишаючись при цьому на стороні закону.

Куб кібербезпеки визначає три типи навичок, які використовуються для забезпечення захисту. Перша навичка включає в себе технології, пристрої та продукти для захисту інформаційних систем і запобігання діям кіберзлочинців. Фахівці з кібербезпеки повинні володіти спеціалізованими технологічними інструментами. Проте, Мак-Камбер нагадує їм, що для перемоги над кіберзлочинцями недостатньо самих лише технологічних засобів. Професіонали з кібербезпеки також повинні вибудовувати потужний захист через налаштування політик, процедур та рекомендацій, які дозволяють користувачам кіберпростору залишатися у безпеці та дотримуватися принципів передової практики. Нарешті, користувачі кіберпростору повинні прагнути більшої обізнаності щодо загроз у кіберпросторі та виробити культуру навчання та усвідомлення у сфері інформаційної безпеки.

# Принципи конфіденційності

Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Синонімом конфіденційності є приватність. Організації обмежують доступ, щоб гарантувати, що тільки уповноважені оператори можуть використовувати дані або інші мережні ресурси. Наприклад, програміст не повинен мати доступ до особистої інформації всіх співробітників.

Організації повинні навчати співробітників кращим методам захисту конфіденційної інформації, щоб захистити їх та себе від атак. Методи, які використовуються для забезпечення конфіденційності, включають шифрування даних, аутентифікацію і контроль доступу.

Захист конфіденційності даних

Організації накопичують великий обсяг даних. Значна частина цих даних є відкритою і не потребує захисту, наприклад, імена співробітників та номери їх телефонів. Проте деякі дані потребують особливого захисту. Конфіденційна інформація - це дані, захищені від несанкціонованого доступу для гарантування безпеки окремій особі або організації. Існує три типи конфіденційної інформації:

* Персональна інформація - це особиста інформація, а саме дані, за допомогою яких можна визначити особистість людини. На рисунку 2 наведена ця категорія даних.
* Ділова інформація - це інформація, яка у разі оприлюднення може створити проблеми для організації. На рисунку 3 наведена ця категорія даних.
* Секретна інформація - це інформація, що належить державним органам, засекречена через високий рівень конфіденційності. На рисунку 4 наведена ця категорія даних.

Керування доступом

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших ресурсів даних. Концепція ААО (англ. AAA) включає в себе три служби безпеки: аутентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу.

Перше «А» в ААО (ААА) позначає аутентифікацію. ***Аутентифікація***перевіряє особу користувача для запобігання несанкціонованому доступу. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором. Окрім того, користувачі повинні підтвердити свою особу за одним із способів, як показано на рисунку 1.

* Надати інформацію яку вони знають (наприклад, пароль)
* Підтвердити наявність чогось (наприклад, токен або картка)
* Надати біометричну інформацію (наприклад, відбитки пальців)

Наприклад, для зняття готівки через банкомат, вам потрібна ваша банківська картка та PIN-код. Це також є прикладом багатофакторної аутентифікації. Для багатофакторної аутентифікації потрібно декілька типів аутентифікації. Найбільш популярною формою аутентифікації є використання паролів.

***Авторизація***, визначає через свою службу до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати, як показано на рисунку 2. Деякі системи реалізують це за допомогою списку керування доступом або ACL (англ. Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження аутентифікації. Те, що ви можете увійти в корпоративну мережу, не означає, що у вас є дозвіл на використання високошвидкісного кольорового принтера. Авторизація також може контролювати, коли користувач має доступ до певного ресурсу. Наприклад, співробітники можуть мати доступ до бази даних продажів в робочий час, але система блокує їх у неробочий час.

***Облік***, відстежує дії користувача, а саме, до яких даних вони зверталися, тривалість використання ресурсів та будь-які зроблені зміни. Наприклад, банк відстежує облікові записи кожного клієнта. Аудит цієї системи може виявити час і кількість всіх транзакцій, а також співробітника або системи, які виконували транзакції. Служби обліку кібербезпеки працюють так само. Система відстежує кожну транзакцію даних і надає результати аудиту. Для запровадження аудиту системи адміністратор може налаштувати політики комп'ютера, як показано на рисунку 3.

Концепція ААО (AAA) аналогічна використанню кредитної картки, як показано на рисунку 4. Кредитна карта ідентифікує, хто може її використовувати, скільки може витратити цей користувач і веде облік товарів або послуг, які користувач придбав.

У сфері кібербезпеки облік виконується у режимі реального часу. Веб-сайти, такі як Norse, показують атаки в режимі реального часу на основі даних, зібраних в рамках системи обліку або відстеження. Натисніть [тут](http://map.norsecorp.com/) щоб відвідати веб-сайт Norse.

# Закони та відповідальність

Конфіденційність і приватність здаються взаємозамінними, але з юридичної точки зору вони означають різні речі. Більшість приватних даних конфіденційні, але не всі конфіденційні дані є приватними. Доступ до конфіденційної інформації відбувається після підтвердження правильної авторизації. Фінансові установи, лікарні, медичні працівники, юридичні фірми та підприємства обробляють конфіденційну інформацію. Конфіденційна інформація має непублічний статус. Збереження конфіденційності - це скоріше етичний обов’язок.

Приватність пов'язана з правильним використанням даних. Коли організації збирають інформацію, надану клієнтами або співробітниками, вони повинні використовувати ці дані лише за прямим призначенням. Більшість організацій зажадають, щоб клієнт або співробітник підписали необхідний документ, надавши організації право використовувати дані.

Всі закони закони США, які перераховані на рисунку 1, включають положення про захист приватного життя. На рисунку 2 наведена вибірка законів інших країн. Більшість з цих законів є відповіддю на масове зростання збору даних.

Зростаюче число законів, що стосуються приватності, створює величезне навантаження для організацій, які збирають і аналізують дані. Політика - кращий спосіб для організації дотримуватися законів, що стосуються конфіденційності. Політики дозволяють організаціям застосовувати певні правила, процедури і процеси при зборі, зберіганні та спільному використанні даних.

# Принцип цілісності даних

Цілісність - це точність, узгодженість і достовірність даних протягом всього життєвого циклу. Іншими словами цілісність - це якість. Дані піддаються деяким операціям, таким як збір, зберігання, вилучення, оновлення та передача. Дані повинні залишатися незмінними під час виконання всіх цих операцій неавторизованими суб'єктами.

Методи, які використовуються для забезпечення цілісності даних, включають хешування, перевірку достовірності даних, перевірку узгодженості даних і керування доступом. Системи цілісності даних можуть включати один або декілька методів, наведених вище.

# Потреба в цілісності даних

Цілісність даних є фундаментальним компонентом інформаційної безпеки. Потреба в цілісності даних залежить від того, як організація використовує дані. Наприклад, Facebook не перевіряє дані, які користувач публікує в профілі. Банк або фінансова організація надають більшого значення цілісності даних, ніж Facebook. Транзакції і рахунки клієнтів повинні бути точними. В організації охорони здоров'я цілісність даних може бути питанням життя або смерті. Інформація в рецептах повинна бути точною.

Захист цілісності даних є постійною проблемою для більшості організацій. Втрата цілісності даних може привести до того, що всі дані будуть недостовірними або непридатними для використання.

# Перевірка цілісності

Перевірка цілісності - це спосіб вимірювання узгодженості набору даних (файлу, зображення або записів). Перевірка цілісності виконується за допомогою такого процесу як хеш-функції для миттєвого формування відбитку даних. Перевірка цілісності використовує цей відбиток аби переконатися, що дані залишилися незмінними.

Контрольна сума є одним із прикладів хеш-функції. Контрольна сума підтверджує цілісність файлів або рядків символів до і після їх передачі з одного пристрою на інший через локальну мережу або Інтернет. Контрольна сума просто перетворює кожну частину інформації в значення і підсумовує їх. Щоб перевірити цілісність даних, система, яка отримала файл, повторює цей процес. Якщо дві суми рівні, дані дійсні (рисунок 1). Якщо вони не рівні, десь в процесі передачі відбулася зміна (рис. 2).

На сьогоднішній день популярні такі хеш-функції як MD5, SHA-1, SHA-256 і SHA-512. Ці хеш-функції використовують складні математичні алгоритми. Значення хешу використовується для порівняння. Наприклад, після завантаження файлу користувач може перевірити його цілісність, порівнюючи хеш-значення джерела з тим, яке генерується будь-яким хеш-калькулятором.

Організації використовують контроль версій для запобігання випадковим змінам від авторизованих користувачів. Два користувачі не можуть оновити один і той самий об'єкт. Об'єктами можуть бути файли, записи бази даних або транзакції. Наприклад, у першого користувача, який відкрив документ, є дозвіл на зміну цього документа. У другого - є версія лише для читання.

Точні резервні копії допомагають зберегти цілісність даних, якщо дані пошкоджені. Організації необхідно перевірити результат резервного копіювання, щоб забезпечити цілісність резервного копіювання до втрати даних.

Авторизація визначає, хто має доступ до ресурсів організації, виходячи з необхідності. Наприклад, дозвіл на доступ до файлів і засоби контролю доступу користувачів гарантують, що тільки деякі користувачі можуть змінювати дані. Адміністратор може встановлювати дозволи для файлу тільки для читання. В результаті користувач, який одержує доступ до цього файлу, не може вносити ніяких змін.

# Принцип доступності

Доступність даних - це принцип, який використовується для опису необхідності постійно підтримувати доступність інформаційних систем і послуг. Кібератаки і збої системи можуть перешкоджати доступу до інформаційних систем і служб. Наприклад, перериванням доступності веб-сайту шляхом виведення його з ладу можуть скористатися конкуренти. Ці атаки типу «відмова в обслуговуванні» (DoS) загрожують доступності системи і не дозволяють користувачам отримувати доступ до інформаційних систем і використовувати їх при необхідності.

Методи, які використовуються для забезпечення доступності, включають системне резервування, резервне копіювання системи, підвищену відмовостійкість системи, технічне обслуговування обладнання, сучасні операційні системи та програмне забезпечення і плани по швидкому відновленню від непередбачених лих.

П'ять дев'яток

Люди використовують різні інформаційні системи в повсякденному житті. Комп'ютери та інформаційні системи контролюють зв'язок, транспорт і виробництво продукції. Постійна доступність інформаційних систем необхідна для сучасного життя. Термін «висока доступність» описує системи, призначені для запобігання простоям. Висока доступність забезпечує рівень продуктивності протягом більш тривалого, ніж зазвичай, періоду. Системи високої доступності найчастіше використовують три принципи проектування (рисунок 1):

* Усунути окремі точки відмови
* Забезпечити надійний план швидкого відновлення роботи на випадок надзвичайної ситуації
* Виявлення збоїв у міру їх виникнення

Мета полягає в тому, щоб продовжувати працювати в екстремальних умовах, наприклад під час атаки. Одна з найпопулярніших технологій високої доступності - п'ять дев'яток. Назва п'ять дев'яток пов’язана з доступністю ресурсу 99,999% часу. Це означає, що час простою становить менше 5,26 хвилин на рік. На рисунку 2 представлені три кроки для досягнення п'яти дев'яток.

Забезпечення доступності

Організації можуть забезпечити доступність, регулярно виконуючи такі дії:

* Обслуговування обладнання
* Оновлення ОС та системи
* Резервне копіювання
* Планування дій на випадок стихійних лих
* Нові технологічні реалізації
* Моніторинг надзвичайної активності
* Перевірка доступності

# Типи сховищ даних

Збережені дані належать до даних у стані спокою. Дані в стані спокою означають, що пристрій зберігання зберігає дані, коли жоден користувач або процес не використовує їх. Пристрій зберігання може бути локальним (на обчислювальному пристрої) або централізованим (в мережі). Існує багато опцій для зберігання даних.

Пряме сховище (direct-attached storage, DAS) - це сховище, що під'єднане до комп'ютера. Жорсткий диск або USB-накопичувач - приклад сховища з прямим підключенням. За замовчуванням системи не налаштовані для спільного використання сховища з прямим підключенням.

Резервний масив незалежних дисків (Redundant array of independent disks, RAID) використовує кілька жорстких дисків у масиві і являє собою об'єднання декількох дисків, які розглядаються операційною системою як один. RAID забезпечує підвищену продуктивність і відмовостійкість.

Мережний пристрій зберігання даних (network attached storage, NAS) - це пристрій, підключений до мережі, який дозволяє авторизованим користувачами зберігати та отримувати дані з централізованого сховища. Пристрої NAS гнучкі і масштабовані, що дозволяє адміністраторам збільшувати ємність у разі необхідності.

Мережа зберігання даних ( storage area network, SAN) - це мережна система зберігання, яка під'єднується до мережі за допомогою високошвидкісних інтерфейсів. Це дозволяє підвищити продуктивність і забезпечує можливість підключення декількох серверів до централізованого дискового сховища.

Хмарне сховище (Cloud storage) - це вид віддаленого сховища, при якому використовується простір на накопичувачах в дата-центрі провайдера, доступ до даних може бути організований з будь-якого комп'ютера з доступом до мережі Інтернет. Google Drive, iCloud і Dropbox - все це приклади постачальників хмарних сховищ.

# Проблеми захисту збережених даних

Збереження даних - це складне завдання для організацій. Для покращення зберігання даних організації можуть вдатися до автоматизації та виконувати централізоване резервне копіювання даних.

Сховище з прямим підключенням може бути одним з найскладніших типів зберігання даних з точки зору контролю та керування. Воно найбільш вразливе до шкідливих атак на локальний хост. Збережені дані можуть також містити дані резервного копіювання. Резервні копії можуть створюватися вручну або автоматично. Організації повинні обмежувати типи даних, що зберігаються в сховищі з прямим підключенням. Зокрема, на них не слід зберігати критично важливі дані.

Мережні системи зберігання пропонують більш безпечний варіант. Такі мережні системи зберігання даних як RAID, SAN і NAS забезпечують більшу продуктивність та надлишковість. Проте мережні системи зберігання складніші для налаштування та керування. Також вони обробляють більші обсяги даних, що створює значний ризик для організації при виході пристрою з ладу. Особливу увагу при використанні мережних систем зберігання даних слід приділяти налаштуванню, тестуванню і моніторингу системи.

Методи передачі даних

Передача даних - це надсилання інформації з одного пристрою на інший. Існує багато способів передачі інформації між пристроями:

* **Sneaker net** - використовує знімні носії для фізичного переміщення даних з одного комп'ютера на інший
* **Дротові мережі** - використовують кабелі для передачі даних
* **Бездротові мережі** - використовують радіохвилі для передачі даних

Організації ніколи не зможуть уникнути використання Sneaker net.

Дротові мережі включають в себе мідні та волоконно-оптичні кабелі. Дротові мережі можуть обслуговувати місцеву географічну зону (локальна мережа), або прокладатися на великі відстані (глобальні мережі).

Бездротові мережі замінюють дротові , стають швидшими і здатні забезпечити більшу пропускну здатність. Бездротові мережі збільшують кількість користувачів, які під’єднуються до них з мобільних пристроїв у невеликих офісах і корпоративних мережах.

У дротових і бездротових мережах використовуються пакети або блоки даних. Термін «пакет» означає одиницю даних, яка переміщується між джерелом і пунктом призначення в мережі. Стандартні протоколи, такі як протокол Інтернету (IP) і протокол передачі гіпертексту (HTTP), визначають структуру і формат пакетів даних. Ці стандарти мають відкриті вихідні коди і є загальнодоступними. Захист конфіденційності, цілісності та доступності переданих даних - один з найважливіших обов'язків фахівця в області кібербезпеки.

Проблеми захисту даних під час передачі

Захист переданих даних є однією з найскладніших задач фахівця з кібербезпеки. Зі зростання кількості мобільних і бездротових пристроїв фахівці в області кібербезпеки несуть відповідальність за щоденний захист даних, які перетинають їх мережу. Фахівець з кібербезпеки повинен вирішити кілька проблем захисту цих даних:

* **Захист конфіденційності даних** - кіберзлочинці можуть перехоплювати, зберігати і викрадати дані під час їх передачі між пристроями. Кібер-професіонали повинні вжити заходів для протидії цим процесам.
* **Захист цілісності даних** - кіберзлочинці можуть перехоплювати і змінювати дані в момент їх передачі. Для запобігання цим діям фахівці з кібербезпеки впроваджують системи підтримки цілісності даних, які перевіряють достовірність і автентичність переданих даних.
* **Захист доступності даних** - кіберзлочинці можуть використовувати шахрайські або неавторизовані пристрої для переривання доступ до даних. Простий мобільний пристрій може являти собою локальну точку бездротового доступу і вводити в оману звичайних користувачів. Кіберзлочинець може перехопити авторизоване підключення до захищеної службі або пристрою. Для протидії цим процесам фахівці з мережної безпеки можуть впроваджувати системи взаємної аутентифікації. Системи взаємної аутентифікації вимагають, щоб користувач авторизувався на сервері, а сервер у відповідь аутентифікував користувача.

# Форми обробки і обчислення даних

Третій стан даних - це дані в обробці. У цьому стані дані перебувають під час початкового введення, зміни, обчислення або виведення.

Захист цілісності даних починається з початкового введення даних. Організації використовують кілька методів для збору даних, таких як ручне введення даних, форми сканування, завантаження файлів і зчитування даних з датчиків. Кожен з цих методів створює потенційну загрозу цілісності даних. Прикладом пошкодження даних під час введення є помилки введення даних або відключені, несправні або непрацюючі системні датчики. До помилок введення належать також неправильне маркування і невірні або неузгоджені формати даних.

Модифікація даних - це будь-яка зміна вихідних даних. Наприклад, коли користувач вручну змінює дані або програма обробляє та оновлює дані, або коли дані змінюються внаслідок відмови обладнання. Процеси, такі як кодування/декодування, компресія/декомпресія і шифрування/дешифрування, є прикладами модифікації даних Шкідливий код також призводить до пошкодження даних.

Пошкодження даних також відбувається під час процесу виведення даних. Вивід даних відповідає передачі даних на принтери, електронні дисплеї або безпосередньо на інші пристрої. Точність вихідних даних має вирішальне значення, оскільки вивід інформації впливає на прийняття рішень. Прикладами пошкодження вихідних даних можуть бути неправильне використання обмежувачів даних, невірні параметри з’єднання і невідповідно налаштовані принтери.

# Проблеми захисту даних у процесі обробці

Захист даних від некоректних змін під час обробки може мати негативний вплив. Помилки програмного забезпечення є причиною багатьох невдач і катастроф. Наприклад, всього за два тижні до Різдва деякі зі сторонніх роздрібних продавців Amazon випадково виставили ціну в один цент на свої товари. Збій тривав одну годину. Помилка призвела до того, що тисячі покупців придбали за безцінь товари, а компанії втратила дохід. У 2016 році термостат Nest зазнав збій і залишив користувачів без тепла. Термостат Nest - це інтелектуальна технологія, що належить Google. Збій програмного забезпечення залишив користувачів, буквально, на холоді. Проблеми з оновленням програмного забезпечення призвели до розрядки акумуляторів пристрою, через що не було можливості контролювати температуру. В результаті клієнти не змогли нагріти свої будинки або отримати гарячу воду в один з найхолодніших вихідних в році.

Для захисту даних під час обробки потрібні ретельно спроектовані системи. Фахівці з кібербезпеки розробляють політики та процедури, які вимагають тестування, обслуговування та оновлення систем, щоб вони працювали з найменшою кількістю помилок.

Технології захисту на основі програмного забезпечення

Програмні засоби захисту - це програми і служби, які захищають операційні системи, бази даних та інші служби, що працюють на робочих станціях, портативних пристроях і серверах. Адміністратори встановлюють програмні запобіжні засоби на окремих хостах або серверах. Існує кілька програмних технологій, які використовуються для захисту даних організації:

* Брандмауери керують віддаленим доступом до системи. Зазвичай брандмаурер входить до складу операційних систем, або користувач може придбати чи завантажити брандмауер від інших виробників.
* Сканери мережі та портів виявляють і контролюють відкриті порти на хості або сервері.
* Аналізатори протоколів або аналізатори сигнатур - це пристрої, які збирають і досліджують мережний трафік. Вони виявляють проблеми з продуктивністю, неправильні конфігурації, додатки, що некоректно працюють, визначають шаблони типового та нормального трафіку і усувають (налагоджують) проблеми зі зв'язком.
* Сканери вразливостей - це комп'ютерні програми, призначені для оцінки слабких місць комп'ютерів або мереж.
* Системи виявлення вторгнень на базі хоста (IDS) перевіряють активність тільки на хост-системах. IDS генерує лог-файли (записи у системному журналі) та попереджувальні повідомлення при виявленні незвичної активності. Система, яка зберігає конфіденційні дані або надає критично важливі, може бути цільовою для використання системи виявлення вторгнень на базі хостів (IDS).

Апаратні засоби захисту

Існує кілька апаратних технологій, що використовуються для захисту даних організацій:

* Брандмауер (апаратний) блокує небажаний трафік на основі правил, які визначають вхідний і вихідний трафік, дозволений у мережі.
* Спеціалізовані системи виявлення вторгнень (IDS) виявляють ознаки атак або незвичного трафіку в мережі і надсилають сповіщення.
* Системи запобігання вторгненням (Intrusion Prevention Systems - IPS) виявляють ознаки атак або незвичного трафіку в мережі, генерують попередження і вживають коригувальних дій.
* Служби фільтрування контенту контролюють доступ і передачу небажаного або образливого вмісту.

Мережні технології захисту

Для захисту даних організації використовуються кілька мережних технологій:

* **Віртуальна приватна мережа (VPN)**) - це безпечна віртуальна мережа, що використовує загальнодоступну мережу (Інтернет). Безпека VPN полягає в шифруванні вмісту пакета між кінцевими точками.
* **Контроль доступу до мережі (Network Access Control - NAC)** - вимагає набору перевірок, перш ніж дозволяти пристрою підключатися до мережі. Такі перевірки можуть стосуватися встановлення останньої версії антивірусного програмного забезпечення або оновлення операційної системи.
* **Безпека бездротової точки доступу** реалізується за допомогою аутентифікації і шифрування.

Хмарні технології захисту

Хмарні технології, переносять технологічний компонент захисту від організації до провайдера хмарних обчислень. Існує три основні служби хмарних обчислень:

* **Програмне забезпечення як послуга (SaaS)** дозволяє користувачам отримувати доступ до прикладного програмного забезпечення та баз даних. Хмарні провайдери управляють інфраструктурою. Користувачі зберігають дані на серверах хмарного провайдера.
* **Інфраструктура як послуга (IaaS)** забезпечує віртуальні обчислювальні ресурси через Інтернет. Провайдер надає у користування апаратне та програмне забезпечення, сервери і компоненти зберігання.
* **Платформа як послуга (PaaS)** забезпечує доступ до інструментів і служб розробки, які використовуються для створення застосунків.

Провайдери хмарних послуг розширили ці опції, включивши ІТ-службу (ITaaS), яка забезпечує ІТ-підтримку для моделей обслуговування IaaS, PaaS і SaaS. У моделі ITaaS організація укладає контракти з постачальником хмарних послуг для отримання необхідних послуг.

Постачальники хмарних послуг використовують віртуальні пристрої безпеки, які працюють у віртуальному середовищі з попередньо упакованою, спрощеною операційною системою, яка працює на віртуалізованому обладнанні.

Впровадження системи освіти та навчання в галузі кібербезпеки

Інвестування великих коштів у технології не спричинить належного ефекту, якщо люди в організації залишатимуться найслабшою ланкою в кібербезпеці. Програма інформування про безпеку надзвичайно важлива для організації. Співробітник може не навмисно вчиняти потенційно небезпечні дії, через те, що не знає як належить поводитись. Існує кілька способів реалізації офіційної навчальної програми:

* Зробити тренінг з безпеки необхідним елементом для початку роботи у компанії
* Враховувати обізнаність з питань безпеки при прийомі на роботу або при оцінці працездатності
* Проведення очних тренінгів
* Проводити онлайн-курси

Таке навчання має проводитися на регулярних засадах, оскільки нові загрози з’являються постійно.

Створення культури обізнаності про кібербезпеку

Члени організації повинні бути поінформовані про політику безпеки і мати необхідні знання, щоб зробити безпеку частиною їх повсякденній діяльності.

Активна програма інформування про безпеку залежить від:

* Внутрішнього середовища організації
* Рівня загрози

Створення культури обізнаності про кібербезпеку - це постійне зусилля, яке вимагає ініціативи вищого керівництва і прихильності всіх користувачів і співробітників. Вплив культури кібербезпеки організації починається з розробки політики та процедур з боку керівництва. Наприклад, багато організацій мають дні обізнаності про кібербезпеку. Організації можуть також розміщувати банери і вивіски для підвищення загальної поінформованості про кібербезпеку. Створення семінарів орієнтованих на кібербезпеку допомагає підвищити рівень обізнаності.

Політики

Політика безпеки - це набір правил для компанії, який включають правила поведінки для користувачів і адміністраторів і визначають системні вимоги. Такі цілі, правила і вимоги в сукупності забезпечують безпеку мережі, даних і комп'ютерних систем всередині організації.

Комплексна політика безпеки виконує кілька завдань:

* Демонструє серйозне ставлення до безпеки.
* Встановлює правила поведінки.
* Забезпечує узгодженість в роботі системи, придбанні та використанні програмного і апаратного забезпечення, а також в його обслуговуванні.
* Визначає юридичні наслідки порушень.
* Надає співробітникам служби безпеки підтримку керівництва.

Політика безпеки інформує користувачів, персонал і керівників про вимоги організації до захисту технологічних і інформаційних активів. Політика безпеки також визначає механізми, необхідні для дотримання вимог безпеки.

Як показано на рисунку, політика безпеки зазвичай включає в себе:

* **Політики ідентифікації і аутентифікації** - визначає уповноважених осіб, які можуть мати доступ до мережних ресурсів і окреслює процедури перевірки.
* **Політика паролів -** забезпечує, щоб паролі відповідали мінімальним вимогам і регулярно змінювалися.
* **Політика використання -** визначає мережні ресурси використання яких, прийнятне для організації. Вона також може визначати наслідки порушень правил.
* **Політика віддаленого доступу -**визначає, як віддалені користувачі можуть отримати доступ до мережі і до чого саме надавати доступ.
* **Політика мережного обслуговування -** визначає операційні системи мережних пристроїв і процедури оновлення додатків для кінцевих користувачів.
* **Політика обробки інцидентів -**описує порядок дій у разі інцидентів пов'язаних з безпекою.

Одним з найбільш поширених компонентів політики безпеки є політика прийнятного використання (acceptable use policy - AUP). Цей компонент визначає, що користувачі можуть і не можуть робити з різними системними компонентами. Для уникнення непорозумінь, політика AUP повинна бути максимально докладною. Наприклад, AUP містить перелік конкретних веб-сайтів, груп новин або програм з інтесивним трафіком, до яких користувачі не мають доступу з робочих комп’ютерів або через мережу компанії.

# Стандарти

Стандарти допомагають ІТ-персоналу підтримувати узгодженість в роботі мережі. Стандартні документи визначають технології, які необхідні конкретним користувачам або програмам, а також програмні вимоги чи критерії, яких слід дотримуватися організації. Це допомагає ІТ-фахівцям підвищити ефективність і спростити проектування, обслуговування та усунення неполадок.

Одним з найважливіших принципів безпеки є послідовність. З цієї причини організаціям необхідно встановлювати стандарти. Кожна організація розробляє стандарти для підтримки свого унікального операційного середовища. Наприклад, організація визначає політику паролів. Стандарт передбачає, що паролі повинні складатися мінімум з восьми букв у верхньому та нижньому регістрів, а також цифр і містити принаймні один спеціальний символ. Користувач повинен міняти пароль кожні 30 днів, а історія паролів з 12 попередніх паролів гарантує, що користувач створює унікальні паролі на один рік.

Методичні рекомендації

Методичні рекомендації - це список пропозицій про те, як робити речі більш ефективно і надійно. Вони схожі на стандарти, але більш гнучкі і зазвичай не є обов'язковими. Ці рекомендації визначають, як розробляються стандарти і гарантують дотримання загальних політик безпеки.

Деякі з найбільш корисних рекомендацій складають кращі практики для роботи організації. Методичні рекомендації також доступні з наступних джерел:

* Національний інститут стандартів і технологій (NIST) Центр ресурсів комп'ютерної безпеки (Рисунок 1)
* Агентство національної безпеки (NSA) (Рисунок 2)
* Загальні стандартні критерії (Рисунок 3)

Використовуючи приклад політики паролів, методичні рекомендації пропонують взяти фразу типу «I have a dream» і перетворити її на надійний пароль, Ihv@dr3@m. Користувач може створювати інші паролі з цієї фрази, змінюючи число, переміщаючи символ або змінюючи знак пунктуації.

# Процедури

Документи процедури більш докладні і детальні, ніж стандарти і рекомендації. Документи процедури включають в себе деталі реалізації, які зазвичай містять покрокові інструкції.

На рисунку показаний приклад процедури, використовуваної для зміни пароля. Великі організації повинні використовувати процедурні документи для дотримання послідовності розгортання, необхідної для безпечного середовища.

# Огляд моделі

Фахівцям в області безпеки необхідно забезпечити захист інформації всередині організації. Це монументальне завдання і необґрунтовано очікувати, що одна людина має всі необхідні для цього знання. Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (IEC) розробила комплексну структуру для керування інформаційною безпекою. Модель кібербезпеки ISO/IEC має таке ж призначення для професіоналів в області кібербезпеки, що і мережна модель OSI для мережних інженерів. Обидві моделі створюють основу для розуміння і виконання складних завдань, спрямованих на забезпечення безпеки.

# Галузі кібербезпеки

ISO/IEC 27000 - це стандарт інформаційної безпеки, опублікований в 2005 році і переглянутий в 2013 році. ISO публікує стандарти ISO 27000. Незважаючи на те, що стандарти не є обов'язковими, більшість країн використовують їх які основу для забезпечення інформаційної безпеки.

Стандарти ISO 27000 описують впровадження комплексної системи керування інформаційною безпекою (ISMS). ISMS складається з усіх адміністративних, технічних і оперативних заходів контролю, що забезпечують безпеку інформації всередині організації. ISO 27000 являє собою практичні рекомендації в дванадцяти незалежних галузях. Ці дванадцять галузей служать для організації, на високому рівні, захисту для широкого спектру інформації.

Структура моделі кібербезпеки ISO відрізняється від моделі OSI тим, що вона використовує галузі, а не шари, для опису категорій безпеки. Причина цього в тому, що модель кібербезпеки ISO не є ієрархічною. Це однорангова модель, в якій кожна сфера має прямий зв'язок з іншою. Модель кібербезпеки ISO 27000 дуже схожа на модель OSI, тому для успішної побудови кар'єри фахівцеві з кібербезпеки дуже важливо розуміти обидві моделі.

Для короткого опису клацніть на кожну галузь на рисунку.

Дванадцять галузей служать спільною основою для розробки стандартів безпеки і ефективних методів керування безпекою. Вони також допомагають полегшити взаємодію між організаціями.

# Цілі контролю

Дванадцять галузей складаються з цілей контролю, визначених у частині 27001 стандарту. .Цілі контролю визначають вимоги високого рівня для впровадження комплексного ISM (керування інформаційною безпекою). Керівництво організації використовує цілі контролю ISO 27001 для визначення і публікації політик безпеки організації. Цілі контролю забезпечують контрольний список для перевірок керування безпекою. Багато організацій мають пройти аудит ISMS, для отримання відзнаки відповідності стандарту ISO 27001.

Сертифікація та відповідність забезпечують довіру організацій, яким необхідно обмінюватися конфіденційними даними і операціями. Перевірки відповідності і безпеки підтверджують, що організації постійно вдосконалюють свою систему керування інформаційною безпекою.

Нижче наведено приклад завдання контролю:

*Контроль доступу до мереж з використанням відповідних механізмів аутентифікації для користувачів і обладнання.*

Контроль

В ISO/IEC 27002 визначаються системи керування інформаційною безпекою. Елементи контролю більш деталізовані, ніж цілі. Цілі контролю повідомляють організації, що робити. Елементи контролю визначають, як досягти мети.

З метою контролю, для керування доступом до мереж з використанням відповідних механізмів аутентифікації для користувачів і обладнання, можна надати таку вказівку:

*Використовуйте надійні паролі. Сильний пароль містить не менше восьми символів, які є комбінацією літер, цифр і символів (@, #, $,% і т. д), якщо це дозволено. Паролі чутливі до регістру, тому сильний пароль містить літери як верхнього так і нижнього регістрів.*

Фахівці з кібербезпеки визнають наступне:

* Елементи контролю не є обов'язковими, але вони широко прийняті і застосовуются.
* Елементи контролю повинні підтримувати нейтралітет по відношенню до постачальника, щоб уникнути схиляння до конкретного продукту або компанії.
* Елементи контролю подібні до рекомендацій. Це означає, що може бути більше одного способу досягнення мети.

# Модель кібербезпеки ISO та тріада КЦД

ISO 27000 є універсальною структурою для кожного типу організації. Для ефективного використання структури, організація повинна визначити які галузі, контрольні цілі і засоби контролю застосовувати для свого середовища та операцій.

Цілі контролю ISO 27001 служать контрольним списком. Першим кроком, який приймає організація, є визначення того, чи можуть бути застосовані ці контрольні цілі до організації. Більшість організацій формують документ під назвою Заява про придатність (Statement of Applicability - SOA). SOA визначає, які цілі контролю необхідно використовувати організації.

Різні організації приділяють більше уваги конфіденційності, цілісності і доступності в залежності від типу галузі. Наприклад, Google надає більшої ваги конфіденційності та доступності даних користувачів, аніж цілісності. Google не перевіряє дані користувача. Amazon приділяє велику увагу доступності. Якщо сайт недоступний, Amazon не виконує продажів. Це не означає, що Amazon ігнорує конфіденційність на користь доступності. Просто для Amazon доступність має більший пріоритет. Таким чином, Amazon може витрачати більше ресурсів, забезпечуючи наявність більшої кількості серверів для обслуговування покупок клієнтів.

Організація адаптує до свого використання доступні контрольні цілі і засоби контролю для найкращого задоволення своїх пріоритетів щодо конфіденційності, цілісності та доступності.

# Модель кібербезпеки ISO і можливі стани даних

Різні групи в межах організації можуть відповідати за дані в кожному стані. Наприклад, група безпеки мережі відповідає за дані під час передачі. Програмісти і користувачі відповідають за дані під час обробки. Фахівці з апаратної і серверної підтримки відповідають за збережені дані. Елементи керування ISO спеціально визначають цілі безпеки для даних в кожному з трьох станів.

У цьому прикладі представники кожної з трьох груп допомагають ідентифікувати застосовувані елементи контролю і визначити пріоритет кожного елемента в своїй області. Представник групи мережної безпеки визначає елементи керування, що забезпечують конфіденційність, цілісність і доступність всіх переданих даних.

# Модель кібербезпеки ISO і технології захисту

Цілі контролю ISO 27001 безпосередньо пов'язані з політикою, процедурами і керівними принципами кібербезпеки організації, які визначає вище керівництво. Елементи керування ISO 27002 забезпечують технічний напрям\

# Розділ 3. Кібербезпека - загрози, вразливості та атаки

Загрози, вразливості та атаки є центром уваги фахівців у галузі кібербезпеки. Загроза - це можливість того, що може відбутися небезпечна подія, яка призведе до втрат, наприклад атака. Вразливість - це вада, яка робить ціль атаки сприйнятливою до нападу. Атака - це навмисне використання виявлених вразливостей комп'ютерних інформаційних систем як з конкретною метою, так і просто для розваги. У кіберзлочинців можуть бути різні мотиви для вибору цілі атаки. Вони постійно шукають та виявляють вразливі системи. Зазвичай жертвами стають системи, на яких не встановлені оновлення або відсутній захист від вірусів і спаму.

У цьому розділі розглядаються найбільш поширені види кібератак. Фахівці з кібербезпеки повинні розуміти алгоритм реалізації кожної з атак, яку вразливість вона використовує і яким чином це впливає на жертву. Розділ починається з пояснення загрози шкідливого ПЗ і зловмисного коду, потім розглядаються типи шахрайства, які є предметом соціальної інженерії. Кібератаки - це тип нападу, який використовується кіберзлочинцями на цільові комп'ютерні системи, мережі та інші комп'ютерні пристрої. Зловмисники атакують як дротові так і бездротові мережі.

# Що таке шкідливе ПЗ?

Зловмисне програмне забезпечення або шкідливе ПЗ - це термін, який використовується для опису програмного забезпечення, призначеного для порушення роботи комп'ютера або отримання доступу до комп'ютерних систем без відому або дозволу користувача. Зловмисне програмне забезпечення стало загальним терміном, який використовується для опису всіх ворожих або нав'язливих програм. Термін "зловмисна програма" описує комп'ютерні віруси, черв'яки, троянські коні, програми-вимагачі, шпигунські програми, рекламне програмне забезпечення, псевдоантивіруси та ін. Деяке шкідливе ПЗ виявити легко, дію інших виявити практично неможливо.

# Віруси, Інтернет-черв'яки та "Троянські коні"

Кіберзлочинці досягають кінцевих пристроїв користувача, встановлюючи на них зловмисне програмне забезпечення. Натисніть кнопку «Перегляд», щоб переглянути анімацію для трьох найбільш поширених типів зловмисного програмного забезпечення.

**Віруси**

Вірус - це шкідливий програмний код, прикріплений до виконуваного файлу, наприклад, легітимної програми. Для більшості вірусів необхідно, щоб користувач запустив заражену програму, також вони можуть активуватися в конкретний час або дату. Комп'ютерні віруси зазвичай поширюються одним із трьох способів: через знімні носії; завантажуються з Інтернету; через вкладення електронної пошти. Віруси можуть бути нешкідливими і просто виводити рисунок на екран, або можуть бути руйнівними, як наприклад ті, що змінюють або видаляють дані. Щоб уникнути виявлення, вірус мутує. Комп'ютер може бути заражений вірусом просто в результаті того, що користувач відкрив файл. Деякі віруси вражають завантажувальний сектор або файлову систему флеш-накопичувачів USB, а з них можуть поширюватися на системний жорсткий диск комп’ютера. Також зараження вірусами може відбуватися при виконанні конкретної програми. Після активації вірусу він постійно заражатиме інші програми на комп'ютері або на інших комп'ютерах в мережі. Вірус Меліса став прикладом вірусу, який поширювався електронною поштою. Меліса завдала шкоди десяткам тисяч користувачів і, за приблизними оцінками, спричинила збитків на 1.2 мільярда доларів. Натисніть [тут](http://www.whoishostingthis.com/blog/2015/06/01/8-worst-viruses/) щоб дізнатись більше про віруси.

**Інтернет-черв'яки**

Черв'яки - це зловмисний код,, який поширюється самостійно, використовуючи вразливості мережної інфраструктури. Зазвичай черв'яки уповільнюють роботу мережі. На відміну від вірусів, які потребують запуску зараженої програми-носія, черв'яки можуть працювати самостійно. Після первинного інфікування черв'яки більше не потребують участі користувача. Після зараження вузла черв'як може швидко поширюватися мережею. Черв'яки діють за єдиним принципом. Всі вони використовують певну вразливість, мають механізм розповсюдження і виконують певну зловмисну дію.

Черв'яки відповідальні за деякі найбільш руйнівні атаки в Інтернеті. Наприклад, в 2001 році черв'як Code Red інфікував 658 серверів. За 19 годин цей черв'як заразив більше ніж 300 тисяч серверів.

**Троянський кінь**

Троянський кінь (троян) - це зловмисне програмне забезпечення, яке здійснює шкідливі дії під виглядом бажаної операції, наприклад онлайн-гри. Цей шкідливий код використовує привілеї користувача, який його запускає. Троянський кінь відрізняється від віруса тим, що прив'язується до невиконуваних файлів, таких як файли зображень, аудіофайли або ігри.

# Логічні бомби (Logic Bombs)

Логічна бомба - це шкідлива програма, яка використовує тригер (активатор) для пробудження шкідливого коду. Наприклад, активатором може бути дата, час, запуск інших програм, або видалення облікового запису користувача. Логічна бомба залишається неактивною, доки не відбудеться подія, що активує цей код. Після активації логічна бомба виконує зловмисний код, який завдає шкоди комп'ютеру. Цей тип зловмисного ПЗ може пошкодити записи в базі даних, видалити файли та атакувати операційні системи або застосунки. Нещодавно фахівці з кібербезпеки виявили новий тип логічних бомб, які атакують та руйнують апаратні компоненти робочих станцій та серверів, а саме вентилятори охолодження, процесор, пам'ять, жорсткі диски та блоки живлення. Логічна бомба примушує ці пристрої працювати в критичному режимі, доки вони не перегріються або не вийдуть з ладу.

# Програми - вимагачі

Програми-вимагачі (Ransomware) блокують комп'ютерну систему, або дані, які вона містить, доки жертва не сплатить викуп. Програми-вимагачі зазвичай шифрують дані на комп'ютері за допомогою ключа, що невідомий користувачу. Користувач має сплатити викуп зловмисникам, щоб зняти обмеження.

Деякі версії програм-вимагачів використовують вразливості конкретної системи для її блокування. Програми-вимагачі розповсюджуються аналогічно до Троянського коня через завантаження файлів або вразливості програмного забезпечення.

Оплата, яку має внести жертва, зазвичай відбувається через платіжну систему, яка не дозволяє відслідковувати отримувача. Після того, як жертва сплатить викуп, зловмисники надають їй програму, що розшифровує файли або надсилають код для розблокування. Натисніть [тут](http://www.exterminate-it.com/malpedia/ransomware-category) щоб дізнатись більше про програми-вимагачі.

# Backdoors та Rootkits

Термін backdoor (чорний хід) відноситься до програми або коду, доданого зловмисником, який скомпроментував систему. Backdoor обходить стандартну аутентифікацію, яка використовується для доступу до системи. До найбільш поширених програм цього типу відносяться Netbus і Back Orifice, що надають віддалений доступ до системи неавторизованим користувачам. Мета backdoor - надавати кібер-злочинцям доступ до системи в майбутньому, навіть після того, як організація виправить вразливість, яка була використана для атаки на систему. Зазвичай, щоб встановити backdoor, злочинці використовують авторизованих користувачів, які несвідомо запускають троянську програму на своєму ПК.

Руткіт (Rootkit) модифікує операційну систему для створення чорного ходу. Потім зловмисники використовують backdoor для віддаленого доступу до комп'ютера. Більшість руткітів використовують вразливості програмного забезпечення для підвищення рівня привілеїв (ескалації прав доступу) та модифікації системних файлів. Ескалація привілеїв можлива через помилки програмування або недоліки проектування і дозволяє зловмисникам отримати підвищений рівень доступу до мережних ресурсів та даних. Також руткіти здійснюють зміни в системи перевірки стану та інструментах моніторингу, що дуже ускладнює виявлення зловмисного ПЗ такого типу. Часто для знищення руткіту доводиться перевстановити операційну систему.

Захист від зловмисного ПЗ

Кілька простих кроків допоможуть захистити ваш комп'ютер від усіх видів зловмисного програмного забезпечення.

* **Антивірусна програма -** Більшість антивірусних пакетів успішно виявляють найпоширеніші форми шкідливого ПЗ. Проте щоденно кіберзлочинці розробляють і розповсюджують нові загрози. Тому ключем до ефективного захисту проти вірусів є постійне оновлення бази вірусних сигнатур. Сигнатура для віруса - це як відбиток пальця для людини. Вона ідентифікує характерні елементи зловмисного коду, за якими його можна розпізнати.
* **Актуальне ПЗ -** багато форм зловмисного ПЗ досягають своїх цілей через використання вразливостей програмного забезпечення як в операційних системах, так і в застосунках. Раніше вразливості операційної системи були основним джерелом проблем, на сьогоднішній день найбільший ризик становлять вразливості застосунків. В той час, як розробники операційних систем все швидше реагують на нові загрози, більшість розробників прикладного ПЗ на жаль нехтують цим.

Спам

Електронна пошта - це універсальний сервіс, що використовується мільярдами людей у всьому світі. Як один з найбільш популярних сервісів, електронна пошта стала головною вразливістю для користувачів та організацій. Спам, також відомий як небажана пошта, або небажаний електронний лист. У більшості випадків спам - це один зі способів реклами. Однак спам може містити небезпечні посилання, зловмисне ПЗ або оманливий вміст. Кінцевою метою такого спаму є отримання конфіденційної інформації користувача, такої як номер соціального страхування або інформація про банківський рахунок. Більшість спаму надходить з великої кількості комп'ютерів, які розташовані в мережах, заражених вірусом або Інтернет-черв'яком. Ці скомпрометовані комп'ютери надсилають максимально можливу кількість повідомлень електронної пошти.

Навіть за умови реалізації функцій захисту від спаму, повністю виключити небажану пошту все ж не вдасться. Ознайомтеся з деякими найбільш поширеними характеристиками спаму:

* В електронному листі відсутня тема.
* Електронний лист вимагає оновлення облікового запису.
* Текст електронного листа містить слова з помилками або дивну пунктуацію.
* Посилання в електронному листі є довгими та/або незрозумілими.
* Електронний лист виглядає як листування з реально існуючою організацією.
* Електронний лист вимагає від користувача відкрити вкладення.

Натисніть [тут](https://www.onguardonline.gov/articles/0038-spam) щоб отримати додаткову інформацію про спам.

Якщо користувач отримує електронний лист, що відповідає одному або декільком з цих характеристик, йому не варто відкривати цей лист або будь-які вкладення. Зазвичай політика використання електронної пошти організації вимагає, щоб користувач, який отримав електронний лист такого типу, повідомив про це співробітникам відділу кібербезпеки. Майже всі поштові сервіси фільтрують спам. На жаль, спам все одно створює навантаження на мережу і сервер отримувача.

# Шпигунське, рекламне ПЗ та пвсевдоантивіруси

Шпигунське ПЗ - це програмне забезпечення, яке дозволяє злочинцям отримувати інформацію про дії користувача за комп'ютером. Шпигунські програми часто містять засоби відстеження активності, набраних на клавіатурі символів та перехоплення даних. Для того, щоб обійти заходи безпеки, шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто прив'язуються до легального ПЗ або розповсюджуються троянами. Багато веб-сайтів, які поширюють умовно-безкоштовні програми (shareware), містять шпигунські програми.

Рекламне ПЗ зазвичай відображає надокучливі спливаючі вікна з метою отримання доходу їх авторами від реклами. Зловмисне програмне забезпечення може аналізувати інтереси користувача, відстежуючи які веб-сайти він відвідує. Потім зловмисне ПЗ може надсилати спливаючу рекламу, яка відповідає тематиці цих сайтів. Деякі версії програмного забезпечення автоматично встановлюють рекламне ПЗ. Деяке рекламне ПЗ дійсно забезпечує тільки доставку реклами, але часто рекламне ПЗ поширюється разом зі шпигунським.

Scareware - це шкідливе ПЗ, яке переконує користувача здійснити конкретну дію, використовуючи його страх. Scareware створює спливаючі вікна, схожі на вікна діалогу операційної системи. Ці вікна містять підроблені повідомлення про те, що система знаходиться під загрозою або необхідно виконання певної програми для повернення до нормальної роботи. Насправді жодних проблем немає і якщо користувач дозволить виконати зазначену програму, вона встановить на його комп'ютер зловмисний код.

# Фішинг

Фішинг - це форма шахрайства. Кіберзлочинці, маскуючись під організацію чи особу з гарною репутацією, використовують електронну пошту, системи миттєвого обміну повідомленнями або соціальні мережі для збору такої інформації, як реєстраційні дані або дані облікового запису. Фішинг відбувається, коли зловмисник надсилає шахрайського електронного листа, який виглядає як такий, що надійшов з надійного джерела. Мета цього повідомлення - змусити одержувача встановити зловмисне програмне забезпечення на своєму пристрої або повідомити персональну чи фінансову інформацію. Прикладом фішингу є фальшивий електронний лист начебто від магазину. В цьому листі користувачу пропонують перейти за посиланням, щоб отримати приз. За цим посиланням користувач переходить на підроблену веб-сторінку, яка запитує персональну інформацію, або встановлює вірус.

Спрямований фішинг (spear phishing)- це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути жертв. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. Перед відправленням такого електронного листа зловмисник вивчає інтереси потенційної жертви. Наприклад, зловмисник дізнався, що ця особа цікавиться автомобілями і хоче придбати конкретну модель. Зловмисник приєднується до того ж обговорення на автомобільному форумі, що і жертва, готує фальшиву пропозицію продажу автомобіля і надсилає її жертві електронною поштою. Електронний лист містить посилання на фотографії автомобіля. Коли жертва переходить за посиланням, вона несвідомо встановлює зловмисне ПЗ на свій комп'ютер. Натисніть [тут](https://www.consumer.ftc.gov/scam-alerts) щоб дізнатись більше про шахрайство засобами електронної пошти.

# Голосовий фішинг, СМС фішинг, фармінг, Whaling

Голосовий фішинг (Vishing) - це фішинг за допомогою технологій голосових комунікацій. Злочинці можуть робити фальшиві дзвінки, представляючись довіреними організаціями, за допомогою технології передачі голосу через IP (VoIP). Жертви також можуть отримати записане повідомлення, яке виглядає легітимним. Таким чином злочинці намагаються отримати номери кредитних карток або іншу інформацію, щоб викрасти персональні дані жертви. Успішність голосового фішингу пояснюється довірою людей до телефонної мережі.

СМС фішинг (Smishing) – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело щоб завоювати довіру жертви. Наприклад, під час СМС фішингу зловмисник може надіслати жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ.

Фармінг (pharming) - це фальшивий веб-сайт, що має вигляд справжнього, щоб змусити користувачів вводити свої облікові дані. Під час фармінгу користувачів спрямовують на фальшивий веб-сайт, який імітує офіційний. Потім жертви вводять свою особисту інформацію, вважаючи, що вони підключені до легітимного сайту.

Whaling (полювання на корпоративних китів)- це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості.

Натисніть [тут](https://www.rsa.com/content/dam/rsa/PDF/h11933-wp-phishing-vishing-smishing.pdf) щоб прочитати статтю від компанії RSA про фішинг, СМС фішинг, голосовий фішинг та whaling.

# Отруєння браузера та плагінів

Зловмисники заражують веб-браузери з метою їх використання для відображення спливаючої реклами, збору особистої інформації або встановлення рекламного ПЗ, вірусів, шпигунських програм. Зловмисний код може бути встановлений у виконуваний файл браузера, компоненти браузера або його плагіни.

**Плагіни**

Плагіни Flash та Shockwave від Adobe дозволяють створювати цікаві графічні та мультиплікаційні зображення, які значно покращують зовнішній вигляд веб-сторінки. Плагіни відображають контент, створений за допомогою відповідного програмного забезпечення.

До недавнього часу плагіни мали дивовижно рекордні показники з точки зору безпеки. Однак з ростом популярності контенту на основі Flash, зловмисники звернули увагу на плагіни та програмне забезпечення Flash, визначили вразливі місця та змогли використати їх у своїх цілях. Успішна атака може викликати збій системи або дозволить зловмисникам взяти її під свій контроль. Прогнозується збільшення втрат даних, оскільки злочинці продовжують досліджувати найбільш популярні плагіни та протоколи у пошуках вразливостей.

**Зловживання пошуковою оптимізацією (SEO Poisoning)**

Пошукові системи, такі як Google, ранжують веб-сторінки за результатами пошукових запитів користувачів. Положення веб-сайту в списку результатів пошуку залежить від релевантності його вмісту. SEO ( абр. від Search Engine Optimization - пошукова оптимізація) - це набір методів, що використовуються для підняття рейтингу веб-сайту у пошукових системах. Хоча багато легітимних компаній спеціалізуються на оптимізації веб-сайтів для покращення їх позиціонування, однак методи зловживання SEO використовують пошукову оптимізацію для того, щоб зловмисний веб-сайт піднявся в ТОП результатів пошуку.

Найпоширенішою метою зловживання SEO є залучення відвідувачів на зловмисні веб-сайти, які можуть містити шкідливе ПЗ або використовувати соціальну інженерію. Щоб забезпечити зловмисному сайту вищу позицію в результатах пошуку, нападники використовують ключові слова з популярних пошукових запитів.

**Browser Hijacker (Викрадач браузерів)**

Викрадач браузерів - це зловмисне ПЗ, яке змінює налаштування веб-браузера на комп'ютері з метою перенаправлення користувача на проплачені веб-сайти. Викрадачі браузерів зазвичай встановлюються без дозволу користувача під час прихованого завантаження (drive-by download). Прихованим завантаженням називають програму, яка автоматично завантажується на комп'ютер, коли користувач відвідує певний веб-сайт або переглядає електронний лист в HTML. Завжди уважно читайте користувацькі угоди, коли завантажуєте програми, щоб уникнути загроз такого типу.

# Захист від атак на електронну пошту та браузери

Методи боротьби зі спамом включають фільтрування електронної пошти, навчання користувачів щодо обережного ставлення до підозрілих електронних листів та використання фільтрів на хостах/серверах.

Важко зупинити спам повністю, але можна зменшити його наслідки. Наприклад, більшість інтернет-провайдерів блокують спам, перш ніж він потрапить до поштової скриньки користувача. Більшість антивірусів та поштових клієнтів автоматично виконують фільтрацію електронних листів. Це означає, що вони виявляють та видаляють спам з електронної поштової скриньки користувача.

Організації також повинні попереджати працівників про небезпеку відкривання вкладень електронної пошти, які можуть містити віруси або Інтернет-черв'яки. Не вважайте, що вкладення електронної пошти є безпечними, навіть якщо вони надійшли від надійного джерела. Комп'ютер відправника може без його відому використовуватися для розповсюдження вуруса. Завжди перевіряйте вкладення електронної пошти перед тим, як їх відкрити.

Антифішингова робоча група (APWG) - це галузева асоціація з протидії викраданню особистих даних та шахрайствам, які виникають в результаті фішингу або підробки електронних листів.

Регулярне оновлення всього програмного забезпечення гарантує, що в системі є всі найновіші виправлення безпеки для усунення відомих вразливостей. Натисніть [тут](http://www.howtogeek.com/228828/7-ways-to-secure-your-web-browser-against-attacks/) щоб дізнатися більше про те, як уникнути атак на браузери.

# Соціальна інженерія

Соціальна інженерія не використовує технічні засоби для збору інформації про майбутню жертву. Соціальна інженерія - це атака, під час якої злочинець намагається маніпулювати людиною, щоб змусити її до певних дій або до розголошення конфіденційної інформації.

Соціальні інженери часто використовують бажання людей бути корисними, а також їх слабкості. Наприклад, зловмисник може подзвонити уповноваженому працівнику з приводу нагальної проблеми, вирішення якої вимагає негайного доступу до мережі. Зловмисник може розраховувати на марнославство співробітника, залякувати керівником або скористатися жадібностю працівника.

Деякі види атак соціальної інженерії:

**Претекстінг (Pretexting)** - атакуючий телефонує конкретній особі і обманом намагається отримати доступ до привілейованих даних. Наприклад, зловмисник вимагає надати персональні або фінансові дані для підтвердження особи одержувача.

**Послуга за послугу (Quid pro quo)** - це коли злочинець запитує персональну інформацію в обмін на щось, наприклад, безкоштовний подарунок.

Тактики соціальної інженерії

Соціальна інженерія спирається на декілька тактик, серед яких наступні:

* **Повноваження** - люди, як правило виконують дії, коли інструкції надходять з "авторитетного джерела".
* **Залякування** - злочинці змушують жертву до відповідних дій.
* **Консенсус/соціальне підтвердження** -люди вчинятимуть певні дії, якщо вони вважають, що інші зробили б так само.
* **Дефіцит** - люди діятимуть, якщо будуть думати, що кількість привабливих пропозицій обмежена.
* **Терміновість** - люди діятимуть, якщо вважатимуть, що мають обмежену кількість часу для прийняття рішення.
* **Близькі відносини/Симпатія**- злочинці будують приязні відносини з жертвою.
* **Довіра**- злочинці створюють довірчі відносини з жертвою, цей підхід може вимагати більше часу.

Натисніть на кожну тактику на рисунку, щоб переглянути приклад її використання.

Професіонали з кібербезпеки несуть відповідальність за ознайомлення інших співробітників організації з тактиками протистояння соціальній інженерії. Натисніть [тут](http://www.informit.com/articles/article.aspx?p=1350956) щоб дізнатись більше про тактики соціальної інженерії.

# "Серфінг через плече" і “Дайвінг у смітнику”

Кіберзлочинець спостерігає за жертвою або виконує “серфінг через плече”, щоб отримати PIN-коди, коди доступу чи номери кредитних карток. Зловмисник може знаходитися максимально близько біля своєї жертви, або використовувати біноклі чи системи відеоспостереження для підглядання. Це одна з причин, чому дані на екранах банкоматів видно лише під певним кутом. Такі запобіжні заходи безпеки ускладнюють підглядання для злочинців.

"Сміття однієї людини - скарб для іншої". Ця фраза особливо підходить для “дайвінгу у смітнику ”, який передбачає досліждення сміття жертви, щоб дізнатися, яку інформацію організація викидає. Рекомендовано обмежити доступ до контейнерів для сміття. Будь-яка конфіденційна інформація має бути належним чином утилізована шляхом подрібнення або використання пакетів для спалення, які зберігають секретні або конфіденційні документи для подальшого знищення вогнем.

# Уособлення і розіграш

Уособлення (імперсоніфікація) - це спосіб видавати себе за когось іншого. Наприклад, нещодавня телефонна афера була спрямована на платників податків. Злочинець, який представлявся співробітником податкового управління, повідомляв жертвам, що вони мають заборгованість, яку жертви повинні сплатити негайно за допомогою банківського переказу. Самозванець погрожував, що відмова від сплати призведе до арешту. Злочинці також використовують уособлення, щоб атакувати інших. Вони можуть підірвати довіру до публічних осіб за допомогою публікацій на веб-сайтах або в соціальних мережах.

Містифікація або розіграш - це дія, призначена для обману. Містифікація в кібер-світі може завдати стільки ж клопоту, як і в реальному. Мета розіграшу - викликати реакцію жертви. Це може бути необгрунтований страх і нелогічна поведінка. Користувачі самі розповсюджують обмани через електронну пошту та соціальні мережі. Натисніть [тут](http://www.hoax-slayer.com/) щоб відвідати веб-сайт, де містяться повідомлення про містифікації.

Несанкціоноване проникнення

Несанкціоноване проникнення на територію (Piggybacking) відбувається тоді, коли зловмисник проникає до зони з обмеженим доступом слідом за уповноваженою особою. Для цього зловмисники використовують декілька способів:

* Вдають ніби супроводжують уповноважену особу.
* Приєднуються до великої групи співробітників, вдаючи що також працюють в організації.
* Вибирають жертву, яка легковажно ставиться до правил безпеки на об'єкті.

Несанкціоноване проникнення слідом за зареєстрованим користувачем (Tailgating) є ще одним терміном, який описує таку саму практику.

Запобігти несанкціонованому проникненню можна використовуючи тамбур-шлюзи з двома дверима. Після того, як співробітники входять у зовнішні двері, ці двері необхідно закрити перед тим як увійти у внутрішні двері.

# Шахрайство в Інтернеті та по електронній пошті

Пересилання фейкових електронних листів з метою розіграшу, жартів, смішних фільмів, листів не пов'язаних із роботою, може порушити політику компанії з використання ІТ-інфраструктури та призвести до дисциплінарних покарань. Натисніть [тут](http://www.snopes.com/) щоб відвідати веб-сайт, який розміщує інформацію про чутки та результати їх перевірки.

Захист від обману

Організаціям необхідно підвищувати рівень поінформованості працівників про тактики соціальної інженерії та навчити працівників запобіжним заходам, таким як:

* Ніколи не надавати конфіденційну інформацію або облікові дані невідомим особам електронною поштою, в чаті, особисто або телефоном.
* Не натискати на привабливі посилання в поштових повідомленнях та на веб-сайтах.
* Звертати увагу на несанкціоновані або автоматичні завантаження.
* Запровадити політику безпеки та ознайомити з нею працівників.
* Працівники повинні відчувати свою відповідальність за рівень безпеки в організації.
* Не піддаватися тиску зі сторони невідомих осіб.

Натисніть [тут](https://niccs.us-cert.gov/awareness/protect-yourself-against-cyber-threats) щоб отримати додаткову інформацію про підвищення інформованості у галузі кібербезпеки.

Відмова в обслуговуванні

Атака типу "Відмова в обслуговуванні" (DoS) - є різновидом мережної атаки. Результатом DoS-атаки є переривання доступу користувачів, пристроїв або застосунків до мережних сервісів. Існує два основних типи DoS-атак:

* **Перевантаження великою кількістю трафіку** - Нападник надсилає величезну кількість даних з такою швидкістю, що мережа, хост або застосунок не встигає їх обробляти. Це спричиняє уповільнення передачі або реагування, іноді призводить до аварійного завершення роботи пристрою чи сервісу.
* **Пакети неправильного формату (Maliciously Formatted Packets)**- Нападник надсилає пакет даних неправильного формату хосту або застосунку і одержувач не може його обробити. Наприклад, програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані. Це призводить до того, що приймаючий пристрій буде працювати дуже повільно або припинить роботу взагалі.

DoS-атаки становлять серйозний ризик, оскільки вони можуть легко переривати обмін інформацією та заподіяти значну втрату часу й грошей. Ці атаки відносно прості для виконання навіть некваліфікованим нападником.

Метою атаки «відмова в обслуговуванні» є припинення доступу для авторизованих користувачів через недоступність мережної інфраструктури (згадайте три основні принципи безпеки: конфіденційність, цілісність та доступність). Натисніть «Перегляд» на Рисунку 1, щоб переглянути анімацію, яка ілюструє DoS атаку.

Розподілена DoS атака (DDoS) подібна до атаки DoS, але вона походить з декількох скоординованих джерел. Наприклад, атака DDoS може розвиватися наступним чином:

Зловмисник створює мережу заражених хостів, яка називається ботнетом і складається з комп'ютерів-зомбі. Зомбі - це заражені хости. Для контролю над зомбі зловмисник використовує спеціальну керуючу систему. Комп'ютери-зомбі постійно сканують мережу і заражають інші хости, створюючи ще більше нових зомбі. Після такої підготовки хакер через керуючу систему дає наказ ботнету розпочати DDoS атаку.

Натисніть "Перегляд" на Рисунку 2, щоб переглянути анімацію, яка ілюструє DDoS атаку. DDoS атака потребує великої кількості пристроїв-зомбі, щоб створити велике навантаження на ціль.

# Аналіз трафіку (Sniffing)

Sniffing є дуже схожим на підглядання за людиною в реальному світі. Хакери досліджують весь мережний трафік, який проходить через їх мережну інтерфейсну карту (NIC), незалежно від того, кому він адресований. Злочинці виконують аналіз трафіку в мережі за допомогою програмного забезпечення, апаратного пристрою або їх комбінації. Як показано на рисунку, Sniffing переглядає весь мережний трафік або виконується фільтрація за певним протоколом, сервісом чи навіть за рядком символів, таких як ідентифікатор користувача або пароль. Деякі мережні аналізатори можуть перевіряти весь трафік і навіть змінювати його частково або повністю.

Sniffing може бути корисним. Мережні адміністратори можуть використовувати такі засоби для аналізу мережного трафіку, визначення проблем з пропускною здатністю та вирішення інших проблем в мережній інфраструктурі.

Фізична безпека має важливе значення для запобігання встановленню аналізаторів трафіку у внутрішній мережі організації.

Підміна

Підміна (Spoofing) – це атака шляхом імперсоніфікації, яка відбувається за рахунок використання довірчих відносин між двома системами. Якщо дві системи підтримують єдину аутентифікацію, користувач, який увійшов до однієї системи, може не проходити повторно процес аутентифікації для доступу до іншої системи. Зловмисник може скористатися цими довірчими відносинами, відправивши пакет до однієї системи, який виглядає як такий, що надійшов з іншої довіреної системи. Оскільки між системами діють довірчі відносини, цільова система може виконати запит без аутентифікації.

Існує кілька типів атак з використанням підміни.

* Підміна MAC-адреси відбувається, коли один комп'ютер приймає пакети даних, адресовані на MAC-адресу іншого комп'ютера.
* IP-spoofing надсилає IP-пакети з підробленої ІР-адреси джерела, щоб замаскувати свою справжню адресу.
* Протокол визначення адрес (ARP) - це протокол, який перетворює IP-адреси в MAC-адреси для передачі даних. При ARP підміні зловмисник розсилає підроблені ARP повідомлення локальною мережею для того, щоб зв'язати свою MAC-адресу з IP-адресою авторизованого користувача мережі.
* Система доменних імен (DNS) асоціює доменні імена з IP-адресами. При підміні DNS відбувається модифікація DNS-сервера для перенаправлення певного доменного імені на іншу IP-адресу, контрольовану злочинцем.

# Man-in-the-middle (людина посередині)

Злочинець, який виконує атаку Man-in-the-middle (MitM), перехоплює повідомлення, якими обмінюються комп'ютери, щоб викрасти інформацію, яка проходить мережею. Злочинець також може маніпулювати повідомленнями та передавати підставні дані між хостами, оскільки вузли не усвідомлюють, що відбулася модифікація повідомлень. MitM дозволяє злочинцю контролювати пристрій без відому користувача.

Натисніть на значки + на рисунку, щоб дізнатися про основні кроки атаки MitM.

Man-In-The-Mobile (MitMo) (людина-в-мобільному) - різновид атаки "Man-in-the-middle ". При MitMo зловмисник отримує контроль над мобільним пристроєм. Заражений мобільний пристрій пересилає конфіденційну інформацію користувача нападникам. ZeuS є прикладом експлойта з можливостями MitMo, який дозволяє атакуючим непомітно перехоплювати SMS-повідомлення 2-етапної авторизації, які надходять користувачам. Наприклад, коли користувач створює обліковий запис Apple, він повинен надати телефонний номер для отримання SMS з тимчасовим кодом підтвердження. Зловмисне ПЗ відстежує ці повідомлення та передає інформацію злочинцям.

При реалізації атаки з повтором зловмисник перехоплює частину даних, які пересилаються між двома хостами, а потім повторно передає записане повідомлення. Такий спосіб дозволяє обійти механізми аутентифікації.

# Атаки нульового дня

Атака нульового дня (zero-day attack), яку іноді називають загрозою нульового дня (zero-day threat), - це комп'ютерна атака, яка намагається використати вразливості ПЗ, що досі невідомі постачальнику програмного забезпечення, або які він приховує. Термін нульова година (zero hour) описує момент, коли хтось виявляє експлойт (шкідливий програмний код). Впродовж часу, доки виробник програмного забезпечення розробляє та випускає виправлення, мережа залишається вразливою для цього експлойту, як показано на рисунку. Для захисту від цих стрімких атак професіоналам з мережної безпеки необхідно більш ретельно продумати архітектуру мережі. В наш час стримувати декілька вторгнень до системи одночасно у різних точках майже не можливо.

# Клавіатурні шпигуни (кейлогери)

Клавіатурний шпигун (кеулогер) - це програма, яка записує або вносить в спеціальний журнал натискання клавіш користувачем системи. Злочинці можуть реалізовувати кейлогери за допомогою ПЗ, встановленого на комп'ютері або через обладнання, фізично приєднане до комп'ютера. Зловмисник налаштовує ПЗ клавіатурного шпигуна таким чином, щоб воно відправляло зібрану в журналі інформацію електронною поштою. Перехоплені та записані до лог-файлу натискання клавіш можуть розкрити імена користувачів, паролі, відвідані веб-сайти та іншу конфіденційну інформацію.

# Захист від атак

Організація може запровадити низку заходів для захисту від різноманітних атак. Налаштуйте міжмережні екрани так, щоб відхиляти будь-які пакети, що надходять ззовні мережі, але мають адреси, які вказують на їх походження з внутрішньої мережі. Така ситуація є незвичайною, і це вказує на те, що кібер-злочинець спробував здійснити атаку з підміною адреси.

Щоб запобігти DoS та DDoS атакам, переконайтеся, що патчі та оновлення є актуальними, розподіляйте навантаження між серверними системами та блокуйте зовнішні ICMP пакети на межі периметру. Мережні пристрої використовують ICMP-пакети для надсилання повідомлень про помилки. Наприклад, команда ping використовує ICMP пакети для перевірки чи може пристрій взаємодіяти з іншими пристроями в мережній інфраструктурі.

Системи можуть попередити повторні напади, шифруючи трафік, використовуючи криптографічну аутентифікацію та включаючи часові мітки до кожної частини повідомлення. Натисніть [тут](http://www.theguardian.com/public-leaders-network/2015/oct/14/how-to-stop-cyber-attacks-on-your-organisation) щоб дізнатися більше про способи запобігання кібератакам.

# Grayware та SMiShing

З ростом популярності смартфонів умовно шкідливе ПЗ (grayware) стає проблемою для безпеки мобільного доступу. Умовно шкідливе ПЗ включає дратівливі або небажані застосунки. Такі застосунки можуть не містити шкідливого ПЗ, але все одно становлять ризик для користувача. Наприклад, Grayware може відстежувати місцезнаходження користувача. Автори умовно шкідливого ПЗ зазвичай підтримують видимість легітимності, включивши опис функцій програми маленьким шрифтом до ліцензійної угоди. Користувачі встановлюють багато мобільних додатків, не ознайомлюючись з їх функціями.

Смішінг (SMiShing) - коротка форма терміну SMS фішинг. Він використовує службу SMS для надсилання підроблених текстових повідомлень. Злочинці обманним шляхом змушують користувача відвідати веб-сайт або зателефонувати за номером телефону. Довірливі жертви можуть надавати таку конфіденційну інформацію, як інформація про кредитні картки. Відвідування веб-сайту може призвести до несвідомого завантаження користувачем шкідливого ПЗ, яке заразить його пристрій.

# Несанкціоновані точки доступу

Несанкціонована точка доступу (Rogue Access Points) - це точка доступу, встановлена в захищеній мережній інфраструктурі без дозволу. Несанкціонована точка доступу може бути налаштована двома способами. Перший спосіб - працівник, керуючись добрими намірами, хоче спростити підключення мобільних пристроїв. Другий спосіб полягає в тому, що злочинці непомітно отримують фізичний доступ на територію організації і встановлюють несанкціоновану точку доступу. Оскільки обидва способи є несанкціонованими, вони становлять ризики для організації.

Несанкціонована точка доступу також може означати точку доступу, яка використовується в злочинних цілях. У цьому випадку злочинці налаштовують точку доступу для атак через посередника (MitM), щоб перехоплювати реєстраційні дані користувачів.

Для атаки типу "злий близнюк" (Evil Twin) використовується несанкціонована точка доступу з потужним сигналом і високою пропускною здатністю, щоб привабити користувачів. Після того, як користувачі підключаються до цієї точки доступу, злочинці можуть аналізувати трафік та виконувати MitM атаки.

# Глушіння радіочастот (RF Jamming)

Бездротові сигнали чутливі до електромагнітних (EMI) та радіочастотних перешкод (RFI), а також до розряду блискавки або завад від флуоресцентних ламп. Бездротові сигнали також чутливі до навмисного глушіння. Радіочастотні перешкоди (Radio frequency (RF) jamming) блокують сигнал радіо або супутникової станції, щоб він не доходив до станції отримувача.

Частота, модуляція та потужність радіочастотних завад мають відповідати характеристикам пристрою, роботу якого хоче порушити злочинець.

luejacking та Bluesnarfing

Bluetooth - малопотужний протокол ближньої дії. Він використовується для передачі даних в персональній мережі (PAN), яка може містити такі пристрої, як мобільні телефони, ноутбуки та принтери. Є кілька версій Bluetooth. Він характеризується легким налаштуванням без необхідності використання мережних адрес. Bluetooth використовує спряження пристроїв для встановлення зв'язку між ними. Після встановлення синхронізації обидва пристрої використовують один і той самий ключ доступу.

Про вразливості Bluetooth давно відомо, але через обмежену зону дії протоколу, жертва та зловмисник повинні знаходитися близько один від одного.

* Bluejacking - це термін, який означає передачу несанкціонованих повідомлень на інший пристрій через Bluetooth. Як варіант цей спосіб використовують для розсилання шокуючих зображень.
* Bluesnarfing (підключення до пристрою Bluetooth з метою крадіжки даних)– це термін, що описує ситуацію, коли зловмисник копіює інформацію жертви з її пристрою. Ця інформація може містити електронні листи та списки контактів.

Атаки на WEP та WPA

Протокол безпеки, аналогічний захисту дротової мережі (Wired Equivalent Privacy, WEP) - це протокол безпеки, у якому розробники намагалися забезпечити в бездротових локальних мережах (WLAN) такий самий рівень безпеки, як в дротовій локальній мережі (LAN). Для захисту дротової локальної мережі застосовують заходи фізичної безпеки. Щоб забезпечити аналогічний захист даних, які передаються бездротовою локальною мережею, у WEP застосовують шифрування.

WEP використовує ключ для шифрування. Керування ключами у WEP не передбачено, тому кількість людей, яким відомий один і той самий ключ, буде постійно зростати. Оскільки всі використовують один і той самий ключ, злочинець отримує доступ до великого обсягу трафіку для виконання аналітичних атак.

Вектор ініціалізації WEP, який є одним з компонентів криптографічної системи, також не бездоганний з точки зору безпеки:

* Це 24-бітове поле, що занадто коротке.
* Це відкритий текст, тобто може бути легко прочитаний.
* Він статичний, тому в завантаженій мережі ключові потоки будуть повторюватися.

Захищений Wi-Fi доступ (Wi-Fi Protected Access, WPA), а потім WPA2 замінили стандарт WEP через його слабкі місця. WPA2 не має таких проблем із шифруванням, оскільки зловмисник не може відновити ключ, аналізуючи трафік. Протокол WPA2 чутливий до атак, у яких кібер-злочинці можуть аналізувати пакети, що передаються між точкою доступу та легітимним користувачем. Кібер-злочинці використовують аналізатори пакетів, а потім запускають атаки в автономному режимі для підбору парольної фрази.

# Захист від атак на бездротові мережі та мобільні пристрої

Для захисту від атак на бездротові мережі та мобільні пристрої необхідно зробити кілька кроків. Більшість WLAN пристроїв використовують налаштування за замовчуванням. Скористайтеся перевагами базових функцій безпеки бездротового зв'язку, такими як аутентифікація та шифрування, змінивши параметри конфігурації за замовчуванням.

Обмежте розташування точок доступу в мережній інфраструктурі, розмістивши ці пристрої за межами міжмережного екрану або у демілітаризованій зоні (DMZ), яка містить інші недовірені пристрої, такі як поштові та веб-сервери.

WLAN утиліти, такі як NetStumbler, можуть виявляти несанкціоновані точки доступу або робочі станції. Розробіть політику гостьового доступу для вирішення задач підключення легітимних користувачів з правами гостя до Інтернету під час візиту до організації. Для віддаленого доступу авторизованих співробітників до WLAN використовуйте віртуальну приватну мережу (virtual private network - VPN).

# Міжсайтовий скриптинг

Міжсайтовий скриптинг (Cross-Site Scripting, XSS) - вразливість, виявлена у веб-застосунках. XSS дозволяє злочинцям вбудовувати скрипти у веб-сторінки, які переглядають користувачі. Такий скрипт може містити зловмисний код.

Міжсайтовий скриптинг включає трьох учасників: злочинець, жертва та веб-сайт. Кібер-злочинець не націлений на жертву напряму. Він використовує вразливість веб-сайту або веб-застосунку. Зловмисники вбудовують клієнтські скрипти до веб-сторінок, які переглядають користувачі-жертви. Шкідливий скрипт передається у браузер користувача без його відому. Шкідливий сценарій такого типу може мати доступ до будь-яких файлів cookie, ідентифікаторів сеансів або іншої конфіденційної інформації. Якщо злочинці отримують cookie-файл сеансу жертви, вони можуть видавати себе за неї.

# Ін'єкція коду

Одним зі способів зберігання даних веб-сайту є використання бази даних. Існує декілька різних типів баз даних, такі як Structured Query Language (SQL) база даних або Extensible Markup Language (XML) база даних. Напади з використанням XML та SQL ін'єкцій використовують недоліки в програмі, такі як неправильна перевірка запитів до бази даних.

**XML-ін'єкція (XML injection)**

При використанні XML у якості бази даних, XML-ін'єкція є атакою, яка може пошкодити дані. Після того, як користувач надає вхідні дані, система відправляє запит для отримання доступу до необхідної інформації в базі даних. Проблема виникає, коли система не належним чином перевіряє вхідний запит користувача. Злочинці можуть маніпулювати запитами, змінюючи їх відповідно до своїх потреб і отримати доступ до інформації в базі даних.

Отримавши доступ до конфіденційних даних, що зберігаються в базі, зловмисники можуть внести будь-які зміни на веб-сайт. Атака XML-ін'єкції загрожує безпеці веб-сайту.

**SQL-ін'єкція (SQL injection)**

Кібер-злочинці використовують вразливості системи, вставляючи шкідливі SQL вирази у поля форм вводу. Як і в попередньому прикладі, система не фільтрує правильність введених користувачем символів в SQL - операторі. Злочинці використовують SQL ін'єкцію на веб-сайтах або в будь-якій SQL базі даних.

Таким чином зловмисники можуть здійснити підміну ідентифікаційних даних користувачів, змінювати або знищувати існуючі дані в базі або стають адміністраторами сервера.

# Переповнення буфера

Переповнення буфера (buffer overflow) - відбувається, коли об'єм даних перевищує розмір виділеного буфера. Буфери - це області пам'яті, виділені для застосунку. Змінюючи дані за межами буфера, програма звертається до пам'яті, яка була виділена для інших процесів. Це може спричинити крах системи, призвести до несанкціонованого доступу до даних або ескалації прав користувача.

За оцінками спеціалістів координаційного центру CERT університету Карнегі-Меллона, майже половина вразливостей комп'ютерних програм так чи інакше обумовлені переповненням буферу. Існує велика кількість варіантів переповнення буфера, таких як: переповнення статичного буфера, помилки індексування, помилки форматування рядків, помилки в форматі рядка, невідповідність розмірів буферів Unicode і ANSI та переповнення динамічної області пам'яті.

# ВІддалений запуск програм

Вразливості дозволяють кібер-злочинцям виконати зловмисний код і отримати контроль над системою з привілеями користувача, який запустив застосунок. Віддалене виконання коду дозволяє злочинцю виконати на цільовій машині будь-яку команду.

Розглянемо, наприклад, Metasploit. Metasploit - це інструмент для розробки та виконання зловмисного коду на віддаленому об'єкті. Meterpreter - це модуль Metasploit, який надає розширену функціональність. Meterpreter дозволяє злочинцям писати свої власні розширення як спільний об'єкт. Злочинці вивантажують і вбудовують ці файли в процес, що запущений на машині жертви. Meterpreter завантажує та виконує всі розширення з пам'яті, тому вони ніколи не залучають ресурси жорсткого диску. Це також означає, що антивірусні програми не можуть їх виявити. Meterpreter має модуль для віддаленого керування веб-камерою. Як тільки злочинець встановлює Meterpreter в систему жертви, він може вести відеоспостереження та робити знімки з веб-камери на пристрої потерпілого.

# Елементи керування ActiveX та Java

Деякі веб-сторінки працюють правильно тільки якщо користувач встановив елементи керування ActiveX. Елементи керування ActiveX використовуються для створення додаткових модулів Internet Explorer. Елементи керування ActiveX - це встановлені користувачем програмні компоненти, які надають розширені можливості. Деякі елементи керування ActiveX пишуться третіми сторонами і можуть виявитися зловмисними. Вони можуть відстежувати історію переглядів веб-сторінок, встановлювати зловмисне програмне забезпечення або записувати натискання клавіш. Елементи керування ActiveX також використовуються в інших застосунках Microsoft.

Програма на Java працює завдяки інтерпретатору - віртуальній машині Java (JVM). JVM дозволяє використовувати функціональність Java-програм. JVM пісочниці (sandboxes) ізолюють ненадійний код від решти операційної системи. Існують вразливості, які дозволяють ненадійному коду обійти обмеження, встановлені пісочницею. В бібліотеці класів Java, яку застосунки використовують для власного захисту, також існують вразливості. Вразливість системи безпеки Java є другою за значенням після плагіну Adobe Flash.

# Захист від атак на застосунки

Перша лінія захисту від атак на застосунки полягає у написанні надійного коду. Незалежно від того, яка мова програмування та джерело вводу інформації використовуються, доцільно розглядати всі вхідні дані як потенційно ворожі. Перевіряйте всі вхідні дані так, ніби вони є потенційною загрозою.

Тримайте все програмне забезпечення, включно з операційними системами та прикладними програмами, оновленими і не ігноруйте повідомлень про оновлення. Не всі програми оновлюються автоматично. Як мінімум, виберіть в налаштуваннях варіант "Оновлення вручну". При оновленні вручну користувачі можуть перевіряти, які саме оновлення встановлюються.

# Розділ 4. Мистецтво захисту таємниць

Принципи криптології визначають, як сучасні протоколи і алгоритми убезпечують зв'язок. Криптологія - це наука створення і зламу секретних кодів. Розробка і використання кодів - це криптографія. Дослідження і злам кодів - це криптоаналіз. Суспільство використовувало криптографію століттями для захисту секретних документів. Наприклад, Юлій Цезар використовував простий алфавітний шифр для повідомлень, які відправляв своїм полководцям. Тільки вони знали ключ, необхідний для дешифрування повідомлень. Сучасні криптографічні методи дають впевненість в безпечності обміну інформацією в наш час.

Контроль доступу дозволяє контролювати доступ до будівлі, кімнати, системи, бази даних, файлу та інформації. Організації використовують різні методи контролю доступу та розмежування для захисту конфіденційності. У цьому розділі будуть розглянуті чотири етапи процесу контролю доступу: 1) ідентифікація, 2) аутентифікація, 3) авторизація та 4) звітність (accountability). Крім того, в розділі описуються різні моделі і типи контролю доступу.

Розділ завершується обговоренням різних способів приховування даних користувачами. Обфускація даних і стеганографія - це два методи, які використовуються для маскування даних.

# Що таке криптографія?

Криптологія - це наука про створення і злам секретних кодів. Криптографія - це спосіб зберігання та передачі даних, який дозволяє читати або обробляти ці дані тільки одержувачу, якому вони були призначені. Сучасна криптографія використовує обчислювально криптостійкі алгоритми, щоб ускладнити несанкціонований доступ кіберзлочинців до захищеної інформації.

Захищеність даних забезпечує конфіденційність, тобто прочитати повідомлення зможе тільки одержувач, якому воно призначене. Сторони досягають цього шляхом шифрування. Шифрування - це процес кодування даних таким чином, щоб неавторизована третя сторона не змогла їх прочитати.

При використанні шифрування даних, відкритий текст називають звичайним або відкритим (plaintext або cleartext), а зашифровану версію - кодованим або криптограмою (ciphertext). Шифрування перетворює читабельне повідомлення з відкритим текстом в зашифрований текст, який є нечитабельним, замаскованим повідомленням. Дешифрування є зворотнім процесом. Для шифрування також потрібен ключ, який відіграє головну роль в шифруванні і дешифруванні повідомлення. Людина,яка володіє ключем, зможе розшифрувати криптограму і отримати відкритий текст.

В історії є приклади використання різних алгоритмів і методів шифрування. Алгоритм - це процес або формула, що використовуються для вирішення поставленої задачі. Кажуть, що Юлій Цезар використовував захищені повідомлення, які отримував, розмістивши два набори алфавіту поруч, і зсунувши один з них на певну кількість позицій. Як ключ використовувалася ця кількість позицій. За допомогою цього ключа він перетворював відкритий текст у зашифрований і тільки його полководці, у яких також був ключ, могли розшифрувати повідомлення. Цей метод називають шифром Цезаря. На рисунку показано секретне повідомлення після використанням шифру Цезаря.

Історія криптографії

Історія криптографії почалася в дипломатичних колах ще кілька тисяч років тому. Королівські гінці передавали зашифровані повідомлення до інших королівств. Іноді сусіди, які не брали участі у переписці, намагалися викрасти повідомлення, відправлені до ворожого королівства. Незабаром після цього, військові командири почали використовувати шифрування для захисту повідомлень.

Протягом століть різні методи шифрування, фізичні пристрої та допоміжні засоби використовувалися для шифрування і розшифровки текстів:

* Скитала (Scytale) (Рисунок 1).
* Шифр Цезаря (Рисунок 2).
* Шифр Віженера (Рисунок 3).
* Шифрувальна машина Enigma (Рисунок 4).

Всі методи шифрування використовують ключ для шифрування або дешифрування повідомлення. Ключ є важливим компонентом алгоритму шифрування. Надійність алгоритму шифрування напряму залежить від надійності ключа, який він використовує. Чим складніший ключ, тим більш безпечний алгоритм. Керування ключами є важливою частиною цього процесу.

Створення криптограми

Кожен метод шифрування використовує спеціальний алгоритм, який називають шифром, для шифрування і дешифрування повідомлень. Шифр - це низка чітко визначених кроків, які використовуються для шифрування/дешифрування повідомлень. Існує кілька способів створення зашифрованого тексту:

* Транспозиція, або перестановка - літери міняють місцями (Рисунок 1).
* Заміна або підстановка - літери замінені (Рисунок 2).
* Схема одноразових шифроблокнотів (One-time pad) - відкритий текст в поєднанні з секретним ключем створює новий символ, який потім об'єднується з відкритим текстом для створення криптограми (Рисунок 3).

В старих алгоритмах шифрування, таких як шифр Цезаря або шифрувальна машина Enigma, конфіденційність забезпечувалася секретністю самого алгоритму. З розвитком технологій зворотне перетворення стало занадто легким, тому зараз використовують стійкі загальнодоступні алгоритми. При використанні більшості сучасних алгоритмів успішне дешифрування вимагає знання відповідних криптографічних ключів. Це означає, що безпека шифрування полягає в секретності ключів, а не алгоритмів.

Деякі сучасні алгоритми шифрування як і раніше використовують транспозицію як частину алгоритму.

Керування ключами - найскладніший аспект проектування криптосистеми. Багато криптосистем зазнали краху через помилки в керуванні ключами. Всі сучасні криптографічні алгоритми містять обов'язкові процедури керування ключами. На практиці більшість атак на криптографічні системи спрямовані на систему керування ключами, а не на сам криптографічний алгоритм.

# Два типи шифрування

Криптографічне шифрування може забезпечити конфіденційність за рахунок поєднання різних інструментів і протоколів.

Існує два підходи до підтримки безпеки даних при використанні шифрування. Перший - захистити алгоритм. Якщо безпека системи шифрування залежить від секретності самого алгоритму, то важливіше за все зберегти тайну алгоритму будь-якою ціною. Якщо хтось розкриє деталі роботи алгоритму, всім учасникам доведеться змінити алгоритм. Цей підхід не виглядає дуже надійним і керованим. Другий підхід - захистити ключі. В сучасній криптографії алгоритми є загальнодоступними. Секретність даних забезпечують криптографічні ключі. Криптографічні ключі - це паролі, які поступають на вхід алгоритму шифрування разом з даними, які необхідно зашифрувати.

Алгоритми шифрування поділяються на два класи:

**Симетричні алгоритми** використовують один і той самий заздалегідь відомий ключ (спільний ключ), іноді його називають парою секретних ключів, для шифрування і дешифрування даних. Як відправник, так і одержувач знають спільний ключ перед початком передачі будь-якого зашифрованого повідомлення. Як показано на рисунку 1, симетричні алгоритми використовують один і той самий ключ для шифрування і дешифрування тексту. Алгоритми шифрування, які використовують спільний ключ, простіші і вимагають менше обчислювальної потужності.

**Асиметричні алгоритми шифрування** - використовують один ключ для шифрування даних, а іншій ключ для дешифрування даних. Один з ключів є відкритим, а інший - закритим. В системі шифрування з відкритим ключем будь-яка людина може шифрувати повідомлення з використанням відкритого ключа одержувача, але тільки цей одержувач зможе розшифрувати його за допомогою свого закритого ключа. Сторони обмінюються захищеними повідомленнями без необхідності попереднього погодження спільного ключа, як показано на рисунку 2. Асиметричні алгоритми більш складні. Ці алгоритми є ресурсоємними і більш повільними у виконанні.

# Процес симетричного шифрування

Симетричні алгоритми шифрування використовують один спільний ключ для шифрування і дешифрування даних. Цей метод також відомий як шифрування з закритим ключем.

Наприклад, Аліса і Боб живуть в різних місцях і хочуть обмінюватися секретними повідомленнями через поштову систему. Аліса хоче відправити Бобу секретне повідомлення.

Шифрування з закритим ключем використовує симетричний алгоритм. Як показано на рисунку, Аліса і Боб мають однакові ключі від одного замку. Обмін ключами відбувся до відправки будь-яких секретних повідомлень. Аліса пише секретне повідомлення і покладе його в маленьку коробку, яку закриє на замок. Вона відправляє коробку Бобу. Повідомлення всередині коробки у безпеці, поки вона йде через поштову систему. Коли Боб отримує коробку, він відкриває замок своїм ключем і виймає повідомлення. Боб може використати ті самі коробку і замок, щоб відправити секретну відповідь Алісі.

Якщо Боб хоче поговорити з Керол, то йому потрібен новий спільний ключ для цього спілкування і він має тримати його в секреті від Аліси. Чим більша кількість людей, з якими Боб хоче спілкуватися приватно, тим більше ключів йому потрібно.

# Типи криптографічних перетворень

Найбільш поширеними типами криптографічних перетворень є блокові і потокові шифри. Ці методи відрізняються тим, як вони групують біти даних під час шифрування.

**Блокові шифри**

Блокові шифри перетворюють блок відкритого тексту фіксованої довжини в блок криптограми розміром 64 або 128 біт. Розмір блоку - це обсяг даних, які шифруються за один раз. Щоб розшифрувати цей зашифрований текст, застосуйте зворотне перетворення до блоку зашифрованого тексту, використовуючи той самий секретний ключ.

Блочні шифри зазвичай характеризуються тим, що вихідні дані більше вхідних, тому що розмір криптограми має бути кратним розміру блоку. Наприклад, стандарт шифрування даних (DES - Data Encryption Standard) є симетричним алгоритмом, який шифрує блоки 64-бітними фрагментами з використанням 56-бітного ключа. Для цього блоковий алгоритм бере дані по одному фрагменту за раз, наприклад, по 8 байтів, поки весь блок не буде заповнений. Якщо вхідних даних менше, ніж один повний блок, алгоритм додає штучні дані або пробіли, поки не використає всі 64 біти повністю, як показано на рисунку 1 ліворуч для 64 біт.

**Потокові шифри**

На відміну від блокових шифрів, потокові шифрують відкритий текст по одному байту або біту за один раз, як показано на рисунку 2. Потокові шифри можна розглядати як блокові з розміром блоку в один біт. За допомогою потокового шифру перетворення цих менших одиниць відкритого тексту виконується по різному в залежності від їх розташування в потоці тексту, що шифрується. Потокові шифри можуть бути набагато швидшими, ніж блокові шифри, і зазвичай не збільшують розмір повідомлення, оскільки можуть шифрувати довільне число бітів.

A5 - це потоковий шифр, який забезпечує конфіденційність голосового зв'язку і шифрує мобільний зв'язок. DES також можна використовувати в режимі потокового шифрування.

Складні криптографічні системи можуть комбінувати блочну та потокову обробку в одному процесі.

# Симетричні алгоритми шифрування

Багато криптографічних систем використовують симетричне шифрування. Розглянемо деякі з поширених криптографічних стандартів, які використовують симетричне шифрування:

**3DES (Triple DES):** Digital Encryption Standard (DES) - це симетричний блоковий шифр із 64-бітовим розміром блоку, який використовує 56-бітний ключ. В якості вхідних даних він приймає 64-бітний блок відкритого тексту, а на виході видає 64-бітний блок зашифрованого тексту. Алгоритм завжди працює з блоками однакового розміру і використовує як перестановки, так і заміни. Перестановка - це спосіб впорядкування всіх елементів набору.

Triple DES шифрує дані тричі і використовує інший ключ для хоча б одного з трьох проходів. Таким чином сумарний розмір ключа становить 112-168 біт. Алгоритм 3DES більш стійкий до атак, але набагато повільніший, ніж DES.

Цикл шифрування 3DES виглядає наступним чином:

1. Дані шифруються першим проходом DES.

2. Дані дешифруються другим проходом DES.

3. Дані повторно шифруються третім проходом DES.

Для розшифровки криптограми використовується зворотній процес.

**IDEA:** Міжнародний алгоритм шифрування даних (The International Data Encryption Algorithm), який використовує 64-бітові блоки і 128-бітові ключі. IDEA виконує вісім циклів перетворень кожного з 16 блоків, які є результатом поділу кожного 64-бітного блоку. Алгоритм IDEA замінив DES і тепер використовується в PGP (Pretty Good Privacy). PGP - це програма, яка забезпечує конфіденційність і аутентифікацію під час передачі даних. GNU Privacy Guard (GPG) є безкоштовною версією PGP з вільною ліцензією.

**AES:** Вдосконалений стандарт шифрування (The Advanced Encryption Standard) має фіксований розмір блоку 128 біт з розміром ключа 128, 192 або 256 біт. Національний інститут стандартів і технологій США (NIST) затвердив алгоритм AES в грудні 2001 року. Уряд США використовує AES для захисту секретної інформації.

AES - стійкий алгоритм, який використовує довші ключі. AES швидший за DES і 3DES, тому він використовується в рішеннях для програмних застосунків, а також в апаратному забезпеченні міжмережних екранів та маршрутизаторах.

Сереж інших блокових шифрів можна згадати Skipjack (розроблений NSA), Blowfish і Twofish.

# Процес асиметричного шифрування

Асиметричне шифрування, також відоме як шифруванням з відкритим ключем, для шифрування використовує ключ, який відрізняється від ключа для дешифрування. Злочинець не може в прийнятні терміни обчислити ключ дешифрування, знаючи ключ шифрування і навпаки.

Якщо Аліса і Боб обмінюються секретними повідомленнями за допомогою шифрування з відкритим ключем, вони використовують асиметричний алгоритм. На цей раз Боб і Аліса не обмінюються ключами до відправки секретних повідомлень. Замість цього у Боба і Аліси є окремі замки з відповідними ключами. Якщо Аліса надсилає секретне повідомлення Бобу, вона має спочатку зв'язатися з ним і попросити його надіслати свій відкритий замок. Боб надсилає замок, але зберігає свій ключ. Коли Аліса отримує замок, вона пише своє секретне повідомлення і вкладає його в маленьку коробку. В ту ж коробку вона кладе свій відкритий замок, але залишає у себе свій ключ. Потім вона замикає коробку замком Боба. Коли Аліса закриє коробку, вона більше не зможе її відкрити, тому що у неї немає ключа до цього замку. Вона відправляє коробку Бобу, і, поки відправлення проходить через поштову систему, ніхто не зможе її відкрити. Коли Боб отримує коробку, він може відкрити її своїм ключем і отримати повідомлення від Аліси. Щоб відправити секретну відповідь, Боб кладе своє секретне повідомлення в коробку разом зі своїм відкритим замком і блокує коробку замком Аліси. Боб відправляє закриту коробку назад Алісі.

Наприклад, на рисунку 1 Аліса запитує і отримує відкритий ключ Боба. На рисунку 2 Аліса використовує відкритий ключ Боба для шифрування повідомлення з використанням узгодженого заздалегідь алгоритму. Аліса відправляє зашифроване повідомлення Бобу, а Боб використовує свій закритий ключ для дешифрування повідомлення, як показано на рисунку 3.

# Асиметричні алгоритми шифрування

Асиметричні алгоритми використовують відомі загальнодоступні формули. Пара незв'язаних ключів робить ці алгоритми безпечними. Розглянемо кілька асиметричних алгоритмів:

**RSA (Rivest-Shamir-Adleman)** використовує добуток двох дуже великих простих чисел рівної довжини - від 100 до 200 цифр. Браузери використовують RSA для встановлення безпечного з'єднання.

**Протокол Діффі-Хеллмана (Diffie-Hellman)** забезпечує метод електронного обміну секретним ключем. Алгоритм Діффі-Хеллмана використовують такі захищені протоколи, як Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH) та Internet Protocol Security (IPsec).

**Схема Эль-Гамаля (ElGamal)** лежить в основі державного стандарту США для цифрових підписів. Цей алгоритм є безкоштовним для використання, оскільки він не запатентований.

**Еліптична криптографія (ECC)** використовує еліптичні криві як частину алгоритму. У США Агентство національної безпеки використовує ECC для генерації цифрового підпису та обміну ключами.

Керування ключами

Керування ключами складається зі створення, обміну, зберігання, використання і заміни ключів, що використовуються в алгоритмі шифрування.

Керування ключами - найскладніша частина проектування криптосистеми. Багато криптосистем були зламані через помилки в керуванні ключами. На практиці більшість атак на криптографічні системи націлені на рівень керування ключами, а не на сам криптографічний алгоритм.

Як показано на рисунку, існує кілька основних характеристик керування ключами, які потрібно враховувати.

Для опису ключів використовуються два терміни:

* **Довжина ключа (Key length)** - також називається розміром ключа, вимірюється в бітах.
* **Простір ключів (Keyspace)** - це кількість можливих варіантів ключів, які дозволяє генерувати конкретна довжина ключа.

Зі зростанням довжини ключа простір ключів збільшується експоненціально. Простір ключів алгоритму це набір усіх можливих значень ключа. Довші ключі більш надійні, проте вони також більш ресурсоємні. В просторі ключів практично кожного алгоритму є кілька слабких ключів, які дозволяють зловмиснику зламати шифр прискореним методом.

# Порівняння типів шифрування

Важливо розуміти різницю між симетричними та асиметричними методами шифрування. Симетричні системи шифрування більш ефективні і можуть обробляти більше даних. Однак керування ключами у симетричних системах шифрування складніше. Асиметрична криптографія більш ефективна для захисту конфіденційності невеликих обсягів даних. Це робить більш безпечним обмін електронними ключами, який має невеликий обсяг даних. У той же час це не підходить для шифрування великих блоків даних.

Збереження конфіденційності важливо для даних, як під час зберігання, так і в процесі передавання. В обох випадках симетричному шифруванню надають перевагу через його швидкість і простоту алгоритму. Деякі асиметричні алгоритми можуть значно збільшити розмір зашифрованого об'єкта. Тому для даних, що передаються, використовуйте криптографію з відкритим ключем під час обміну секретним ключем, а потім симетричну криптографію для забезпечення конфіденційності відправлених даних.

Застосунки

Існує багато варіантів застосування як симетричних, так і асиметричних алгоритмів.

Токен, який генерує одноразові паролі, - це апааратний пристрій, у якому для генерації одноразового паролю застосовується криптографія. Одноразовий пароль - це автоматично згенерований цифровий або букво-цифровий рядок символів, який аутентифікує користувача тільки для однієї транзакції і тільки під час одного сеансу. Пароль змінюється приблизно кожні 30 секунд. Пароль сеансу відображається на дисплеї пристрою і користувач вводить його для входу.

В індустрії електронних платежів використовується алгоритм 3DES. Операційні системи використовують DES для захисту файлів користувача і системних даних за допомогою паролів. Більшість шифруваних файлових систем, таких як NTFS, використовують стандарт AES.

Алгоритми з асиметричним ключем використовуються у чотирьох протоколах:

* Internet Key Exchange (IKE), який є основним компонентом мереж VPN, що використовують протокол IPsec.
* Secure Socket Layer (SSL), який є засобом реалізації криптографії у веб-браузері.
* Secure Shell (SSH), який забезпечує захищений віддалений доступ до мережних пристроїв.
* Pretty Good Privacy (PGP), комп'ютерна програма, що забезпечує криптографічну конфіденційність і аутентифікацію для підвищення безпеки електронної пошти.

VPN - це приватна мережа, яка використовує загальнодоступну мережу, зазвичай Інтернет, для створення безпечного каналу зв'язку. VPN з'єднує дві кінцеві точки, такі як два віддалених офіси через Інтернет, щоб створити з'єднання.

Мережі VPN використовують IPsec. IPsec - це набір протоколів, розроблених для реалізації безпечних мережних сервісів. Сервіси IPsec забезпечують аутентифікацію, цілісність, контроль доступу та конфіденційність. За допомогою IPsec віддалені вузли можуть обмінюватися зашифрованою і перевіреною інформацією.

У багатьох організаціях виникає все більше проблем з даними, що використовуються. Під час використання дані більше не захищені, оскільки користувачу необхідно відкривати і змінювати їх. В системній пам'яті можуть зберігатися конфіденційні дані, наприклад ключ шифрування. Якщо злочинці скомпрометують дані під час їх використання, вони будуть мати доступ до даних, які зберігаються та переміщуються.

Контроль фізичного доступу

Контроль фізичного доступу - це розгорнуті реальні бар'єри, які мають запобігти прямому контакту з системами. Мета полягає в тому, щоб запобігти несанкціонованому фізичному доступу неавторизованих користувачів до об'єктів, обладнання та інших ресурсів організації.

Контроль фізичного доступу визначає ХТО, ДЕ і КОЛИ може увійти до яких приміщень (або вийти).

Приклади контролю фізичного доступу:

* Охоронці (Рис. 1) контролюють об'єкт.
* Паркани (Рис. 2) захищають периметр.
* Детектори руху (Рис. 3) виявляють рухомі об'єкти.
* Замки для ноутбуків (Рис. 4) захищають портативне обладнання.
* Двері з замком (Рис. 5) запобігають несанкціонованому доступу.
* Магнітні карти (Рис. 6) надають доступ до зон обмеженого доступу.
* Сторожові собаки (Рис. 7) захищають територію.
* Відеокамери (Рис. 8) здійснюють моніторинг об'єкту шляхом збору і запису зображення.
* Тамбури-шлюзи (mantraps) (Рис. 9) дозволяють отримати доступ до захищеної зони після зачинення двері №1.
* Аварійна сигналізація (Рис. 10) виявляє вторгнення.

Системи розмежування логічного доступу

Розмежування логічного доступу забезпечують апаратні і програмні рішення для керування доступом до ресурсів та систем. Ці технологічні рішення включають інструменти та протоколи, які використовуються комп'ютерними системами для ідентифікації, аутентифікації, авторизації та звітності.

До засобів логічного розмежування доступу відносять:

* Шифрування - це процес перетворення відкритого тексту на зашифрований текст.
* Смарт-карти, які містять вбудований мікрочіп.
* Паролі - це захищені рядки символів.
* Біометричні дані - фізичні характеристики користувачів.
* Списки контролю доступу (Access Control Lists, ACL) визначають тип трафіку, який дозволений в мережі.
* Протоколи - це набір правил, які регулюють обмін даними між пристроями.
* Міжмережні екрани - блокують небажаний мережний трафік.
* Маршрутизатори з'єднують, як мінімум, дві мережні інфраструктури.
* Системи виявлення вторгнень виконують моніторинг мережі на наявність підозрілих дій.
* Рівні відсікання (Clipping Levels) - є певними допустимими пороговими значеннями помилок до спрацювання сигналу тривоги.

Для отримання додаткової інформації клацніть на кожному типі розмежування логічного контролю на рисунку.

Адміністративний контроль доступу

Засоби адміністративного контролю доступу - це політики і процедури, визначені організацією для впровадження та забезпечення дотримання всіх аспектів контролю несанкціонованого доступу. Засоби адміністративного контролю зосереджені на персоналі і діловій практиці. До засобів адміністративного контролю відносять:

* Політики - це твердження про наміри.
* Процедури - докладні кроки, необхідні для виконання певних дій.
* Практика найму співробітників - включає в себе кроки, що вживаються організацією для пошуку кваліфікованих співробітників.
* Перевірка біографії - це вибіркова перевірка інформації про співробітників, яка включає інформацію з попередніх місць працевлаштування, кредитну історію та наявність судимостей.
* Категоризація даних впорядковує дані по категоріям залежно від секретності.
* Тренінги з питань безпеки інформують співробітників про політики безпеки, які діють в організації.
* Перевірки та ревізії дозволяють оцінити продуктивність роботи співробітника.

# Обов'язкове розмежування доступу

Обов'язкове розмежування доступу (Mandatory Access Control, MAC) обмежує дії, які суб'єкт може виконувати з об'єктом. Суб'єктом може бути користувач або процес. Об'єктом може бути файл, порт або пристрій вводу/виводу. Правило авторизації вказує, чи може суб'єкт отримати доступ до об'єкту.

Організації використовують MAC, якщо існують різні рівні секретності. У кожного об'єкта є мітка і у кожного суб'єкта є допуск. Система MAC обмежує доступ суб'єкта у відповідності до рівня секретності об'єкта та мітки користувача.

Наприклад, візьміть військову класифікацію з рівнями «Таємно» та «Цілком таємно». Якщо якийсь файл (об'єкт) вважається зовсім секретним, він класифікується (позначається) «Цілком таємно». Такий файл (об'єкт) можуть переглядати тільки співробітники (суб'єкти), у яких є допуск рівня "Цілком таємно". Механізм розмежування доступу повинен гарантувати, що співробітник (суб'єкт) з доступом тільки до секретної інформації ніколи не одержить доступу до файлу з міткою «Цілком таємно». Також користувач (суб'єкт) з доступом до інформації з грифом «Цілком таємно» не може змінити класифікацію файлу (об'єкту) з «Цілком таємно» на "Таємно". Крім того, користувач з доступом до інформації з грифом «Цілком таємно» не зможе відправити файл з міткою «Цілком таємно» користувачу з доступом тільки до інформації з грифом "Таємно".

# Дискреційне розмежування доступу

Власник об'єкта визначає, чи дозволяти доступ до об'єкта з дискреційним розмежуванням доступу (Discretionary Access Control, DAC). DAC відкриває або обмежує доступ до об'єкта, на основі рішення власника. Як випливає з назви, цей тип розмежування доступу є дискреційним (вибірковим), оскільки власник об'єкта з певними правами доступу може надавати ці ж права доступу іншому суб'єкту на власний розсуд.

У системах, що використовують дискреційне розмежування доступу, власник об'єкта може сам вирішувати, які суб'єкти будуть мати доступ до об'єкта і на якому рівні. Як показано на рисунку, одним з найпоширеніших методів є дозволи. Власник файлу може вказати, які конкретні дозволи (читання/ запис/ виконання) можуть мати інші користувачі.

Списки контролю доступу - є ще одним поширеним механізмом, що використовується для реалізації дискреційного розмежування доступу. У списках контролю доступу застосовуються правила для визначення дозволеного вхідного та вихідного трафіку в мережі.

# Контроль доступу на основі ролей

Контроль доступу на основі ролей (Role-Based Access Control, (RBAC) працює в залежності від ролі суб'єкта. Ролі - це посадові обов'язки в організації. Конкретні ролі вимагають певних дозволів для виконання певних операцій. Користувачі отримують дозволи у рамках своєї ролі.

RBAC може працювати в комбінації з DAC або MAC, застосовуючи відповідні політики. RBAC допомагає адмініструвати системи безпеки у великих організаціях з сотнями користувачів і тисячами можливих дозволів. Організації широко використовують RBAC для керування дозволами комп'ютерів у середині системи або застосунку. І вважають це найкращою практикою безпеки.

# Розмежування доступу на основі правил

Під час контролю доступу на основі правил використовуються списки контролю доступу (ACL), які допомагають визначити, чи надавати доступ користувачу. В ACL міститься певна кількість правил, як показано на рисунку. Можливість надання доступу залежить від цих правил. Наприклад, одне з правил полягає в тому, що жоден співробітник не зможе отримати доступ до файлу платіжної відомості після завершення робочого дня або у вихідні.

Як і у випадку з MAC, користувачі не можуть змінювати правила доступу. Організації можуть комбінувати розмежування доступу на основі правил з іншими стратегіями для реалізації обмеження доступу. Наприклад, впровадження методів MAC може використовувати підхід, заснований на правилах.

# Що таке ідентифікація?

В процесі ідентифікації застосовуються правила, що встановлені політикою авторизації. Суб'єкт запитує доступ до системного ресурсу. Кожен раз, коли суб'єкт запитує доступ до ресурсу, засоби контролю доступу визначають, надавати чи забороняти доступ. Наприклад, політика авторизації визначає, які дії користувач зможе виконувати з ресурсом.

Унікальний ідентифікатор забезпечує правильний зв'язок між дозволеними діями і суб'єктами. Ім'я користувача - найбільш поширений метод, який використовується для ідентифікації користувача. Ім'я користувача може бути букво-цифровою комбінацією, персональним ідентифікаційним номером (PIN), смарт-картою або біометричними даними (відбитком пальця, скануванням сітківки або розпізнаванням голосу).

Унікальний ідентифікатор гарантує, що система може ідентифікувати кожного окремого користувача, що дозволяє авторизованому користувачеві виконувати необхідні дії з конкретним ресурсом.

# Контроль ідентифікації

Політика кібербезпеки визначає, які засоби контролю ідентифікації слід використовувати. На основі ступеня чутливості інформації та інформаційних систем визначається, наскільки суворо має контролюватися доступ. Збільшення кількості випадків витоку даних змусило багато організацій посилити контроль ідентифікації. Наприклад, індустрія кредитних карт в Сполучених Штатах вимагає від всіх постачальників перейти на системи ідентифікації через смарт-карти.

# Щось, що ми знаємо (фактор знань)

Паролі, парольні фрази або PIN-коди є прикладами того, що знає користувач. Паролі є найпопулярнішим методом, що використовується для аутентифікації. Парольну фразу, код доступу, ключ доступу та PIN-код часто також називають паролями. Пароль - це послідовність символів, що використовується для підтвердження особи користувача. Якщо ці символи якимось чином пов'язані з користувачем (наприклад, містять ім'я, дату народження або адресу), кібер-злочинцям буде простіше підібрати його пароль.

У багатьох публікаціях рекомендується використовувати пароль довжиною не менше восьми символів. Не слід створювати занадто довгі паролі, які важко запам'ятати, або навпаки, настільки короткі, що вони стають вразливими для підбору. Паролі повинні містити комбінацію літер верхнього та нижнього регістрів, цифр та спеціальних символів. Натисніть [тут](https://howsecureismypassword.net/) щоб протестувати свої поточні паролі.

Користувачам слід використовувати різні паролі для різних систем. В іншому випадку, якщо злочинець зламає пароль користувача один раз, він отримає доступ до всіх його облікових записів. Менеджер паролів може допомогти користувачеві створювати та запам'ятовувати надійні паролі. Натисніть [тут](http://strongpasswordgenerator.com/) щоб відкрити генератор надійних паролів.

# Щось, що ми маємо (фактор володіння)

Смарт-карти, ключі-брелоки безпеки - це приклади того, що користувач має при собі.

**Смарт-карта безпеки (рисунок 1).** Смарт-карта - це невелика пластикова картка розміром з кредитну, в яку вбудовано невеликий чіп. Чіп - це інтелектуальний носій даних, здатний обробляти, зберігати та захищати дані, що зберігаються. На смарт-картах зберігається приватна інформація, наприклад номери банківських рахунків, інформація особистої ідентифікації, медичні записи та цифрові підписи. Смарт-карти забезпечують аутентифікацію та шифрування для захисту даних.

**Ключ-брелок безпеки (рисунок 2)** - це невеликій пристрій, який можна прикріпити до зв'язки ключів. Він використовує процес, який називається двофакторною аутентифікацією, що є більш безпечним, ніж комбінація імені користувача та пароля. Спочатку користувач вводить персональний ідентифікаційний номер (PIN-код). У випадку, якщо код введено правильно, на дисплеї ключа-брелока безпеки відобразиться номер. Це другий етап аутентифікаціїктор, у якому користувач повинен ввести цей номер для входу на пристрій або до мережної інфраструктури.

Щось, що є частиною нас (фактор властивості)

Унікальні фізичні характеристики, такі як відбитки пальців, сітківка ока або голос, які ідентифікують конкретного користувача, називають біометричними даними. У системах біометричної безпеки, під час перевірки достовірності користувача, порівнюються фізичні характеристики зі збереженими профілями для аутентифікації користувачів. Профіль - це файл даних, що містить відомі характеристики особи. Система надає користувачеві доступ, якщо його характеристики відповідають збереженим параметрам. Прикладом розповсюдженого біометричного пристрою є пристрій для считування відбитків пальців.

Існує два типи біометричної ідентифікації. Через:

* **Фізіологічні характеристики** - до них відносяться відбитки пальців, ДНК, обличчя, кисті рук, сітківка ока або особливості форми вух.
* **Поведінкові характеристики** - включають в себе моделі поведінки, такі як жести, голос, характер набору тексту або хода користувача.

Біометричні технології стають дедалі популярнішими у системах громадської безпеки, побутовій електроніці та торгових терміналах. В біометричних системах використовують зчитувач або сканер, програмне забезпечення, яке перетворює скановану інформацію у цифрову форму, а також базу даних, яка зберігає біометричні дані для порівняння.

# Багатофакторна аутентифікація

Багатофакторна аутентифікація використовує принаймні два методи перевірки. Хорошим прикладом є ключ-брелок безпеки. Двома факторами є те, що вам відомо, наприклад, пароль і те, що ви маєте, наприклад, ключ-брелок безпеки. Можна підвищити безпеку, додавши біометрію, наприклад сканування відбитку пальця.

Багатофакторна аутентифікація може зменшити частоту випадків крадіжки особистих даних, оскільки знання пароля не дає кібер-злочинцям доступу до інформації про користувача. Наприклад, веб-сайт для онлайн-банкінгу може вимагати пароль та PIN-код, який користувач отримує на свій смартфон. Як показано на рисунку, зняття готівки з банкомату - це ще один приклад багатофакторної аутентифікації. Користувач повинен мати банківську картку та знати PIN-код, перш ніж банкомат буде видавати готівку.

# Що таке авторизація?

Засоби контролю авторизації визначають, що користувач може і що не може робити в мережі після успішної аутентифікації. Після того, як користувач підтвердить свою особистість, система перевіряє, до яких мережних ресурсів користувач може отримати доступ і які дії користувач може виконувати з цими ресурсами. Як показано на рисунку, авторизація відповідає на запитання: "Які права (читання, копіювання, створення, видалення) має користувач?"

Авторизація використовує набір атрибутів, який описує доступ користувача до мережної інфраструктури. Система порівнює ці атрибути з інформацією, що міститься в базі даних аутентифікації, визначає сукупність обмежень для цього користувача та передає її локальному маршрутизатору, до якого підключений користувач.

Авторизація виконується автоматично і не вимагає від користувачів додаткових дій після аутентифікації. Авторизація має бути виконана одразу після успішної аутентифікації користувача.

# Використання авторизації

Визначення правил авторизації - це перший крок контролю доступу. Ці правила встановлює політика авторизації.

Групова політика визначає параметри авторизації на основі приналежності користувача до певної групи. Наприклад, всі співробітники організації мають магнітну карту, яка забезпечує доступ на об'єкт. Якщо посада працівника не вимагає доступу до серверної кімнати, його карта безпеки не дозволить йому туди увійти.

Політика на рівні повноважень визначає права доступу на основі статусу працівника в організації. Наприклад, лише старші працівники ІТ-відділу можуть заходити до серверної кімнати.

# Що таке звітність?

Засоби звітності відстежують дії користувача та процесів, які стосуються внесення змін до системи, збирають цю інформацію і повідомляють дані про використання. Організація може використовувати ці дані для таких цілей, як аудит або виставлення рахунків. Зібрані дані можуть включати в себе: час входу користувача, відомості про успішні та невдалі спроби входу в систему, а також дані до яких мережних ресурсів користувач звертався. Таким чином організація може відслідковувати дії, помилки та відхилення під час аудиту або розслідування.

# Впровадження звітності

Звітність забезпечується за рахунок відповідних технологій, політик, процедур та навчання. З файлів журналу можна одержати детальну інформацію у відповідності з вибраними параметрами. Наприклад, в організації можуть переглядати журнал на предмет успішних або невдалих спроб входу в систему. Невдалі спроби входу в систему можуть свідчити про те, що злочинці намагалися зламати обліковий запис. Успішні спроби входу в систему показують, які користувачі використовували які ресурси системи та коли до них звертались. Наприклад, чи є нормальним для авторизованого користувача входити до корпоративної мережі о 3:00 ранку? Політики та процедури організації визначають, які дії слід фіксувати та яким чином створюються, перевіряються та зберігаються файли журналів.

Дотримання термінів зберігання даних, правил утилізації носіїв інформації та інших нормативних вимог сприяють належній звітності. Багато законів вимагають здійснення спеціальних заходів для захисту різних типів даних. Ці закони стимулюють організацію до правильного способу обробки, зберігання та знищення даних. Відповідне навчання та обізнаність співробітників щодо корпоративних політик, процедур та пов'язаних з ними законів також посилюють відповідальність.

# Превентивні засоби контролю

Превентивні засоби означає попереджувальні. Превентивні засоби розмежування доступу запобігають небажаним або несанкціонованим діям. Для авторизованого користувача превентивне розмежування доступу означає обмеження. Призначення конкретних прав доступу користувачам в системі є прикладом превентивного контролю. Незважаючи на те, що користувач є авторизованим, система встановлює обмеження його прав, щоб запобігти можливим несанкціонованим діям. Міжмережний екран, який блокує доступ до порту або сервісу, якими можуть скористатися кіберзлочинці, також є засобом превентивного контролю.

# Ефективні механізми розкриття порушень

Виявлення - це акт або процес виявлення чого-небудь. Ефективні механізми розкриття порушень дозволяють виявити різні типи несанкціонованих дій. Системи виявлення можуть бути дуже простими, наприклад, детектор руху або охоронець. А можуть бути більш складними, наприклад, система виявлення вторгнень (IDS). Всі ефективні механізми розкриття порушень мають кілька спільних рис: вони відслідковують незвичні або заборонені дії. Вони також надають методи реєстрації подій та оповіщення операторів системи про потенційний несанкціонований доступ. Ефективні механізми розкриття порушень не запобігають чому-небудь, а працюють більше за фактом події.

# Стримуючі засоби контролю

Стримуючий фактор є протилежністю заохоченню. Заохочення стимулюють людей чинити правильні дії, в той час як стримуючий фактор перешкоджає їм робити неправильні дії. Спеціалісти та організації, що займаються кібер-безпекою, використовують стримуючі засоби для обмеження або мінімізації певних дій чи поведінки, але їх недостатньо для повного запобігання. Стримуючі засоби розмежування доступу перешкоджають одержанню несанкціонованого доступу до інформаційних систем та конфіденційних даних. Стримуючі засоби розмежування доступу перешкоджають атакам на системи, крадіжці даних та розповсюдженню шкідливого коду. Організації використовують стримуючі засоби розмежування доступу для підсилення дотримання політик кібербезпеки.

Стримуючі фактори застерігають потенційних кіберзлочинців проти вчинення злочину. На рисунку представлені розповсюджені стримуючі засоби розмежування доступу, що використовуються в сфері кібербезпеки.

# Коригуючі засоби контролю

Коригуючі заходи протидіють небажаним діям. Організації впроваджують коригуючі засоби розмежування доступу після того, як система зазнала загрози. Коригуючі заходи дозволяють відновити конфіденційність, цілісність та доступність системи. Вони також можуть повернути системи до нормального стану після несанкціонованих дій.

# Засоби відновлення

Відновлення - це повернення до нормального стану. Засоби відновлення розмежування доступу призначені для відновлення ресурсів, функцій і можливостей після порушення політики безпеки. Засоби відновлення можуть усунути пошкодження та запобігти збитків у подальшому. Ці засоби мають більш розширені можливості в порівнянні з коригуючими засобами контролю та розмежування доступу.

# Компенсуючі засоби контролю

Компенсація означає одержання чогось на заміну. Компенсуючі засоби розмежування доступу розширюють можливості інших засобів для більш суворого контролю за дотриманням політики безпеки.

Компенсуючі засоби можуть застосовуватись як заміна інших засобів, які неможливо використати в даних умовах. Наприклад, організація не має можливості тримати собаку для охорони, тому встановлює детектор руху з прожектором і звуком, що імітує гавкання собаки.

# Що таке маскування даних?

Технологія маскування даних захищає дані, замінюючи конфіденційну інформацію на її неконфіденційну версію. Неконфіденційна версія виглядає як оригінал і виконує його функції. Це означає, що в бізнес-процесі можуть використовуватися неконфіденційні дані і немає необхідності змінювати додатки підтримки або системи зберігання даних. У більшості випадків використання маскування дозволяє обмежити поширення конфіденційних даних у середині ІТ-систем, шляхом заміни на сурогатні для тестування і аналізу. Інформація може маскуватися динамічно, якщо система або програма визначають запит користувача на одержання конфіденційної інформації як ризикований.

Технології маскування даних

Маскування даних може замінити конфіденційні дані у невиробничих середовищах для захисту базової інформації.

Існує декілька методів маскування даних, які гарантують, що дані зберігають значення, але змінюються достатньо, щоб захистити їх конфіденційність:

* Підстановка замінює дані значеннями, які виглядають як достовірні для збереження анонімності записів.
* Перетасування створює набір даних заміщення з того ж набору даних, який користувач хоче замаскувати. Наприклад, цей метод добре підходить для фінансової інформації в тестовій базі даних.
* Обнулення застосовує нульове значення до обраного поля, що повністю запобігає моніторингу даних.

# Що таке стеганографія?

Стеганографія дозволяє приховати дані (повідомлення) в іншому файлі, такому як графічне зображення, аудіо або інший текстовий файл. Перевага стеганографії над криптографією полягає в тому, що приховане повідомлення не привертає до себе уваги. Наприклад, переглядаючи файл як в електронному, так і в друкованому вигляді зрозуміти, що рисунок містить приховане повідомлення, неможливо.

У приховуванні даних бере участь кілька компонентів. По-перше, є вбудовані дані, що є прихованим повідомленням. Текстовий контейнер (зображення, звук) приховує вбудовані дані, створюючи стеготекст (стегозображення, стегозвук). Стегоключ визначає процес приховування.

# Методи стеганографії

Підхід, який використовується для вбудовування даних в зображення-контейнер, використовує метод заміни молодших бітів (Least Significant Bits, LSB). У цьому методі використовують біти кожного пікселя у зображенні. Піксель - це основна одиниця програмування кольору в комп'ютерному зображенні. Колір конкретного пікселя - це суміш трьох кольорів: червоного, зеленого та синього (RGB). Три байти даних визначають колір пікселя (один байт для кожного кольору). Вісім бітів складають байт. 24-бітова система кольорів використовує всі три байти. Метод LSB використовує по одному біту з кожного компоненту червоного, зеленого та синього кольорів. Кожен піксель може зберігати 3 біти.

На рисунку показано три пікселі 24-бітного кольорового зображення. Однією з літер у прихованому повідомленні є літера T і вставка символу Т змінює лише два біти кольору. Людське око не здатне розпізнати зміни, внесені до молодших бітів. Результатом є - прихований символ.

У середньому, достатньо змінити не більше половини бітів у зображенні, щоб ефективно приховати секретне повідомлення.

# Соціальна стеганографія

Соціальна стеганографія приховує інформацію, що знаходиться у всіх на очах. Для цього створюються повідомлення, скриту частину яких зможуть зрозуміти тільки посвячені у таємницю. Інші, хто просто прочитає повідомлення, не побачать прихованого послання. Підлітки в соціальних мережах використовують цю тактику для спілкування з найближчими друзями, при цьому всі інші, в тому числі батьки, не знають що насправді означає повідомлення. Так, наприклад, фраза "йдемо в кіно" може означати "похід на пляж".

Люди в країнах, де існує цензура засобів масової інформації, також використовують соціальну стеганографію, публікуючи повідомлення з завідомо неправильною орфографією або з прихованими посиланнями. По суті, вони спілкуються одночасно з різними аудиторіями.

# Виявлення

Стеганаліз - це процес виявлення прихованої інформації. Метою стеганалізу є виявлення прихованих відомостей.

Структури, що повторюються в стегозображенні викликають підозру. Наприклад, диск може мати невикористані області, у яких приховується інформація. Утиліти для аналізу дисків можуть повідомляти про приховану інформацію в невикористаних кластерах пристроїв зберігання даних. Фільтри можуть перехоплювати пакети даних, що містять приховану інформацію в заголовках. Обидва ці методи використовують стеганографічні сигнатури.

Порівнюючи вихідне зображення зі стего-зображенням, аналітик може візуально помітити структури, що повторюються.

# Обфускація

Обфускація даних - це практичне використання методів маскування даних та стеганографії в галузі кібербезпеки та кіберрозвідки. В результаті обфускації зміст повідомлення стає заплутаним, неоднозначним або важчим для розуміння. Система може навмисно кодувати повідомлення, щоб запобігти несанкціонованому доступу до конфіденційної інформації.

# Програми

Технологія цифрових водяних знаків захищає програмне забезпечення від несанкціонованого доступу або модифікації. Технологія захисту програмного забезпечення за допомогою цифрових водяних знаків передбачає ін'єкцію у виконуваний код програми прихованого повідомлення, яке слугує доказом права власності. Приховане повідомлення є цифровим водяним знаком, за допомогою якого захищається програмне забезпечення. Якщо хтось спробує видалити цифровий водяний знак, то код стане непрацездатним.

Обфускація програмного забезпечення перетворює його у версію, еквівалентну оригіналу, але значно важчу для аналізу зловмисниками. Програма буде працювати, як раніше, але при спробі декомпіляції видаватиме незрозумілі результати.

# Розділ 5. Мистецтво забезпечення цілісності даних

Забезпечення цілісністі гарантує, що дані залишаються незмінними і заслуговують довіри весь свій життєвий цикл. Цілісність даних є важливим компонентом для проектування, реалізації та використання будь-якої системи, яка зберігає, обробляє або передає дані. Розділ починається з опису різноманітних засобів контролю цілісності даних, зокрема алгоритми хешування, додавання солі (salting) та аутентифікації повідомлень з використанням ключа та хеш-суми (HMAC). Далі розглядається використання цифрових підписів і сертифікатів за допомогою яких перевіряється автентичність повідомлень та документів. В кінці розділу обговорюється забезпечення цілісності баз даних. Наявність добре контрольованої і чітко структурованої системи цілісності даних підвищує стабільність, продуктивність і зручність в обслуговуванні систем баз даних.

# Що таке хешування?

В багатьох випадках необхідний механізм, який гарантує, що дані залишаються незмінними під час їх зберігання або передаванні. Хешування - це інструмент, який забезпечує цілісність даних, використовуючи вхідні бінарні дані (повідомлення) і створюючи з них вихідні дані фіксованої довжини, які називають хеш-значенням або дайджестом, як показано на рисунку.

У системах хешування застосовуються криптографічно стійкі хеш-функції, які і забезпечують перевірку та гарантію цілісності даних. Віни також можуть застосовуватись для перевірки аутентифікації. Незашифровані паролі та ключі шифрування можна замінити відповідними хеш-функціями. Це означає, що під час хешування одного і того ж пароля, за допомогою конкретного алгоритму хешування, завжди буде одержано однаковий результат хеш-суми. Імовірність співпадіння хеш-сум є надзвичайно мізерною. Крім того, хеш функції є незворотніми - відновити вхідні дані за значенням хеш-суми дуже складно.

Кожен раз, коли дані змінюються, значення хеш-суми також змінюється. Через це криптографічні хеш-суми часто називають цифровими відбитками. Хеш-суми застосовують для того, щоб виявляти дублікати файлів даних, контроль зміни версії файлів та інші аналогічні задачі. Хешування допомагає запобігти випадковому або зловмисному пошкодженню або зміні даних. Хешування також є дуже ефективним. Хеш-сума як великого файлу так і вміст всього диска під час хешування призводять до однакових за розміром результатів.

Властивості хеш-функцій

Хешування - це незворотня математична функція, яку відносно легко обчислити, але значно складніше знайти аргумент за її значенням. Незворотність функції можна навести, як аналог з меленою кавою. Легко змолоти кавові зерна, але майже неможливо відновити їх з змелених кусочків.

Криптографічна хеш-функція має такі властивості:

* Вхідні дані можуть бути будь-якої довжини.
* Вихідні дані мають фіксовану довжину.
* Хеш-функція є одностороння і незворотна.
* З двох різних вхідних множин значень майже ніколи неможливо отртмати однакові значення хеш-сум.

# Алгоритми хешування

Хеш-функції дозволяють визначити, що дані змінились через помилку користувача або через збій в процесі передавання. Наприклад, відправник може переконатися, що повідомлення дійшло до одержувача без змін. Для цього передавальний пристрій обчислює хеш-суму повідомлення (відбиток фіксованої довжини).

**Простий алгоритм хешування (8-бітна контрольна сума)**

8-бітна контрольна сума є одним з перших алгоритмів хешування. Це є найпростіша форма хеш-функції. Під час розрахунку хеш-суми за цим алгоритмом 8-розрядна контрольна сума обчислює хеш, перетворюючи повідомлення в двійкові числа, а потім організовуючи рядок двійкових чисел в 8-бітові набори. Далі 8-бітові значення сумуються. Останній крок - перетворити результат у доповняльний код. Перетворення у доповняльний код відбувається наступним чином: розряди двійкового числа інвертуються, після чого до до числа додається одиниця. Це означає, що нулі перетворюється в одиниці, а одиниці перетворюються в нулі. Останній крок - додати 1. Таким чином отримується 8-бітна хеш-сума.

Натисніть [тут](http://easyonlineconverter.com/converters/checksum_converter.html) щоб розрахувати 8-бітну хеш-суму для повідомлення **BOB**.

1. Перетворіть повідомлення BOB в двійковий код з використанням таблиці кодів ASCII, як показано на рисунку 1.

2. Перетворіть двійкові числа в шістнадцяткові, як показано на рисунку 2.

3. Введіть шістнадцяткові числа в калькулятор (42 4F 42).

4. Натисніть кнопку **Calculate** (Обчислити) Результатом є хеш-сума **2D**

Спробуйте обчислити наступні приклади:

SECRET = “S”=53 “E”=45 “C”=43 “R”=52 “E”=45 “T”=54

ХЕШ-СУМА = 3A

MESSAGE = “M”=4D “E”=45 “S”=53 “S”=53 “A”=41 “G”=47 “E”=45

ХЕШ-СУМА = FB

Сучасні алгоритми хешування

На сьогоднішній день широко застосовується велика кількість сучасних алгоритмів хешування. Двома найпопулярнішими є MD5 і SHA.

**Алгоритм Message Digest 5 (MD5)**

Рон Рівест розробив алгоритм хешування MD5 і цей алгоритм використовується в Інтернеті для певного кола задач. MD5 - це незворотня функція, яка дозволяє легко обчислити хеш із заданих вхідних даних, але робить складним обчислення вхідних даних при наявності лише значення хешу.

MD5 формує 128-бітове значення хеш-суми. У 2012 році була реалізована атака шкідливим ПЗ Flame, яке скомпрометувало безпеку MD5. Автори ПЗ Flame використовували колізію MD5 для підробки сертифіката підпису коду Windows. Натисніть [тут](https://blogs.technet.microsoft.com/srd/2012/06/06/flame-malware-collision-attack-explained/) щоб прочитати опис колізійної атаки шкідливим ПЗ Flame.

**Алгоритм безпечного хешування (Secure Hash Algorithm, SHA)**

У Національному інституті стандартів і технологій США (NIST) був розроблений алгоритм SHA, який включено у стандарт безпечного хешування (Secure Hash Standard, SHS). NIST опублікував SHA-1 в 1994 році. Сімейство алгоритмів SHA-2 замінило SHA-1, додавши чотири додаткові хеш-функції для створення сімейства SHA:

* SHA-224 (224 біт)
* SHA-256 (256 біт)
* SHA-384 (384 біт)
* SHA-512 (512 біт)

SHA-2 - більш стійкіший алгоритм і він все частіше застосовується замість MD5. SHA-256, SHA-384 і SHA-512 є алгоритмами наступного покоління.

Хешування файлів і цифрових носіїв

За допомогою механізму перевірки цілісності можна переконатись, що дані та інформація не зазнали змін на шляху від відправника до одержувача. Впевненість у цілісності даних є важливою, коли користувач завантажує файл з Інтернету або під час криміналістичного дослідження цифрових носіїв.

Щоб перевірити цілісність всіх образів IOS, Cisco надає контрольні хеш-суми MD5 і SHA на веб-сайті програмного забезпечення для завантаження. Користувач може порівняняти значення MD5-дайджесту на сайті з дайджестом MD5 образу IOS, встановленого на пристрої, як показано на рисунку. Якщо хеш-суми співпадають, користувач може бути впевненим в тому, що файл образу IOS було завантажено та встановлено у незміненому вигляді.

**Примітка**: Команда **verify /md5** результат виконання якої показано на рисунку, виходить за рамки цього курсу.

У сфері цифрової криміналістики хешування використовується для перевірки цифрових носіїв, що містять файли. Наприклад, експерт розраховує хеш-суму і створює побітну копію носія з файлами, формуючи таким чином цифровий клон. Потім експерт порівнює хеш-суму оригінального носія з хеш-сумою копії. Якщо значення хеш-сум співпадають, то копія є ідентична оригіналу. Повна ідентичність бітів копії бітам оригіналу доводить незмінність. Спираючись на цю незмінність, можна відповісти на наступні питання:

* Чи дійсно експерт має у свому розпорядженні файли з оригінального носія?
* Чи можна стверджувати, що дані пошкоджені або змінені?
* Чи може експерт довести, що файли не пошкоджені?

Теким чином експерт м.ожуть дослідити копії цифрових доказів не ризикуючи оригінальним носієм.

# Хешування паролів

Алгоритми хешувальння формують хеш-суму (цифровий відбиток) фіксованої довжини на основі вхідних даних будь-якого обсягу. Злочинець не зможе за допомогою лише хеш-суми, відновити вхідні дані. Якщо вхідні дані змінюються, це призводить до формування іншої хеш-суми. Такі властивості добре підходить і для захисту паролів. Паролі, що зберігаються у системі повинні бути надійно захищені, але система також повинна мати можливість пррівняти пароль, що вводиться під час входу, з тим, що зберігається у системі.

На рисунку показано процес реєстрації облікового запису користувача і аутентифікації з використанням хешування. Система ніколи не записує пароль на жорсткий диск, вона зберігає тільки цифровий хеш.

Застосування

Криптографічні хеш-функції слід використовувати в наступних цілях:

* Забезпечення підтвердження достовірності. У цьому випадку хеш-функція застосовується спільно з симетричним ключем аутентифікації. Наприклад таким чином працюють протоколи IP Security (IPsec) або протоколи аутентифікації маршрутизаторів.
* Аутентифікацію шляхом генерації одноразових і односторонніх відповідей на запити протоколу аутентифікації.
* Надання доказів перевірки цілісності повідомлень, зокрема, які використовуються в контрактах з цифровим підписом, і сертифікатах інфраструктури відкритого ключа (PKI), (такі сертифікати застосовуються, наприклад, для доступу до захищеного сайту з використанням браузера).

При виборі алгоритму хешування рекомендується використовувати, як мінімум, SHA-256 або більш стійкі алгоритми, оскільки вони є в даний час найбільш безпечними. Уникайте використання SHA-1 і MD5 через виявлені в них серйозні вразливості безпеки. У промислових мережах слід застосовувати SHA-256 або більш стійкі алгоритми.

Хешування може виявити випадкові зміни, але воно не може запобігти навмисній зміні даних. Результат хешування не містить унікальної інформації, за допомогою якої можна було б однозначно визначити відправника. Це означає, що будь-хто може обчислити значення хеш-функції для будь-яких даних, якщо у нього є доступ до алгоритму потрібної хеш-функції. Наприклад, зловмисник може перехопити повідомлення, що передається через мережу, змінити його, перерахувати значення хеш-функції і додати до нового(підробленого) повідомлення. Приймаючий пристрій перевірятиме тільки те значення хешу, яке додане до повідомлення. Тому хешування вразливе для атак типу «людина по середині» і не захищає переданих даних.

# Злам хешу

Щоб одержати хеш-код, для входу в систему, зловмисник повинен вгадати пароль. Дві найбільш популярні атаки, що використовуються для зламування паролів, - це атаки перебору за допомогою словників та атака грублої сили (brute-force attacks).

Атака методом перебору за допомогою словника використовує файл, який містить розповсюджені слова, фрази і паролі. Файл має розраховані хеші. Така атака порівнює хеш-суми у файлі з значенням хешу пароля. Якщо хеш збігається, зловмисник дізнається групу потенційно правильних паролів.

Атака грубої сили намагається використовувати будь-яку можливу комбінацію символів для заданої довжини пароля. Такі атаки вимагають потужних обчислювальних ресурсів, але якщо наявний великий запас часу, то цей метод виявить пароль з сто відсотковою точністю. Тому паролі повинні бути досить довгими, щоб зробити час, необхідний для виконання атаки занадто довгим для успішності атаки. Хешування паролів ускладнює зловмисникам задачу вгадування паролів.

# Що розуміють під додаванням солі?

Додавання солі під час хешування забезпечує більш надійний захист пароля. Якщо у двох користувачів однаковий пароль, вони також будуть мати однакові значення хешів паролів. Сіль, яка є випадковим рядком символів, додається до паролю перед хешуванням. Це створює різний хеш-результат для двох паролів, як показано на рисунку. База даних зберігає як хеш, так і сіль.

На рисунку показано приклад у якому хеш-суми однакових паролів відрізняються, тому що сіль в кожному випадку є різною. В якості солі використовується випадкове число, тому сіль не обов'язково тримати у секреті.

# Запобігання атакам

Додавання солі не дозволяє зловмисникові використовувати атаку перебору за словником, щоб спробувати вгадати пароль. Крім того, наявність солі також не дозволяє використовувати таблиці пошуку і таблиці веселки, щоб зламати хеш.

**Таблиці пошуку**

У таблицях пошуку зберігаються попередньо обчислені хеш-суми паролів, які взяті з відповідних словників, а також самі ці паролі. За допомогою таблиць пошуку можна перевіряти сотні хеш-сум в секунду. Натисніть [тут](https://crackstation.net/) щоб дізнатися, як швидко можна зламати хеш за допомогою таблиці пошуку.

**Реверсивні таблиці пошуку**

За допомогою таких таблиць кіберзлочинці реалізують атаку методом грубої сили або перебором за допомогою словника з перевіркою великої кількості хеш-сум без попередньо побудованої таблиці пошуку. Використовуючи викрадену базу даних облікових записів, зловмисник створює таблицю пошуку, яка містить список хеш-сум усіх правильних паролів та список користувачів. Зловмисник хешує кожен ймовірний пароль і за допомогою таблиці пошуку, отримує список користувачів, паролі яких співпали з ймовірними, як показано на рисунку. Така атака є ефективною, оскільки багато користувачів має однакові паролі.

**Веселкові таблиці**

Веселкові таблиці, у порівнянні зі звичайними таблицями пошуку, мають менший об'єм. Скорочення об'єму досягається шляхом зменшення швидкості зламу. Скоротивши об'єм таблиці, зловмисник може перевірити більшу кількість хеш-сум використовуючи однаковий об'єм пам'яті.

Реалізація механізму додавання солі

Криптографічно стійкий генератор псевдовипадкових чисел ( Cryptographically Secure Pseudo-Random Number Generator, CSPRNG) - кращий вибір для генерування солі. Такий генератор генерує випадкове число, яке має високий ступінь випадковості і абсолютно непередбачуване, тому воно забезпечує криптографічну стійкість.

Впроваджуючи механізм додавання солі, необхідно дотримуватись наступних рекомендацій:

* Формувати унікальну сіль для кожного пароля користувача.
* Ніколи не використовувати одну і туж сіль багаторазово.
* Довжина солі повинна бути рівною довжині вихідного значення хеш-функції.
* Завжди виконуйте хешування на сервері в веб-застосунку.

Захист можна також підсилити за допомогою методу розтягнення ключа. Розтягнення ключа робить роботу хеш-функції дуже повільною. Що знижує ефективність атаки, роблячи високопродуктивне обладнання, яке може обчислювати мільярди хешів в секунду менш ефективним.

Кроки, які використовуються застосунком бази даних для зберігання і перевірки пароля з додаванням солі, показані на рисунку.

# Що таке HMAC?

Наступний рівень захисту від атак методом грубої сили, або атаки з допомогою словника забезпечується поєднанням секретного ключа і хеш-суми. У такій схемі тільки той, хто знає хеш-суму, може перевірити пароль. Одним із способів зробити це - включити секретний ключ в хеш-суму, використовуючи спеціальний алгоритм хешування, який називається кодом аутентифікації повідомлень з використанням хеш-функцій (Keyed-hash Message Authentication Code, HMAC або KHMAC). HMAC використовує додатковий секретний ключ у якості вхідних даних для хеш-функції. Використання HMAC дозволяє не тільки перевірити цілісність даних, але й забезпечує аутентифікацію. HMAC використовує спеціальний алгоритм, який об'єднує криптографічну хеш-функцію з секретним ключем, як показано на рисунку.

Тільки відправник і одержувач знають секретний ключ, а результат хеш-функції залежить як від вхідних даних, так і від секретного ключа. Таким чином, тільки той, хто знає секретний ключ, може обчислити коректну хеш-суму функції HMAC. Ця властивість дозволяє запобігти атакці типу «людина-по-середині» і забезпечує аутентифікацію джерела даних.

# Принцип дії механізму HMAC

Розглянемо приклад, коли відправник хоче гарантувати, що повідомлення залишаються незмінними під час передавання і хоче надати одержувачу можливість аутентифікації джерела даних.

Як показано на рисунку 1, пристрій, що передає, вводить дані (наприклад, інформацію про оплату для Террі Сміта у $100 і секретний ключ) на вхід алгоритму хешування і обчислює відбиток, або хеш-суму HMAC фіксованої довжини. Одержувач отримує аутентифікований відбиток, прикріплений до повідомлення.

На рисунку 2 приймаючий пристрій відділяє відбиток від повідомлення і використовує повідомлення у відкритому тексті у поєднанні з секретним ключем в якості вхідних даних для тієї ж функції хешування. Якщо приймаючий пристрій обчислює відбиток, рівний відправленому відбитку, повідомлення одержано в незмінному вигляді. Крім того, одержувач може бути впевненим у походженні повідомлення, тому що тільки відправнику відомий спільний секретний ключ. Функція HMAC підтвердила достовірність повідомлення.

Використання HMAC

HMAC також можна використовувати для аутентифікації Інтернет-користувачів. На багатьох веб-сервісах використовують базову аутентифікацію, у якій ім'я користувача і пароль передаються у незашифрованому вигляді. Якщо ж аутентифікація відбувається з використанням механізму HMAC, то користувач зобов'язаний передати ідентифікатор приватного ключа і хеш-суму НМАС. Сервер знаходить приватний ключ користувача та обчислює хеш-суму HMAC. Обчислена сервером хеш-сума повинна співпасти з хеш-сумою HMAC, яка була одержана від користувача.

За допомогою функції НМАС проводиться аутентифікація джерела кожного з пакетів та перевірка цілісності даних в VPN-мережах, що базуються на протоколі IPsec.

Як показано на рисунку, продукти Cisco використовують хешування для аутентифікації об'єктів, перевірці цілісності і достовірності даних:

* Маршрутизатори Cisco IOS під час роботи використовують схему аналогічну HMAC: в повідомлення про оновлення протоколу маршрутизації додається аутентифікаційна інформація за допомогою секретного ключа.
* Шлюзи та клієнти IPsec перевіряють цілісність та достовірність пакетів використовує алгоритми хешування, зокрема MD5 і SHA-1 в режимі HMAC.
* Образи програмного забезпечення Cisco, які розміщені на сайті Cisco.com містять контрольну суму на основі MD5, щоб клієнти могли перевіряти цілісність завантажених образів.

**Примітка**: Термін "об'єкт" означає пристрій або систем всередині організації.

# Що таке цифровий підпис?

Рукописні підписи і печатки на документах підтверджують авторство. Цифрові підписи можуть забезпечувати ті ж функції.

Внести зміни у незахищений цифровий документ дуже легко. Цифровий підпис дозволяє визначити, чи редагувався документ після його підпису користувачем. Цифровий підпис - це математичний метод, який використовується для перевірки достовірності та цілісності повідомлення, цифрового документа або програмного забезпечення.

У багатьох країнах цифрові підписи мають таку ж юридичну силу, як документ, підписаний вручну. Електронний підпис, що стоїть під електронним контрактом, договором або будь-яким іншим документом, який у паперовому вигляді вимагає рукописного підпису, має повну юридичну силу. Для вирішення задач, що пов'язані з юридичним захистом та регулюванням, передбачені та ведуться відповідні журнали подій, відстежують історію змін у електронному документі.

Цифровий підпис допомагає встановити справжність, цілісність і неможливість відмови (невідхильність). Цифрові підписи мають характерні властивості на яких побудовано механізм аутентифікації об'єкта і перевірки цілісності даних, як показано на рисунку.

Цифрові підписи є альтернативою механізму HMAC.

# Неможливість відмови (невідхильність)

Під відхиленням розуміють відмову від авторства. Невідхильність - це спосіб гарантувати, що відправник повідомлення або документа не може відмовитись у надсиланні, а одержувач не може відмовитись у отриманні повідомлення або документа.

Наявність цифрового підпису гарантує, що відправник електронним способом підписав повідомлення або документ. Кожен з користувачів має унікальний цифровий підпис, тому той, хто створив підпис під документом, не зможе пізніше заперечувати свого авторства.

# Процес створення цифрового підпису

В основі цифрових підписів є асиметрична криптографія. Алгоритм відкритого ключа, такий як RSA, генерує два ключі: один закритий і інший відкритий. Ці ключі математично пов'язані між собою.

Аліса хоче відправити Бобу електролист, у якому міститься важлива інформація про вихід нового продукту на ринок. Боб повинен бути абсолютно впевненим, що повідомлення прийшло саме від користувача Аліса і доставлено в незмінному вигляді.

Аліса створює повідомлення та дайджест (хеш-суму) повідомлення. Вона шифрує дайджест повідомлення своїм закритим ключем, як показано на рисунку 1. Аліса пов'язує повідомлення, зашифрований дайджест повідомлення і відкритий ключ для створення підписаного цифровим підписом документа. Одержаний результат Аліса відправляє Бобу, як показано на рисунку 2.

Боб отримує повідомлення і читає його. Щоб переконатися, що повідомлення прийшло від Аліси, він створює дайджест повідомлення. Він бере зашифрований дайджест повідомлення, отриманий від Аліси, і розшифровує його за допомогою відкритого ключа Аліси. Боб порівнює дайджест повідомлення, отриманий від Аліси, з тим, який він створив. Якщо вони збігаються, Боб знає, що може довіряти отриманим даним і що ніхто не підробляв повідомлення, як показано на рисунку 3.

Натисніть [тут](https://www.youtube.com/watch?v=E5FEqGYLL0o) щоб переглянути відео, що пояснює процес створення цифрового сертифікату.

Використання цифрових підписів

Замість підписування всього документа можна підписати тільки його хеш-суму. Така схема підвищує ефективність та спрощує задачі пов'язані з перевіркою цілісніості та забезпечення сумісності. Впровадивши в організації систему електронного документообігу, що відповідає усім юридичним вимогам, можна повністю відмовитись від паперових документів та та традиційних печаток.

Нижче наводяться два приклади використання цифрових підписів:

* **Підписання коду** - використовується для перевірки цілісності виконуваних файлів, що завантажуються з веб-сайту постачальника. Підписання коду також використовує підписані цифрові сертифікати для аутентифікації і перевірки аутентичності веб-сайту (рисунок 1).
* **Цифрові сертифікати** - використовуються для перевірки організації або окремого користувача, а також для аутентифікації веб-сайту постачальника і встановлення зашифрованого з'єднання для обміну конфіденційними даними (рисунок 2).

# Порівняння алгоритмів цифрового підпису

Найбульш поширеними є три алгоритми цифрового підпису - Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA) і Elliptic Curve Digital Signature Algorithm (ECDSA). Всі три алгоритми містять механізми створення та перевірки цифрових підписів. Ці алгоритми функціонують на основі асиметричного шифрування з використанням відкритих ключів. Робота з цифровими підписами базується на двох операціях:

1. Генерація ключа

2. Перевірка ключа

Обидві операції вимагають шифрування і дешифрування ключів.

Алгоритм DSA базується на складності обчислень дискретних логарифмів. У багатьох країнах алгоритм DSA використовують у державному секторі для створення цифрових підписів. Можливості алгоритму DSA обмежуються формуванням та перевіркою цифрового підпису.

RSA є найбільш поширеним алгоритмом шифрування з відкритим ключем, з тих, які використовуються сьогодні. RSA створено в 1977 році. Названий на честь авторів: Рона Ривеста, Аді Шаміра і Леонарда Адлемана. В основі RSA лежить асиметричне шифрування. RSA можна використовувати не тільки для роботи з цифровими підписами, а також шифрування повідомлення.

DSA працює швидше, ніж RSA, в якості підпису для цифрового документа. Алгоритм RSA краще підходить для ситуацій, коли крім вимог підпису і перевірки електронних документів необхідне ще й шифрування повідомлень.

Як і більшість криптографічних систем, алгоритм RSA базується на двох математичних компонентах: модульній арифметиці і задачі факторизації великих цілих чисел. Натисніть [тут](https://www.youtube.com/watch?v=wXB-V_Keiu8) щоб дізнатися більше про те, як у RSA використовується модульна арифметика і факторизація великих цілих чисел.

ECDSA - це новий алгоритм цифрового підпису, який поступово замінює RSA. Його перевага полягає в тому, що він може використовувати набагато менші розміри ключа при такому ж рівні безпеки і вимагає значно менших об'ємів обчислень, ніж RSA.

# Що таке цифровий сертифікат?

Цифровий сертифікат це аналог електронного паспорту. Він дозволяє користувачам, хостам і організаціям безпечно обмінюватися інформацією через Інтернет. Цифровий сертифікат підтверджує автентичність користувача, який надсилає повідомлення. Цифрові сертифікати також можуть забезпечити конфіденційність для одержувача за допомогою засобів шифрування відповіді.

Цифрові сертифікати схожі на фізичні сертифікати. Наприклад, паперовий сертифікат Cisco Certified Network Associate Security (CCNA-S) на рисунку 1 містить відомості про те кому, ким (джерело сертифікатів) і на який тармін видано цей сертифікат. Зверніть увагу, як цифровий сертифікат на рисунку 2 містить аналогічні відомості.

# Використання цифрових сертифікатів

Щоб зрозуміти, як використовувати цифровий сертифікат, звернімося до рисунку 1. Користувач Боб підтверджує замовлення у користувача Аліса. Веб-сервер Аліси використовує цифровий сертифікат для захисту транзакції.

**Крок 1:** Користувач Боб переходить на веб-сайт користувача Аліса. Успішно встановивши безпечне з'єднання, браузер, як правило, відображає значок замка в рядку стану безпеки.

**Крок 2:** Веб-сервер Аліси надсилає цифровий сертифікат в браузер користувача Боб.

**Крок 3:** Браузер Боба перевіряє сертифікат, що зберігається в налаштуваннях браузера. Транзакція може бути продовжена тільки за наявності довіреного сертифіката.

**Крок 4:** Веб-браузер Боба створює унікальний одноразовий ключ сеансу.

**Крок 5:** Веб-браузер Боба використовує відкритий ключ веб-сервера, що відповідає сертифікату веб-сервера для шифрування сеансу.

**Крок 6:** В результаті тільки веб-сервер Аліси може читати транзакції, відправлені з браузера Боба.

# Що таке центр сертифікації?

Підхід, який вимагає багатократної взаємної ідентифікації усіх сторін в Інтернеті, є незручним. Тому сторони погоджуються довіряти нейтральній третій стороні. Передбачається, що третя сторона ретельно проводить перевірку учасників, що бажають одержати посвідчення. Після такої ретельної перевірки, третя сторона видає посвідчення, яке важко підробити. З цього моменту усі учасники, які довіряють цій третій стороні, просто приймають посвідчення, які видає ця третя сторона.

Наприклад, на рисунку Аліса подає заяву для отримання водійських прав. У цьому процесі вона представляє документи, що засвідчують її особистість (свідоцтво про народження, посвідчення особи з фотографією та ін) у відповідний державний орган. Державний орган перевіряє особистість Аліси і допускає її пройти екзамен для одержання водійського посвідчення. Після успішного завершення екзамену державний орган видає Алісі водійське посвідчення. Пізніше Алісі потрібно перевести в готівку банківський чек. Після пред'явлення чеку, працівник банку запитує у неї посвідчення, яке засвідчує її особу. Банк, оскільки він довіряє державному органу, який видав документ, приймає цей документ у якості посвідчення особи під час переведення грошей з чеку в готівку.

Центр сертифікації (СА) функціонує аналогічно, як державний орган в попередньому прикладі. СА видає цифрові сертифікати, для аутентифікації організацій і користувачів. Ці сертифікати також використовують для підписування та перевірки цілісності повідомлень.

# Що містить у собі цифровий сертифікат?

Якщо цифровий сертифікат відповідає стандартній структурі, то його може прочитати та зрозуміти будь-яка система незалежно від того, ким він був виданий. X.509 є стандартом для інфраструктури відкритих ключів (public key infrastructure, PKI) для керування цифровими сертифікатами. PKI - це політики, ролі і процедури, необхідні для створення, поширення, використання, зберігання та відкликання цифрових сертифікатів, а також керування ними. Згідно стандарту X.509 цифрові сертифікати повинні містити стандартну інформацію, яка показана на рисунку.

Процес валідації

Браузери і застосунки виконують обов'язкову валідацію(перевірку) сертифіката, щоб переконатись, що він є дійсний. Перевірка включає в себе наступні три процеси:

* Дослідження сертифіката - прослідковується шлях сертифікації, з перевіркою кожного сертифікату, починаючи з сертифікату кореневого джерела сертифікатів (СА).
* Перевірка шляху - вибір сертифікату емітента (СА) для кожного сертифікату у ланцюжку
* Перевірка на відкликання - дозволяє переконатись у тому, що тсертифікат не був відкликаний; якщо сертифікат відкликаний, то під час цієї перевірки встановлюється причина відкликання.

# Шлях сертифікату

Суб'єкт отримує сертифікат для відкритого ключа від комерційного СА. Сертифікат є частиною ланцюжка сертифікатів, яку також називають ланцюжком довіри. Кількість сертифікатів в ланцюжку залежить від ієрархічної структури СА.

На рисунку показаний ланцюжок сертифікатів для дворівневого СА. Є автономний кореневий центр сертифікації і підлеглий центр сертифікації в мережі. Причиною застосування дворівневої структури є те, що механізм підписування за стандартом X.509 дозволяє спростити усунення наслідків несанкціоного доступу. Якщо є автономний центр сертифікації, то він може підписати новий сертифікат для хоста в мережі. Якщо б автономний центр сертифікації був відсутнім, то довелося б встановлювати новий сертифікат корневого СА на кожному клієнтському комп'ютері, телефоні або планшеті.

Цілісність даних

Бази даних - це ефективний спосіб зберігання, вилучення та аналізу даних. Об'єми даних, які збираються зростають, як і степінь їх конфіденційності, кількість баз даних збільшується і спеціалісти з забезпечення кібербезпеки відіграють значну роль у їх захисті. Базу даних можна розглядати як електронну шафу-картотеку. Під терміном "цілісність даних" розуміють точність, узгодженість і надійність даних, що зберігаються в базі даних. Відповідальність за забезпечення цілісності даних лежить на тих, хто проектує, розробляє та керує експлуатацією баз даних.

Є чотири правила або обмеження цілісності даних:

* **Цілісність об'єктів**: Кожен рядок повинен мати унікальний ідентифікатор, що називається первинним ключем (рисунок 1).
* **Цілісність доменів**: Всі дані, що зберігаються в стовпці, повинні відповідати одному і тому ж формату і відповідати єдиному спільному визначенню (рисунок 2).
* **Цілісність посилань**: Зв'язки між таблицями повинні залишатися незмінними. Тому користувач не може видалити запис, який пов'язаний з іншим записом(рисунок 3).
* **Визначена користувачем цілісність**: Набір правил, визначених користувачем, які не відносяться до жодної з інших категорій. Наприклад, клієнт робить нове замовлення, як показано на рисунку 4. Спочатку перевіряється, чи це новий клієнт. Якщо це так, то додаємо нового клієнта до таблиці клієнтів.

Засоби контролю введення даних

Введення даних в систему частіше за все здійснюють користувачі. Відповідні засоби контролю допомагають забезпечити коректність даних, які вводяться.

**Керування вводом даних за допомогою випадаючих списків**

Ввід даних на основі таблиці за допомогою випадаючих списків замість того щоб вводити дані вручну. Наприклад, можна стандартизувати ввід місця знаходження, застосувавши випадаючий список, що формується на основі бази даних системи поштової адресації США.

**Засоби контролю перевірки значень у полях даних**

Встановивити правила для базової перевірки. Наприклад:

* Обов'язковість введення даних (введення неможливо закінчити, якщо в обов'язкових полях не будуть міститись дані;
* Маска введення (дозволяє виключити введення некоректних даних та забезпечити єдиний формат даних, наприклад, для номерів телефону);
* Додатні значення грошових сум;
* Діапазони даних (гарантують, що користувач не зможе ввести дані за межами заданого діапазону, наприклад, дата народження, не може бути введена як 01-18-1820)
* Обов'язкове затвердження другою особою (наприклад, обов'язкове узгодження з другою або третьою особою у випадках, коли працівник банку отримує запит на зарахування або зняття з рахунку, на суму, що перевищує вказане обмеження);
* Ліміт на кількість змінених записів (наприклад, якщо кількість змінених записів перевищує заданий ліміт за певний проміжок часу, то система заблокує обліковий запис користувача до тих пір, поки менеджер не визначить, чи є ці транзакції правомірними);
* Відстеження незвичної поведінки (система блокується, коли виявляє аномальну активність)

Правила перевірки (валідації)

Правило валідації перевіряє чи дані відповідають параметрам, які визначені конструктором бази даних. Правило валідації допомагає забезпечити повноту, правильність і узгодженість даних. Критерії, що використовуються під час валідації, включають наступні критерії:

* Розмір - перевіряє кількість символів в елементі даних;
* Формат - перевіряє відповідність даних заданому формату;
* Узгодженість - перевірка узгодженості кодів у зв'язаних елементах даних;
* Діапазон - перевіряє, що дані знаходяться в межах між мінімальним і максимальним значенням;
* Контрольна цифра - використання додаткових обчислень для створення контрольної цифри, що призначена для виявлення помилок.

# Перевірка типу даних

Перевірка типу даних - це найпростіший метод перевірки правильності даних, який дозволяє переконатись у тому, що дані введені користувачем є потрібного типу. Наприклад, номер телефону не може містити інших символів крім цифр. В базах даних передбачено три типи даних: ціле число, стрічка і десяткові дроби.

# Перевірка вхідних даних

Одним з найбільш важливих аспектів забезпечення цілісності бази даних є контроль над процесом введення даних. Відсутність такого контролю стає причиною багатьох вразливостей. Багато відомих атак реалізуються за рахунок некоректного вводу в базу даних. Такі атак можуть привести до зависання або інших порушень у роботі застосунків, а також до витоку конфіденційної інформації. Кіберзлочинці можуть використовувати автоматизовані атаки некоректного вводу.

Наприклад, користувач підписується на розсилання новин, заповнюючи форму у веб-застосунку. Програма-застосунок бази даних автоматично генерує і відправляє підтвердження через електнну пошту. Одержавши електронне повідомлення з посиланням для підтвердження підписки, кіберзлочинці модифікують URL-адресу цього розсилання. Наприклад, змінюють ім'я користувача, адресу електронної пошти або статус підписки. Електронне повідомлення повертається назад на сервер, на якому працює програма-застосунок бази даних. Якщо веб-сервер не перевіряє відповідність адреси електронної пошти або іншої облікової інформації, тим даним, які були введені в форму, то у базу даних попадає некоректна інформація. Хакери можуть автоматизувати цю атаку і таким чином внести тисячі некоректних записів в базу даних з інформацію про підписників.

# Перевірка аномалій

Під виявленням аномалій розуміють виявлення неочікуваних признаків та поведінку даних. До таких признаків відносять значення, які різко виділяються, вийнятки, відхилення та інші аномальні прояви в різноманітних застосунках баз даних. Виявлення і перевірка аномалій є важливим контрзаходом або захистом з визначення шахрайства. Виявлення аномалії у базах даних можна розпізнати шахрайські операції з кредитними картками та страховими полісами. Засоби виявлення аномаліїй у базі даних також може допомогти запобігти значних руйнувань або змін даних.

Під перевіркою даних на аномалії мають на увазі тестові запити або зміни даних, коли система виявляє незвичайні або несподівані явища. Прикладом аномалії можуть бути запити транзакцій для однієї і тієїж кредитної картки з віддалених один від одного регіонів за дуже короткий період часу. Якщо запит на транзакцію з Нью-Йорка відбувається о 10:30 ранку, а другий запит надходить з Чикаго о 10:35 ранку, то система запускає перевірку другої транзакції.

Другий приклад - зміна адрес електронної пошти в незвичайно великій кількості записів бази даних. Адреси електроної пошти застосовуються під час організації DoS-атак, то їх зміна у сотнях записів бази даних може вказувати на те, що зловмисник використовує корпоративну базу даних як інструмент для організації DoS-атаки.

# Цілісність об'єкта

Базу даних можна розглядати як електронну шафу-картотеку. Належна підтримка файлової системи є першочерговим завданням забезпечення достовірності та практичної цінності даних в базі даних. База даних складається з таблиць, записів, полів та даних в кожному з полів. Для забезпечення цілісності файлової системи бази даних, користувачі повинні дотримуватись певних правил. Цілісність об'єкта - це правило цілісності, в якому говориться, що кожна таблиця повинна мати первинний ключ і що стовпець або стовпці, вибрані як первинний ключ, повинні бути унікальними і не містити пустих значень (NULL). Null в базі даних означає, що значення відсутні або невідомі. Цілісність об'єкта дозволяє належним чином організувати дані в записах, як показано на рисунку.

# Розділ 6. Концепція п'яти дев'яток

Організації, які хочуть максимально збільшити доступність своїх систем і даних, можуть вживати надзвичайних заходів для мінімізації або усунення втрат даних. Мета полягає в тому, щоб звести до мінімуму час простою критично важливих процесів. Якщо працівники не можуть виконувати свої регулярні обов'язки, організація може втратити свої прибутки.

Організації вимірюють доступність у відсотках безперебійної роботи. Цей розділ починається з пояснення концепції п'яти дев'яток. Багато галузей повинні підтримувати найвищі стандарти доступності, оскільки час простою може означати різницю між життям і смертю.

У цьому розділі розглядаються різні підходи, які можуть вжити організації для досягнення їхніх цілей доступності. Резервування забезпечує резервне копіювання та містить додаткові компоненти для комп'ютерів або мережних систем, щоб забезпечити їх доступність. Резервні компоненти можуть включати в себе обладнання, таке як диски, сервери, комутатори і маршрутизатори або програмне забезпечення, таке як операційні системи, програми та бази даних. У розділі також обговорюється відмовостійкість, здатність сервера, мережі або центру обробки даних швидко відновлюватися і продовжувати роботу.

Організації повинні бути готові реагувати на інцидент, встановлюючи процедури, які вони виконують, після того, як відбулася подія. Наприкінці розділу обговорюється планування аварійного відновлення і безперервності бізнесу, яке має вирішальне значення для підтримки доступності ресурсів організації.

Що означає п'ять дев'яток?

П'ять дев'яток означають, що системи і служби доступні в 99,999% випадків. Це також означає, що як запланований, так і незапланований час простою становить менше 5,26 хвилин на рік. На рисунку наведено порівняння часу простоїв для різних відсотків доступності.

Висока доступність залежить від системи чи компонентів, які постійно працюють на певному проміжку часу. Для забезпечення високої доступності необхідно:

* Усунення окремих точок збою
* Дизайн для надійності
* Виявлення несправностей, коли вони виникають

Підтримка високої доступності за стандартом п'яти дев'яток може збільшити витрати та використовувати багато ресурсів. Збільшені витрати пов'язані з придбанням додаткового устаткування, такого як сервери та компоненти. Оскільки організація додає компоненти і, як результат, збільшується складність конфігурації. На жаль, підвищена складність конфігурації збільшує фактори ризику. Чим більше рухомих частин задіяно, тим більша ймовірність відмови компонентів.

Середовища, які вимагають п'яти дев'яток

Хоча витрати на підтримку високої доступності можуть бути надто великими для деяких галузей, для окремих організацій п'ять дев'яток є необхідними.

* Фінансовій індустрії необхідно підтримувати високу доступність для постійної торгівлі, відповідаючи довірі клієнтів. Натисніть [тут](http://www.datacenterdynamics.com/it-networks/new-york-stock-exchange-fails-due-to-configuration-problems/94401.article) щоб прочитати про чотири години простою на Нью-Йоркській фондовій біржі в 2015 році.
* Оздоровчі установи вимагають високої доступності, щоб забезпечити цілодобовий догляд пацієнтів. Натисніть [тут](http://www.fiercehealthit.com/story/data-center-downtime-cost-averages-7900-minute/2013-12-05) щоб прочитати про середні витрати, пов'язані з простоєм центру обробки даних в галузі охорони здоров'я.
* Індустрія охорони громадської безпеки включає в себе агентства, які забезпечують безпеку та обслуговування спільноти, держави чи нації. Натисніть [тут](http://www.nextgov.com/defense/2014/05/pentagon-police-agency-hit-catastrophic-network-outage/83842/) щоб прочитати про відключення мережі в поліцейському агентстві США Пентагону.
* Роздрібна торгівля залежить від ефективних ланцюгів постачання та доставки продуктів споживачам. Збитки можуть бути руйнівними, особливо під час періодів високого попиту, таких як святкові дні.
* Люди сподіваються, що галузь новин передаватиме інформацію про події, коли вони стаються. Цикл новин працює цілодобово, 24/7.

Загрози доступності

Наступні загрози представляють високий ризик доступності даних і інформації:

* Несанкціонований користувач успішно проникає і компрометує основну базу даних організації
* Успішна DoS атака значною мірою впливає на операції
* Організація страждає від значної втрати конфіденційних даних
* Критично важливе ПЗ перестає працювати
* Стається компрометація адміністратора або root користувача
* Виявлення міжсайтового скрипта або незаконного загального доступу до файлового сервера
* Пошкодження веб-сайту організації впливає на зв'язок з громадськістю
* Сильний шторм, такий як ураган або торнадо
* Катастрофічні події, такі як терористичні акти, підрив або підпал будівель
* Довгостроковий збій служб або постачальника послуг
* Збиток від води в результаті повені або відмови зрошувальної системи

Класифікація рівня впливу для кожної загрози допомагає організації оцінити вплив загрози у доларах. Натисніть на категорії загроз на рисунку, щоб побачити приклад кожної з них.

# Проектування системи високої доступності

Висока доступність включає три основні принципи досягнення мети безперервного доступу до даних та послуг:

1. Ліквідація або зменшення одиничних точок відмови

2. Системна стійкість

3. Відмовостійкість

Натисніть на кожен принцип на рисунку для короткого опису.

Важливо розуміти шляхи вирішення єдиної точки відмови. Одиничною точкою відмови може бути центральний маршрутизатор або комутатор, мережні служби та навіть висококваліфікований ІТ персонал. Ключовим є те, що втрата системи, процесу або людини може мати дуже руйнівний вплив на всю систему. Також ключовими є процеси, ресурси та компоненти, які зменшують кількість одиничних точок відмови. Кластери з високою доступністю - це один із способів забезпечення надлишковості. Ці кластери складаються з групи комп'ютерів, які мають доступ до спільного сховища та володіють ідентичними конфігураціями мережі. Всі сервери беруть участь у обробці служби одночасно. Зовні серверна група виглядає як один пристрій. Якщо сервер в кластері перестає працювати, інші сервери продовжують обробляти ту ж саму службу, що й пристрій, який вийшов з ладу.

Системна стійкість - це здатність підтримувати доступність даних та оперативну обробку, незважаючи на атаки або порушення діяльності. Як правило, для цього потрібні надлишкові системи з точки зору як потужності, так і обробки, щоб, якщо одна система виходить з ладу, інша могла виконувати операції без будь-якого порушення обслуговування. Системна стійкість - це більше, ніж засоби для зміцнення; вона вимагає, щоб, і дані, і послуги були доступними навіть під час атаки.

Відмовостійкість дозволяє системі продовжувати працювати, якщо один або кілька компонентів дають збій.. Віддзеркалення даних є одним із прикладів відмовостійкості. Якщо виникає «помилка», що викликає порушення у роботі пристрою, такого як контролер диска, система віддзеркалення надає необхідні дані, не перериваючи обслуговування користувача.

Ідентифікація активів

Організація повинна знати, яке апаратне і програмне забезпечення є в наявності, як передумова для визначення необхідних параметрів конфігурації. Керування активами включає в себе повну інвентаризацію апаратного та програмного забезпечення.

Це означає, що організація повинна знати всі компоненти, які можуть піддаватися ризикам безпеки, зокрема:

* Кожна апаратна система
* Кожна операційна система
* Кожний апаратний мережний пристрій
* Кожна операційна система мережного пристрою
* Кожний програмний застосунок
* Вся прошивка
* Усі мовні середовища виконання
* Всі окремі бібліотеки

Організація може вибрати автоматичне рішення для відстеження активів. Адміністратор повинен досліджувати будь-яку змінену конфігурацію, оскільки це може означати, що конфігурація не є актуальною. Це також може означати, що відбуваються несанкціоновані зміни.

# Класифікація активів

Класифікація активів розподіляє всі ресурси організації у групи, засновані на спільних характеристиках. Організація повинна застосовувати систему класифікації активів до документів, записів даних, файлів та дисків. Найважливіша інформація повинна отримувати найвищий рівень захисту і навіть може вимагати спеціальної обробки.

Організація може прийняти систему маркування відповідно до того, наскільки цінною, чутливою і критичною є інформація. Щоб визначити та класифікувати активи організації, виконайте наступні кроки:

1. Визначити правильну категорію ідентифікації активів.

2. Встановити відповідальність за активи, вказавши власника для всіх інформаційних активів і прикладного програмного забезпечення.

3. Визначити критерії класифікації.

4. Впровадити схему класифікації.

# Стандартизація активів

Керування активами керує життєвим циклом і інвентаризацією технологічних активів, включаючи пристрої та програмне забезпечення. В рамках системи керування ІТ-активами організація визначає прийнятні ІТ-активи, які відповідають її цілям. Ця практика ефективно зменшує різні типи активів. Наприклад, організація буде встановлювати застосунки, що відповідатимуть їхнім рекомендаціям. Коли адміністратори вилучають програми, які не відповідають рекомендаціям, вони ефективно підвищують безпеку.

Стандарти активів визначають конкретні апаратні та програмні продукти, які використовує та підтримує організація. Коли відбувається збій, оперативне реагування допомагає підтримувати як доступ, так і безпеку. Якщо організація не стандартизує вибір свого апаратного забезпечення, персоналу може бути потрібен час, щоб знайти компонент для заміни. Нестандартні середовища вимагають більшого досвіду для керування і вони збільшують вартість контрактів на технічне обслуговування та інвентаризацію. Натисніть [тут](http://mil-embedded.com/articles/the-cots-systems-play/) щоб прочитати про те, як військові перейшли на стандартні апаратні засоби для своїх військових комунікацій.

Ідентифікація загроз

Комп'ютерна команда екстреної готовності США (US-CERT) та Міністерство внутрішньої безпеки США підтримують словник загальної уразливості і впливу (CVE). CVE містить стандартний ідентифікаційний номер з коротким описом і посилання на відповідні звіти про уразливості та рекомендації. Корпорація MITRE підтримує список CVE та його загальнодоступний веб-сайт.

Ідентифікація загрози починається з процесу створення ідентифікатора CVE для загальнодоступних вразливостей кібербезпеки. Кожен ідентифікатор CVE включає в себе наступне:

* Номер ідентифікатора CVE
* Короткий опис вразливості системи безпеки
* Будь-які важливі посилання

Натисніть [тут](http://cve.mitre.org/cve/identifiers/) щоб дізнатись більше про ідентифікатор CVE.

Аналіз ризиків

Аналіз ризиків - це процес аналізу небезпек, пов'язаних з природними та антропогенними подіями, для активів організації.

Користувач виконує ідентифікацію активів, щоб визначити, які активи захищати. Аналіз ризиків має чотири мети:

* Визначення активів та їх вартості
* Визначення вразливості та загроз
* Оцінити ймовірність та вплив виявлених загроз
* Збалансувати вплив загрози на вартість контрзаходів

Є два підходи до аналізу ризиків.

**Кількісний аналіз ризиків**

Кількісний аналіз присвоює числа процесу аналізу ризиків (Рисунок 1). Вартість активу - це вартість заміщення активу. Вартість активу також може бути виміряна доходами, отриманими за рахунок використання активу. Коефінієнт впливу (EF) являє собою суб'єктивне значення, виражене у відсотках, яке активи втрачають через конкретну загрозу. Якщо відбувається повна втрата, EF дорівнює 1,0 (100%). У кількісному прикладі, сервер має вартість активу 15 000 доларів США. Коли сервер не працює, відбувається загальна втрата (EF дорівнює 1,0). Вартість активу в розмірі 15 000 доларів, помножена на коефіцієнт впливу 1, призводить до одиночної очікуваної втрати у розмірі 15 000 доларів США.

Річна ставка виникнення (ARO) - ймовірність того, що збиток відбудеться протягом року (також виражається у відсотках). ARO може бути більшим, ніж 100%, якщо збиток може виникати більше одного разу на рік.

Розрахунок щорічної очікуваної втрати (ALE) дає керівництву деякі дані щодо того, що воно повинно витратити для захисту активу.

**Якісний аналіз ризиків**

Якісний аналіз ризиків використовує думки та сценарії. На рисунку 2 наведено приклад таблиці, яка використовується для якісного аналізу ризиків, що вказує на ймовірність загрози та її вплив. Наприклад, загроза відмови сервера може бути вірогідною, але її вплив може бути незначним.

Команда оцінює кожну загрозу для активу і відображає її в таблиці. Команда оцінює результати та використовує їх як керівництво. Вони можуть вирішити вживати заходів лише щодо загроз, які потрапляють в червону зону.

Числа, використані в таблиці, безпосередньо не пов'язані з жодним аспектом аналізу. Наприклад, катастрофічний вплив 4 не є вдвічі більшим, ніж незначний вплив 2. Цей метод є суб'єктивним за своєю природою.

Пом'якшення

Пом'якшення наслідків передбачає зменшення тяжкості чи ймовірності втрати. Багато технічних засобів керування знижують ризик, включаючи системи аутентифікації, дозволи на доступ до файлів і брандмауери. Спеціалісти з організації та безпеки повинні розуміти, що зменшення ризику може мати як позитивний, так і негативний вплив на організацію. Гарне пом'якшення ризиків знаходить баланс між негативним впливом контрзаходів і контролю і вигодою від зниження ризику. Існує чотири загальні способи зменшення ризику:

* Прийняти ризик і періодично повторно оцінювати його
* Знизити ризик шляхом впровадження засобів контролю
* Уникати ризику шляхом повної зміни підходу
* Передати ризик третій стороні

Короткострокова стратегія полягає у прийнятті ризику, що вимагає створення планів на випадок надзвичайних ситуацій для цього ризику. Люди та організації повинні приймати ризик на щоденній основі. Сучасні методології знижують ризик, розвиваючи програмне забезпечення поступово, надаючи регулярні оновлення та виправлення для усунення вразливостей та неправильних конфігурацій.

Аутсорсингові послуги, придбання страхування або контрактів на обслуговування - це все приклади передачі ризиків. Наймання фахівців для виконання критичних завдань для зменшення ризику може бути хорошим рішенням і забезпечувати кращі результати при менш довгострокових інвестиціях. Хороший план зменшення ризику може включати дві або більше стратегії.

# Використання багаторівневих систем захисту

Глибокий захист не забезпечить непроникного кібер-щита, але допоможе організації мінімізувати ризик, утримуючи її на крок попереду кіберзлочинців.

Якщо для забезпечення безпеки інформації та даних є лише один рівень захисту, кіберзлочинець повинен лише обійти цей захист. Щоб переконатися, що дані та інформація залишаються доступними, організація повинна створити різні рівні захисту.

Багатошарований підхід забезпечує найповніший захист. Якщо кібер-злочинці проникають через один шар, вони все ще повинні боротися з декількома іншими шарами, кожен з яких складніший, ніж попередній.

# Обмеження

Обмеження доступу до даних та інформації зменшує можливість загрози. Організація повинна обмежувати доступ, щоб користувачі мали лише рівень доступу, необхідний для виконання своєї роботи. Наприклад, люди в відділі маркетингу не потребують доступу до записів заробітної плати для виконання своїх робочих обов’язків.

Технологічні рішення, такі як використання дозволів файлів, є одним із способів обмеження доступу; організація також повинна виконувати процедурні заходи. Повинна бути передбачена процедура, яка забороняє працівникові виносити конфіденційні документи з приміщення.

# Різноманітність

Якби всі захищені шари були однаковими, для кіберзлочинців було б дуже просто провести успішну атаку. Тому шари повинні бути різними. Якщо кібер-злочинці проникнуть в один шар, то ж техніка не буде працювати на всіх інших шарах. Порушення одного рівня безпеки не ставить під загрозу всю систему. Організація може використовувати різні алгоритми шифрування або системи автентифікації для захисту даних у різних станах.

Для досягнення різноманітності організації можуть використовувати продукти безпеки, вироблені різними компаніями, для багатофакторної аутентифікації. Наприклад, сервер, що містить надзвичайно секретні документи, знаходиться в заблокованій кімнаті, де потрібна swipe-картка від однієї компанії та біометрична автентифікація, надана іншою компанією.

# Маскування

Маскування інформації також може захистити дані та інформацію. Організація не повинна розкривати будь-яку інформацію, яку кіберзлочинці можуть використовувати, щоб з'ясувати, яка версія операційної системи працює на сервері або тип використовуваного ним обладнання. Наприклад, повідомлення про помилки не повинні містити жодних відомостей, які кіберзлочинці могли б використати для визначення наявних вразливостей. Приховування певних типів інформації ускладнює зловмисникам боротьбу з системою.

# Простота

Складність не обов'язково гарантує безпеку. Якщо організація запроваджує складні системи, які важкі для зрозуміння і усування несправностей, це може значно послабити систему. Якщо працівники не розуміють, як належним чином налаштовувати складні рішення, може статися так, що кібер-злочинці зможуть скомпрометувати ці системи. Щоб забезпечити доступність, рішення безпеки має бути простим зсередини, але складним ззовні.

# Одиночні точки відмови

Єдина точка відмови - це критична операція всередині організації. Інші операції можуть залежати від неї, а відмова припиняє цю критичну операцію. Єдиною точкою відмови може бути конкретна частина апаратного забезпечення, процес, конкретний фрагмент даних або навіть найважливіша утиліта. Точками відмови є слабкі ланки ланцюга, які можуть спричинити зрив роботи організації. Як правило, для вирішення проблеми єдиної точки відмови потрібно змінити критичну операцію так, щоб вона не покладалася лише на один елемент. Також при виконанні критичних операцій організація може вбудовувати резервні компоненти, які б могли перебрати на себе процес, якщо одна з цих точок відмовить

# N + 1 Резервування

Резервування за принципом N + 1 забезпечує доступність системи у разі відмови компонента. Компоненти (N) повинні мати щонайменше один резервний компонент (+1). Наприклад, в автомобілі є чотири шини (N) та запасна шина у багажнику на випадок проколу (+1).

У центрі обробки даних N + 1 означає, що конструкція системи може протистояти втраті компонента. N відноситься до багатьох різних компонентів, які складають центр обробки даних, включаючи сервери, блоки живлення, комутатори та маршрутизатори. +1 є додатковим компонентом або резервною системою, яка зможе долучитися до роботи, якщо буде потрібно.

Прикладом резервування N + 1 в центрі обробки даних є генератор енергії, який починає працювати, коли щось трапляється з основним джерелом живлення. Хоча система N + 1 містить резервне обладнання, вона не є повністю резервованою системою.

RAID

Надлишковий масив незалежних дисків (RAID) поєднує в собі декілька фізичних жорстких дисків в єдиний логічний блок, що забезпечує надмірність даних та покращує продуктивність. RAID приймає дані, які зазвичай зберігаються на одному диску і поширює їх на декілька дисків. Якщо деякий диск вийде з ладу, користувач зможе відновити дані з інших дисків, які також містять ці дані.

RAID також може збільшити швидкість відновлення даних. Використання декількох дисків допоможе швидше отримувати запитані дані замість того, щоб покладатися тільки на один диск для виконання роботи.

Рішення RAID може бути апаратним або програмним. Для апаратного рішення потрібен спеціальний апаратний контролер в системі, яка містить диски RAID. Наступні терміни описують, як RAID зберігає дані на різних дисках:

* **Парність** - виявлення помилок даних.
* **Чергування** - запис даних на кількох дисках.
* **Віддзеркалення** - зберігання дубльованих даних на другому диску.

Доступні декілька рівнів RAID, як показано на рисунку.

Натисніть [тут](http://www.acnc.com/raid) для перегляду керівництва по рівням RAID, яке пояснює технологію RAID.

Остовне дерево

Надлишковість покращує доступність інфраструктури, захищаючи мережу від єдиної точки відмови, наприклад, відімкнення мережного кабелю або несправності комутатора. При проектуванні фізичної надлишковості у мережі, можуть виникати зациклювання та дублювання кадрів , які матимуть серйозні негативні наслідки для комутованої мережі.

Протокол остовного дерева (Spanning Tree Protocol) вирішує ці проблеми. Основна функція STP полягає в тому, щоб запобігти циклічності в мережі, коли комутатори з'єднуються через кілька шляхів. STP гарантує, що надмірні фізичні канали не мають петель. Це гарантує наявність лише одного логічного шляху між усіма пунктами призначення в мережі. STP навмисно блокує резервні шляхи, які можуть спричинити цикл.

Блокування надлишкових шляхів має вирішальне значення для запобігання циклів у мережі. Фізичні шляхи все ще існують для забезпечення надмірності, але STP вимикає ці шляхи, щоб запобігти виникненню циклів. Якщо мережний кабель або комутатор виходить з ладу, STP перераховує шляхи і розблоковує необхідні порти для активування резервного шляху.

Натисніть кнопку «Переглянути» на рисунку, щоб переглянути роботу STP, коли трапляється помилка:

* PC1 відправляє широкомовне повідомлення в мережу.
* Магістральна лінія між S2 та S1 вийшла з ладу, що призвело до порушення основного шляху.
* S2 розблоковує попередньо заблокований порт для Магісталі 2 і дозволить передавати широкомовний трафік альтернативним шляхом, не перериваючи з’єднання.
* Якщо зв'язок між S2 і S1 починає працювати знову, STP знову блокує зв'язок між S2 і S3.

# Резервування маршрутизатора

Шлюз за замовчуванням (default gateway) зазвичай є маршрутизатором, який забезпечує доступ до іншої частини мережі або до Інтернету. Якщо як шлюз за замовчуванням використовується лише один маршрутизатор, він становить єдину точку відмови. Організація може встановити додатковий маршрутизатор в режим очікування.

На рисунку 1, маршрутизатор в режимі переадресації та маршрутизатор в режимі очікування використовують протокол резервування для визначення того, який маршрутизатор повинен відігравати активну роль при переадресації трафіку. На кожному маршрутизаторі налаштовується фізична IP-адреса та IP-адреса віртуального маршрутизатора. Кінцеві пристрої використовують віртуальну IP-адресу як шлюз за замовчуванням. Маршрутизатор, що передає трафік, очікує на дані, які прямують за адресою 192.0.2.100. Маршрутизатор переадресації та маршрутизатор очікування використовують свої фізичні IP-адреси для надсилання періодичних повідомлень. Ці повідомлення допомагають переконатися, що обидва маршрутизатори доступні і залишаються на зв'язку. Якщо резервний маршрутизатор у режимі очікування не отримує ці періодичні повідомлення від основного маршрутизатора, він перейде до виконання функції переадресації, як показано на рисунку 2.

Здатність мережі динамічно відновлюватися після відмови пристрою, який виконує функції шлюзу, відома як надлишковість першого кроку

Параметри резервування маршрутизатора

Наведений нижче список визначає параметри доступні для резервування маршрутизатора на основі протоколу, який забезпечує зв'язок між мережними пристроями:

* **Hot Standby Router Protocol(HSRP)**- HSRP гарантує високу доступність мережі, забезпечуючи надлишковість маршрутизації першого кроку. Група маршрутизаторів використовує HSRP для вибору активного пристрою та пристрою очікування. У групі інтерфейсів пристрою активним вважається той пристрій, що направляє пакети, а резервним – той, що починає працювати при виході з ладу активного пристрою. Резервний маршрутизатор HSRP контролює робочий статус групи HSRP та швидко бере на себе відповідальність за переадресацію пакетів, якщо активний маршрутизатор відмовляє.
* **Virtual Router Redundancy Protocol (VRRP)** - маршрутизатор VRRP запускає протокол VRRP разом з одним або кількома іншими маршрутизаторами, підключеними до локальної мережі. У конфігурації VRRP обраний маршрутизатор є головним віртуальним маршрутизатором, а інші маршрутизатори є запасними на випадок відмови головного віртуального маршрутизатора.
* **Gateway Load Balancing Protocol (GLBP)** - GLBP захищає трафік даних від відмов маршрутизатора або схеми, наприклад HSRP і VRRP, а також дозволяє балансувати навантаження (також відоме як розподіл навантаження) між елементами групи резервних маршрутизаторів.

Резервне розташування

Організації може знадобитись резервне розташування в залежності від її потреб. Нижче описано три форми розміщення резервів.

**Синхронна**

* Синхронізує обидва місця в режимі реального часу
* Потребує високої пропускної здатності
* Місцеположення повинні бути близькими один до одного, щоб зменшити затримку

**Асинхронна реплікація**

* Не синхронізовано в реальному часі, але близько до цього
* Потребує меншої пропускної здатності
* Розташування можуть бути на більшій відстані, оскільки затримка не є проблемою

**Реплікація у певний момент часу**

* Періодично оновлює резервні копії даних
* Заощаджується більша частина пропускної здатності, оскільки схема не вимагає постійного з'єднання.

Належний баланс між вартістю та доступністю визначатиме правильний вибір для організації.

# Стійкий дизайн

Стійкість - це методи і конфігурації, які використовуються для забезпечення стійкості системи або мережі до відмови. Наприклад, мережа може мати резервні зв'язки між комутаторами з запущеним STP. Хоча STP надає альтернативний шлях через мережу при виході з ладу з'єднання, перемикання може відбуватися не одразу, якщо конфігурація не оптимальна.

Протоколи маршрутизації також забезпечують стійкість, проте тонке налаштування може покращити перехід і зробити його непомітним для користувачів мережі. Адміністратори повинні досліджувати нестандартні налаштування в тестовій мережі, щоб дізнатися, чи можуть вони поліпшити час відновлення мережі.

Стійкий дизайн - це не просто додавання надлишковості. Дуже важливо розуміти бізнес-потреби організації, а потім включати резервність для створення стійкої мережі.

# Стійкість ПЗ

Стійкість застосунків - це здатність застосунка реагувати на проблеми в одному зі своїх компонентів при роботі без припинення виконання. Час простою пов'язаний з відмовами, викликаними помилками застосунків або збоями інфраструктури. Адміністратор в кінцевому підсумку повинен закрити програми для виправлення, оновлення версій або для розгортання нових функцій. Час простою також може бути результатом пошкодження даних, збоїв обладнання, помилок застосунка і людських помилок.

Багато організацій намагаються збалансувати витрати на досягнення стійкості інфраструктури ПЗ ціною втрати клієнтів або бізнесу через збій програми. Висока доступність застосунка є складною і дорогою. На рисунку наведено три шляхи вирішення проблеми стійкості застосунків. Оскільки коефіцієнт доступності кожного рішення збільшується, складність і вартість також зростають.

# Стійкість IOS

Cisco Internetwork Operating System (Cisco IOS) для маршрутизаторів і комутаторів включає в себе функцію стійкої конфігурації. Це дає змогу швидкого відновлення при зловмисному або ненавмисному форматуванні флеш-пам'яті або при видаленні конфігураційного файлу запуску. Ця функція підтримує безпечну робочу копію файлу образу IOS маршрутизатора і копію поточного файлу конфігурації. Користувач не може видалити ці захищені файли, також відомі як primary bootset.

Команди, показані на рисунку, захищають образ IOS та поточний файл конфігурації.

Підготовка

Реакція на інцидент - це процедура, якій слідує організація після того, як подія виходить за рамки звичайного. Витік даних випускає інформацію до ненадійного середовища. Витік даних може виникнути в результаті випадкової або навмисної дії. Витік даних відбувається, коли неавторизована особа копіює, передає, переглядає, викрадає або отримує доступ до конфіденційної інформації.

Коли відбувається інцидент, організація повинна вміти реагувати на нього. Організація повинна розробити план реагування на інцидент та зібрати команду з реагування на інциденти в галузі комп'ютерної безпеки (Computer Security Incident Response Team) для керування реагуванням. Команда виконує наступні функції:

* Дотримується плану реагування на інцидент
* Турбується, щоб її члени знали про план
* Перевіряє план
* Отримує схвалення плану від керівництва

CSIRT може бути встановленою групою всередині організації або окремою організацією. Команда дотримується набору заздалегідь визначених кроків, щоб переконатись, що їхній підхід є рівномірним і що вони не пропускають жодних кроків. Національний CSIRT наглядає за інцидентами у країні.

Виявлення та аналіз

Виявлення починається, коли хтось помічає інцидент. Організації можуть придбати найсучасніші системи виявлення; однак, якщо адміністратори не переглядають журнали та моніторинг сповіщень, ці системи є марними. Правильне виявлення дає змогу зрозуміти як відбувався інцидент, які дані і системи він включає. Повідомлення про порушення поширюється на вище керівництво і керівників, відповідальних за дані і системи, щоб залучити їх до відновлення і ремонту. Виявлення та аналіз включають в себе наступне:

* Оповіщення та сповіщення
* Моніторинг та подальшу діяльність

Аналіз інциденту допомагає визначити джерело, ступінь, вплив та деталі витоку даних. Організація може вирішити, чи потрібно залучати команду експертів для проведення судової експертизи.

# Стримування і викорінення, а також відновлення

Стримуючі зусилля включають негайні дії, такі як відключення системи від мережі, щоб зупинити витік інформації.

Після виявлення витоку організація повинна стримати та викорінити його. Це може потребувати додаткового простою для систем. Стадія відновлення включає в себе дії, які організація повинна вжити, щоб вирішити проблему та відновити задіяні системи. Після виправлення організація повинна відновити всі системи до їх первісного стану до інциденту.

Спостереження за системою після інциденту

Після відновлення нормального стану усіх операцій, організація повинна розглянути причину інциденту та поставити такі запитання:

* Які дії запобігатимуть повторенню інциденту?
* Які запобіжні заходи потребують зміцнення?
* Як це може покращити моніторинг системи?
* Як це може мінімізувати час простою під час процесу стримування, викорінення та відновлення?
* Як керування може мінімізувати вплив на бізнес?

# Контроль доступу до мережі

Контроль доступу до мережі (Network Admission Control, NAC) дозволяє авторизованим користувачам з сумісними системами отримувати доступ до мережі. Сумісна система відповідає всім вимогам політики організації. Наприклад, ноутбук, який є частиною домашньої бездротової мережі, може не мати можливості дистанційного підключення до корпоративної мережі. NAC оцінює пристрій на відповідність політикам мережі. NAC також проводить карантин систем, які не відповідають вимогам та керує відновленням невідповідних систем.

Структура NAC може використовувати існуючу мережну інфраструктуру і додаткове програмне забезпечення для запровадження політики безпеки для усіх кінцевих точок. Окрім того, пристрій NAC контролює доступ до мережі, оцінює відповідність і застосовує політику безпеки. Загальні перевірки систем NAC включають:

1. Оновлення антивірусу

2. Патчі та оновлення операційних систем

3. Комплексний захист паролем

Системи виявлення вторгнень

Системи виявлення вторгнень (Intrusion Detection Systems) пасивно контролюють трафік у мережі. На рисунку показано, що пристрій з підтримкою IDS копіює потік трафіку та аналізує скопійований трафік, а не фактичні переадресовані пакети. Працюючи в автономному режимі, він порівнює захоплений потік трафіку з відомими шкідливими сигнатурами, аналогічно програмному забезпеченню, яке перевіряє наявність вірусів. Робота в автономному режимі означає кілька речей:

* IDS працює пасивно
* Пристрій IDS фізично розташований в мережі так, щоб трафік мав бути віддзеркалений, щоб досягти його
* Мережний трафік не проходить через IDS, якщо він не віддзеркалюється

Пасивність означає, що IDS контролює та звітує про трафік. Він не робить жодних дій. Це визначення роботи у змішаному режимі.

Перевага роботи з копією трафіку полягає в тому, що IDS не робить негативного впливу на потік пакетів трафіку, що пересилається. Недоліком роботи з копією трафіку є те, що IDS не може зупинити атаки шкідливих одиничних пакетів від досягнення цілі, перш ніж відреагує на атаку. У боротьбі з атаками IDS часто потребує допомоги від інших мережних пристроїв, таких як маршрутизатори та брандмауери.

Кращим рішенням є використання пристрою, який може негайно виявляти та припиняти атаку. Цю функцію виконує система запобігання вторгненням (Intrusion Prevention System, IPS).

# Системи запобігання вторгненням

IPS будується на технології IDS. Однак пристрій IPS працює в режимі Inline. Це означає, що весь вхідний і вихідний трафік повинен проходити через нього для обробки. Як показано на рисунку, IPS не дозволяє пакетам входити до захищеної частини мережі, поки він не проаналізував пакети. Він може виявляти і негайно вирішувати мережну проблему.

IPS контролює мережний трафік. Він аналізує вміст і корисне навантаження пакетів для більш складних вбудованих атак, які можуть включати шкідливі дані. Деякі системи використовують поєднання технологій виявлення, включаючи виявлення вторгнень на основі сигнатур, на основі профілю і на основі протоколу. Цей більш глибокий аналіз дозволяє IPS ідентифікувати, зупиняти та блокувати атаки, які пройдуть через традиційний брандмауер. Коли пакет надходить через інтерфейс на IPS, вихідний або довірений інтерфейс не отримує цей пакет, поки IPS не проаналізує пакет.

Перевага роботи в інтегрованому режимі полягає в тому, що IPS може зупинити атаки одного пакета до досягнення цільової системи. Недоліком є те, що погано сконфігурований IPS може чинити негативний вплив на потік пакетів трафіку, що пересилається.

Найбільша відмінність між IDS та IPS полягає в тому, що IPS одразу реагує і не дозволяє передавати будь-який шкідливий трафік, тоді як IDS дозволяє передати шкідливий трафік до вирішення проблеми.

NetFlow і IPFIX

NetFlow - це технологія Cisco IOS, яка забезпечує статистику пакетів, що проходять через маршрутизатор Cisco або багаторівневий комутатор. NetFlow - це стандарт для збору операційних даних з мереж. Інженерна рада Інтернету (IETF) використовувала Cisco NetFlow Version 9 як основу для IP Flow Information Export (IPFIX).

IPFIX - це стандартний формат для експорту інформації про потоки мережного трафіку на основі даних маршрутизатора. IPFIX працює з маршрутизаторами та програмами керування, що підтримують протокол. Менеджери мереж можуть експортувати інформацію про мережний трафік з маршрутизатора та використовувати цю інформацію для оптимізації продуктивності мережі.

Програми, що підтримують IPFIX, можуть відображати статистику з будь-якого маршрутизатора, який підтримує цей стандарт. Збір, зберігання та аналіз сукупної інформації, що надається пристроями, що підтримуються IPFIX, надає наступні переваги:

* Захищає мережу від внутрішніх та зовнішніх загроз
* Діагностує помилки мережних збоїв швидко та точно
* Аналізує потоки мереж для планування пропускної здатності

Натисніть [тут](http://video.cisco.com/detail/videos/products/video/2534277650001/cybersecurity-enabled-by-flexible-netflow-in-campus-access) щоб подивитися відео про те, як Cisco NetFlow може допомогти у виявленні загроз безпеки.

Розширений аналіз загроз

Розширений аналіз загроз може допомогти організаціям виявляти атаки на одному з етапів кібер-атаки, а іноді і раніше, за наявності відповідної інформації.

Організації можуть виявляти ознаки атаки у своїх журналах і системних звітах для таких попереджень безпеки:

* Блокування облікових записів
* Усі події бази даних
* Створення та вилучення активів
* Модифікація конфігурації систем

Розширений аналіз загроз - це тип події або даних профілю, які можуть сприяти моніторингу безпеки і реагуванню. Оскільки кіберзлочинці стають все більш витонченими, важливо розуміти маневри зловмисних програм. Завдяки покращеній видимості методів нападу, організація може швидше реагувати на інциденти.

Типи катастроф

Вкрай важливо підтримувати функціонування організації, коли відбувається лихо. Катастрофа включає в себе будь-яку природну або антропогенну подію, яка шкодить майну, і погіршує здатність організації продовжувати свою діяльність.

**Стихійні лиха**

Стихійні лиха відрізняються залежно від місця розташування. Деякі з цих подій важко передбачити. Стихійні лиха поділяються на такі категорії:

* Геологічні катастрофи включають землетруси, зсуви, вулкани та цунамі
* Метеорологічні катастрофи включають урагани, торнадо, сніжні бурі, молнії та град
* До лих зі здоров'ям відносяться широко поширені хвороби, карантини і пандемії
* До числа інших лих відносяться пожежі, повені, сонячні бурі і лавини

**Антропогенні катастрофи**

Антропогенні катастрофи пов'язані з людьми або організаціями і поділяються на такі категорії:

* Сфера трудових відносин включає страйки, прогули і уповільнення діяльності
* Соціально-політичні події включають вандалізм, блокади, протести, саботаж, тероризм та війну
* До матеріальних подій включають розливи небезпечних речовин та пожежі
* Комунальні збої включають збої живлення і зв'язку, брак палива і радіоактивні опади

Натисніть [тут](http://www.nytimes.com/interactive/2011/03/13/world/asia/satellite-photos-japan-before-and-after-tsunami.html) щоб переглянути супутникові фотографії Японії до та після землетрусу та цунамі 2011 року.

План відновлення після стихійних лих

Організація втілює план аварійного відновлення (Disaster Recovery Plan, DRP) під час катастрофи і співробітники намагаються забезпечити роботу критично важливих систем. DRP включає в себе заходи організації, що проводяться для оцінки, усунення та відновлення пошкоджених об'єктів або активів.

Щоб створити DRP, відповідайте на наступні питання:

* Хто відповідає за цей процес?
* Що робити людині для виконання цього процесу?
* Де особа виконує цей процес?
* Який процес?
* Чому процес критичний?

DRP повинен визначити, які процеси в організації є найбільш критичними. У процесі відновлення організація відновлює свої критично важливі системи в першу чергу.

Впровадження заходів аварійного відновлення

Засоби аварійного відновлення зменшують наслідки катастрофи, щоб ресурси та бізнес-процеси могли відновити роботу.

Є три типи заходів для відновлення IT-компанії після аварій:

* Запобіжні заходи включають в себе засоби контролю, які запобігають катастрофі. Ці заходи спрямовані на виявлення ризиків.
* Розпізнавальні заходи включають в себе засоби контролю, які виявляють небажані події. Ці заходи відкривають нові потенційні загрози.
* Корегувальні заходи охоплюють засоби, які відновлюють систему після катастрофи чи події.

Натисніть на елементи керування на рисунку, щоб побачити приклади кожного з них.

# Потреба в безперервності бізнесу

Безперервність бізнесу є однією з найважливіших концепцій комп'ютерної безпеки. Незважаючи на те, що компанії роблять все можливе, щоб запобігти катастрофам та втраті даних, неможливо передбачити кожен можливий сценарій. Важливо, щоб компанії мали плани, які забезпечують безперервність бізнесу незалежно від того, що може статися. План безперервності бізнесу - це більш широкий план, аніж DRP, оскільки він передбачає переміщення критичних систем до іншого місця під час ремонту вихідного об'єкта. Персонал продовжує виконувати всі бізнес-процеси альтернативним способом, доки не будуть відновлені звичайні операції.

Доступність гарантує, що ресурси, необхідні для підтримки організації, будуть і надалі доступні персоналу та системам, на які вони покладаються.

Міркування про безперервність бізнесу

Контроль безперервності бізнесу - це не просто резервне копіювання даних та надання резервного обладнання. Організаціям потрібні працівники для належного налаштування та управління системами. Дані можуть бути марними до тих пір, поки вони не нададуть інформацію. Організація повинна розглянути наступне:

* Перебування потрібних людей у потрібних місцях
* Документування конфігурацій
* Створення альтернативних каналів зв'язку для передачі голосу та даних
* Забезпечення живлення
* Визначення всіх залежностей для програм та процесів, щоб їх можна було правильно зрозуміти
* Розуміння того, як виконувати вручну автоматичні завдання

# Найкращі практики безперервності бізнесу

Як показано на рисунку, Національний інститут стандартів і технологій (NIST) розробив такі найкращі практики:

1. Напишіть політику, яка надає керівництво для розробки плану безперервності бізнесу та призначає ролі для виконання завдань.

2. Визначте критичні системи та процеси та встановіть їх пріоритет на основі необхідності.

3. Визначте вразливості, загрози та розрахуйте ризики.

4. Визначте і упровадьте заходи контролю і контрзаходи для зниження ризику.

5. Розробіть методи швидкого відновлення критичних систем.

6. Розробіть процедуру підтримки функціонування організації в хаотичному стані.

7. Перевірте план. 8. Оновлюйте план регулярно.

**Розділ 7. Захист домену кібербезпеки**

Захист вашого домену - це постійний процес захисту мережної інфраструктури організації. Він вимагє, щоб працівники постійно проявляли пильність до загроз і вживали заходи для запобігання будь-яких порушень. У цьому розділі розглядаються технології, процеси та процедури, які застосовують спеціалісти з кібербезпеки для захисту систем, пристроїв та даних, що складають мережну інфраструктуру.

Безпека мережі визначається міцністю її найслабшої ланки. Важливо гарантувати безпеку кінцевих пристроїв, що знаходяться в мережі. Це включає в себе захист пристроїв мережної інфраструктури в локальній мережі (LAN) та кінцевих пристроїв, таких як робочі станції, сервери, IP-телефони та точки доступу.

Зміцнення безпеки пристроїв є найважливішим завданням при забезпеченні безпеки мережі. Воно передбачає впровадження перевірених методів фізичної безпеки мережних пристроїв. Деякі з цих методів передбачають захист адміністративного доступу, збереження паролів та впровадження безпечного зв'язку.

Безпека операційної системи

Операційна система відіграє критично важливу роль в роботі комп'ютерної системи і є об'єктом багатьох атак. Безпека операційної системи надає каскадного впливу на загальну безпеку комп'ютерної системи.

Адміністратор керує роботою операційної системи, змінюючи конфігурацію за замовчуванням, щоб зробити її безпечнішою від зовнішніх загроз. Цей процес включає видалення непотрібних програм і служб. Ще однією критичною вимогою підвищення захисту операційних систем є застосування виправлень уразливості і оновлень. Компанії випускають виправленя уразливості і оновлення з метою усунення уразливості і виправлення помилок в своїх продуктах.

Організація повинна організувати системний підхід до оновлення шляхом:

* Створення процедур для моніторингу інформації, пов'язаної з безпекою
* Оцінка застосовності оновлень
* Планування установки виправлень і оновлень застосунків
* Установка оновлень з використанням документованого плану

Ще однією критичною вимогою щодо безпеки операційних систем є виявлення потенційних вразливостей. Це може бути досягнуто шляхом встановлення базових показників. Встановлення базових показників дозволяє адміністратору проводити порівняння поточних показників роботи системи з базовими.

Аналізатор безпеки Microsoft Baseline Security Analyzer (MBSA) знаходить відсутні оновлення безпеки і неправильні конфігурації безпеки в Microsoft Windows. MBSA перевіряє наявність порожніх, простих або неіснуючих паролей, налаштування брандмауера, статус облікового запису гостя, дані облікового запису адміністратора, аудит подій безпеки, непотрібні служби, спільно використовувані мережні ресурси і параметри реєстру. Після підвищення захисту операційної системи адміністратор створює політики і процедури для підтримки високого рівня безпеки.

Захист від шкідливих програм

До шкідливого ПЗ відносяться віруси, черв'яки, троянські програми, кейлогери, шпигунське ПЗ і рекламне ПЗ. Всі вони порушують конфіденційність, крадуть інформацію, завдають шкоди системі або видаляють і пошкоджують дані.

Важливо захистити комп'ютери і мобільні пристрої, використовуючи надійне програмне забезпечення для захисту від шкідливих програм. Доступні такі типи такого ПЗ:

* **Антивірусний захист** - програма постійно відстежує наявність вірусів. У випадку виявлення вірусу програма попереджає користувача і намагається відправити у карантин або видалити вірус, як показано на рисунку 1.
* **Захист від шкідливого рекламного ПЗ** - постійно шукає програми, що відображають рекламу на комп'ютері.
* **Захист від фішингу** - програма блокує IP-адреси відомих фішингових сайтів і попереджає користувача про підозрілі сайти.
* **Захист від шпигунського ПЗ** - програма шукає клавіатурних шпигунів та інші шпигунські програми.
* **Довірені/ненадійні джерела** - програма попереджає користувача про спроби встановити небезпечні програми або про небезпечні веб-сайти, перш ніж користувач їх відвідає.

Для повного видалення всіх шкідливих програм може знадобитися кілька різних програм і кілька сканувань. Запускайте тільки одну програму захисту від шкідливих програм за раз.

Кілька авторитетних організацій безпеки, такі як McAfee, Symantec і Kaspersky, пропонують комплексний захист від шкідливих програм для комп'ютерів і мобільних пристроїв.

Будьте обережні зі шкідливими шахрайськими антивірусами, які можуть з'являтися при перегляді Інтернету. Більшість таких шахрайських антивірусів показують оголошення або спливаюче вікно, схоже на вікно попередження Windows, як показано на рисунку 2. Зазвичай вони кажуть, що шкідливе ПЗ вражає комп'ютер і пропонують користувачеві очистити його. Клацання в будь-якому місці вікна може фактично розпочати завантаження і установку шкідливого ПЗ.

Несанкціоноване або несумісне програмне забезпечення - це не лише програми, які користувач ненавмисно встановлює на комп'ютер. Це можуть бути програми, які навмисно встановлюють користувачі. Це ПЗ може бути не шкідливим та все ж порушувати політику безпеки. Цей тип ПЗ може нашкодити програмному забезпеченню компанії або її мережним службам. Користувачі повинні негайно видалити несанкціоноване програмне забезпечення.

Захист від шкідливих програм

До шкідливого ПЗ відносяться віруси, черв'яки, троянські програми, кейлогери, шпигунське ПЗ і рекламне ПЗ. Всі вони порушують конфіденційність, крадуть інформацію, завдають шкоди системі або видаляють і пошкоджують дані.

Важливо захистити комп'ютери і мобільні пристрої, використовуючи надійне програмне забезпечення для захисту від шкідливих програм. Доступні такі типи такого ПЗ:

* **Антивірусний захист** - програма постійно відстежує наявність вірусів. У випадку виявлення вірусу програма попереджає користувача і намагається відправити у карантин або видалити вірус, як показано на рисунку 1.
* **Захист від шкідливого рекламного ПЗ** - постійно шукає програми, що відображають рекламу на комп'ютері.
* **Захист від фішингу** - програма блокує IP-адреси відомих фішингових сайтів і попереджає користувача про підозрілі сайти.
* **Захист від шпигунського ПЗ** - програма шукає клавіатурних шпигунів та інші шпигунські програми.
* **Довірені/ненадійні джерела** - програма попереджає користувача про спроби встановити небезпечні програми або про небезпечні веб-сайти, перш ніж користувач їх відвідає.

Для повного видалення всіх шкідливих програм може знадобитися кілька різних програм і кілька сканувань. Запускайте тільки одну програму захисту від шкідливих програм за раз.

Кілька авторитетних організацій безпеки, такі як McAfee, Symantec і Kaspersky, пропонують комплексний захист від шкідливих програм для комп'ютерів і мобільних пристроїв.

Будьте обережні зі шкідливими шахрайськими антивірусами, які можуть з'являтися при перегляді Інтернету. Більшість таких шахрайських антивірусів показують оголошення або спливаюче вікно, схоже на вікно попередження Windows, як показано на рисунку 2. Зазвичай вони кажуть, що шкідливе ПЗ вражає комп'ютер і пропонують користувачеві очистити його. Клацання в будь-якому місці вікна може фактично розпочати завантаження і установку шкідливого ПЗ.

Несанкціоноване або несумісне програмне забезпечення - це не лише програми, які користувач ненавмисно встановлює на комп'ютер. Це можуть бути програми, які навмисно встановлюють користувачі. Це ПЗ може бути не шкідливим та все ж порушувати політику безпеки. Цей тип ПЗ може нашкодити програмному забезпеченню компанії або її мережним службам. Користувачі повинні негайно видалити несанкціоноване програмне забезпечення.

# Брандмауери на основі хоста і системи виявлення вторгнень

Рішення на основі хоста - це програмний застосунок, який виконується на локальному комп'ютері для його захисту. Працюючи разом з операційною системою, це ПЗ допомагає запобігти атакам.

**Брандмауери на основі хоста**

Програмний брандмауер - це програма, яка працює на комп'ютері, щоб дозволити або заборонити трафік між комп'ютером і іншими підключеними пристроями. Програмний брандмауер застосовує набір правил для передачі даних за допомогою перевірки і фільтрації пакетів даних. Брандмауер Windows є прикладом програмного брандмауера. Він встановлюється за замовчанням разом з операційною системою Windows.

Користувач може управляти типом даних, що відправляються на комп'ютер і з нього, відкриваючи або блокуючи окремі порти. Брандмауери блокують вхідні та вихідні мережні підключення, якщо не визначені виключення для відкриття і закриття портів, необхідних для роботи цієї программі.

На рисунку 1 користувач вибирає вхідні правила для налаштування типів трафіку, дозволених для проходження в систему. Налаштування вхідних правил допоможе захистити систему від небажаного трафіку.

**Системи виявлення вторгнень на основі хоста**

Система виявлення вторгнень на основі хоста (Host Intrusion Detection System, HIDS) - це програмне забезпечення, яке виконується на головному комп'ютері, який контролює підозрілу активність. На кожну серверну або настільну систему, яка потребує захисту, необхідно встановити це програмне забезпечення, як показано на рисунку 2. HIDS контролює системні виклики і доступ до файлової системи, щоб гарантувати, що ці запити не є результатом зловмисної діяльності. Вона також може контролювати параметри реєстру системи. У реєстрі містяться відомості про конфігурацію комп'ютера.

HIDS зберігає всі дані журналу локально. Це ресурсоємний процес і може вплинути на продуктивність системи. Система виявлення вторгнень на основі хоста не може контролювати мережний трафік, який не досягає системи хоста, але він контролює операційну систему і критичні системні процеси, специфічні для цього хоста.

# Безпечний зв'язок

При підключенні до локальної мережі та обміну файлами зв'язок між комп'ютерами залишається в межах цієї мережі. Дані захищені, оскільки комп'ютери відключені від інших мереж і знаходяться поза Інтернетом. Для зв'язку і спільного використання ресурсів по незахищеній мережі користувачі використовують віртуальну приватну мережу (Virtual Private Network, VPN).

VPN - це приватна мережа, яка з'єднує разом віддалені сайти або користувачів через загальнодоступну мережу, наприклад Інтернет. Найбільш поширений вид VPN - доступ до корпоративної приватної мережі. VPN використовує виділені захищені з'єднання, маршрутизовані через Інтернет, від корпоративної приватної мережі до віддаленого користувача. При підключенні до корпоративної приватної мережі користувачі стають її частиною і мають доступ до всіх служб і ресурсів, ніби вони фізично підключилися до корпоративної LAN.

Для отримання віддаленого доступу користувачі повинні встановити на своїх комп'ютерах клієнт VPN, щоб сформувати безпечне з'єднання з корпоративною приватною мережею. Клієнтське програмне забезпечення VPN шифрує дані перед відправкою через Інтернет на VPN-шлюз в корпоративній приватній мережі. VPN-шлюзи встановлюють, керують і управляють VPN-з'єднаннями, також відомими як VPN-тунелі.

Операційні системи зазвичай включають VPN-клієнт, який налаштовується користувачем для VPN-з'єднання.

# WEP

Одним з найважливіших компонентів сучасних обчислень є мобільні пристрої. Більшість пристроїв в сьогоднішніх мережах - це ноутбуки, планшети, смартфони та інші бездротові пристрої. Мобільні пристрої передають дані за допомогою радіосигналів, які може отримати будь-який пристрій із сумісною антеною. З цієї причини комп'ютерна індустрія розробила ряд стандартів, продуктів і пристроїв для забезпечення безпеки бездротового або мобільного зв'язку. Ці стандарти шифрують інформацію, передану мобільними пристроями через радіохвилі.

Wired Equivalent Privacy (WEP) є одним з перших і широко використовуваних стандартів безпеки Wi-Fi. Стандарт WEP забезпечує захист через аутентифікацію і шифрування. Стандарти WEP застаріли, але багато пристроїв як і раніше підтримують WEP для забезпечення сумісності. WEP став стандартом безпеки Wi-Fi в 1999 році, коли бездротовий зв'язок лише започатковувався. Незважаючи на зміни в стандарті і збільшений розмір ключа, WEP страждав від численних недоліків в області безпеки. Кіберзлочинці можуть зламати паролі WEP в лічені хвилини, використовуючи вільно доступне програмне забезпечення. Незважаючи на поліпшення, WEP залишається дуже вразливим і користувачі повинні оновлювати системи, які грунтуються на WEP.

# WPA/WPA2

Наступним важливим поліпшенням безпеки бездротового зв'язку стало впровадження WPA і WPA2. Технологія WPA (Wi-Fi Protected Access, WPA) була відповіддю комп'ютерної індустрії на слабкість стандарту WEP. Найбільш поширеною конфігурацією WPA є WPA-PSK (Pre-Shared Key). В WPA використовуються 256-бітні ключі, що значно перевищує кількість 64-бітних і 128-бітних ключів в WEP-системі.

Стандарт WPA забезпечив кілька поліпшень безпеки. По-перше, WPA додав перевірку цілісності повідомлень (message integrity checks, MIC), яка могла б виявити, що зловмисник перехопив і змінив дані, передані між точкою бездротового доступу і бездротовим клієнтом. Іншим ключовим аспектом підвищення безпеки був протокол цілісності тимчасового ключа (Temporal Key Integrity Protocol, TKIP). Стандарт TKIP надав можливість краще обробляти, захищати і змінювати ключі шифрування. Симетричний алгоритм блочного шифрування (Advanced Encryption Standard, AES) замінив TKIP для ще кращого керування ключами і надійнішого шифрування.

WPA, як і його попередник WEP, мав багато відомих вразливостей. В результаті в 2006 році був випущений стандарт Wi-Fi Protected Access II (WPA2). Одним з найбільш значних поліпшень безпеки WPA2 в порівнянні з WPA було обов'язкове використання алгоритмів AES і введення блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol, CCM) в якості заміни TKIP.

# Взаємна аутентифікація

Однією з суттєвих вразливостей бездротових мереж є використання неавторизованих точок доступу. Точками доступу є пристрої, які взаємодіють з бездротовими пристроями і підключають їх до дротової мережі. Будь-який пристрій, який має бездротовий передавач і дротовий інтерфейс для підключення до мережі, може потенційно діяти як неавторизована точка доступу. Така точка доступу може імітувати авторизовану точку доступу. В результаті бездротові пристрої в бездротовій мережі встановлюють зв'язок з неавторизованою точкою доступу замість авторизованої.

Така «підробка» може отримувати запити на з'єднання, копіювати дані в запиті і пересилати їх в авторизовану мережну точку доступу. Цей тип атаки «людина-в-середині» (man-in-the-middle) дуже важко виявити і вона може призвести до крадіжки облікових даних для входу і даних, які передаються. Щоб запобігти цьому, комп'ютерна індустрія розробила взаємну аутентифікацію. Взаємна аутентифікація, також звана двостороння аутентифікація, являє собою процес або технологію, в яких обидва об'єкти в каналі зв'язку аутентифіковані один з одним. У середовищі бездротової мережі клієнт аутентифікує точку доступу і точка доступу аутентифікує клієнта. Це удосконалення дозволило клієнтам виявляти неавторизовані точки доступу до підключення до них.

Контроль доступу до файлів

Дозволи - це правила, налаштовані для обмеження доступу до папки або файлу для окремої особи або для групи користувачів. На рисунку показані дозволи, які можна задати для файлів і папок.

**Принцип найменших привілеїв**

Користувачі повинні бути обмежені тільки ресурсами, які їм потрібні в комп'ютерній системі або мережі. Наприклад, вони не повинні мати доступ до всіх файлів на сервері, якщо їм потрібен тільки доступ до однієї папки. Може бути простіше надати користувачам доступ до всього диску, але більш безпечно обмежувати доступ тільки папкою, в якій вони повинні виконувати свою роботу. Це принцип найменших привілеїв. Обмеження доступу до ресурсів також запобігає доступу шкідливих програм до цих ресурсів, якщо комп'ютер користувача заражений.

**Обмеження прав користувачів**

Якщо адміністратор забороняє доступ до мережного ресурсу для окремої особи або групи, ця заборона скасовує будь-які інші налаштування дозволу. Наприклад, якщо адміністратор забороняє комусь доступ до загального мережного ресурсу, користувач не зможе отримати доступ до цього ресурсу, навіть якщо він є адміністратором або частиною групи адміністраторів. Локальна політика безпеки повинна вказувати, які ресурси і тип доступу дозволені для кожного користувача і групи.

Коли користувач змінює права доступу до папки, він має можливість застосовувати ті ж самі права доступу до всіх підпапок. Це називається успадкуванням дозволів. спадкування дозволів - це простий спосіб швидко застосувати дозволи для багатьох файлів і папок. Після того, як встановлені права батьківської папки, папки і файли, створені всередині неї, успадковують її дозволи.

Крім того, розташування даних і дії, які виконують над ними, визначають поширення дозволу:

* Дані, переміщені в межах одного і того ж тому, будуть зберігати вихідні дозволи
* Дані, скопійовані в межах одного і того ж тому, успадковують нові дозволи
* Дані, переміщені на інший том, успадковують нові дозволи
* Дані, скопійовані на інший том, успадковують нові дозволи

# Шифрування файлів

Шифрування - це інструмент, який використовується для захисту даних. Шифрування перетворює дані з використанням складного алгоритму, щоб зробити їх нечитабельними. Спеціальний ключ повертає нечитабельну інформацію назад в читабельні дані. Програми можуть шифрувати файли, папки і навіть цілі диски.

Шифрування файлової системи (Encrypting File System, EFS) - це функція Windows для шифрування даних. Реалізація Windows EFS безпосередньо пов'язана з конкретним обліковим записом користувача. Тільки користувач, який зашифрував дані, зможе отримати доступ до зашифрованих файлів або папок.

Користувач також може вибрати шифрування всього жорсткого диска в Windows за допомогою функції BitLocker. Щоб використовувати BitLocker, на жорсткому диску мають бути присутні як мінімум два томи.

Перед використанням BitLocker користувачеві необхідно включити Trusted Platform Module (TPM) в BIOS. TPM - це спеціалізований чіп, встановлений на материнській платі. TPM зберігає інформацію, специфічну для хост-системи, таку як ключі шифрування, цифрові сертифікати і паролі. Застосунки, такі як BitLocker, які використовують шифрування, можуть використовувати чіп TPM. Натисніть «Адміністрування TPM», щоб переглянути відомості про TPM, як показано на рисунку.

BitLocker To Go шифрує знімні носії. BitLocker To Go не використовує чіп TPM, але як і раніше забезпечує шифрування даних і вимагає пароля.

Резервне копіювання системи і даних

Організація може втратити дані, якщо кіберзлочинці вкрадуть їх, обладнання зазнає сбою або станеться надзвичайна ситуація. З цієї причини важливо регулярно створювати резервні копії даних.

Резервне копіювання даних зберігає копію інформації з комп'ютера на знімний носій резервного копіювання. Оператор зберігає резервний носій в надійному місці. Резервне копіювання даних є одним з найбільш ефективних способів захисту від втрати даних. Якщо комп'ютерне обладнання виходить з ладу, користувач може відновити дані з резервної копії, як тільки система буде працювати.

Політика безпеки організації повинна включати резервне копіювання даних. Користувачі повинні регулярно створювати резервні копії даних. Резервні копії даних зазвичай зберігаються далеко від основного носія для захисту резервного носія, якщо щось відбудетьсяся з основним об'єктом.

Ось деякі міркування щодо резервного копіювання даних:

* Частота - резервне копіювання може зайняти багато часу. Іноді легше зробити повну резервну копію щомісяця або щотижня, а потім робити часті часткові резервні копії будь-яких даних, які були змінені з моменту останньої повної резервної копії. Однак при наявності великої кількості часткових резервних копій збільшується час, необхідний для відновлення даних.
* Зберігання - для забезпечення додаткової безпеки переносьте резервні копії в автономне сховище щоденно, щотижнево або щомісячно, як того вимагає політика безпеки.
* Безпека - захистіть резервні копії паролями. Перед відновленням даних з резервного носія оператор повинен бути ввести пароль.
* Перевірка - завжди перевіряйте резервні копії, щоб забезпечити цілісність даних.

Фільтрація і блокування контенту

Програми контролю вмісту обмежують доступ користувача до певного вмісту веб-браузера через Інтернет. Програми контролю вмісту можуть блокувати сайти, які містять певні типи матеріалів, такі як порнографія, або суперечливі матеріали релігійного або політичного змісту. Батьки можуть встановити таку програму на комп'ютері, який використовується дитиною. Бібліотеки та школи також впроваджують це програмне забезпечення для запобігання доступу до неприпустимого вмісту.

Адміністратор може використовувати такі типи фільтрів:

* Фільтри на основі браузера через стороннє розширення браузера
* Фільтри електронної пошти через клієнтський або серверний фільтр
* Фільтри на стороні клієнта, встановлені на комп'ютері
* Фільтри контенту на основі маршрутизатора, які блокують трафік на вході в мережу
* Фільтрація контенту на основі пристрою, подібна до фільтра на основі маршрутизатора
* Фільтрація контенту на основі хмарних технологій

Пошукові системи, такі як Google, пропонують можливість включення фільтра безпеки, щоб виключити небажані посилання з результатів пошуку.

Натисніть [тут](https://en.wikipedia.org/wiki/Comparison_of_content-control_software_and_providers) , щоб порівняти постачальників програм контролю вмісту

Клонування диску і утиліта Deep Freeze

Багато сторонніх застосунків доступно для відновлення системи до стану за замовчуванням. Це дозволяє адміністратору захищати операційну систему і конфігураційні файли системи.

Клонування диска копіює вміст жорсткого диска комп'ютера в файл образу. Наприклад, адміністратор створює необхідні розділи в системі, форматує розділ і потім встановлює операційну систему. Вона встановлює все необхідне прикладне програмне забезпечення і налаштовує все обладнання. Потім адміністратор використовує програмне забезпечення для клонування диска для створення файлу образу. Адміністратор може використовувати клоноване зображення наступним чином:

* Щоб автоматично стерти систему і відновити чистий основний образ
* Для розгортання нових комп'ютерів в організації
* Щоб забезпечити повну резервну копію системи

Натисніть [тут](https://en.wikipedia.org/wiki/Comparison_of_disk_cloning_software) , щоб порівняти програмне забезпечення для клонування диска.

Deep Freeze «заморожує» розділ жорсткого диска. Коли користувач перезавантажує систему, система повертається до «замороженої» конфігурації. Система не зберігає ніяких змін, внесених користувачем, тому будь-які зміни, встановлені затосунки або збережені файли, втрачаються під час перезапуску системи.

Якщо адміністратору необхідно змінити конфігурацію системи, він повинен спочатку «розморозити» захищений розділ, відключивши Deep Freeze. Після внесення змін він повинен знову включити програму. Адміністратор може налаштувати перезапуск Deep Freeze після виходу користувача з системи, вимкнення після періоду бездіяльності або в запланований час.

Ці продукти не забезпечують захист в режимі реального часу. Система залишається вразливою до тих пір, поки користувач або запланована подія не перезапустять систему. Однак система, заражена шкідливим кодом, повністю очищається після перезавантаження.

Захисні кабелі та замки

Існує кілька способів фізичного захисту комп'ютерної техніки:

* Використовуйте кабельні замки для обладнання, як показано на рисунку 1.
* Тримайте кімнати с телекомунікаціями зачиненими.
* Використовуйте захисні клітки навколо обладнання.

Багато портативних пристроїв і дорогі комп'ютерні монітори мають спеціальний захисний слот зі сталевим кронштейном, вбудованим для використання в поєднанні з кабельними замками.

Найбільш поширеним типом дверного замка є стандартний замок з ключем. Він не блокується автоматично, коли двері зачиняються. Крім того, людина може вставити тонку пластикову карту, наприклад, кредитну карту між замком і дверцятами, щоб відкрити двері. Дверні замки в комерційних будівлях відрізняються від звичайних замків. Ригель замка забезпечує додатковий захист. Однак будь-який захист, що вимагає ключа, являє собою вразливість, якщо ключ втрачено, вкрадено або дубльовано.

Замок із шифруванням, показаний на рисунку 2, використовує кнопки, які користувач натискає в заданій послідовності, щоб відкрити двері. Замок із шифруванням можна запрограмувати. Це означає, що код користувача може працювати тільки в певні дні або певні моменти часу. Наприклад, замок із шифруванням може дозволяти тільки доступ Боба до серверної кімнаті між 7 годиною ранку та 6 годинами вечора з понеділка до п'ятниці. Замок із шифруванням також може зберігати запис при відкритті дверей і використаний код.

# Таймери виходу

Співробітник встає на перерву і залишає свій комп'ютер. Якщо співробітник не робить ніяких дій для забезпечення безпеки своєї робочої станції, будь-яка інформація про цю систему стає доступною для неавторизованого користувача. Організація може вжити таких заходів для запобігання несанкціонованому доступу:

**Тайм-аут очікування і блокування екрану**

Співробітники можуть вийти або ні зі свого комп'ютера, коли вони покидають робоче місце. Тому найкраще налаштувати таймер простою, після спрацювання якого користувач автоматично виходить із системи, а екран блокується. Користувач повинен увійти в систему, щоб розблокувати екран.

**Час входу**

У деяких випадках організація може зажадати, щоб співробітники аутентифікувалися в системі в певні години, наприклад, з 7:00 до 18:00. Система блокує логіни входу за межами вказаного інтервалу часу.

# Відстеження GPS

Глобальна система позиціонування (Global Positioning System, GPS) використовує супутники і комп'ютери для визначення місцезнаходження. Технологія GPS - це стандартна функція на смартфонах і забезпечує відстеження місця розташування в реальному часі. GPS-відстеження може визначити місце розташування в межах 100 метрів. Ця технологія дозволяє відстежувати дітей, літніх людей, домашніх тварин і транспортних засобів. Однак використання GPS для пошуку стільникового телефону без дозволу користувача є вторгненням в особисте життя і це незаконно.

Багато застосунків для стільникових телефонів використовують GPS для відстеження місця розташування телефону. Наприклад, Facebook дозволяє користувачам робити геомітку, яка потім відображається людям в їх мережах.

# Інвентаризація та RFID-мітки

Радіочастотна ідентифікація (Radio frequency identification, RFID) використовує радіохвилі для ідентифікації та відстеження об'єктів. Системи інвентаризації використовує RFID-мітки, прикріплені до всіх предметів, які організація хоче відстежувати. Мітки містять інтегральну схему, яка з'єднується з антеною. RFID-мітки невеликі і споживають дуже мало енергії, тому їм не потрібна батарея для зберігання інформації та обміну нею з пристроєм зчитування. RFID може допомогти автоматизувати відстеження активів або бездротове блокування, розблокування або налаштування електронних пристроїв.

Системи RFID працюють на різних частотах. Низькочастотні системи мають більш короткий діапазон зчитування і більш низькі швидкості читання даних, але не настільки чутливі до радіохвильових перешкод, викликаних присутніми рідинами і металами. Більш високі частоти мають більшу швидкість передачі даних і на більшій відстані, але більш чутливі до радіохвильових перешкод.

# Керування віддаленим доступом

Поняття віддалений доступ відноситься до будь-якої комбінації апаратного та програмного забезпечення, яка дозволяє користувачам віддалено звертатися до локальної внутрішньої мережі.

В операційній системі Windows технічні фахівці можуть використовувати віддалений робочий стіл (Remote Desktop) і віддалений помічник (Remote Assistance) для ремонту та оновлення комп'ютерів. Віддалений робочий стіл, як показано на рисунку, дозволяє технічним фахівцям переглядати і управляти комп'ютером з віддаленого місця. Віддалений помічник дозволяє технічним фахівцям допомагати клієнтам в проблемах з віддаленого місця. З його допомогою клієнт також може в реальному часі переглядати на екрані дії по ремонту або оновленню.

За замовчуванням процес установки Windows не включає віддалений робочий стіл. Включення цієї функції відкриває порт 3389 і може привести до уразливості, якщо користувач не потребує роботи цієї служби

# Telnet, SSH та SCP

Secure Shell (SSH) - це протокол, що забезпечує безпечне (зашифроване) з'єднання керування з віддаленим пристроєм. Для безпечного керування віддаленими з'єднанями SSH повинен замінити Telnet. Telnet - це застарілий протокол, який використовує незахищену незашифровану передачу як даних, так і параметрів аутентифікації (ім'я користувача і пароль), що передаються між комунікаційними пристроями. SSH забезпечує безпеку віддалених підключень через надійне надійне шифрування даних аутентифікації пристрою (ім'я користувача і пароль) і передачу даних між комунікаційними пристроями. SSH використовує TCP-порт 22. Telnet використовує TCP-порт 23.

На рисунку 1 кіберзлочинці відстежують пакети з використанням Wireshark. На рисунку 2 кіберзлочинці перехоплюють ім'я користувача і пароль адміністратора з сеансу Telnet.

На рисунку 3 показаний вид Wireshark для сеансу SSH. Кіберзлочинці відстежують сеанс, використовуючи IP-адресу пристрою адміністратора, але на рисунку 4 в сеансі ім'я користувача і пароль зашифровані.

Протокол безпечного копіювання файлів (Secure copy, SCP) надійно передає комп'ютерні файли між двома віддаленими системами. SCP використовує SSH для передачі даних (включаючи елемент аутентифікації), забезпечуючи таким чином аутентичність і конфіденційність при передачі даних.

# Захист портів і служб

Кіберзлочинці використовують служби, запущені в системі, тому що вони знають, що більшість пристроїв запускають більше сервісів або програм, ніж їм потрібно. Адміністратор повинен проаналізувати кожну службу, щоб перевірити її необхідність і оцінити ризик. Видаляйте всі непотрібні служби.

Простим методом, яким багато адміністраторів користуются для захисту мережі від несанкціонованого доступу, є відключення всіх невикористовуваних портів на комутаторі. Наприклад, якщо комутатор має 24 порти і є три підключення Fast Ethernet, рекомендується відключити інші непотрібні порти.

Процес включення і відключення портів може зайняти багато часу, але він підвищує безпеку в мережі і коштує витрачених зусиль.

Привілейовані облікові записи

Кіберзлочинці намагаються отримати доступ до привілейованих облікових записів, оскільки вони мають найбільш повні права в організації. Привілейовані облікові записи мають облікові дані для доступу до систем і забезпечують підвищений або необмежений рівень доступу. Адміністратори використовують ці облікові записи для розгортання та керування операційними системами, програмами та мережежними пристроями. На рисунку представлені типи привілейованих облікових записів.

Організація повинна прийняти наступну передову практику для їх захисту:

* Визначити та зменшити кількість привілейованих облікових записів
* Використовувати принцип найменших привілеїв
* Створити процес відкликання прав, коли співробітники виїжджають або змінюють роботу
* Виключити загальні облікові записи з паролями, термін дії яких не закінчується
* Необхідно забезпечити надійне зберігання паролів
* Не використовувати спільні облікові дані для декількох адміністраторів
* Автоматична зміна паролів привілейованих облікових записів кожні 30 або 60 днів
* Слід вести запис привілейованих сеансів
* Запровадити процес зміни вбудованих паролів для скриптів і облікових записів служб
* Реєструвати всю активність користувача
* Генерувати попередження для незвичайної поведінки
* Відключити неактивні привілейовані облікові записи
* Використовувати багатофакторну аутентифікацію для всіх адміністративних доступів
* Впровадження шлюзу між кінцевим користувачем і конфіденційними ресурсами, щоб обмежити мережу від впливу шкідливого ПЗ

Блокування привілейованих облікових записів має вирішальне значення для безпеки організації. Забезпечення безпеки цих облікових записів має бути безперервним процесом. Організація повинна проводити цей процес, згідно специфіки роботи компанії, щоб внести будь-які необхідні корективи для підвищення безпеки.

# Групова політика

У більшості мереж, що використовують комп'ютери на Windows, адміністратор налаштовує Active Directory з доменами на Windows Server. Комп'ютери Windows є членами домену. Адміністратор налаштовує політику безпеки домена, яка застосовується до всіх комп'ютерів в мережі. Правила облікового запису автоматично встановлюються, коли користувач входить в Windows.

Коли комп'ютер не є частиною домену Active Directory, користувач налаштовує політики відповідно до політики локальної безпеки Windows. У всіх версіях Windows, крім Home edition, введіть команду **secpol.msc**в меню «Виконати», щоб відкрити інструмент «Локальна політика безпеки».

Адміністратор налаштовує політики облікового запису користувача, такі як політики паролів і політики блокування, в меню “Політика облікового запису > Політика паролів”. З налаштуваннями, показаними на рисунку 1, користувачі повинні змінювати свої паролі кожні 90 днів і використовувати новий пароль протягом як мінімум одного (1) дня. Паролі повинні містити вісім (8) символів і три з наступних чотирьох категорій: великі літери, малі літери, цифри і символи. Нарешті, користувач може повторно використовувати пароль після 24 унікальних паролів.

Політика блокування облікового запису блокує комп'ютер на заданий час, коли відбувається занадто багато неправильних спроб входу в систему. Наприклад, політика, показана на рисунку 2, дозволяє користувачеві вводити неправильне ім'я користувача та/або пароль п'ять разів. Після п'яти спроб обліковий запис користувача блокується на 30 хвилин. Через 30 хвилин кількість спроб скидається до нуля і користувач може спробувати знову увійти в систему.

Додаткові параметри безпеки можна отримати, розгорнувши папку **Local Policies** Політика аудиту створює файл журналу безпеки, який використовується для відстеження подій, перерахованих на рисунку 3.

Журнали і попередження

Журнал реєструє всі події в хронологічному порядку. Записи журналу складають файл журналу, а запис в журналі містить всю інформацію, пов'язану з конкретною подією. Найважливіше значення мають журнали, які стосуються комп'ютерної безпеки.

Наприклад, журнал аудиту відстежує спроби аутентифікації користувача, а журнал доступу надає всі деталі запитів на певні файли в системі. Журнали систем моніторингу можуть визначати, як сталася атака, і чи був успішно розгорнутий захист.

Зі збільшенням кількості файлів журналів, створених для цілей комп'ютерної безпеки, організації слід розглянути процес керування журналами. Керування журналом визначає процес створення, передачі, зберігання, аналізу та видалення даних журналів комп'ютерної безпеки.

**Журнали операційної системи**

Журнали операційної системи записують події, виконувані операційною системою. Системні події включають наступне:

* Запити клієнтів і відповіді сервера, такі як успішна аутентифікація користувачів
* Інформація про використання, яка містить кількість і розмір транзакцій за певний період часу

**Журнали застосунка безпеки**

Організації використовують мережне або системне програмне забезпечення для виявлення шкідливих дій. Це програмне забезпечення створює журнал безпеки, що містить дані про стан комп'ютерної безпеки. Журнали корисні для проведення аналізу аудиту та виявлення тенденцій і довгострокових проблем. Журнали також дозволяють організації надавати документацію, що вона дотримується законів і нормативниїх вимог.

Живлення

Критично важливий елемент захисту інформаційних систем - електроживлення і споживана потужність. Постійне електроживлення має вирішальне значення в сучасних масивах серверів і сховищах даних. Ось деякі загальні правила побудови ефективних систем електропостачання:

* Центри обробки даних повинні знаходитися на іншому джерелі живлення від іншої частини будівлі
* Резервні джерела живлення: два або більше каналів, що надходять від двох або більше електричних підстанцій
* Стабілізація електроживлення
* Часто необхідно використовувати системи резервного живлення
* Для коректного вимикання систем повинні бути доступні джерела безперебійного живлення (ДБЖ)

Організація повинна захищати себе від декількох проблем при проектуванні своїх систем електроживлення.

**Перевищення потужності**

* Різкий стрибок: миттєва висока напруга
* Стрибок: тривала висока напруга

**Втрата потужності**

* Переривання: короткочасна втрата потужності
* Блокування: повна втрата потужності

**Зниження потужності**

* Падіння: миттєва низька напруга
* Провал напруги: більш тривале зниження напруги
* Пусковий струм: початковий стрибок потужності

# Опалення, вентиляція і кондиціювання повітря (ОВК)

Системи ОВК (Heating, Ventilation, and Air Conditioning, HVAC) вкрай важливі для безпеки людей та інформаційних систем на об'єктах організації. При проектуванні сучасних ІТ-систем ці системи відіграють дуже важливу роль в забезпеченні загальної безпеки. Системи ОВК керують навколишнім середовищем (температура, вологість, повітряний потік і повітряна фільтрація) і повинні плануватися і використовуватися разом з іншими компонентами центру обробки даних, такими як комп'ютерне обладнання, кабельні системи, сховище даних, протипожежний захист, системи фізичної безпеки і потужність. Практично всі апаратні засоби фізичного комп'ютера мають вимоги до середовища, які включають прийнятні діапазони температури і вологості. Вимоги до навколишнього середовища містяться в документі технічних характеристик продукту або в керівництві по фізичному плануванню. Вкрай важливо підтримувати ці вимоги для запобігання збоїв системи і продовження терміну служби ІТ-систем. Комерційні системи ОВК та інші системи керування будівлею тепер підключаються до Інтернету для віддаленого моніторингу та керуванння. Недавні події показали, що такі системи (часто звані «розумні системи») також викликають серйозні наслідки для безпеки.

Одним з ризиків, пов'язаних з інтелектуальними системами, є те, що особи, які отримують доступ і керують системою, працюють на підрядника або стороннього постачальника. Оскільки технічним фахівцям з ОВК повинно швидко знаходити інформацію, важливі дані, як правило, зберігаються в кількох місцях, що робить її доступними для ще більшої кількості людей. Така ситуація дозволяє широкій мережі приватних осіб, включаючи навіть партнерів підрядників, отримати доступ до облікового запису для системи ОВК. Втручання до цих систем може становити значний ризик для інформаційної безпеки організації.

# Моніторинг обладнання

Моніторинг обладнання часто зустрічається в крупних фермах серверів. Ферма серверів - це об'єкт, в якому розміщуються сотні або тисячі серверів для компаній. У Google є багато ферм серверів по всьому світу для надання оптимальних послуг. Навіть більш дрібні компанії будують локальні серверні ферми для розміщення зростаючого числа серверів, необхідних для ведення бізнесу. Системи моніторингу обладнання використовуються для моніторингу працездатності цих систем і скорочення часу простою сервера і застосунків. Сучасні системи апаратного моніторингу використовують USB і мережні порти для передачі стану температури процесора, стану джерела живлення, швидкості обертання вентилятора і температури, стану пам'яті, дискового простору і стану мережної карти. Системи моніторингу обладнання дозволяють технічному фахівцю відстежувати сотні або тисячі систем з одного терміналу. У міру зростання кількості ферм серверів, системи апаратного моніторингу стали важливим заходом безпеки.

# Оперативні центри

Центр керування мережею (Network Operation Center, NOC) - це одне або кількарозташувань, які надають адміністраторам інструменти детального моніторингу стану мережі організації. NOC - це точка відліку для діагностики мережі, моніторингу продуктивності, поширення та оновлення програмного забезпечення, керування комунікаціями та пристроями.

Центр забезпечення безпеки (Security Operation Center, SOC) - це спеціалізований майданчик, який контролює, оцінює і захищає інформаційні системи організації, такі як веб-сайти, застосунки, бази даних, центри обробки даних, мережну інфраструктур, сервери і призначені для користувача системи. SOC - це група аналітиків безпеки, які виявляють, аналізують, реагують, повідомляють і запобігають інцидентам в кібербезпеки.

Обидва цих об'єкта використовують ієрархічну структуру для обробки подій. Перший рівень обробляє всі події та ескалацію їх на другий рівень, якщо не може обробити. Співробітники Рівня 2 детально розглядають цю подію, щоб спробувати знайти вирішення. Якщо це не вдається зробити, вони передають подію на рівень 3, експертам по предмету.

Для оцінки загальної ефективності роботи оперативного центру, організація проводить практичні навчання і реалістичні вправи. Симуляція вправ - це структуроване проходження командою за сценарієм, що імітує події, з метою оцінки ефективності роботи центру. Більш ефективний захід полягає в симуляції повноцінного вторгнення без попередження. Це передбачає використання Red Team, незалежної групи людей, яка кидає виклик процесам всередині організації, для оцінки ефективності захисту організації. Наприклад, Red Team повинна атакувати критичну бізнес-систему і включати розвідку і атаку, ескалацію привілеїв і віддалений доступ.

# Комутатори, маршрутизатори і мережні пристрої

Мережні пристрої не мають паролів або мають пароль за замовчуванням. Змініть паролі за замовчуванням перед підключенням будь-якого пристрою до мережі. Документуйте і запишіть в журнал зміни в мережних пристроях. Нарешті, дослідіть всі журнали конфігурації.

У наступних розділах описані деякі заходи, які адміністратор може вжити для захисту різних мережних пристроїв.

**Комутатори**

Мережні комутатори є основою сучасної мережі передачі даних. Основною загрозою для мережних комутаторів є крадіжка, хакерство та віддалений доступ, атаки проти мережних протоколів, таких як ARP/STP, або атаки на продуктивність апарату та на його доступність. Засоби контролю і заходи захисту від загроз для мережних комутаторів включають поліпшену фізичну безпеку, розширену конфігурацію та введення відповідних системних оновлень та виправлень за потребою. Інший ефективний спосіб контролю - це реалізація безпеки портів. Адміністратор повинен захистити всі порти (інтерфейси) комутатора перед його використанням в робочих умовах. Один із способів захисту портів - це реалізація функції безпеки портів (функція Port Security). Безпека портів обмежує кількість дійсних MAC-адрес, дозволених на даний порт. Комутатор дозволяє отримувати доступ до пристроїв зі схваленими MAC-адресами, тоді як відхиляє всім іншим MAC-адресам.

**Мережі VLAN**

VLAN забезпечують спосіб групування пристроїв у локальній мережі та на окремих комутаторах. VLAN використовують логічні з'єднання замість фізичних. Окремі порти комутатора можуть бути призначені для конкретної VLAN. Інші порти можуть бути використані для фізичного взаємоз'єднання комутаторів один з одним і дозволяють пересилати трафік декількох VLAN. Ці порти називаються магістральними (trunks).

Наприклад, у відділі кадрів (HR) необхідно захистити конфіденційні дані. VLAN дозволяють адміністратору сегментувати мережі по функціям, проектним групам або застосуванням незалежно від фізичного розташування користувача або пристрою, як показано на рисунку 1. Пристрої всередині VLAN діють так, як ніби вони знаходяться у власній незалежній мережі, навіть якщо вони мають спільну інфраструктуру з іншими VLAN. VLAN може відокремити групи, які мають конфіденційні дані, від решти мереж, зменшуючи ймовірність витоку цих даних. Магістральні канали забезпечують можливість фізичного підключення користувачів мережі VLAN HR до кількох комутаторів.

Існує багато різних типів вразливостей і атак на VLAN. Вони можуть включати в себе атаки на VLAN та "Trucking" протоколи. Деталі ціх атаки виходять за рамки цього курсу. Хакери також можуть організовувати атаки на продуктивність і доступність мереж VLAN. Поширені заходи захисту від загроз включають в себе моніторинг змін і показників VLAN, додаткові налаштування і регулярне оновлення IOS.

**Брандмауери**

Брандмауери (Firewalls) - це апаратні або програмні рішення, що забезпечують політику безпеки мережі. Брандмауер фільтрує неавторизований або потенційно небезпечний трафік, запобігаючи його проникнення в мережну інфраструктуру. Простий брандмауер забезпечує основні можливості фільтрації трафіку за допомогою списків контролю доступу (access control lists, ACL). Адміністратори використовують ACL, щоб зупинити трафік або дозволити лише певний трафік у своїх мережах. ACL - це послідовний список дозволів або заборон, які застосовуються до адрес або протоколів. ACL - це потужний спосіб контролювати трафік у мережі та за його межами. Брандмауери утримують атаки на приватні мереж і поширеною метою хакерів є злам захисту брандмауера. Головною загрозою брандмауерів є крадіжка, хакерська діяльність та віддалений доступ, атаки на ACL або атаки, націлені на зниження продуктивності і доступності пристрою. Поширені заходи захисту брандмауерів включають в себе: поліпшена фізична безпека, додаткові налаштування, безпечний віддалений доступ та аутентифікація, а також відповідні системні оновлення та виправлення за потребою.

**Маршрутизатори**

Маршрутизатори утворюють основу Інтернету та зв'язок між різними мережами. Маршрутизатори взаємодіють один з одним, щоб визначити найкращий шлях доставки трафіку до різних мереж. Маршрутизатори використовують протоколи маршрутизації для прийняття рішення маршрутизації. В маршрутизатори також можуть бути інтегровані інші сервіси, такі як функції комутаторів і брандмауерів. В результаті маршрутизатори стають першочерговою метою зловмисників. Основною загрозою для мережних маршрутизаторів є крадіжка, хакерська діяльність та віддалений доступ, атаки на протоколи маршрутизації, такі як RIP/OSPF, або атаки націлені на зниження продуктивності і доступності пристрою. Поширені заходи захисту мережних маршрутизаторів включають в себе: поліпшена фізична безпека, додаткові налаштування, використання протоколів безпечної маршрутизації з аутентифікацією та відповідні оновлення системи та виправлення за потребою.

Бездротові та мобільні пристрої

Бездротові і мобільні пристрої стали переважаючим типом пристроїв в більшості сучасних мереж. Вони забезпечують мобільність та зручність, але створюють безліч вразливостей. До таких вразливостей відносяться крадіжки, хакерська діяльність та несанкціонований віддалений доступ, сніффінг (аналіз трафіку), атаки man-in-the-middle (“Людина посередині”) та атаки націлені на зниження продуктивності і доступності пристрою. Найкращий спосіб захистити бездротову мережу - використання аутентифікації та шифрування. Початковий бездротовий стандарт 801.11 ввів два типи аутентифікації, як показано на рисунку:

* Аутентифікація відкритої системи - будь-який бездротовий пристрій може підключитися до бездротової мережі. Використовуйте цей метод у ситуаціях, коли безпека не викликає занепокоєння.
* Авторизація спільного ключа - надає механізми аутентифікації та шифрування даних, переданих між бездротовим клієнтом і точкою доступу (АР) або бездротовим маршрутизатором.

У мережах WLAN доступні три варіанти аутентифікації за допомогою спільного ключа:

* Wired Equivalent Privacy (WEP) - це початкова специфікація 802.11 забезпечення безпеки WLAN. Однак, ключ шифрування ніколи не змінюється при обміні пакетами, тому його легко зламати.
* Wi-Fi Protected Access (WPA) - цей стандарт використовує WEP, але забезпечує захист даних за допомогою набагато сильнішого алгоритму шифрування Temporal Key Integrity Protocol (TKIP). TKIP змінює ключ для кожного пакета, що робить його важчим до зламання.
* IEEE 802.11i/WPA2 - IEEE 802.11i тепер є галузевим стандартом для захисту WLAN. 802.11i і WPA2 використовують симетричний алгоритм блочного шифрування (Advanced Encryption Standard, AES), який в даний час є самим стійким.

З 2006 року будь-який пристрій, який має логотип Wi-Fi Certified, сертифікований WPA2. Тому сучасні WLAN завжди повинні використовувати стандарт 802.11i/WPA2. Інші заходи захисту включають покращену фізичну безпеку пристроїв та їх регулярні системні оновлення та виправлення.

# Мережні служби та служби маршрутизації

Кібер злочинці використовують уразливі мережні служби для атаки на пристрій або використовують їх як частину атаки. Щоб перевірити наявність незахищених мережних служб, використовуйте сканер портів для пошуку відкритих портів на пристрої. Порт-сканер - це програма, перевіряє на пристрої відкриті порти, відправивши повідомлення на кожний порт і чекаючи відповіді. Відповідь вказує, як використовується порт. З цією ж метою кіберзлочинці також використовують сканери портів. Для безпеки мережних сервісів тільки необхідні порти повинні бути доступні для використання і виявлення.

**Протокол динамічної конфігурації хоста (DHCP)**

DHCP використовує сервер, щоб автоматично призначати IP-адресу та інші параметри конфігурації мережним пристроям. По суті, пристрій отримує від сервера DHCP дозвіл на використання мережної інфраструктури. Зловмисники можуть атакувати DHCP-сервери, щоб заборонити доступ до пристроїв у мережі. На рисунку 1 наведено контрольний перелік безпеки для DHCP.

**Доменна система імен (DNS)**

DNS (Domain Name System) перетворює URL-адресу універсального ресурсу або адресу веб-сайту (наприклад, http://www.cisco.com) в IP-адрес сайту. Коли користувачі вводять веб-адресу в адресний рядок, DNS-сервери перетворюють його в фактичну IP-адресу призначення. Зловмисники можуть атакувати DNS-сервери, щоб заборонити доступ до мережних ресурсів або перенаправляти трафік на шахрайські веб-сайти. Клацніть на рисунок 2, щоб переглянути контрольний список безпеки для DNS. Для захисту від атак використовуйте безпечні служби та аутентифікацію між DNS-серверами.

**Міжмережний протокол керуючих повідомлень (ICMP)**

Мережні пристрої використовують ICMP (Internet Control Messaging Protocol ) для надсилання повідомлень про помилки, наприклад, якщо запитувана служба недоступна або хосту не вдалося зв'язатися з маршрутизатором. Команда ping - це мережна утиліта, яка використовує ICMP для перевірки доступності хоста в мережі. Ping надсилає ICMP-повідомлення на хост і чекає відповіді. Кіберзлочинці можуть втручатися в роботу ICMP для зловмісних цілей, перерахованих на рисунку 3. DoS-атака використовує ICMP, тому багато мереж фільтрує певні запити ICMP для запобігання подібних атак.

**Протокол маршрутизації RIP**

RIP (Routing Information Protocol ) обмежує кількість транзитних ділянок по мережі від вихідного пристрою до місця призначення. RIP допускає не більше 15 транзитних ділянок. RIP - це протокол маршрутизації, який використовується для обміну даними маршрутизації, в тому числі, які мережі може досягти кожен маршрутизатор і як далеко розташовані ці мережі. RIP обчислює найкращий маршрут на основі кількості переходів. На рисунку 4 наведено вразливості RIP та засоби захисту від атак на нього. Хакери можуть атакувати маршрутизатори та протокол RIP. Атаки на служби маршрутизації можу вплинути на продуктивність і доступність. Деякі атаки можуть навіть призвести до перенаправлення трафіку. Для захисту служб маршрутизації, таких як RIP, використовуйте безпечні служби з аутентифікацією та здійснюйте системні оновлення та виправлення.

**Мережний протокол часу (NTP)**

Важливе значення має правильний час в усіх мережах. Правильні відмітки часу точно відслідковують події мережі, такі як порушення безпеки. Крім того, синхронізація часу має вирішальне значення для правильної інтерпретації подій в файлах системного журналу syslog, а також для цифрових сертифікатів.

Мережний протокол часу (Network Time Protocol, NTP) - це протокол, який синхронізує час комп'ютерних систем по мережі. NTP дозволяє мережним пристроям синхронізувати свої налаштування часу за допомогою NTP-сервера. На рисунку 5 перераховані різні методи, що використовуються для безпечної синхронізації в мережі. Кіберзлочинці атакують сервери часу, щоб порушити безпечний обмін даними на основі цифрових сертифікатів і приховати інформацію про атаку, наприклад її точний час.

VoIP обладнання

Голос через IP (Voice over IP, VoIP) використовує такі мережі, як Інтернет, для здійснення та отримання телефонних дзвінків. Обладнання, необхідне для VoIP, включає в себе підключення до Інтернету плюс телефон. Для телефону є кілька варіантів:

* Традиційний телефон з адаптером (адаптер виступає як апаратний інтерфейс між традиційним, аналоговим телефоном та цифровою VoIP-лінією)
* Телефон із підтримкою VoIP
* Програмне забезпечення VoIP, встановлене на комп'ютері

Більшість споживачів VoIP-послуг використовують Інтернет для телефонних дзвінків. Багато організацій, однак, використовують свої приватні мережі, оскільки вони забезпечують більшу якість безпеки та якість обслуговування. Безпека VoIP безпосередньо залежить від безпеки мережі. Кіберзлочинці атакують ці системи, щоб отримати доступ до безкоштовних телефонних послуг, підслуховувати телефонні дзвінки або впливати на продуктивність і доступність.

Впроваджуйте наступні заходи захисту для забезпечення безпеки VoIP:

* Шифруйте пакети голосових повідомлень для захисту від прослуховування.
* Використовуйте SSH для захисту шлюзів і комутаторів.
* Змінюйте всі стандартні паролі.
* Використовуйте систему виявлення вторгнення для виявлення таких атак, як отруєння ARP.
* Використовуйте сильну аутентифікацію для мінімізації ризику підміни реєстрації (кіберзлочинці перенаправляють на себе всі вхідні дзвінки жертв), імітації проксі (кіберзлочинці хитрістю змушують жертву звертатися до створеного ними проксі-сервера) і перехоплення дзвінка (дзвінок перехоплюється і перенаправляється, перш ніж досягне місця призначення).
* Впроваджувати брандмауери, які розпізнають VoIP, для моніторингу потоків та фільтрації аномальних сигналів.

Порушення роботи мережі також веде до порушення голосового зв'язку.

# Камери

Інтернет-камера надсилає та отримує дані через локальну мережу та/або Інтернет. Користувач може дистанційно переглядати пряме відео за допомогою веб-браузера на широкому колі пристроїв, включаючи комп'ютерні системи, ноутбуки, планшети та смартфони.

Камери поставляються в різних формах, включаючи традиційну камеру безпеки. Інші варіанти включають в себе інтернет-камери, сховані в радіогодинниках, книгах або DVD-програвачах.

Інтернет-камери передають цифрове відео через з'єднання передачі даних. Камера з'єднується безпосередньо з мережею і має все необхідне для передачі зображень по мережі. На рисунку перераховані найкращі практики для систем відеонагляду.

# Обладнання для відеоконференцзв'язку

Відеоконференції дозволяють двом або більше клієнтам у різних місцеположеннях спілкуватися одночасно за допомогою телекомунікаційних технологій. Ці технології використовують нові стандарти відео високої якості. Продукти, такі як Cisco TelePresence, дозволяють групі людей в одному місці зв'язатися з групою людей з інших регіонів у режимі реального часу. Відеоконференції є частиною звичайних щоденних операцій у таких галузях, як медична. Лікарі можуть оглядати пацієнта та проконсультуватися з експертами по виявленим симптомам з метою визначення можливих методів лікування.

У багатьох місцевих аптеках працюють фельдшери, які можуть зв'язуватися з лікарями, використовуючи телеконференції, щоб запланувати візит або проконсультуватися при наданні надзвичайної допомоги. Багато виробничіх організацій використовують телеконференції, щоб допомогти інженерам та технікам виконувати складні операції або завдання з технічного обслуговування. Обладнання для відеоконференцій може бути надзвичайно дорогим та представляти інтерес для злодіїв та кіберзлочинців. Натисніть [тут](https://youtu.be/WlDkiwzzv3M) щоб переглянути відео про можливості систем відеоконференцзв'язку. Кіберзлочинці атакують ці системи, щоб підслухувати відеодзвінки або впливати їх продуктивність та доступність.

# Мережні датчики і датчики IoT

Одним із найбільш швидкозростаючих напрямів інформаційних технологій є використання інтелектуальних пристроїв та датчиків. Комп'ютерна індустрія брендує цей сектор як Інтернет речей (Internet of Things, IoT). Підприємства та споживачі використовують пристрої IoT для автоматизації процесів, моніторингу стану навколишнього середовища та попередження користувачів про несприятливі умови. Більшість пристроїв IoT підключаються до мережі через бездротові технології. У число таких пристроїв входять камери, дверні замки, датчики близькості, світла та інші типи датчиків, які використовуються для збору інформації про навколишнє середовище або стан пристрою. Деякі виробники приладів використовують IoT, щоб інформувати користувачів про необхідність заміни компонентів, збої компонентів, або їх запаси вичерпуються.

Підприємства використовують ці пристрої для відстеження інвентарю, транспортних засобів та наявність персоналу. Пристрої IoT містять геопросторові датчики. Користувач може глобально відслідковувати та контролювати зміни навколишнього середовища, такі як температура, вологість та освітлення. ІоТ-індустрія становить величезну проблему для фахівців з інформаційної безпеки, оскільки багато пристроїв IoT збирають та передають конфіденційну інформацію. Кіберзлочинці атакують ці системи, щоб перехопити дані або впливати на продуктивність та доступність систем.

Огородження та барикади

Фізичні бар'єри - це перше, що приходить на розум, коли мислимо про фізичну безпеку. Це зовнішній рівень безпеки і ці рішення є найбільш загальнодоступними. Система охорони периметра зазвичай складається з наступних компонентів:

* Система огорожі периметра
* Система безпеки воріт
* Блокатори руху (короткий пост, який використовується для захисту від вторгнень автомобіля, як показано на рисунку 2)
* Перешкоди для в'їзду автомобіля
* Охоронні приміщення

Огорожа являє собою бар'єр, який охоплює безпечні зони та визначає межі власності. Усі бар'єри повинні відповідати специфічним вимогам до дизайну та специфікаціям виробництва. Області з високим рівнем безпеки часто потребують додаткових коштів охорони на верхній частині огорожі, наприклад, використання колючого дроту або колючої стрічки. При проектуванні системи огородження периметра використовують такі правила:

* Огорожа висотою 1 метр (3-4 фути) лише стримує випадкових порушників
* Огорожа висотою 2 метри (6-7 футів) занадто висока для випадкових порушників
* Огорожа висотою 2,5 метри (8 футів) тимчасово затримає порушника, навмисно проникаючого на територію

Колючий дріт нагорі забезпечує додатковий стримуючий ефект і може затримати порушника, серйозно поранивши його. Однак зловмисники можуть використовувати ковдру або матрац для зменшення цієї загрози. Місцеві правила можуть обмежувати тип системи огородження, яку може використовувати організація.

Регулярно оглядайте системи огородження. Тварини можуть підкопувати під огорожею, або земля може вимиватися, залишаючи огородження нестійким, забезпечуючи легкий доступ для вторгнення. Регулярно оглядайте системи огородження. Забороняється паркування транспортних засобів поблизу огорожі. Припаркована машина біля огорожі може допомогти зловмисникові піднятися або пошкодити її. Натисніть [тут](http://www.chainlinkinfo.org/security-fencing-guidelines/) для додаткових рекомендацій щодо огородження.

# Біометрія

Біометрія описує автоматизовані методи розпізнавання особи на основі фізіологічних або поведінкових характеристик. Біометричні системи аутентифікації включають вимірювання обличчя, відбитків пальців, геометрії рук, райдужній оболонці і сітківці ока, рукописному почерку та голосу. Біометричні технології можуть стати основою для добре захищених рішень ідентифікації та посвідчення особи. Збільшення кількості порушень безпеки і шахрайства з транзакціями призвело до зростання популярності використання біометричних систем. Біометрія забезпечує конфіденційність фінансових операцій та особистих даних Наприклад, Apple використовує технологію відбитків пальців у смартфонах. Відбиток пальця користувача розблоковує пристрій і отримується доступ до різних застосунків, таких як онлайн-банкінг або платні додатки.

При порівнянні біометричних систем слід врахувати кілька важливих факторів: точність, швидкість або пропускну здатність, прийнятність для користувачів, унікальність біометричного органу або дії, стійкість до фальсифікації, надійність, вимоги щодо зберігання даних, час реєстрації та зручність процедури сканування. Найважливішим фактором є точність. Точність виражена за типом помилок і її показниками.

Перший клас - це помилки типу I або помилкові відхилення. Вони відбуваються, коли відмовлено в доступі зареєстрованому авторизованому користувачеві. З точки зору розмежування доступу, якщо потрібно перешкодити доступ зловмисникам, помилкове відхилення є найменш важливою помилкою. Однак у багатьох біометричних застосунках помилкові відмови можуть мати дуже негативний вплив на бізнес. Наприклад, банківський або роздрібний магазин повинен ідентифікувати клієнта та залишок на рахунку. Неправильне відхилення означає, що транзакція або продаж не будуть виконані і замовник засмутиться. Більшість банків та роздрібних магазинів готові допустити кілька помилкових подій, якщо їх кількість мінімальна.

Відсоток пропуску помилкових подій вказує частку визнання системою незареєстрованих користувачів або шахраїв як легітимних користувачів. Помилкове прийняття є помилкою типу II. Помилки типу II дозволяють пройти зловмисникам, тому вони, як правило, вважаються найбільш важливими помилками в біометричній системі контролю доступу.

Найбільш широко використовуваним методом для вимірювання точності біометричної аутентифікації є Crossover Error Rate (CER). CER - це така оцінка, коли коефіцієнт помилкового відхилення та коефіцієнт помилкового прийняття рівні, як показано на рисунку.

# Перепустки та журнали доступу

Перепустка дозволяє людині отримати доступ до області з автоматизованими точками входу. Точка входу може бути: двері, турнікет, ворота або інший бар'єр. В перепустках використовуються різні технології, такі як магнітна смуга, штрихкод або біометрія.

Картрідер зчитує номер, що міститься на перепустці. Система надсилає номер на комп'ютер, який приймає рішення щодо доступу на основі наданих облікових даних. Система реєструє транзакцію і згодом можна звернутися до цієї інформації. У звітах вказуються, хто увійшов, час і точка входу.

# Охорона і супровід

Всі фізичні засоби контролю доступу, включаючи системи стримування та виявлення, в кінцевому підсумку залежать від персоналу, який повинен втручитися та припинити фактичний напад або вторгнення. На об'єктах з системою інформаційної охорони високого рівня доступ до особливо важливих зон організації контролюється охоронцями. Перевага використання охоронців полягає в тому, що вони можуть адаптуватися краще, ніж автоматизовані системи. Охорона може дослідити і розрізнити різні умови та ситуації і прийняти рішення на місці. Це є кращим рішенням для контролю доступу, коли ситуація вимагає миттєвої і адекватної реакції. Однак охоронці не завжди є найкращим рішенням. Існують численні недоліки використання охоронців, включаючи витрати і неможливість контролювати і реєструвати великий обсяг трафіку. Використання охоронців також вносить фактор людської помилки.

# Відеоспостереження і спостереження з використанням електронних засобів

Відеоспостереження і спостереження з використанням електронних засобів може доповнити, а в деяких випадках і замінити охоронців. Переваги відеоспостереження або спостереження з використанням електронних засобів - це можливість відслідковувати зони навіть за відсутності охоронців або персоналу, здатність записувати та реєструвати відео та дані спостереження протягом тривалого періоду часу, а також можливість використання детекторів руху та сповіщення.

Крім того, можна забезпечити більш високу точність фіксації подій навіть після того, як вони відбулися. Іншою важливою перевагою цього типу забезпечення безпеки є можливість вести спостереження з точок, важкодоступних для охоронців. Також може бути набагато економічніше використовувати камери для моніторингу всього периметру об'єкта. В добре захищеній організації відеоспостереження або спостереження з використанням електронних засобів повинні бути розміщені на всіх входах, виходах, вантажних відсіках, сходах та місцях збирання сміття. У більшості випадків ці системи доповнюють охоронців.

# RFID та бездротовий нагляд

Відстеження розташування важливих ресурсів інформаційної системи та керування ними є ключовим завданням для більшості організацій. Зростання кількості мобільних пристроїв та пристроїв IoT зробило цю роботу ще більш складнішою. Час, витрачений на пошук критичного обладнання, може призвести до дорогих затримок або простоїв. Використання пристроїв радіочастотної ідентифікації (Radio Frequency Identification, RFID) дозволяє істотно полегшити роботу персоналу служби безпеки. Організація може помістити зчитувачі RFID в дверних рамах захищених приміщень так, щоб вони не були непомітні для людей.

Перевага інвентаризаційних RFID-міток полягає в можливості відстежувати будь-який актив, який фізично залишає захищену зону. Нові системи інвентаризаційних RFID-міток можуть одночасно зчитувати кілька міток. RFID-система не вимагає прямої видимості для сканування міток. Ще однією перевагою RFID є можливість читати пристрої, які не видно.

**Розділ 8. Як стати спеціалістом з кібербезпеки**

Розвиток технології забезпечив появу ряду пристроїв, які щоденно використовуються у світіі для спілкування та зв'язку. Однак це вдосконалення методів комунікації призволо до збільшення ризику крадіжки, шахрайства та зловживань у всій технологічній інфраструктурі. Цей розділ класифікує інфраструктуру інформаційних технологій на сім доменів. Для кожного домену потрібні відповідні засоби контролю безпеки щоб дотримуватися вимогам тріади CIA.

У розділі розглядаються закони, які впливають на технології та вимоги до кібербезпеки. Багато з цих законів зосереджено на різних типах даних, що знаходяться в різних галузях промисловості, і містять концепції конфіденційності та інформаційної безпеки. Кілька агентств в уряді США регулюють дотримання організаціями цих законів. Спеціаліст з кібербезпеки повинен розуміти, як приймати етичні рішення, керуючись законом та інтересами організації. Кібер-етика розглядає вплив використання комп'ютерів та технологій на людей та суспільство.

Організації використовують фахівців з кібербезпеки на різних посадах, таких як тестувальники вразливостей, аналітики безпеки та інші спеціалісти з безпеки мереж. Фахівці з кібербезпеки допомагають захистити особисті дані та можливість використання мережних служб. У розділі розглядається шлях становлення фахівця з кібербезпеки. Нарешті, в цьому розділі розглядаються низка інструментів, які доступні фахівцям з кібербезпеки.

Загальні загрози та вразливості користувачів

Домен користувача включає в себе користувачів, які мають доступ до інформаційної системи організації. Користувачами можуть бути працівники, клієнти, підрядники та інші особи, які потребують доступу до даних. Користувачі часто є найслабшою ланкою в системах інформаційної безпеки та створюють значну загрозу конфіденційності, цілісності та доступності даних організації.

Ризиковані або погані практики користувачів часто підривають навіть кращу систему безпеки. Нижче перераховані загальні загрози користувачів, виявлені в багатьох організаціях:

* **Відсутність обізнаності про безпеку** - користувачі повинні знати про конфіденційні дані, політики та процедури безпеки, технології та контрзаходи, що надаються для захисту інформації та інформаційних систем.
* **Погано застосовані політики безпеки** - всі користувачі повинні знати про політики безпеки та наслідки невиконання політик організації.
* **Крадіжка даних** - крадіжка даних користувачами можуть дорого коштувати організації,, так як наносять шкоду її репутації або спричиняють юридичну відповідальність, пов'язану з розголошенням конфіденційної інформації.
* **Неавторизовані завантаження** - багато атак на мережі та робочі станції стаються через користувачів, які завантажують несанкціоновані електронні листи, фотографії, музику, ігри, програми та відеозаписи до робочих станцій, мереж або пристроїв зберігання даних.
* **Неавторизовані носії** - використання неавторизованих носіїв, таких як компакт-диски, USB-накопичувачі та мережні пристрої зберігання даних, може призвести до інфікування шкідливими програмами та атак.
* **Неавторизовані VPN** - VPN-мережі можуть приховувати крадіжку інформації. Передбачається, що шифрування має забезпечувати захист конфіденційності, але воно також може використовуватися для несанкціонованої передачі даних непомітно для фахівців служби ІТ-безпеки.
* **Неавторизовані веб-сайти** - доступ до несанкціонованих веб-сайтів може становити загрозу для даних користувача, пристроїв та організації. Багато веб-сайтів пропонують відвідувачам завантажувати скріпти або плагіни, які насправді містять шкідливий код або рекламне ПЗ. Деякі сайти можуть перехоплювати контроль над камерами і застосунками.
* **Руйнування систем, застосунків або даних** - випадкове або навмисне знищення або порушення роботи систем, застосунка та даних представляє великий ризик для всіх організацій. Активісти, незадоволені співробітники та конкуренти галузі можуть видаляти дані, знищувати або переналаштувати пристрої, щоб зробити дані та інформаційні системи недоступними.

Немає технічного рішення, методів контролю або контрзаходів, які роблять інформаційні системи більш безпечними, ніж поведінка та процеси людей, які використовують ці системи.

Керування загрозами користувачів

Організації можуть впроваджувати різні заходи для керування загрозами від користувача:

* Проведення тренінгів з підвищення обізнаності про безпеку, розміщення тематичних плакатів, вставляючи в них нагадування про безпеку, і відправка співробітникам на електрону пошту нагадувань .
* Щорічне навчання користувачів з питань політик, оновлення робочих інструкцій і керівництв для співробітників.
* Оцінка ефективності співробітника з урахуванням його знань принципів і заходів безпеки.
* Увімкнення фільтрування вмісту та антивірусне сканування для вкладень електронної пошти.
* Використовування фільтрування вмісту, щоб дозволити або заборонити певні доменні імена згідно з прийнятними правилами використання (AUP).
* Вимкнення внутрішніх дисководів компакт-дисків та USB-портів.
* Увімкнення автоматичного сканування антивірусів для вставлених мультимедійних дисків, файлів та вкладень електронної пошти.
* Обмеження доступу користувачів тільки тими системами, програми та даними, які необхідні для виконання їх роботи.
* Надання дозволу на запис і видалення даних тільки їх власнику.
* Відстеження і контроль нетипової поведінки співробітників, порушень під час виконання службових обов'язків і використання інфраструктури ІТ в неробочий час
* Впровадження процедури блокування доступу на основі моніторингу та дотримання AUP.
* Увімкнення моніторингу системи виявлення вторгнення/запобігання вторгнення (IDS/IPS) в разі доступу до конфіденційної інформації і для відповідних співробітників.

Таблиця, яка показана на рисунку, ставить у відповідність загрози домена користувача з контрзаходами, які використовуються для керування цими загрозами.

Загальні загрози для пристроїв

Пристрій - це будь-який настільний комп'ютер, ноутбук, планшет або смартфон, який підключається до мережі.

Нижче приведено загрози для пристроїв:

* **Робочі станції без нагляду** – робочі станції, залишені ввімкненими і без нагляду, створюють ризик несанціонованого доступу до мережних ресурсів
* **Завантаження користувачів** - завантажені файли, фотографії, музика чи відео можуть стати транспортним засобом для шкідливого коду
* **Неоновлене програмне забезпечення** - вразливості програмного забезпечення забезпечує слабкі сторони, якими можуть користуватися кіберзлочинці
* **Шкідливе програмне забезпечення** - щодня з'являються нові віруси, черв'яки та інший шкідливий код
* **Неавторизовані носії** - користувачі, що вставляють USB-накопичувачі, компакт-диски чи DVD-диски, можуть заносити шкідливе ПЗ або створювати ризик компрометації даних, що зберігаються на робочій станції
* **Порушення політики прийнятного користування** - Політики існують для захисту IT-інфраструктури організації

Керування загрозами пристроїв

Організації можуть впроваджувати різні заходи для керування загрозами пристроїв:

* Встановити політику для захисту паролем та порогових блокуваннь на всіх пристроях.
* Увімкнути блокування екрану під час бездіяльності.
* Вимкнути адміністративні права для користувачів.
* Визначити політику контролю доступу, стандарти, процедури та рекомендації.
* Оновити та виправити всі операційні системи та програмні застосунки.
* Впровадити автоматизовані антивірусні рішення, які сканують систему та оновлюють антивірусне програмне забезпечення для забезпечення належного захисту.
* Деактивувати всі CD, DVD та USB-порти.
* Увімкнути автоматичне сканування антивірусу для всіх вставлених компакт-дисків, DVD-дисків або USB-накопичувачів.
* Використовувати фільтрації контенту.
* Обов'язкове щорічне навчання принципам і заходам безпеки або проведення інформаційних кампаній та програм, присвячених підвищенню рівня знань принципів і заходів безпеки, протягом усього року.

Таблиця, яка показана на рисунку, ставить у відповідність загрозу домену пристроїв з контрзаходами, які використовуються для керування нею.

Загальні загрози для локальної мережі

Локальна мережа (LAN) - це сукупність пристроїв, з'єднаних між собою за допомогою кабелів або радіохвиль. Домен LAN вимагає надійних засобів захисту та контролю доступу, оскільки користувачі можуть отримати доступ до систем, застосунків і даних організації з домену локальної мережі.

Нижче приведено загрози для локальної мережі:

* Несанкціонований доступ до локальної мережі - кабельні шафи, центри обробки даних та комп'ютерні приміщення повинні залишатися захищеними
* Несанкціонований доступ до систем, програм і даних
* Вразливості мережної операційної системи
* Оновлення мережної операційної системи
* Несанкціонований доступ сторонніх користувачів до бездротових мереж
* Експлуатація даних під час передачі
* LAN-сервери з різним обладнанням або операційними системами - керування та усунення неполадок серверів стає більш складним з різними конфігураціями
* Неавторизоване сканування мережі та портів
* Неправильно налаштований брандмауер

Керування загрозами локальної мережі

Організації можуть впроваджувати різні заходи для керування загрозами локальної мережі:

* Захистити шафи, інформаційні центри та комп'ютерні приміщення. Заборонити доступ без належних повноважень.
* Визначити суворі правила контролю доступу, стандарти, процедури та рекомендації.
* Обмежити права доступу для певних папок і файлів на основі необхідності.
* Вимагати парольні фрази або аутентифікацію для бездротових мереж.
* Впровадити шифрування між пристроями та бездротовими мережами для збереження конфіденційності.
* Впровадити стандарти конфігурації локальної мережі.
* Провести тестування на проникнення після конфігурації.
* Вимкнути сканування ping та сканування портів.

Таблиця, яка показана на рисунку, ставить у відповідність загрози домену локальної мережі з контрзаходами, які використовуються для керування ними.

Загальні загрози приватної хмари

Домен приватноъ хмари включає в себе приватні сервери, ресурси та ІТ-інфраструктуру, доступну членам організації через Інтернет.

Наступне створює загрозу для приватної хмари:

* Неавторизоване сканування мережі та портів
* Неавторизований доступ до ресурсів
* Вразливість маршрутизатора, брандмауера або операційної системи мережного пристрою
* Помилка конфігурації маршрутизатора, брандмауера або мережного пристрою
* Віддалені користувачі отримують доступ до інфраструктури організації та завантажують конфіденційні дані

Керування загрозами приватної хмари

Організації можуть застосовувати різні заходи для керування загрозами приватної хмари:

* Вимкнути ping та сканування портів.
* Впровадити системи виявлення та запобігання вторгнень.
* Моніторити аномалії вхідного IP-трафіку.
* Оновлювати пристрої за допомогою виправлень безпеки та оновлень.
* Проводити тестування на проникнення після конфігурації.
* Перевіряти вхідний і вихідний трафік.
* Впровадити стандарт класифікації даних.
* Реалізувати моніторинг і сканування передачі файлів для невідомих типів файлів.

Таблиця, яка показана на рисунку, ставить у відповідність загрози домену приватної хмари з контрзаходами, які використовуються для керування ними.

Загальні загрози для публічної хмари

Домен публічної хмари включає послуги, що надаються провайдером хмарних обчислень, постачальником послуг або інтернет-провайдером. Хмарні провайдери реалізують засоби контролю безпеки для захисту хмарного середовища, але організації несуть відповідальність за захист своїх ресурсів у хмарі. Є три різні моделі обслуговування, з яких організація може вибрати:

* **Програмне забезпечення як послуга (SaaS)** - модель на основі підписки, яка забезпечує доступ до програмного забезпечення, яке централізовано розміщується та доступ до якого здійснюють користувачі через веб-браузер.
* **Платформа як послуга (PaaS)** - це платформа, яка дозволяє організації розробляти, запускати та керувати своїми програмами на апаратному забезпеченні за допомогою інструментів, які надає ця послуга.
* **Інфраструктура як послуга (IaaS)** - надає віртуалізовані обчислювальні ресурси, такі як апаратне забезпечення, програмне забезпечення, сервери, сховище та інші компоненти інфраструктури через Інтернет.

Наступні речі представляють загрозу для публічної хмари:

* Витік даних
* Втрата чи крадіжка інтелектуальної власності
* Компрометування облікових даних
* Злом сховищ федеративних посвідчень зловмисниками
* Викрадення облікового запису
* Відсутність розуміння з боку організації
* Атаки соціальної інженерії, які заманюють жертву
* Порушення дотримання правил

Керування загрозами для публічної хмари

Організації можуть впроваджувати різні заходи з керування загрозами фізичних об'єктів:

* Багатофакторна аутентифікація
* Використання шифрування
* Впровадження одноразових паролів, автентифікації на основі телефону та смарт-карток
* Розповсюдження даних та програм у кількох зонах
* Процедури резервного копіювання даних
* Юридична експертиза
* Програми підвищення рівня обізнаності про безпеку
* Політики

Таблиця, яка показана на рисунку, ставить у відповідність загрози домену публічної хмари з контрзаходами, що використовуються для керування ними.

# Загальні загрози фізичним об'єктам

Домен фізичних об'єктів включає всі послуги, які використовуються організацією, включаючи HVAC, воду і системи виявлення пожежі. Цей домен також включає в себе механізми фізичної безпеки, що використовуються для захисту об'єкта.

Загрози для об'єктів організації:

* Природні загрози, включаючи погодні проблеми та геологічні небезпеки
* Несанкціонований доступ до об'єктів
* Переривання живлення
* Соціальна інженерія, щоб дізнатися про процедури безпеки та офісну політику
* Порушення електронного захисту периметру
* Крадіжка
* Відкриті загальнодоступні приміщення, що дозволяють відвідувачам безперешкодно проникати в приміщення організації
* Відкритий центр обробки даних
* Відсутність нагляду

# Керування загрозами для фізичних об'єктів

Організації можуть впроваджувати різні заходи для керування загрозами фізичним об'єктам:

* Розмежування доступу і установка засобів відеоспостереження на всіх входах.
* Встановити правила та процедури для гостей, які відвідують об'єкт.
* Перевірити безпеку будівель, використовуючи як кібер, так і фізичні засоби для прихованого отримання доступу.
* Впровадити шифрування бейджів для доступу до входу.
* Розробити план аварійного відновлення.
* Розробити плану безперервності бізнесу.
* Регулярно проводити тренінг з підвищення рівня обізнаності з безпеки.
* Впровадження системи маркування ресурсів.

Таблиця, яка показана на рисунку, ставить у відповідність загрози домену фізичних об'єктів з контрзаходами, які використовуються для керування ними.

# Загальні загрози для застосунків

Домен застосунка включає всі критичні системи, програми та дані. Крім того, він включає в себе обладнання та будь-який необхідний логічний дизайн. Організації використовують такі застосунки як електронна пошта, моніторинг безпеки та керування базами даних у хмарі.

Основні загрози для застосунків:

* Несанкціонований доступ до центрів обробки даних, комп'ютерних приміщень та комутаційних шаф
* Час простою сервера для технічного обслуговування
* Вразливість в мережній операційній системі
* Несанкціонований доступ до систем
* Втрата даних
* Простій IT-систем протягом тривалого періоду часу
* Уразливості клієнтів/сервеа або веб-застосунка

# Керування загрозами для застосунків

Організації можуть впроваджувати різні заходи для керування загрозами застосунків:

* Впровадити політику, стандарти та процедури для персоналу та відвідувачів, щоб забезпечити безпеку об'єктів.
* Провести тестування програмного забезпечення до запуску.
* Запровадити стандарти класифікації даних.
* Розробити політику для вирішення проблем програм та оновлень операційної системи.
* Впровадити процедури резервного копіювання
* Розробити план безперервності бізнесу для критичних застосунків для підтримки доступності операцій.
* Розробити план аварійного відновлення для критичних програм та даних.
* Реалізувати ведення журналу.

Таблиця, показана на рисунку, ставить у відповідність загрози домену застосунків з контрзаходами, які використовуються для керування ними.

# Етика спеціаліста з кібербезпеки

Етичні цінності лежать в підсвідомості спеціаліста з кібербезпеки і підказують йому стосовно того, що він повинен чи не повинен робити, навіть якщо це законно Організація довіряє фахівцеві з кібербезпеки найбільш конфіденційні дані та ресурси. Спеціаліст з кібербезпеки повинен розуміти, як закон та інтереси організації допомагають керувати етичними рішеннями.

Кіберзлочинці, які вламуються в систему, крадуть номери кредитних карт і впускають черв'яків, виконують неетичні дії. Як організація розглядає дії спеціаліста з кібербезпеки, якщо вони схожі на дії кіберзлочинця? Наприклад, спеціаліст з кібербезпеки може запобігти розповсюдженню черв'яка шляхом його виправлення. По суті, він впускає черв'яка. Цей черв'як не є шкідливим, але чи означає це, що можна так поступати?

Наступні етичні системи розглядають етику з різних точок зору.

**Утилітарна етика**

У 19-му столітті Джеремі Бентан і Джон Стюарт Мілл створили Утилітарну етику. Керівний принцип полягає в тому, що будь-які дії, які забезпечують більшу кількість добра, ніж зла, є етичним вибором.

**Правовий підхід**

Керівним принципом правового підходу є те, що особи мають право самостійно робити вибір. У цій перспективі розглядається, як дія впливає на права інших, щоб судити про те, чи є дія правильною або неправильною. Ці права включають право на правду, конфіденційність та безпеку і суспільство справедливо застосовує закони до всіх членів суспільства.

**Підхід загального блага**

Підхід загального блага пропонує, що загальне благо це те, що приносить користь суспільству. У цьому випадку спеціаліст з кібербезпеки розглядає, як дія впливає на загальне благо суспільства чи спільноти.

Чіткі відповіді не дають очевидних рішень етичних питань, з якими стикаються спеціалісти з кібербезпеки. Відповідь на те, що правильно або неправильно, може змінитися в залежності від ситуації і етичної перспективи.

# Інститут комп'ютерної етики (Computer Ethics Institute)

Інститут комп'ютерної етики (CEI) є ресурсом для виявлення, оцінки та реагування на етичні проблеми в галузі інформаційних технологій. CEI був однією з перших організацій, яка визнала етичні проблеми та проблеми публічних політик, що виникають внаслідок швидкого розвитку інформаційних технологій. На рисунку перераховані Десять заповідей комп'ютерної етики, які створені Інститутом комп'ютерної етики.

# 

# Кіберзлочинність

Закони забороняють небажану поведінку. На жаль, досягнення в технологіях інформаційної системи набагато більші, ніж правова система компромісу та законодавства. Ряд законів та положень впливають на кіберпростір. Кілька конкретних законів керують політиками та процедурами, розробленими організацією, для забезпечення їх відповідності.

**Кіберзлочинність**

Комп'ютер може бути задіяний у кіберзлочинності кількома різними способами. Так, комп'ютер може бути засобом здійснення злочину, його метою або грати другорядну роль. Дитяча порнографія є прикладом комп'ютерного опосередкованого злочину - комп'ютер є запам'ятовуючим пристроєм і не є фактичним інструментом, який використовується для вчинення злочину.

Зростання кіберзлочинів обумовлено низкою різних причин. В даний час в Інтернеті є безліч інструментів і потенційним користувачам не потрібен великий досвід використання цих інструментів.

**Організації, які створені для боротьби з кіберзлочинністю**

Існує низка агентств та організацій, які допомагають боротися з кіберзлочинністю. Натисніть на кожне з посилань на рисунку, щоб відвідати веб-сайти цих організацій.

# Цивільні, кримінальні та нормативні кібер-закони

У Сполучених Штатах існує три основних джерела законів і правил: нормативне право, адміністративне право і загальне право. Всі три джерела пов'язані з комп'ютерною безпекою. Конгрес США створив федеральні адміністративні установи і нормативну базу, яка включає як цивільні, так і кримінальні покарання за недотримання правил.

Кримінальні закони забезпечують дотримання загальноприйнятого морального кодексу, підкріпленого повноваженнями уряду. Положення встановлюють правила, призначені для вирішення наслідків у швидко мінливому суспільстві, що забезпечують покарання за порушення цих правил. Наприклад, Закон про комп'ютерні шахрайства і зловживання є нормативним законом. Адміністративно FCC і Федеральна комісія з торгівлі займалися такими питаннями, як розкрадання інтелектуальної власності та шахрайство. Нарешті, справи загального права працюють через судову систему, надаючи прецеденти і конституційні основи для законів.

**Федеральний закон про керування інформаційною безпекою (FISMA)**

Конгрес створив FISMA у 2002 році, щоб змінити підхід американської влади до інформаційної безпеки. Як найбільший творець і користувач інформації, федеральні ІТ-системи є високоцінними мішенями для кіберзлочинців. FISMA застосовується до інформаційних систем федеральних агентств та встановлює, що агентства створюють програму інформаційної безпеки, яка включає в себе наступне:

* Оцінка ризиків
* Річна інвентаризація ІТ-систем
* Політика та процедури зменшення ризику
* Тренінги з підвищення рівня обізнаності про кібербезпеку
* Тестування і оцінка всіх елементів керування ІТ-системами
* Процедура відповіді на інцидент
* План безперервності операцій

# Галузеві закони

Багато галузевих законів мають компонент безпеки та/або конфіденційності. Уряд США вимагає дотримання цих законів від організацій в цих галузях. Фахівці з кібербезпеки повинні мати можливість перевести юридичні вимоги в політику і практику безпеки.

**Закон Грема-Ліча-Блайлі (GLBA)**

Закон Грема-Ліча-Блайлі - це частина законодавства, яка в основному стосується фінансової галузі. Проте, частина цього законодавства включає в себе положення щодо приватних осіб. Положення передбачає методи відмови, щоб особи могли контролювати використання інформації, наданої в рамках бізнес-операції з організацією, яка є частиною фінансової установи. GLBA обмежує обмін інформацією з сторонніми фірмами.

**Закон Сарбейнса-Окслі (SOX)**

Після кількох гучних скандалів корпоративного обліку в США з'їзд прийняв Закон Сарбейнса-Окслі (SOX). Мета SOX полягала в тому, щоб переглянути стандарти фінансового та корпоративного обліку та конкретно орієнтуватися на стандарти публічних торгівельних фірм в Сполучених Штатах.

**Стандарт безпеки даних для платіжних карток (PCI DSS)**

Приватна промисловість також визнає, наскільки важливі єдині і зобов'язуючі стандарти. Рада зі стандартів безпеки, що складається з провідних корпорацій в індустрії платіжних карток, розробила ініціативу приватного сектора для поліпшення конфіденційності мережних комунікацій.

Стандарт безпеки даних для платіжних карток (PCI DSS) являє собою набір договірних правил, що регулюють способи захисту даних кредитних карт, коли продавці і банки обмінюють транзакцію. PCI DSS є добровільним стандартом (теоретично), а продавці/постачальники можуть вибрати, чи хочуть вони дотримуватися стандарту. Проте невідповідність постачальника може призвести до значно вищої комісії, штрафів до 500000 доларів США і, можливо, навіть втрати можливості обробляти кредитні картки.

**Імпортні/Експортні обмеження на шифрування**

З часів Другої світової війни Сполучені Штати регулювали експорт криптографії через міркування національної безпеки. Бюро промисловості та безпеки Департаменту торгівлі зараз контролює невійськовий експорт криптографії. Ще існують експортні обмеження для держав-ізгоїв і терористичних організацій.

Країни можуть вирішити обмежити імпорт технологій криптографії з наступних причин:

* Технологія може містити бекдор або вразливість системи безпеки.
* Громадяни можуть анонімно спілкуватися та уникати будь-якого моніторингу.
* Криптографія може підвищити рівень конфіденційності вище прийнятного.

# Закони про сповіщення в разі порушення безпеки

Підприємства збирають все більшу кількість особистої інформації про своїх клієнтів, від паролів облікових записів та адрес електронної пошти до надзвичайно важливої медичної та фінансової інформації. Великі та малі підприємства визнають цінність великих даних та аналітичних даних. Це спонукає організації збирати та зберігати інформацію. Кібер-злочинці завжди шукають шляхи отримання такої інформації або доступу та використання найбільш конфіденційних даних компанії. Організації, які збирають конфіденційні дані, повинні бути хорошими хранителями даних. У відповідь на це зростання в зборі даних кілька законів вимагають, щоб організації, які збирали особисту інформацію, повідомляли людей, якщо відбувається витік їх особистих даних. Щоб переглянути список цих законів, натисніть [тут](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

**Закон про конфіденційність електронних повідомлень (ECPA)**

У Законі про конфіденційність електронних повідомлень (ECPA) розглядається безліч питань конфіденційності, пов'язаних з використанням комп'ютерів і інших технологій, специфічних для телекомунікацій. Розділи цього закону стосуються електронної пошти, стільникового зв'язку, конфіденційності робочих місць та безлічі інших питань, які пов'язані із спілкуванням електронним шляхом.

**Закон про комп'ютерне шахрайство та зловживання (1986 рік)**

Закон про комп'ютерні шахрайства та зловживання (CFAA) дія більше 20 років. CFAA забезпечує основу для законів США, що криміналізують несанкціонований доступ до комп'ютерних систем. CFAA робить злочином свідомий доступ без дозволу до комп'ютера, який розглядається як урядовий комп'ютер або комп'ютер, що використовується у міжнародній торгівлі. CFAA також криміналізує використання комп'ютера в злочині, який носить міждержавний характер.

Закон передбачає кримінальну відповідальність за торгівлю паролями або подібною інформацією для доступу і цей зако робить злочином передачу програми, коду чи команди, що свідомо заподіює шкоду.

# Захист конфіденційності

Наведені нижче закони США захищають конфіденційність.

**Закон про конфіденційність 1974 року**

Цей закон встановлює Кодекс добросовісної інформаційної практики, який регулює збір, обслуговування, використання та поширення особистої ідентифікованої інформації, яка зберігається в системах обліку федеральними агентствами.

**Закон про свободу інформації (FOIA)**

FOIA забезпечує доступ громадськості до державних записів США. FOIA несе презумпцію розкриття інформації, тому уряд повинен дати пояснення стосовно того, чому він не дає доступ до інформації.

Є дев'ять винятків щодо розкриття інформації, що відносяться до FOIA.

* Інформація про національну безпеку і зовнішню політику
* Правила і практика внутрішнього керування агентства
* Інформація, яка спеціально звільнена законом
* Конфіденційна ділова інформація
* Між- або внутрішньоорганізаційне спілкування, яке підлягає обговоренню, судовому розгляду та іншим привілеям
* Інформація, яка, якщо вона буде розкрита, стане явно необґрунтованим втручанням у приватне життя
* Записи правоохоронних органів, які містять одну з перелічених проблем
* Інформація агентства від фінансових установ
* Геологічна та геофізична інформація щодо свердловин

**Закон про сімейні права на освіту та недоторканність особистого життя (FERPA)**

Цей федеральний закон надав студентам доступ до своїх документів про освіту. FERPA працює на основі принципу вибору, оскільки студент повинен затвердити розкриття інформації перед фактичним розкриттям. Коли студенту виповнюється 18 років або він вступає до вищого навчального закладу в будь-якому віці, ці права за FERPA переходять від батьків студента до самого студента.

**Закон США про боротьбу з шахрайством і зловживаннями (CFAA)**

Цей федеральний закон застосовується до онлайн-збору персональної інформації особами чи організаціями під юрисдикцією США від дітей віком до 13 років. Перш, ніж інформація може бути зібрана та використана від дітей (віком від 13 років і молодше), потрібно отримати дозвіл батьків.

**Закон про захист конфіденційності дітей в Інтернеті (COPPA)**

Цей федеральний закон застосовується до онлайн-збору персональної інформації особами чи організаціями під юрисдикцією США від дітей віком до 13 років. Перш, ніж інформація може бути зібрана та використана від дітей (віком від 13 років і молодше), потрібно отримати дозвіл батьків.

**Закон про захист дітей в Інтернеті (CIPA)**

Конгрес США прийняв CIPA у 2000 році для захисту дітей до 17 років від непристойних матеріалів.

**Закон про захист конфіденційності відео (VPPA)**

Закон про захист конфіденційності відео забезпечує таємницю особистих клієнтів компаній по прокату відеокасет, DVD та ігр, які взяті в оренду, і не будуть розкриті іншій стороні. Статут забезпечує захист за замовчуванням, тому компанія, що займається прокатом відео, отримує згоду орендаря відмовитися від захисту, якщо компанія хоче розкрити особисту інформацію про оренду. Багато захисників конфіденційності вважають VPPA найсильнішим законом про конфіденційність у США.

**Закон про спадкоємність і підзвітність медичного страхування**

Стандартні мандати гарантують фізичне зберігання, обслуговування, передачу та доступ до інформації про здоров'я людей. HIPAA доручає, щоб організації, які використовують електронні підписи, повинні відповідати стандартам, що забезпечують цілісність інформації, автентифікацію підписувача та непідтвердження.

**Канадський сенатський законопроект 1386 (SB 1386)**

Каліфорнія була першим штатом, який прийняв закон про повідомлення про несанкціоноване розкриття особистої ідентифікованої інформації. З тих пір багато інших штатів послідували за цим прикладом. Кожен з цих законів про розкриття інформації відрізняється від інших, що є передумовою для створення єдиного федерального закону. Цей акт вимагає від агентств надавати споживачам інформацію про їх права та обов'язки. Він зобов'язує штати повідомляти громадян про будь-які втрати чи розголошення PII. З часу прийняття SB 1386, численні інші штати моделювали законодавство навколо цього законопроекту.

**Політика конфіденційності**

Політики є найкращим способом забезпечення відповідності в організації і політика конфіденційності відіграє важливу роль в організації, особливо з численними законами, прийнятими для захисту конфіденційності. Одним з прямих результатів правових актів, пов'язаних з конфіденційністю, став розвиток необхідності дотримання корпоративної політики конфіденційності, пов'язаної із збиранням даних.

**Оцінка впливу на конфіденційність (PIA)**

Оцінка впливу на конфіденційність гарантує, що персоналізована інформація (ПІІ) буде належним чином оброблятися по всій організації.

* Встановити масштаб PIA.
* Визначте ключових зацікавлених сторін.
* Документуйте всі контакти з PII.
* Перегляньте юридичні та нормативні вимоги.
* Документуйте потенційні проблеми, що виникають при порівнянні вимог і практик.
* Перегляньте результати з основними зацікавленими сторонами.

# Міжнародні закони

З ростом Інтернету і глобальних мережних підключень, несанкціоноване проникнення в комп'ютерну систему або комп'ютерне вторгнення стало проблемою, яка може мати національні і міжнародні наслідки. Національні закони про комп'ютерні порушеннях існують у багатьох країнах, але завжди можуть бути прогалини в тому, як ці країни поводяться з цим видом злочинів.

**Конвенція про кіберзлочинність**

Конвенція про кіберзлочинність є першим міжнародним договором про злочини в Інтернеті (ЄС, США, Канада, Японія тощо). Загальні політики борються з кіберзлочинністю та стосуються таких проблем: порушення авторських прав, комп'ютерне шахрайство, дитяча порнографія та порушення безпеки мережі. Натисніть [тут](https://en.wikipedia.org/wiki/Convention_on_Cybercrime) щоб дізнатись більше про Конвенцію про кіберзлочинність.

**Інформаційний центр електронної конфіденційності (EPIC)**

EPIC сприяє забезпеченню конфіденційності та відкритих державних законів та політики у всьому світі та зосереджена на відносинах між ЄС та США. Натисніть [тут](https://epic.org/privacy/intl/) щоб отримати останні новини.

# Національна база даних вразливостей

Національна база даних вразливостей (NVD) - це державне сховище даних про стандарти керування вразливостями, яке використовує протокол автоматизації керування даними безпеки (SCAP). SCAP - це метод використання спеціальних стандартів для автоматизації керування вразливостями, вимірювання та оцінки відповідності політиці. Натисніть [тут](https://nvd.nist.gov/home.cfm) щоб відвідати веб-сайт Національної бази даних вразливостей.

SCAP використовує відкриті стандарти, щоб визначити недоліки безпеки та проблеми конфігурації програмного забезпечення. Специфікації організовують і вимірюють інформацію, пов'язану з безпекою, стандартизованими способами. Спільнота SCAP - це партнерство між приватним та державним сектором з метою просування стандартизації технічних операцій безпеки. Натисніть [тут](https://scap.nist.gov/) щоб відвідати веб-сайт протоколу автоматизації керування даними безпеки.

NVD використовує загальну систему оцінювання вразливості для оцінки впливу вразливостей. Організація може використовувати оцінки, щоб оцінити ступінь тяжкості вразливостей, які вона знаходить у своїй мережі. Це, в свою чергу, може допомогти визначити стратегію пом'якшення наслідків.

На сайті також міститься ряд контрольних списків, в яких містяться рекомендації по налаштуванню операційних систем і застосунків для забезпечення зміцненого середовища. Натисніть [тут](https://web.nvd.nist.gov/view/ncp/repository) щоб відвідати Національний реєстр контрольних списків.

# CERT

Інститут програмного забезпечення (SEI) в Університеті Карнегі-Меллона допомагає урядовим та галузевим організаціям розробляти, експлуатувати та підтримувати програмні системи, які є інноваційними, доступними та надійними. Це федеральний центр досліджень та розвитку спонсорований Міністерством оборони США.

CERT відділ SEI вивчає і вирішує проблеми в галузі кібербезпеки, включаючи вразливі місця в програмних продуктах, зміни в мережних системах та тренінги, що допомагають поліпшити кібербезпеку. CERT надає наступні послуги:

* Допомагає вирішувати уразливості програмного забезпечення
* Розробляє інструменти, продукти та методи проведення судових експертиз
* Розробляє інструменти, продукти та методи аналізу вразливостей
* Розробляє інструменти, продукти та методи моніторингу великих мереж
* Допомагає організаціям визначати, наскільки ефективними є їх практика безпеки

CERT має велику базу даних про вразливості програмного забезпечення та шкідливий код, що допомагає розробляти рішення та стратегії відновлення. Натисніть [тут](http://www.cert.org/) щоб відвідати веб-сайт CERT.

# nternet Storm Center

Internet Storm Center (ISC) надає безкоштовний аналіз та попередження для користувачів Інтернету та організацій. Він також співпрацює з постачальниками послуг Інтернету для боротьби з кібер-злочинцями. Internet Storm Center щодня збирає мільйони записів журналів із систем виявлення вторгнень з використанням датчиків, які охоплюють 500 000 IP-адрес у більш ніж 50 країнах. ISC ідентифікує сайти, які використовуються для атак і надає дані про типи нападів, здійснених проти різних галузей промисловості та регіонів світу.

Натисніть [тут](https://isc.sans.edu/) щоб відвідати Internet Storm Center. На веб-сайті пропонуються наступні ресурси:

* Архів журналу щоденного блогу InfoSec
* Підкасти, до яких належать Daily Stormcasts, щоденні 5-10 хвилин інфомації про загрози безпеки
* Оголошення про роботу в InfoSec
* Новини інформаційної безпеки
* Інструменти InfoSec
* Звіти InfoSec
* Форуми SANS ISC InfoSec

Інститут SANS підтримує Internet Storm Center. SANS є надійним джерелом навчання, сертифікації та досліджень в галузі інформаційної безпеки.

# Центр просунутої кібербезпеки

Центр просунутої кібербезпеки (ACSC) є некомерційною організацією, яка об'єднує промисловість, науку та уряд для вирішення сучасних кіберзагроз. Організація ділиться інформацією про кіберзагрози, займається дослідженнями та розробками в галузі кібербезпеки та створює освітні програми для просування професій в галузі кібербезпеки.

ACSC визначив чотири завдання, які допоможуть сформувати уявлення про його пріоритети:

* Побудова стійких систем, здатних до відновлення після атак і збоїв.
* Підвищення безпеки мобільних пристроїв.
* Розвиток обміну про загрози в режимі реального часу.
* Інтеграція кібер-ризиків з корпоративними ризиками.

Натисніть [тут](http://www.acscenter.org/) щоб відвідати Центр просунутої кібербезпеки.

# Сканери вразливостей

Сканер уразливостей оцінює слабкі сторони комп'ютерів, комп'ютерних систем, мереж або програм. Сканер уразливостей допомагає автоматизувати аудит безпеки шляхом сканування мережі на предмет наявності ризиків безпеки та створення пріоритетного списку для усунення слабких сторін. Сканер уразливостей шукає наступні типи вразливостей:

* Використання паролів за замовчуванням або часто використовуваних паролів
* Відсутність патчів
* Відкриті порти
* Неправильне налаштування операційних систем та програмного забезпечення
* Активні IP-адреси

Оцінюючи сканер уразливості, подивіться, наскільки він є точним, надійним, масштабованим та звітним. Існує два типи сканерів вразливостей для вибору: програмні або хмарні.

Сканування вразливостей є критичним для організацій з мережами, що включають велику кількість мережних сегментів, маршрутизаторів, брандмауерів, серверів та інших бізнес-пристроїв. Натисніть [тут](http://sectools.org/tag/vuln-scanners/) щоб переглянути декілька доступних варіантів для комерційних та безкоштовних версій.

# Тестування на проникнення

Тест на проникнення (pen testing) - це метод тестування слабких місць в системах за допомогою використання різні зловмисні методи. Тестування на проникнення не те ж саме, що тестування на вразливості. Тест на вразливості виявляє потенційні проблеми. Тестування на проникнення включає спеціаліста з кібербезпеки, який зламує веб-сайт, мережу або сервер з дозволу організації, намагаючись отримати доступ до ресурсів, у яких можуть міститися логіни, паролі та інше. Важливою різницею між кіберзлочинцями та фахівцями з кібербезпеки є те, що фахівці з кібербезпеки мають дозвіл організації на проведення тестів.

Однією з основних причин того, що організація використовує тестування на проникнення, є пошук і виправлення будь-якої вразливості перед тим, як її знайдуть кіберзлочинці. Тест на проникнення також відомий як етичний злам.

# Аналізатори пакетів

Аналізатори трафіку (або сніффери) перехоплюють і реєструють мережний трафік. Аналізатор пакетів захоплює кожен пакет, показує значення різних полів в пакеті і аналізує його вміст. Сніффер може захоплювати мережний трафік як у дротовій, так і у бездротовій мережі. Аналізатори пакетів виконують наступні функції:

* Аналіз проблем мережі
* Виявлення спроб втручання в мережу
* Ізоляція експлуатованої системи
* Ведення журналів трафіку
* Виявлення неправильного використання мережі

Натисніть [тут](https://en.wikipedia.org/wiki/Comparison_of_packet_analyzers) щоб побачити порівняння аналізаторів пакетів.

# Інструменти безпеки

Немає єдиного рішення, коли мова заходить про кращі інструменти безпеки. Багато чого буде залежати від ситуації, обставин та особистих уподобань. Спеціаліст з кібербезпеки повинен знати, куди йти, щоб отримати достовірну інформацію.

**Kali**

Kali - це дистрибутив безпеки Linux з відкритим вихідним кодом. ІТ-фахівці використовують Kali Linux для перевірки безпеки своїх мереж. Kali Linux включає понад 300 програм тестування на проникнення та аудиту безпеки на платформі Linux. Натисніть [тут](https://www.kali.org/) щоб відвідати веб-сайт.

**Мережна ситуаційна обізнаність**

Організація потребує можливості контролювати мережі, аналізувати отримані дані та виявляти зловмисну діяльність. Натисніть [тут](http://www.cert.org/netsa/tools/index.cfm) щоб отримати доступ до набору інструментів аналізу трафіку, розроблених CERT.

# Визначення ролей фахівців з кібербезпеки

Стандарт ISO визначає роль фахівців з кібербезпеки. Система ISO 27000 вимагає:

* Старший менеджер, відповідальний за ІТ та ISM (часто аудиторський спонсор)
* Спеціалісти з інформаційної безпеки
* Адміністратори безпеки
* Менеджер фізичної безпеки та контактів об'єктів
* Зв'язок з персоналом для HR питань, таких як дисциплінарні дії та тренінги
* Системні та мережні менеджери, архітектори безпеки та інші спеціалісти з інформаційних технологій

Посади в інформаційній безпеці можна розбити на наступні види:

* Персонал з розробки вимог забезпечує політики, керівні принципи та стандарти, а також включає консультантів, які проводять оцінку ризиків та розробляють продукти та технічні архітектури, та осіб старшого рівня в організації, які мають широкі знання, але не мають багато вузькопрофільних знань.
* Розробники є справжніми технічними спеціалістами, які створюють та встановлюють рішення безпеки.
* Персонал моніторингу керує інструментами безпеки, виконують функції моніторингу безпеки та вдосконалюють процеси.

Натисніть на кожну позицію інформаційної безпеки, яка відіграє ключову роль у будь-якій організації, щоб вивчити основні компоненти кожної з них.