МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **Механізми захисту інформації корпоративної мережі**

Студент групи СЗД-41 Огнєв Артем Євгенович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

Реферат

Актуальність теми. У сучасному світі, де цифрові технології проникають у всі сфери життя, захист інформації в корпоративних мережах є все важливим завданням. Злочинці та хакери постійно шукають шляхи для несанкціонованого доступу до конфіденційних даних компаній, що може призвести до серйозних фінансових втрат, порушення репутації та правових проблем. Тому розробка та впровадження ефективних механізмів захисту інформації стає надзвичайно важливим завданням для будь-якої корпоративної мережі. Сьогодні ми не зможземо уявити бізнес без невеликої локальної мережзі. Звязок робочих місць та серверів у мережах обміну інформації дає змогу синхронізувати роботу невеликої кількості робітників, офісів, підприємств чи урядових структур. Переоцінити вплив корпоративних мереж важко, бо майже кожна компанія бажає мати хочаб якусь маленьку корпораційну мережу, для того щоб оптимізувати роботу свої співрогбітникив та зробити їх більш продуктивними.

Об'єктом дослідження є методи та засоби захисту корпоративних мереж

Предметом дослідження є теоретичні, методологічні та практичні засади впровадження методів захисту корпоративних мереж.

Мета даного дослідження полягає в аналізі та оцінці методів захисту корпоративних мереж з метою розробки оптимальних рекомендацій методів забезпечення безпекиу корпоративних мережах.

Для досягнення вказаної мети виконуються такі основні задачі:

1. Аналіз систем захисту інформації корпоративних мереж.
2. Огляд технологій захисту інформації в корпоративних мережах.
3. Формування вимог до методів систем захисту корпоративних мереж
4. Формування рекомендацій щодо методів забезпечення безпекиу корпоративних мережах

Галузь застосування. Результатами створення рекомендацій, отриманими в ході виконання даної роботи можуть користуватися підприємаства при впровадженні систем захисту інформації корпоративних мереж під час планування політики безпеки компанії.

Зміст

Вступ

Захист інформації корпоративної мережі є надзвичайно важливим аспектом для будь-якої організації. У сучасному цифровому світі, де загрози та кібератаки стають все більш складними та винахідливими, захист інформації стає викликом, з яким стикаються компанії будь-якого розміру та галузі. Механізми захисту інформації в корпоративній мережі є комплексними системами, що включають в себе різноманітні технології, методи та процедури для запобігання несанкціонованому доступу, виявлення та вирішення

інцидентів безпеки, а також забезпечення конфіденційності, цілісності та доступності даних. Ця дипломна робота присвячена вивченню та аналізу механізмів захисту інформації в корпоративній мережі. Метою дослідження є розкриття різних аспектів захисту інформації, від використання технічних засобів до розробки політик та процедур безпеки. Дипломна робота покладається на базові принципи кібербезпеки, а також враховує актуальні тенденції та виклики, з якими стикаються організації в сфері захисту інформації. У рамках дослідження будуть розглянуті такі ключові аспекти механізмів захисту інформації, як: файрвол, авторизація та аутентифікація, системи виявлення та запобігання вторгнень, шифрування даних, резервне копіювання та відновлення, аналіз наслідків взлому та багато іншого. Крім того, буде проведений аналіз і створені рекомендації щодо ефективних механізмів захисту інформації в корпоративних мережах. Результати дослідження допоможуть організаціям удосконалити свої механізми захисту інформації, а також прийняти обґрунтовані рішення щодо вибору та впровадження відповідних технологій та практик безпеки. Ця дипломна робота виконує важливу роль у підвищенні рівня захищеності корпоративних мереж та сприяє забезпеченню цілісності, конфіденційності та доступності інформації. Таким чином, дослідження механізмів захисту інформації корпоративної мережі є актуальним та необхідним кроком у напрямку створення надійних та безпечних інформаційних середовищ.

1. Огляд систем захисту інформації у корпоративних мережах

1.1 Захист інформації у корпоративних мережах

Захист інформації у корпоративних мережах (далі – КМ) є критично важливою задачею, оскільки КМ зазвичай містять конфіденційні дані та цінну інформацію про підприємство чи галузь. У світі, де цифрова інформація стає все більш цінною та чутливою, компанії повинні забезпечувати високий рівень захисту своїх даних від несанкціонованого доступу, втрати або пошкодження. Особливо у вимірах корпоративних мереж, які об'єднують багато комп'ютерів, серверів та пристроїв. [1]

Корпоративна мережа (КМ) – це мережа, яка існує для оптимізації підприємства чи бізнес процесі в компанії будь якого напрямку. Серед користувачв, корпоративна мережа включає лише аутентифікованих співробітників підприємства чи бізнесу (рисунок 1). Також залежно від завдання та розміру підприємства, КМ можуть мати різні структури та типи обладнання. Захищеність залежить від політики безпеки компанії, яка використовує мережу. Можна з упевненістю сказати, що скрізь, де використовуються комп'ютерні системи, існує потенційна загроза законним власникам та користувачам цих комп'ютерів. Також треба звернути увагу на питання питання цнності самої інформації. Однак, у світовій комп'ютерній практиці прийнято, що інформація коштує рівно стільки, скільки коштує збитків від її втрати в поєднанні з видатками на її відновлення. [1]

Захист інформації в корпоративних мережах має декілька важливих цілей:

— Конфіденційність. Забезпечення конфіденційності даних є одним з найважливіших аспектів захисту. Компанії повинні використовувати механізми шифрування для захисту конфіденційних даних, щоб унеможливити їх читання чи розуміння несанкціонованими особами.

— Цілісність даних, означає забезпечення їхньої недоторканості та незмінності. Бізнеси повинні використовувати механізми контролю цілісності, які виявляють будь-які небажані зміни в даних та системах.

— Доступність. Забезпечення доступності даних та ресурсів є важливим аспектом корпоративного захисту. Це означає, що дозвіл на доступ до інформації та систем має бути належно контрольованим, а системи повинні бути стійкими до відмови та готовими до відновлення після інцидентів.

— Соціальний інжиніринг, крім технічних заходів, важливо навчати персонал компанії принципам безпеки та виявленню соціального інжинірингу. Це допомагає запобігти атакам, які базуються на маніпулюванні людей. [2]

Дані цілі захисту інформації в КМ, мають взаємозв'язок та вимагають комплексного підходу. Розробка та реалізація політики безпеки, регулярне оновлення програмного забезпечення, практика резервного копіювання та відновлення даних, аудит безпеки та навчання персоналу є важливими кроками для забезпечення надійного захисту інформації у корпоративній мережі. Один з найважливіших аспектів захисту інформації - це усвідомлення загроз і впровадження відповідних заходів безпеки. Компанії повинні бути готовими до сучасних кібератак та вміти адаптуватися до нових загроз, оскільки кіберзлочинці постійно розвиваються. Захист інформації передбачає використання різноманітних методів та технологій, таких як шифрування даних, фізична та логічна безпека, мережеві файрволи, системи виявлення вторгнень та багато інших. [2]

Шифрування даних - це процес перетворення інформації у зашифрований код, що забезпечує конфіденційність під час її передачі та зберігання. Воно гарантує, що навіть якщо дані потраплять у руки зловмисника чи несанкціонованої особи, вони будуть незрозумілі та непридатні для використання. Шифрування може застосовуватися на різних рівнях, від захисту окремих файлів до захисту цілої мережі. Крім шифрування, фізична та логічна безпека є важливими аспектами захисту інформації. Фізична безпека передбачає захист фізичного обладнання, серверних кімнат та інших приміщень від несанкціонованого доступу. Логічна безпека охоплює використання паролів, аутентифікацію користувачів, контроль доступу до ресурсів, мережеві файрволи та інші методи, що запобігають несанкціонованому доступу до системи.

Крім технологічних заходів, важливо також забезпечити свідомість і навчаність персоналу, бо захист інформації в корпоративних мережах - це складний та постійний процес, що вимагає поєднання технологій, організаційних моментів та психологічних аспектів. Користувачі мережі повинні бути свідомі та уникати ризиків, пов'язаних з кібербезпекою, і дотримуватися політик інформаційної безпеки компанії у якій працюють. Регулярні тренінги та навчання з кібербезпеки допомагають підвищити обізнаність персоналу та запобігти соціальному інжинірингу. Компанії повинні бути готовими до викликів кібербезпеки, постійно оновлювати свої методи та технології, а також бути прозорими та реагувати на потенційні інциденти безпеки.

Захист інформації повинен бути вбудованим у культуру компанії та стати пріоритетом на всіх рівнях організації, якщо такої культури в компанії немає, то в майбутньому велика вірогідність мати інформаційні витоки з КМ, хакерські атаки, або навіть внутрішнього крота, який буде заважати мережі правильно функцонувати (проводити диверсії, в иводити з ладу сервер створюючи багато сміттевих запросів у КМ, і т.д.).

Комп'ютерні мережі - це взаємодія людей і комп'ютерів, вони забезпечують швидку обробку інформації. Ідея об’єднати комп’ютери в цілі мережі з’явилася понад тридцять років тому, коли можливості процесорів та мережевого обладнання зросли, розвиток мережевих технологій значно прискорився.

На сьогоднішній день, корпоротивні мережі можна класифікувати за різними критеріями:

— Віддаленість комп'ютерів,
— призначення,
— топологія,
— перелік послуг,
— принципи керування,
— способи комутації,
— способи доступу,
— види середовища передачі,
— швидкість передачі даних. [2]

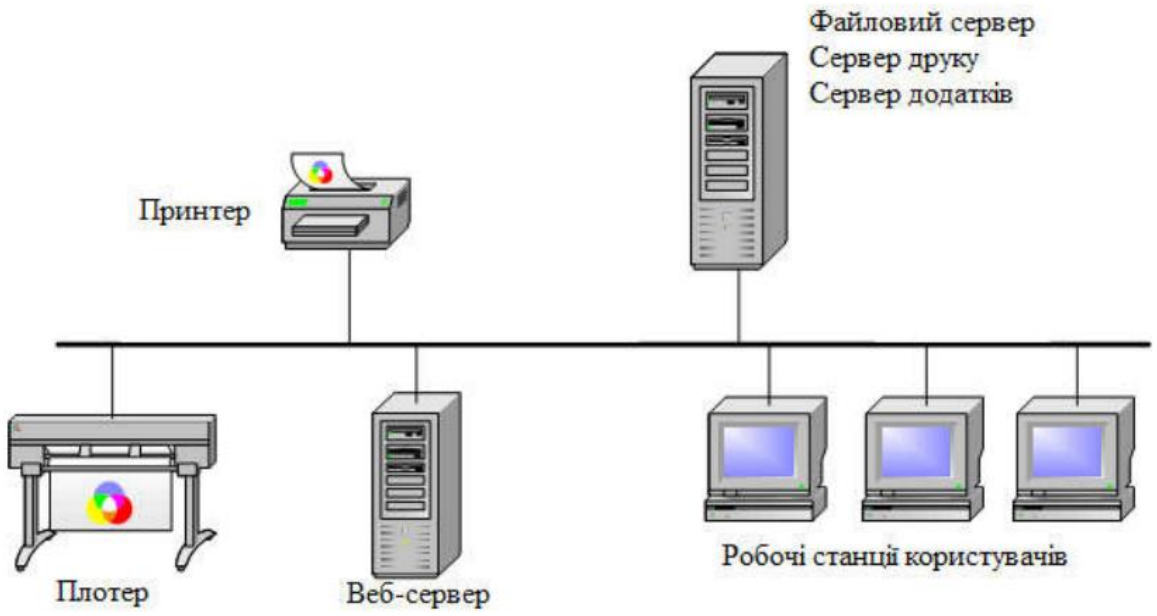

Рисунок - 1.1 Типова корпоративна мережа.

1.2 Важливість захисту інформації корпоративних структур.

Важливість захисту інформації корпоративних структур полягає у забезпеченні безпеки, конфіденційності та надійності даних, що належать компанії. У цифрову еру, коли обмін інформацією відбувається швидко та за допомогою різноманітних технологій, велика кількість даних є вразливою до кіберзагроз. Отже, захист інформації стає критично важливим для успіху та надійності корпоративних структур та мереж. Перш за все, захист інформації допомагає запобігти несанкціонованому доступу до конфіденційних даних компанії. Інформація про бізнес-процеси, клієнтів, фінансові операції та інші цінні активи можуть бути викрадені або використані несанкціонованими особами, що може призвести до серйозних фінансових втрат, зруйнувати репутацію компанії та правових проблем.[1]

Захист інформації забезпечує цілісність даних, це означає, що дані не піддаються несанкціонованій модифікації або порушенню. Зміна або втрата інформації може спотворити правильність прийняття рішень, спричинити

втрату довіри клієнтів та дуже нашкодити ділові процеси компанії. Тому захист інформації забезпечує збереження її цілісності та недоторканості. Крім того, захист інформації є важливим аспектом дотримання правових норм і вимог, що стосуються конфіденційності даних. Багато країн мають законодавство, що регулює обробку, зберігання та передачу конфіденційних даних, Україна також має стандарти захисту інформації та законодавство з інформаційної безпеки. Компанії повинні дотримуватися цих правових норм, аби уникнути штрафів, санкцій та інших правових проблем, пов'язаних з порушенням конфіденційності інформації. Окрім огляду законодавства, захист інформації в корпоративних структурах допомагає зберегти довіру клієнтів та партнерів. Захищена інформація гарантує конфіденційність та надійність бізнес-відносин, сприяє підвищенню репутації компанії та збільшенню задоволеності клієнтів. Клієнти та партнери повинні мати впевненість, що їхні дані будуть оброблені, а далі збережені в безпечному середовищі. В цілому, захист інформації в корпоративних структурах є важливим для забезпечення безпеки, конфіденційності та надійності даних. Він допомагає запобігти несанкціонованому доступу, зберегти цілісність даних, дотримуватися правових норм та зберегти довіру клієнтів і партнерів. Захист інформації повинен бути вбудованим у культуру компанії та стати пріоритетом на всіх рівнях організації. [3]

Захист корпоративної мережі надає численні переваги і вигоди для організації, такі як:

— Конфіденційність даних. Захист даних у корпоративній мережі дозволяє зберегти важливу інформацію про клієнтів, співробітників і т.д. Це потрібно для захисту комерційних та клієнтських

даних, бізнес-секретів, фінансової інформації та інших конфіденційних даних компанії чи навіть країни.

— Забезпечення цілісності даних. Захищена мережа дозволяє забезпечити цілісність даних, запобігаючи їхньому несанкціонованому зміненню або пошкодженню. Це гарантує, що дані залишаться недоторканними та незмінними протягом всього їхнього життєвого циклу, якщо власник цих даних не вирішить їх змінити, або замінити.

— Запобігання несанкціонованому доступу- ефективний захист мережі дозволяє запобігти несанкціонованому доступу до систем та ресурсів компанії. Це включає в себе контроль доступу до мережевих ресурсів, аутентифікацію та авторизацію користувачів, застосування механізмів ідентифікації та багатошарового захисту.

— Забезпечення неперервності бізнесу, означає що захищена мережа допомагає забезпечити неперервність бізнес-процесів, запобігаючи витоку чутливих даних, атакам та інших загрозам. Це дозволяє компанії продовжувати свою діяльність без перебоїв та мінімізувати вплив потенційних загроз на бізнес-операції.[3]

— Збереження репутації. Захист мережі допомагає зберегти репутацію компанії шляхом запобігання втраті даних клієнтів, порушенню конфіденційності або викриттю бізнес-секретів. Це важливо для підтримання довіри клієнтів, партнерів та інших зацікавлених сторін.

Загалом, хороший захист корпоративної мережі допомагає забезпечити безпеку, конфіденційність та надійність інформації, зберегти цілісність даних, запобігти несанкціонованому доступу та зберегти репутацію компанії. Хороший захист корпоративної мережі, створює умови для успішного функціонування бізнесу та досягнення поставлених цілей.

1.3 Аудит захисту корпоративної мережі.

Аудит захисту корпоративної мережі - це процес оцінки та перевірки заходів, політик, процедур та технологій, що використовуються для захисту корпоративної мережі. Його метою є виявлення потенційних загроз, недоліків, та недостатнього рівня безпеки мережі, що можуть призвести до порушення загальної безпеки даних або несанкціонованого доступу третій особі, або зловмиснику. Аудит захисту допомагає виявити слабкі місця в системі безпеки та розробити рекомендації для вдосконалення захисту й підвищення рівня безпеки мережі. [4]

Важливість аудиту систем безпеки корпоративних мереж полягає у тому, що аудит дозволяє організаціям перевірити ефективність власних безпекових заходів. Він допомагає виявити потенційні уразливості, недоліки в системах безпеки та потенційні кібер загрози. Насамперед аудит сприяє забезпеченню більш високого рівня безпеки в мережі та захисту конфіденційної інформації, проведення аудиту дозволяє виявити несанкціоновані доступи до мережі та попередити інциденти безпеки, сприяє дотриманню вимог стандартів безпеки та вимог безпекової політики компанії. Він допомагає ідентифікувати слабкі місця в системах безпеки та прийняти відповідні заходи, також допомагає забезпечити належну настройку та конфігурацію систем безпеки.

Він гарантує контроль за вторгненнями і зловживанням привілегіями в мережі, сприяє своєчасному виявленню та реагуванню на порушення безпеки, покращує освідомленість про безпеку серед працівників організації. Аудит допомагає виявити недостатню кваліфікацію адміністраторів мережі та спеціалістів безпеки, допомогає виявити недолікі у фізичній безпеці мережевих пристроїв та інфраструктури корпоративної мережі бізнесу.

Аудит сприяє підвищенню довіри клієнтів та партнерів організації до їх безпекових практик. Він забезпечує регулярну перевірку та оновлення безпекових заходів організації. Аудит допомагає забезпечити сталість безпекових процедур і запобігти їх знеціненню з часом.

Процес аудиту забезпечує оцінку стану безпеки системи, прийнятих безпекових рішень та сприяє введеню нових функій чи заміні старого обладняння на нове.[4]

Процес проведення аудиту захисту корпоративної мережі.

	— Зібрати відповідну документацію, включаючи політики, процедури, конфігураційні файли тощо. — Провести інтерв'ю зі спеціалістами, адміністраторами мережі та іншими зацікавленими сторонами для отримання детальної інформації про систему.
	— Визначити потенційні загрози, які можуть вплинути на безпеку мережі. — Оцінити ризики, пов'язані з цими загрозами, з урахуванням ймовірності виникнення та впливу на бізнес.
	— Перевірити, чи відповідає мережа встановленим стандартам безпеки та політикам компанії. — Перевірити виконання рекомендацій та вимог, що стосуються безпеки мережі.[5]
	— Провести технічну оцінку існуючих заходів безпеки, включаючи налаштування файрволу, систем виявлення вторгнень, аутентифікацію, шифрування тощо. — Виявити потенційні уразливості та слабкі місця в мережі.

	— Проаналізувати зібрані дані та результати перевірок. — Підготувати детальний звіт, в якому будуть вказані виявлені проблеми, рекомендації щодо поліпшення безпеки, а також прийняті заходи для їх усунення.
	— Зробити необхідні зміни та покращення в мережі згідно з рекомендаціями, після проведеного аудиту.
	— Постійно моніторити стан безпеки мережі та вчасно вживати потрібних заходів для попередження імовірних загроз і вразливостей у безпеці КМ. — Проводити повторні аудити для перевірки ефективності вжитих заходів безпеки інформаціїї у КМ, та для знаходження нових потенційних ризиків.[5]

Таблиця - 1.1 Виконання аудиту

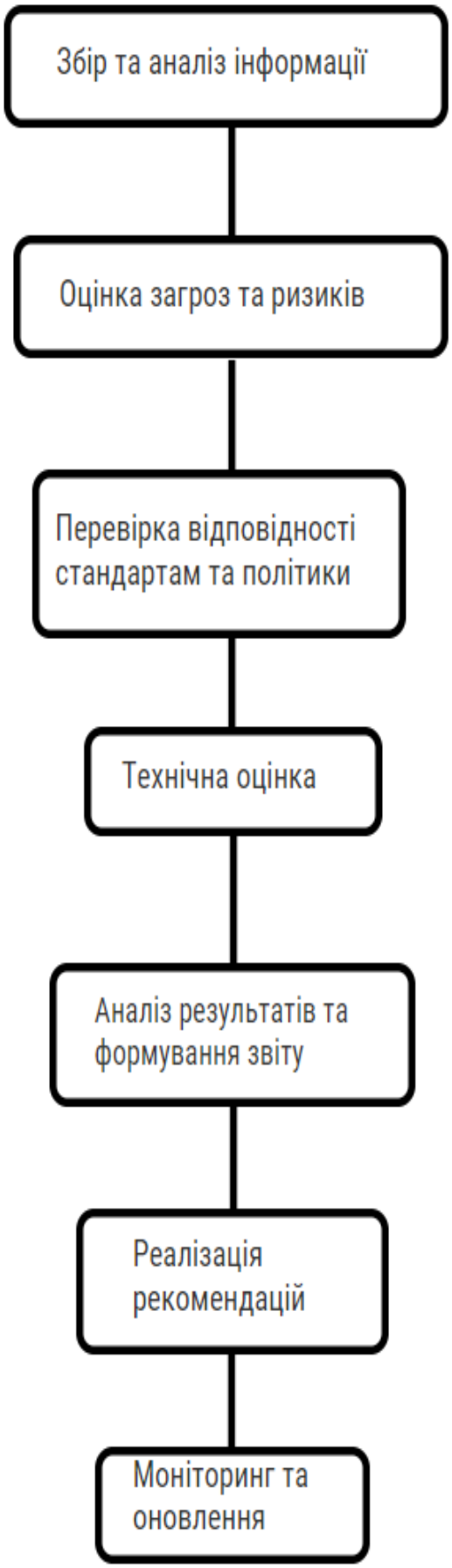

Рисунок - 1.2 Етапи проведення аудиту.

Варто зауважити, що кожен процес аудиту може бути унікальним і залежати від особливостей конкретної корпоративної мережі та її потреб. Також, для проведення аудиту можуть використовуватися спеціалізовані інструменти та методи, такі як сканування портів, тестування на проникнення тощо.

Для проведення аудиту корпоративної системи можуть використовуватись такі інструменти:

— Сканери вразливостей, дозволяють автоматично сканувати мережу та системи на наявність вразливостей і потенційних загроз.

— Журнали подій (лог-файли), записують інформацію про події, які відбуваються у системі, що дозволяє виявляти підозрілу або аномальну активність.

— Аналізатори трафіку, проводять моніторинг та аналізують мережевий трафік для виявлення підозрілої активності, атак або незвичайних підключень.

— Інструменти аудиту доступу, допомагають перевірити налаштування системи контролю доступу, права користувачів і груп, та виявити можливі недоліки.

— Аналізатори програмного забезпечення, використовуються для виявлення вразливостей і помилок у програмному забезпеченні, що використовується в корпоративній системі.

— Системи виявлення вторгнень (IDS/IPS), моніторять аномальну активність в мережі, спроб вторгнення або зловживання привілеями.

— Аудиторські звіти, створюються після аудиту для документування виявлених проблем, рекомендацій і результатів аудиту.

Дані інструменти допомагають проводити детальний аналіз системи, виявляти вразливості та ризики, контролювати доступ до даних та ресурсів, і підвищувати рівень безпеки корпоративної мережі.[5]

2. Технології захисту у корпоративних мережах.

2.1 Методи та засоби шифрування даних.

Шифрування даних - це процес перетворення звичайного тексту або даних у зашифрований код за допомогою спеціальних алгоритмів і ключів.

Шифрування даних в корпоративних мережах відіграє важливу роль у забезпеченні конфіденційності та захисту інформації, це процес перетворення звичайного тексту або даних у шифрований формат, який може бути розшифрований лише за допомогою спеціального ключа чи пристрою. Одною з головних переваг шифрування даних є захист від несанкціонованого доступу та перехоплення інформації. За допомогою шифрування, дані стають незрозумілими для потенційних зловмисників, які намагаються проникнути у мережу або перехопити передачу даних під час транспортування інформації по мережі. [6]

Крім того, шифрування даних забезпечує відповідність вимогам законодавства та нормативним актам щодо захисту конфіденційної інформації. Багато галузей, таких як: фінансові установи, медичні заклади чи фармацевтичних компаній, що працюють з особистими даними клієнтів, мають обов'язкові вимоги щодо шифрування даних. Також шифрування

дозволяє зменшити ризик втрати даних при фізичному зломі обладнання або крадіжці пристроїв. Шифровані дані не будуть доступні зловмисникам, навіть якщо вони отримають фізичний доступ до збереженої на них інформації.

Однак, важливо зазначити, що шифрування даних повинно супроводжуватись належними ключами та розробкою міцних політик безпеки. Недостатньо просто застосувати методи шифрування, необхідно також забезпечити безпеку ключів і їх правильне використання.

Узагалі, шифрування даних в корпоративних мережах є важливим елементом для захисту конфіденційності, цілісності та доступності інформації. Воно допомагає зменшити ризики несанкціонованого доступу та зловживання даними, а також забезпечує відповідність вимогам законодавства. Існує багато методів та засобів шифрування даних, які можуть бути використані для захисту конфіденційності та безпеки інформації в корпоративних мережах. Приведені далі методи шифрування даних дозволяють забезпечити конфіденційність, цілісність та надійність захисту інформації, а також зменшити ризики несанкціонованого доступу та зловживання даними в корпоративних мережах.[6]

Найпоширеніші методи шифруання данних у корпоративних мережах:

- Симетричне шифрування: Використовує один ключ як для шифрування, так і розшифрування даних. Алгоритми симетричного шифрування включають AES (Advanced Encryption Standard) та DES (Data Encryption Standard).
- Асиметричне шифрування: Використовує два ключі - публічний та приватний. Публічний ключ використовується для шифрування даних, а приватний ключ - для розшифрування. RSA та ECC

(еліптична криптографія) є популярними алгоритмами асиметричного шифрування.[7]

- Хеш-функції: Використовуються для створення унікального відбитка (хеша) вхідних даних. Хеш-функції, такі як SHA-256 (Secure Hash Algorithm) і MD5 (Message Digest Algorithm 5), дозволяють перевірити цілісність даних.
- Віртуальні приватні мережі (VPN): Використовують шифрування для створення безпечного тунелю між віддаленими корпоративними мережами або пристроями. VPN забезпечує конфіденційність даних під час їх передачі через незахищені мережі, такі як Інтернет.
- Шифрування дискового простору: Застосовується для шифрування цілого диска або його окремих розділів. Дозволяє забезпечити захист даних на зберігаючих пристроях, таких як жорсткі диски чи флеш-накопичувачі.
- Шифрування електронної пошти: Використовується для захисту вмісту електронних листів. Протоколи шифрування електронної пошти включають S/MIME (Secure/Multipurpose Internet Mail Extensions) та PGP (Pretty Good Privacy).
- SSL/TLS: Використовується для шифрування передачі даних між веб-сервером та веб-браузером. Забезпечує безпечне з'єднання і захищає конфіденційні дані, такі як особисті дані або банківські реквізити. [8]

SSL (Secure Sockets Layer) і TLS (Transport Layer Security) - це протоколи шифрування та безпеки, які використовуються для захищеної передачі даних через мережі, зокрема через Інтернет. SSL був розроблений як стандарт для

забезпечення безпеки під час передачі конфіденційних даних, наприклад: кредитні дані, особисті дані людини, облікові номери, тощо.

У свою чергу TLS став наступною версією протоколу SSL з метою поліпшення його безпеки та функціональності. SSL/TLS використовує криптографічні алгоритми для шифрування даних під час їх передачі, забезпечуючи конфіденційність та цілісність інформації. Це дозволяє встановити захищене з'єднання між веб-браузером та веб-сервером, а також між іншими типами клієнтських і серверних програм, це особливо корисно при використані у корпоративній мережі.8[]

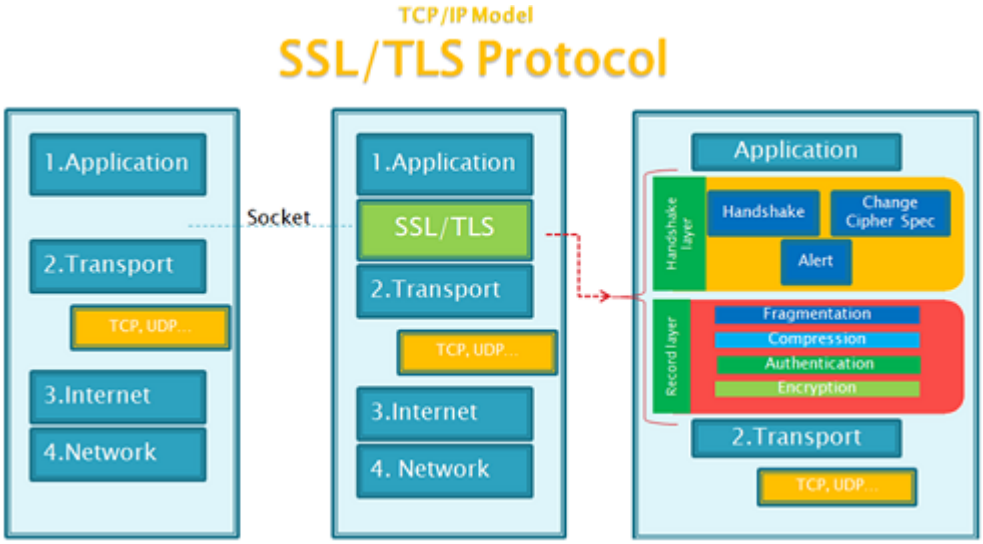

Рисунок - 2.1 Протокол SSL/TLS

Вагомі плюси для використання саме SSL/TLS:

— Конфіденційність, дані, які передаються між клієнтом і сервером, шифруються, що запобігає несанкціонованому доступу до них.
— Цілісність, інформація не може бути змінена під час передачі, оскільки будь-які зміни виявляються за допомогою цифрових підписів і хеш-функцій.
— Аутентифікація - SSL/TLS дозволяє перевіряти ідентичність веб-сервера, забезпечуючи впевненість, що користувач спілкується з правильним ресурсом.

— Довіреність, використовуються сертифікати, видані довіреними організаціями, які підтверджують, що сервер аутентичний та надійний.[8]

SSL/TLS є важливим механізмом захисту в корпоративних мережах, особливо при обміні чутливою інформацією. Він допомагає забезпечити конфіденційність клієнтських даних, захистити веб-додатки та безпеку комунікації між користувачами та серверами.

2.1.1 Використовування VPN у захисті корпоротивної мережі

У корпоративних мережах VPN (Virtual Private Network) використовується для створення безпечного тунелю зв'язку між віддаленими користувачами та ресурсами корпорації. Він дозволяє підключатися до корпоративної мережі з будь-якого місця, надаючи зручний та безпечний доступ до внутрішніх ресурсів.

Завдяки VPN віддалені користувачі можуть підключатися до корпоративних серверів та додатків, ніби вони фізично присутні в офісі. Всі дані, що передаються між віддаленим користувачем та корпоративною мережею, шифруються, що забезпечує конфіденційність та захист інформації.[9]

Використання VPN в корпоративних мережах дозволяє:

— Забезпечити безпеку та конфіденційність даних під час їх передачі через незахищені мережі, такі як Інтернет.
— Захистити віддалених користувачів від загроз, таких як перехоплення даних, зловмисні атаки та несанкціонований доступ.

— Забезпечити безпечний доступ до внутрішніх ресурсів корпорації, таких як файли, бази даних, додатки та інші корпоративні ресурси.
— Дозволити співробітникам працювати з будь-якого місця та пристрою, що забезпечує більшу гнучкість та продуктивність роботи.

Використання VPN у корпоративних мережах є важливим елементом кібербезпеки, що допомагає забезпечити безпечний та надійний доступ до корпоративних ресурсів навіть поза офісом. Використання VPN поліпшує роботу корпоративної мережі шляхом забезпечення безпеки, розширення географічного охоплення, контролю підключень та зниження ризиків зовнішніх загроз. Для коректної роботи VPN використовується VPN-агент.

VPN-агент - це програмне забезпечення, яке встановлюється на кінцевому пристрої (наприклад, комп'ютері, смартфоні або планшеті) та відповідає за встановлення та керування VPN-з'єднанням з VPN-сервером. Він забезпечує шифрування трафіку та передачу даних через захищений тунель між кінцевим пристроєм та корпоративною мережею. VPN-агенти також мають додаткові функції, такі як наприклал, автоматичне підключення до VPN під час запуску пристрою або управління налаштуваннями з'єднання.[9]

Функції VPN-агента:

— Шифрування трафіку. VPN-агент використовує криптографічні методи для захисту передачі даних між кінцевим пристроєм і VPN-сервером. Це забезпечує конфіденційність і недоступність інформації для сторонніх осіб.
— Захист від перехоплення, використовуючи VPN-агент, трафік перенаправляється через захищений тунель, що ускладнює можливість перехоплення чи перехвату даних зовнішніми атакуючими.

— Зміна IP-адреси, VPN-агент дозволяє змінити IP-адресу кінцевого пристрою, підключаючись до VPN-сервера. Це може бути корисно для забезпечення анонімності та обхіду обмежень доступу до контенту.
— З'єднання з корпоративною мережею. VPN-агент дозволяє віддаленим працівникам підключатися до корпоративної мережі з-за меж офісу, забезпечуючи безпечний доступ до внутрішніх ресурсів та даних.
— Управління налаштуваннями. Деякі VPN-агенти мають інтерфейс для налаштування параметрів з'єднання, таких як протокол шифрування, сервери VPN, автоматичне підключення тощо.

В цілому, VPN-агент гарантує безпеку, конфіденційність та зручність при використанні VPN-з'єднання у корпоративній мережі або в особистих цілях.[10]

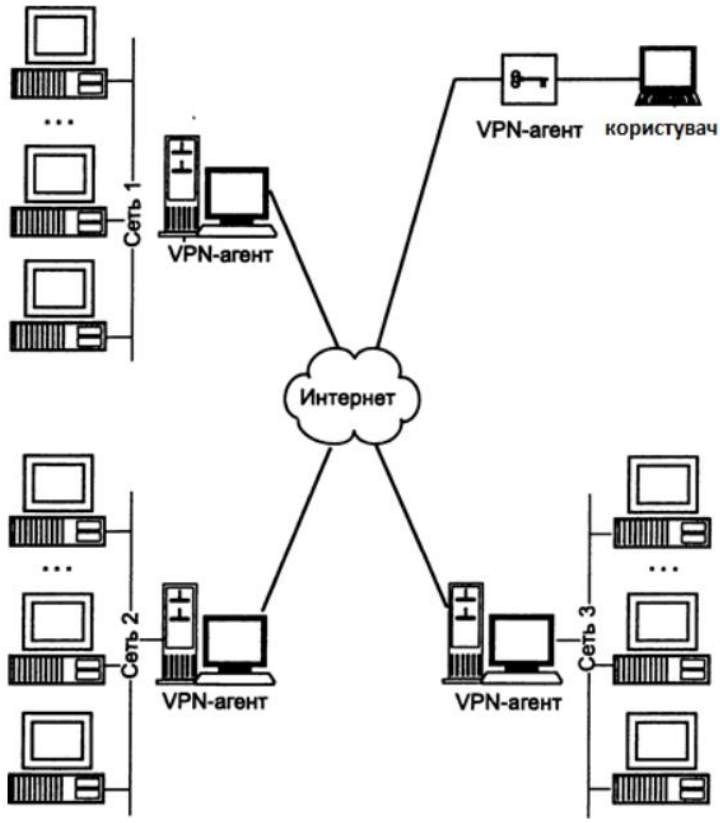

Рисунок - 2.2 Використання VPN у КМ

2.2 Використання антивірусного програмного забезпечення.

Антивірусне програмне забезпечення є критично важливим для забезпечення безпеки комп'ютерних систем та корпоративних мереж. Антивірусне ПЗ допомагає виявляти, блокувати і нейтралізувати шкідливі програми, такі як віруси, троянські програми, черв'яки, шпигунське ПЗ та інші загрози. Антивірусне ПЗ сканує систему на наявність вірусів та інших шкідливих програм, виявляючи їхні сигнатури або незвичну поведінку. Воно блокує вторгнення і нейтралізує загрози, перешкоджаючи їх поширенню та виконанню небажаних дій. Виявлення та блокування загроз, це основна користь та роль антивірусів у захисті корпоративної мережі та будь яких комп’ютерних систем. Використання антивірусного програмного забезпечення є необхідним елементом в захисті комп'ютерних систем та корпоративних мереж. Воно забезпечує надійний захист від шкідливих програм, зберігає конфіденційність даних і забезпечує стабільну та безпечну роботу системи.[11]

Також антивіруси корисні наступними функціями:

- Захист від нових загроз. Антивірусне ПЗ використовує оновлені бази даних, що містять інформацію про нові віруси та шкідливі програми. Це дозволяє виявляти й блокувати недавно з'явлені загрози, забезпечуючи актуальний рівень захисту.
- Система виявлення вторгнень. Багато антивірусних програм мають функції виявлення вторгнень, які спостерігають за незвичними або підозрілими активностями в системі. Вони

сповіщають про можливі загрози або небажані дії, що дозволяє прийняти відповідні заходи для захисту.

— Оптимізація продуктивності, антивірус забезпечує оптимізацію продуктивності системи, використовуючи мінімальні ресурси для своєї роботи. Воно працює в фоновому режимі, не заважаючи користувачам, але постійно перевіряє наявність загроз та вживає заходів для їх запобігання.

— Захист конфіденційності. Антивірусне ПЗ допомагає забезпечити конфіденційність інформації, запобігаючи її втраті або розголошенню через шкідливі програми. Воно блокує спроби доступу до конфіденційних даних та запобігає їх витоку.

— Забезпечення витривалості системи, хороший антивірус, допомагає зберегти цілісність та функціональність системи, запобігаючи впливу шкідливих програм на роботу комп'ютера. Воно допомагає уникнути втрати даних, пошкодження файлів і зниження продуктивності системи.

— Відстеження інцидентів безпеки. Багато антивірусних програм мають функції реєстрації та відстеження інцидентів безпеки. Вони записують спроби вторгнення, сповіщають про них та надають звіти для подальшого аналізу та вдосконалення захисту.[11]

Антивіруси також можуть вчасно повідомляти адміністратору про можливе шкідливе програмне забезпечення. Антивірус виявляє програми-кроти та інші небезпеки за допомогою різних методів та технологій, спрямованих на виявлення шкідливих програм та їхню класифікацію. Основні методи, які використовує антивірус, є: сигнатурний аналіз, аналіз поведінки, сканування пам’яті та веб-фільтрація.

Сигнатурний аналіз – це процес роботи антивіруса під час якого програмне забезпечення сканує бази даних сигнатур, які містять унікальні ідентифікатори або підписи відомих вірусів та шкідливих програм. Під час сканування файлів

антивірус порівнює їх з цими сигнатурами, щоб виявити відповідність і визначити, чи є файл інфікованим.

Аналіз поведінки – це процес роботи антивірусної програми, яка використовує метод аналізу поведінки, яка спостерігає за активністю програми та її взаємодії з системою. Цей сетод виявляє підозрілі або незвичні дії, які можуть свідчити про наявність шкідливої програми.

Сканування пам'яті – антивіруси можуть сканувати активну пам'ять комп'ютера для виявлення шкідливих процесів або вразливостей, які можуть бути використані вірусами для інфікування системи.

Веб-фільтрація – деякі антивірусні програми використовують технологію фільтрації веб-трафіку для виявлення і блокування інтернет сторінок або завантажуваного контенту, які можуть містити шкідливий код, програми кроти або віруси.[11]

Ці методи використовуються в антивірусних програмах для постійного моніторингу системи, виявлення шкідливих програм та запобігання їхньому поширенню. Комбінація цих методів дозволяє антивірусному ПЗ ефективно захищати комп'ютерну систему від різноманітних загроз і зберігати її безпеку.

2.3 Аутентифікація та авторизація.

Аутентифікація та авторизація є двома важливими процесами управління доступом в інформаційних системах і мережах.

Аутентифікація - визначає, чи є суб'єкт (наприклад, користувач) тим, за кого він себе видає. Аутентифікація може здійснюватися за допомогою різних факторів, таких як пароль, біометричні дані (відбиток пальця, розпізнавання обличчя тощо), картка доступу або двофакторна аутентифікація. Після успішної аутентифікації система визнає особу або пристрій як правильного і дозволяє продовжити процес.

Авторизація - визначає, які ресурси, функції або послуги можуть бути використані авторизованими особами. Авторизація забезпечує контроль над тим, що конкретний користувач або пристрій може робити в системі, і встановлює обмеження на основі прав доступу. Наприклад, користувач може мати право доступу лише до певних файлив, директорій або функцій, в залежності від своєї ролі або привілеїв.

Аутентифікація та авторизація взаємодіють у такий спосіб: після успішної аутентифікації, система перевіряє права доступу, пов'язані зі зазначеною ідентичністю, і надає відповідний рівень авторизації. Тобто, аутентифікація підтверджує, що особа або пристрій є вірним, а авторизація визначає, які дії чи доступ є дозволеними для цієї особи або пристрою. Узгоджений інтегрований процес аутентифікації та авторизації є основою безпеки інформаційних систем, оскільки вони дозволяють забезпечити впевненість у тому, що лише правильно ідентифіковані користувачі отримують доступ до ресурсів і мають визначені права для виконання необхідних операцій. [12]

Ключовими елементами безпеки аутентифікація та авторизація системи в тому числі є і систем (IDS/IPS).

Аутентифікація визначає процес перевірки та підтвердження ідентичності користувача, пристрою або системи. Це може включати введення облікових даних. Авторизація, з іншого боку, визначає права і повноваження, які має особа або пристрій після успішної аутентифікації. Вона встановлює,

які дії або ресурси доступні користувачу або пристрою. У контексті систем IDS/IPS, авторизація визначає, які операції можуть бути виконані користувачем, наприклад, перегляд алертів, налаштування правил виявлення або відправлення повідомлень про події.

Системи IDS/IPS використовують аутентифікацію та авторизацію для забезпечення безпеки та контролю доступу до своїх функцій та можливостей. Це дозволяє обмежити доступ до системи IDS/IPS тільки авторизованим користувачам або пристроям, які мають необхідні дозволи. Використання аутентифікації та авторизації взаємодіє з системою IDS/IPS, допомагаючи забезпечити безпеку, ідентифікувати авторизованих користувачів та контролювати їх доступ до функцій системи.[13]

Авторизація - це процес надання прав доступу користувачу, пристрою або системі після успішної аутентифікації. Вона визначає, які ресурси, функції чи послуги можуть бути використані авторизованими особами в корпоративній мережі. Ролью авторизації в корпоративних мережах є контроль доступу та забезпеченні обмежень щодо використання ресурсів. Після успішної аутентифікації, авторизація визначає, до яких даних, систем або функцій має право доступу конкретний користувач або пристрій. Це забезпечує виконання принципу "найменше привілеїв", де кожен користувач отримує доступ лише до тих ресурсів, які необхідні для виконання його обов'язків або завдань.

Авторизація забезпечує контроль над правами доступу та дозволяє установлювати політики безпеки, обмеження та розподіл привілеїв в корпоративній мережі. Вона дозволяє встановлювати групи доступу, рівні авторизації та обмеження на основі ролей, що спрощує управління правами

доступу та забезпечує захист конфіденційної інформації. Також авторизація грає важливу роль у виявленні та запобіганні несанкціонованим діям або зловживанню привілеями. Вона дозволяє встановлювати обмеження на основі правил та політик безпеки, визначає, хто має право вносити зміни до системи та інформації, виконувати критичні операції або отримувати доступ до конфіденційної інформації.

Таким чином, авторизація в корпоративних мережах відіграє роль фільтра, тому що лише правильно автентифіковані користувачі або пристрої отримують доступ до ресурсів та функцій, що забезпечує безпеку, конфіденційність та цілісність даних, а також уникнення потенційних загроз безпеці.[12]

Аутентифікація - це процес перевірки та підтвердження ідентичності користувача, пристрою або системи перед наданням доступу до ресурсів чи функцій корпоративної мережі. Роль аутентифікації у корпоративних мережах полягає в забезпеченні безпеки, в контролі доступу та в запобіганні несанкціонованого входу до системи. Аутентифікація дозволяє впевнитись, що особа або пристрій, які намагаються отримати доступ, є дійсними та мають необхідні дозволи. Це зменшує ризик несанкціонованого доступу до конфіденційної інформації, зловживання привілегіями та інших безпекових порушень.[12]

Аутентифікація може використовувати різні методи, такі як введення логіна та пароля, біометричні дані (відбиток пальця, розпізнавання обличчя), токени безпеки, сертифікати тощо. Ці методи дозволяють перевірити ідентичність користувача або пристрою перед наданням доступу до ресурсів мережі. Аутентифікація є важливою складовою безпеки корпоративних

мереж, оскільки дозволяє обмежити доступ до конфіденційної інформації лише авторизованим особам, забезпечує ідентифікацію користувачів та слідкує за їхніми діями. Це сприяє запобіганню несанкціонованому доступу, зловживанням та інцидентам безпеки, а також допомагає встановити відповідальність за вчинені дії. Усе це роблять аутентифікацію важливим елементом захисту корпоративної мережі та сприяє забезпеченню конфіденційності, цілісності та доступності інформації.[12]

Двофакторна аутентифікація (2FA), також відома як дворівнева авторизація або двоетапна перевірка, є методом захисту доступу, який вимагає від користувача подання двох незалежних факторів аутентифікації для підтвердження своєї ідентичності. Це додатковий шар безпеки, який зменшує ризик несанкціонованого доступу до системи.

Зазвичай двофакторна аутентифікація включає комбінацію чогось, що користувач знає (наприклад, пароль або ПІН-код) і чогось, що користувач має (наприклад, фізичний пристрій, такий як смартфон або ключ-токен) або що користувач є (наприклад, біометричні дані, такі як відбиток пальця або розпізнавання обличчя). Прикладами є введення пароля разом з одноразовим кодом, отриманим через смс або мобільний додаток, або використання біометричних даних разом з паролем. Тож, завдяки двофакторній аутентифікації, якщо хтось зламає чи вкраде користувацький пароль, він не зможе отримати доступ до системи без додаткової дії аутентифікації. Це значно підвищує безпеку, оскільки необхідно мати обидва фактори для успішного входу в систему. Двофакторна аутентифікація є ефективним способом захистити особисті дані, фінансову інформацію та конфіденційну інформацію у корпоративних мережах.[14]

2.3.1 Системи виявлення та запобігання вторгнень (IDS/IPS).

IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) - це системи виявлення та запобігання вторгненням в комп'ютерну мережу або систему.

IDS використовується для виявлення небезпечних або недозволених дій, атак або аномалій, які можуть відбуватися у мережі. Він аналізує мережевий трафік, журнали подій та інші джерела інформації для виявлення підозрілих патернів або зловмисних дій. IDS може сповістити про аномальність або потенційну атаку, але не має можливості безпосередньо блокувати атаку або вторгнення.

IPS володіє розширеними можливостями порівняно з IDS. Він не тільки виявляє потенційні атаки або вторгнення, але й активно приймає заходи для їх запобігання або заблокування. Це може включати блокування певного трафіку, відправку попереджень адміністраторам, відключення підозрілих вузлів або автоматичне застосування заходів безпеки.

IDS/IPS використовуються для підвищення безпеки корпоративних мереж, виявлення шкідливого трафіку, запобігання атакам та вторгненням. Вони допомагають ідентифікувати загрози, реагувати на них та забезпечувати безпеку мережі та інформації. Завдяки IDS/IPS, компанії можуть бути більш свідомими про потенційні загрози та здійснювати вчасні заходи для їх запобігання та захисту своїх систем.[13]

IDS/IPS (Intrusion Detection System/Intrusion Prevention System) є важливими складовими засобами захисту корпоративних мереж від зловмисних атак. Вони мають свої плюси і мінуси, які слід враховувати при їх впровадженні. Ось кілька плюсів та мінусів IDS/IPS:

Плюси IDS/IPS:

— Виявлення загроз: IDS/IPS можуть виявляти широкий спектр загроз, включаючи вторгнення, шкідливі програми, аномалії в мережевому трафіку та інші атаки.

— Реакція в реальному часі: IDS/IPS дозволяють виявляти загрози майже в реальному часі і приймати заходи для їх припинення або запобігання.
— Захист мережі: Вони забезпечують активний захист мережі, блокуючи атаки та запобігаючи їх поширенню в системі.
— Запобігання втратам даних: IDS/IPS можуть допомогти виявити спроби незаконного доступу до цінної інформації та запобігти втраті даних.[13]

Мінуси IDS/IPS:

— Велика кількість ложнопозитивних сигналів. IDS/IPS можуть генерувати велику кількість ложнопозитивних сигналів, що потребує великого обсягу ресурсів для перевірки та обробки.
— Складність налаштування. Правильна настройка та конфігурація IDS/IPS може бути складною задачею, вимагаючи глибокого розуміння мережевої інфраструктури та вміння виявити та налаштувати правила для конкретних загроз.
— Відсутність повного захисту, IDS/IPS можуть бути обмежені виявленням нових атак або шкідливих програм, які ще не відомі системі, що може залишити мережу вразливою до нових загроз.
— Потреба в постійному оновленні. IDS/IPS потребують постійного оновлення, включаючи оновлення бази даних відомих загроз, щоб виявляти нові типи атак.[13]

Ці плюси і мінуси слід ретельно зважувати при впровадженні IDS/IPS в корпоративну мережу, забезпечуючи належний рівень захисту та враховуючи особливості організації і потреби в безпеці.

2.4 Файрвол та як його використовують у захисті корпоративної мережі.

Терміни "брандмауер" і "файрвол" використовуються як синоніми і вказують на одну й ту ж систему захисту мережі. Брандмауер (firewall) і файрвол (firewall) означають програмний або апаратний захисний механізм, який контролює трафік, що проходить через мережу, і встановлює правила доступу на основі заданих політик безпеки. Його основна мета полягає в запобіганні несанкціонованому доступу, фільтрації небажаного трафіку та забезпеченні безпеки мережі.

Файрвол є основним засобом захисту мережі в рамках системи керування корпоративною безпекою (КМ). Це програмна або апаратна система, яка контролює вхідний та вихідний мережевий трафік і встановлює правила доступу на основі заданих політик безпеки. Файрвол дозволяє організаціям створювати обмеження і контролювати комунікацію між різними частинами мережі, а також між мережею і зовнішнім середовищем, забезпечуючи безпеку та захист інформації.[15]

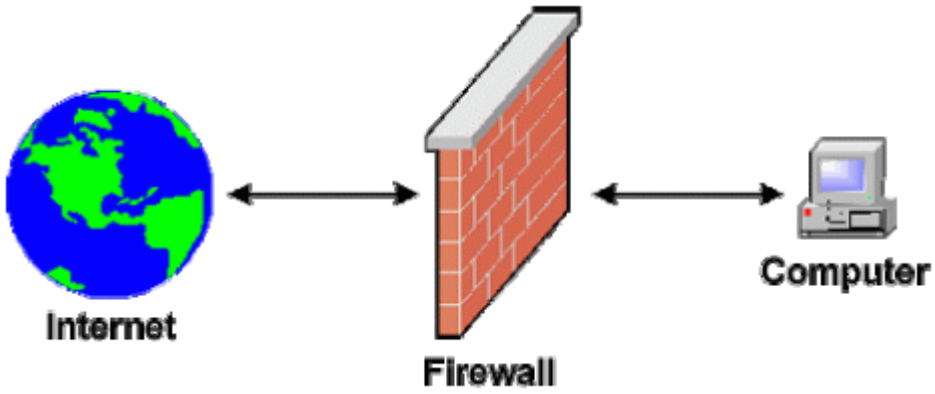

Рисунок - 2.3 Файрвол

Основні функції файрволу в КМ, це Захист від несанкціонованого доступу, фільтрація трафіку, сегментація мережі, моніторинг та аналіз трафіку, забезпечення виконання політик безпеки.

Захист від несанкціонованого доступу. Брандмауер контролює трафік, що входить до мережі, і блокує небажані або потенційно шкідливі підключення. Він виявляє та блокує спроби несанкціонованого доступу, такі як вторгнення або зловживання правами доступу.

Фільтрація трафіку. Файрвол перевіряє пакети даних, що проходять через нього, згідно з налаштованими правилами. Він фільтрує небажаний трафік, такий як шкідливі програми, віруси або спам, що сприяє покращенню ефективності мережі і зменшенню ризиків безпеки.

Сегментація мережі. Брандмауер дозволяє розділяти мережу на логічні сегменти та контролювати комунікацію між ними. Це допомагає управляти доступом до різних рівнів конфіденційності та обмежувати поширення загроз у разі компрометації одного з сегментів мережі.

Моніторинг та аналіз трафіку. Файрвол здатний аналізувати мережевий трафік що проходить через нього та документувати його. Це дозволяє виявляти підозрілі активності, вторгнення або аномалії в мережі, що потенційно може допомгти у розслідуванні та реагуванні на потенційні загрози безпеки.

Забезпечення виконання політик безпеки, це означає що файрвол виконує налаштовані правила та політики безпеки, які визначають правила доступу до ресурсів мережі, обмеження комунікації та контроль за використанням мережевих послуг. Він гарантує, що доступ до мережі та ресурсів надається лише авторизованим користувачам, забезпечуючи безпеку та конфіденційність інформації.[15]

Файрволи, як будь-який інший елемент системи безпеки, також можуть бути піддані різноманітним загрозам. Ось деякі загрози, з якими можуть стикатися файрволи:

— Атаки на файрвол під час авторизації. Хакери можуть спробувати знайти слабкі місця у файрволі, щоб отримати несанкціонований доступ до мережі.[15]

— Denial of Service (DoS) атаки: Нападники можуть намагатися перевантажити файрвол широким потоком недійсних або зловмисних запитів, що може призвести до відмови в обслуговуванні легітимного трафіку. DoS розшифровується як "Denial of Service", що означає "Відмова в обслуговуванні". Це тип атаки, в якій зловмисники намагаються перевантажити ресурси системи чи мережі таким чином, що легітимні користувачі не можуть отримувати послуги або доступ до ресурсів. Під час DoS-атаки, зловмисники використовують різні методи для перевантаження цільової системи, такі як надсилання великої кількості запитів, заборона доступу до послуг або ресурсів, або злам системи таким чином, що вони стають недоступними для легітимних користувачів. Ці атаки можуть призвести до недоступності важливих послуг або ресурсів, впливати на роботу корпоративних мереж і спричиняти фінансові втрати. Наприклад, атака DoS може призвести до перевантаження мережевих пристроїв або серверів, що призведе до відмови в обслуговуванні легітимних користувачів. Для захисту від атак DoS використовуються різні методи, такі як фільтрація трафіку, налаштування мережевих пристроїв для виявлення та блокування підозрілого трафіку, використання загальних послуг захисту мережі, таких як файрволи та IPS (Intrusion Prevention System), а також готовність до відновлення після атаки, включаючи резервне копіювання даних та резервування ресурсів. Запобігання атакам DoS є важливою складовою безпеки корпоративних мереж, оскільки воно забезпечує надійну доступність та функціонування системи для легітимних користувачів, запобігає потенційним втратам часу та ресурсів, а також допомагає зберегти репутацію організації.[16]

— Проникнення через додатки – Якщо файрвол не належним чином налаштований або оновлюється, зловмисники можуть використовувати вразливості в програмному забезпеченні, що використовується файрволом, для проникнення у систему.
— Витік інформації – Якщо файрвол неправильно налаштований або належним чином не відфільтровує трафік, то можуть виникати ситуації, коли конфіденційна інформація може витікати з мережі.
— Соціальна загроза. Зловмисники можуть намагатися обійти файрвол шляхом використання маніпуляцій або переконування персоналу компанії чи відділу, для отримання несанкціонованого доступу до мережі.[15]

Це лише кілька загроз, з якими можуть стикатися файрволи. Для забезпечення ефективного захисту важливо налаштувати та оновлювати файрволи згідно з найкращими практиками та використовувати інші заходи безпеки, щоб зменшити ризики та забезпечити надійний захист мережі.

Загалом, файрвол в КМ є ключовим компонентом захисту корпоративної мережі, допомагаючи запобігати несанкціонованому доступу, фільтрувати небажаний трафік, контролювати комунікацію та забезпечувати виконання політик безпеки. Він є необхідним інструментом для забезпечення безпеки та надійності мережевого середовища в корпоративних структурах.[15]

3 Процес захисту інформації у корпоративних мережах.

3.1 Резервне копіювання та відновлення даних.

Резервне копіювання — це процес створення копії даних на спеціальних носіях (стримери, дискові масиви тощо), призначений для відновлення даних на їх основне місце розташування у разі пошкодження або знищення. Резервне

копіювання необхідно для швидкого і недорогого оновлення інформації (документів, програм) у разі втрати робочої копії інформації з будь-якої причини. Важливо зберігати носій резервних копій окремо від вихідних даних.

Повне резервне копіювання зазвичай впливає на всю операційну систему та всі дані. Створення тижневих, місячних і квартальних архівів передбачає повне резервне копіювання. Перше щотижневе резервне копіювання має бути повним резервним копіюванням, яке зазвичай виконується в п’ятницю або на вихідних, і повинно створювати резервні копії всіх потрібних файлів. Подальші резервні копії, з понеділка по четвер до наступного повного резервного копіювання, можуть бути додатковими або диференціальними, щоб заощадити час і простір на носіях. Повну резервну копію потрібно робити принаймні щотижня.[17]

Диференціальне резервне копіювання, передбачає копіювання кожного файлу, який змінився з часу останнього повного резервного копіювання. Дане резервне копіювання пришвидшує процес відновлення та вимагає лише останньої повної та останньої диференціальної резервної копії для відновлення. Диференціальне резервне копіювання стає все популярнішим, оскільки всі копії файлів створюються в певні моменти часу, що, наприклад, дуже важливо у випадку вірусна інфекція.

Інкрементне або додаткове резервне копіювання (incremental backup) передбачає копіювання лише тих файлів, які були змінені з часу останнього повного або додаткового резервного копіювання. Подальше інкрементне резервне копіювання додає лише файли, які змінилися після попереднього інкрементного резервного копіювання. Це резервне копіювання займає менше часу, оскільки копіюється менше файлів.Однак процес відновлення даних займає більше часу, оскільки необхідно відновити дані з останньої повної резервної копії та дані з усіх наступних додаткових резервних копій. У цьому випадку, на відміну від диференціального резервного копіювання, нові або змінені файли не замінюють старі, а додаються на носій самостійно.[17]

Реплікація даних - це віддалене резервне копіювання, яке, на відміну від звичайного резервного копіювання, передбачає виділення додаткових ресурсів, таких як віддалені системи архівування, підключені до ICS організації через канали зв'язку. Різноманітність схем і варіантів тиражування даних дає можливість вибрати найбільш ефективне і раціональне рішення для кожної конкретної задачі.

Періодична реплікація або планова, допомагають зберігати копію даних у фіксований момент часу у минулому у віддаленому місці. Основним недоліком цього методу є втрата актуальності даних протягом періоду часу, який дорівнює інтервалу між реплікаціями. Однак планова реплікація є дуже рентабельним рішенням для організацій, де час відновлення не є критичним і допустима невелика втрата даних.

Синхронна реплікація – гарантує високий рівень надійності, забезпечуючи ідентичність усіх копій даних. З високими вимогами до каналів зв'язку синхронна реплікація найчастіше використовується для найважливіших програм, де потрібен максимальний захист даних.

Асинхронна реплікація – забезпечує безперервність передачі даних, навіть якщо канали зв'язку нестабільні.Цей метод допомагає підтримувати високу продуктивність інформаційних систем і контролювати завантаження каналів передачі даних, але не забезпечує такого ж високого рівня релевантності даних, як синхронна реплікація.

Останнім часом часто використовуються багаторазові схеми реплікації, коли дані передаються з основного обчислювального центру відразу в кілька резервних центрів. Часто в таких випадках використовуються навіть різні методи реплікації для більш надійного та комплексного захисту даних.

Реплікація даних має деякі переваги перед традиційними методами резервного копіювання:

— дистанційне копіювання не вимагає участі користувача і забезпечує необмежений час зберігання даних;
— Деякі віддалені служби резервного копіювання можуть працювати безперервно, копіюючи зміни до файлів. Однак реплікація має кілька важливих[17]

У разі втрати або пошкодження оригінальних даних, резервна копія може бути використана для відновлення втрачених або пошкоджених файлів та інформації. Це дозволяє організаціям забезпечити неперервну доступність та цілісність даних, а також зменшити ризик втрати важливої інформації. Резервне копіювання також відіграє важливу роль у відновленні даних після випадків, як от технічні несправності, вірусних атак, природних катастроф або навіть випадкового видалення файлів. Воно дозволяє підтримувати бізнес-процеси без перебоїв та забезпечує більш високий рівень надійності та відновлюваності інформації. Основні принципи резервного копіювання включають регулярність створення копій, зберігання копій у безпечних місцях, перевірку цілісності копій, а також тестування процедур відновлення. Всі ці заходи спрямовані на забезпечення ефективного резервного копіювання та максимальне відновлення даних в разі необхідності.

Є багато різних пристроїв та засобів, які використовуються для резервного копіювання даних, з розповсюджених можна виділити:

Зовнішні жорсткі диски – це простий і доступний спосіб зберігання резервних копій даних. Зовнішній жорсткий диск підключається до комп'ютера або сервера і може бути використаний для збереження копій важливих файлів та папок.[18]

Рисунок - 3.1 Зовнішній жорсткий диск

Мережеві пристрої зберігання (NAS) – NAS пристрої дозволяють створювати мережеве сховище для резервного копіювання даних. Вони підключаються до мережі і можуть забезпечувати централізоване зберігання копій для кількох комп'ютерів або серверів.[19]

Рисунок - 3.2 Пристрої резервного копіювання даних (NAS)

Хмарні сховища. Хмарні сховища є популярним варіантом для резервного копіювання даних. Вони дозволяють зберігати копії даних в інтернет-хмарі, що забезпечує доступ до них з будь-якого місця та пристрою з Інтернет-підключенням.

Внутрішні сервери зберігання (SAN) – SAN системи є потужними пристроями, які забезпечують централізоване зберігання даних для корпоративних мереж. Вони можуть використовуватись для резервного копіювання і забезпечення високої доступності даних, являє собою великий сервер компанії.[20]

Рисунок - 3.3 SAN системи

Спеціалізовані програми резервного копіювання. Існують різні програмні засоби, які спеціально розроблені для проведення резервного копіювання даних. Вони надають функції автоматичного резервного копіювання, планування, шифрування та відновлення даних.

Ці пристрої та програмні засоби можуть використовуватися окремо або в поєднанні, залежно від потреб користувача та масштабу інфраструктури.

Відновлення даних - це процес відновлення втрачених або пошкоджених даних до їх попереднього стану. Це важлива процедура, яка забезпечує можливість відновити доступ до цінної інформації, яка була втрачена через помилки, випадкове видалення, атаки зловмисників або технічні проблеми.

Відновлення даних зазвичай починається з ідентифікації втрачених або пошкоджених даних. Потім необхідно визначити джерело резервних копій, де зберігаються дані, що можуть бути використані для відновлення. Для цього можуть використовуватися зовнішні жорсткі диски, мережеві пристрої зберігання, хмарні сховища або інші носії інформації. Після визначення

джерела резервних копій проводиться процес відновлення даних. Це включає копіювання або відновлення втрачених або пошкоджених файлів з резервних носіїв на їхнє початкове місце призначення. Після відновлення даних рекомендується перевірити їх цілісність, щоб переконатися, що вони не пошкоджені. Це може включати перевірку хеш-сум, контрольних сум або інших механізмів перевірки цілісності.[21]

Окрім самого процесу відновлення, важливим етапом є також тестування функціональності відновлених даних. Це допомагає переконатися, що дані працюють так, як очікується, і що системи або програми, які використовують ці дані, працюють належним чином. Після успішного відновлення даних рекомендується оновлювати резервні копії для забезпечення подальшого захисту від втрати або пошкодження даних. Таким чином, резервне копіювання і відновлення даних є важливими елементами стратегії забезпечення надійності та безпеки корпоративних мереж.

Тестування функціональності відновлених даних є важливою частиною процесу відновлення. Його основна мета - переконатися, що відновлені дані працюють належним чином і можуть бути використані для відновлення нормальної роботи системи або програми.

Під час тестування функціональності відновлених даних перевіряються різні аспекти їх роботи. Наприклад, перевіряється, чи можуть відновлені файли бути відкриті і прочитані, чи можуть дані бути записані знову у систему, чи зберігається правильна структура і формат файлів. Тестування може включати перевірку взаємодії відновлених даних з іншими системами або програмними засобами. Наприклад, переконатися, що відновлені бази даних працюють з програмами, які до них звертаються, або що відновлені файли можуть бути використані в програмах, які їх використовують.

Тестування функціональності може включати перевірку продуктивності системи після відновлення даних. Наприклад, переконатися, що система працює з заданою швидкістю, що відновлені дані не сповільнюють роботу

системи і не викликають проблем з продуктивністю. У результаті тестування функціональності відновлених даних можна зробити висновки про їхню готовність до використання. Якщо тестування показує, що дані працюють належним чином і відновлення було успішним, то можна продовжувати нормальну роботу з системою або програмою, використовуючи відновлені дані.

3.2 Виявленя та реагування на взлом корпоративної мережі.

Виявлення взлому корпоративної мережі є важливою задачею для забезпечення безпеки мережі, системи і даних. Цей процес включає пошук, аналіз і реагування на ознаки незвичайної або підозрілої активності, що може свідчити про несанкціонований доступ до мережі. Один з способів виявлення взлому – це моніторинг системних журналів та мережевої активності. При цьому аналізуються записи про спроби неавторизованого доступу, незвичайну активність або аномалії у поведінці системи чи мережі. Також можуть використовуватися системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), які спеціалізуються на виявленні й запобіганні атакам.

Поряд з моніторингом активності, важливо також аналізувати логи, журнали подій та іншу інформацію, що вказує на можливі підозрілі дії або вразливості системи. Для цього можуть застосовуватися спеціалізовані інструменти, такі як системи управління інцидентами безпеки (SIEM), які збирають і аналізують дані з різних джерел для виявлення зловмисної активності.

SIEM (Security Information and Event Management) - це системи управління інформацією та подіями безпеки. Вони спеціалізовані програмні

рішення, призначені для збору, агрегації, аналізу та візуалізації інформації про безпекові події та події зв'язані зі станом безпеки в корпоративних мережах. Робота SIEM систем базується на зборі лог-файлів, журналів подій, мережевої активності та інших даних з різних джерел, таких як файрволи, IDS/IPS системи, антивірусні програми, сервери та мережеві пристрої. Ці дані індексуються і аналізуються з використанням різних алгоритмів та правил, які дозволяють виявляти аномальну або підозрілу активність.

SIEM системи можуть використовувати бази даних інцидентів та підозрілих сценаріїв, що допомагають визначити потенційні загрози та виявляти незвичайні активності на основі попередньо встановлених правил. Вони також можуть використовувати технології машинного навчання та штучного інтелекту для виявлення складних зразків атак. Після аналізу даних SIEM системи забезпечують візуалізацію результатів, генерацію звітів та сповіщення про виявлені аномалії або підозрілу активність. Це дозволяє командам безпеки реагувати на потенційні загрози, приймати відповідні заходи для запобігання інцидентам та вживати кроки для зміцнення безпеки мережі.[22]

SIEM системи грають важливу роль у забезпеченні безпеки корпоративних мереж, допомагаючи виявляти, аналізувати та реагувати на загрози безпеки у реальному часі, а також вдосконалювати стратегії безпеки на основі накопиченої інформації та статистики.

Використання SIEM систем включає кілька ключових кроків.

По-перше, необхідно встановити SIEM систему та налаштувати її для збору даних з різних джерел в мережі. Дані можуть включати лог-файли, журнали подій, мережеву активність тощо.

По-друге, необхідно налаштувати правила аналізу та виявлення подій. Це можуть бути правила, які визначають нормальну активність, а також

правила, які виявляють підозрілу або аномальну активність. Правила можуть бути налаштовані з урахуванням конкретних потреб та характеристик мережі.

По-третє, SIEM система буде аналізувати дані, використовуючи встановлені правила та алгоритми. Вона буде шукати збіги, аномалії та підозрілу активність на основі зазначених правил. Якщо буде виявлено підозрілу активність, система може надсилати сповіщення або активувати автоматичні заходи безпеки.

По-четверте, важливо реагувати на виявлені події та загрози. SIEM система може надавати звіти та візуалізації результатів, що допомагають команді безпеки прийняти відповідні заходи. Це може включати розслідування подій, прийняття заходів для блокування загроз, вживання запобіжних заходів та оновлення стратегій безпеки.

Взагалі, використання SIEM систем вимагає налагодження інтеграції з різними системами та джерелами даних, правильного налаштування правил та аналітичних алгоритмів, а також ефективного реагування на виявлені події та загрози. Воно дозволяє забезпечити цілісність, конфіденційність та доступність корпоративної інформації, а також швидку виявлення та реагування на потенційні загрози безпеки.

Незважаючи на багато переваг, SIEM системи також мають деякі недоліки, про які варто знати. Вони можуть вимагати значних витрат, як фінансових, так і людських ресурсів. Реалізація, налаштування та підтримка SIEM системи можуть вимагати великого обсягу ресурсів, що може бути недоцільним для деяких організацій. Також, SIEM системи можуть стикатися з великим обсягом ложнопозитивних та ложнододатних сигналів. Це може стати проблемою, оскільки аналітики безпеки можуть витрачати багато часу на перевірку та фільтрацію таких сигналів, збільшуючи навантаження на персонал та можливість пропуску справжніх загроз.

SIEM системи можуть мати обмежену здатність аналізувати та виявляти нові типи атак або складні мульти-векторні загрози. Швидкі зміни в кіберзлочинності означають, що SIEM системи повинні постійно оновлюватися та вдосконалюватися, щоб виявляти нові загрози та методи атак. Крім того, SIEM системи можуть бути залежними від точності та актуальності вхідних даних. Якщо дані, які надходять до SIEM системи, неправильні або неактуальні, це може призвести до недостовірних результатів аналізу та виявлення. Взагалі, SIEM системи мають свої обмеження і вимагають уважного підходу. Їх вартість, взаємодія з іншими системами, кількість ложнопозитивних сигналів та здатність до виявлення нових загроз - це всі аспекти, які потрібно враховувати при розгляді недоліків SIEM систем.[22]

Після виявлення підозрілого або небезпечного вторгнення необхідно негайно реагувати і вживати заходів для зупинення атаки, відновлення безпеки системи та аналізу події для запобігання подібним інцидентам у майбутньому. Це може включати ізоляцію компрометованих систем, зміну паролів, патчінг вразливостей, збереження доказів і співпрацю зі спеціалізованими службами безпеки. Загальна мета виявлення взлому полягає в тому, щоб забезпечити безпеку КМ, ідентифікувати потенційні загрози та вчасно вживати заходів для їх запобігання та реагування. Регулярний моніторинг, аналіз та вдосконалення процесів виявлення взлому допомагають зберегти систему від потенційних ризиків та захистити конфіденційні дані.

Реагування на взлом корпоративної мережі є критично важливою складовою у збереженні цілістності конфеденційної інформації та всієї мережі взагалі. Коли виявляється вторгнення або порушення безпеки, швидра реакція та ефективні заходи по відновленню контролю є вирішальними. Реагування на взлом включає такі етапи, як виявлення порушення, припинення небезпеки, відновлення систем та дослідження інциденту.

Важливо оперативно виявляти незвичні активності чи незадовільний стан системи. Це може включати моніторинг мережевої активності, реєстрацію логів подій та використання систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS). Після виявлення взлому важливо припинити небезпеку та зупинити діяльність зловмисника. Це може включати блокування компрометованих акаунтів, зміну паролів, відключення компрометованих систем або навіть припинення мережевого з'єднання. Наступним кроком є відновлення нормальної роботи систем та мережі. Це може охопити відновлення даних з резервних копій, виправлення вразливостей, проведення аудиту безпеки та зміцнення заходів безпеки. Окрім того, розслідування взлому має важливе значення для з'ясування причин та наслідків інциденту. Це включає аналіз логів подій, відновлення послідовності подій та визначення вразливостей, які були використані зловмисником.

Реагування на взлом корпоративної мережі вимагає дисциплінованого та координованого підходу залучених сторін. Це включає співпрацю між IT-командою, безпековими експертами, керівництвом організації та, за потреби, зовнішніми консультантами з безпеки (кіберполіція). Швидка реакція та ефективне виконання заходів безпеки можуть значно зменшити вплив взлому та зберегти безпеку організації.

3.2.1 Аналіз наслідків взлому.

Аналіз наслідків взлому корпоративної мережі потрібен не лише для криміналістики, а й під час процесу відновлення безпеки та нормального функціонування організації. Аналіз наслідків допомагає розуміти обсяг і характер пошкоджень, зроблених зловмисником, а також виявити вразливості та недоліки, які дозволили взлому статися. Після виявлення взлому проводиться комплексний аналіз наслідків. Це включає оцінку збитків, втрати даних, порушення конфіденційності та цілісності інформації, вплив на репутацію організації та її клієнтів, а також можливість фінансових втрат. Аналіз наслідків допомагає виявити можливі зловживання або несанкціонований доступ до систем та даних.[23]

Результати аналізу наслідків дозволяють прийняти відповідні заходи для відновлення безпеки та запобігання подібним інцидентам у майбутньому. Це можуть бути зміни в політиках безпеки, підвищення рівня захисту систем, проведення додаткових навчань та тренінгів для персоналу, а також вдосконалення механізмів виявлення та відповіді на подібні атаки. Аналіз наслідків взлому корпоративної мережі допомагає організації зрозуміти причини і вплив інциденту, а також вжити необхідні заходи для запобігання подібним вразливостям у майбутньому. Це важлива складова безпекового циклу, яка сприяє підвищенню рівня безпеки та захисту організації.

Заходи, які треба вжити для того, щоб провести якісний аналіз наслідків кібератаки (взлому):

- Збір інформації. Починаючи з деталей самого взлому, збираються всі доступні дані про подію, включаючи час, місце, методи, використані інструменти, а також виявлені наслідки та можливі IP логи.
- Класифікація наслідків – це оцінка серйозності наслідків взлому, включаючи втрати даних, фінансові збитки, порушення

конфіденційності та цілісності інформації, а також можливий вплив на репутацію організації.

— Виявлення вразливостей. Проводиться аналіз системи, який допомагає виявити вразливості та недоліки, які були використані зловмисником. Це можуть бути слабкі місця в мережевих протоколах, недостатні заходи безпеки або помилки в конфігурації систем.

— Відновлення даних та систем. Після виявлення вразливостей та наслідків взлому проводиться процес відновлення даних та систем до стану перед-інциденту. Це може включати відновлення резервних копій, поновлення конфігурацій та встановлення оновлень безпеки.

— Аналіз причин – це процес, який вимагає детальний аналіз причин взлому, зокрема способів проникнення, використаних експлойтів та вразливостей. Цей аналіз допомагає розуміти, як уникнути подібних вразливостей у майбутньому.

— Прийняття заходів – це процес який виконується на основі виявлених причин та недоліків розробляються та впроваджуються відповідні заходи для підвищення рівня безпеки. Це можуть бути зміни в політиках безпеки, підвищення рівня захисту систем, навчання та тренінги для персоналу, а також аудит безпеки для виявлення потенційних слабких місць.

— Моніторинг та виявлення. Після відновлення системи встановлюються механізми моніторингу та виявлення подібних вразливостей або атак. Це дозволяє вчасно виявляти та реагувати на потенційні загрози та уникати подібних інцидентів у майбутньому.[24]

3.3 Розробка рекомендацій щодо ефективних методів захисту корпоративних мереж.

Ефективні методи захисту корпоративних мереж є запорукою безпеки компанії. При розробці рекомендацій щодо таких методів були враховані усі життєво важливі функції для створення безпеки корпоративної мережі, тому щоб створити дійсно ефективну систему безпеки корпоративної мережі, потрібно враховувати рекомендовані щодо методів захисту.

Перш за все, треба ввести політику інформаційної безпеки. Політика безпеки інформації в корпоративній мережі - це набір документованих правил, процедур, стандартів та рекомендацій, які визначають стратегію та вимоги щодо захисту інформації в мережі організації. Політика встановлює рамки та вказівки, які допомагають забезпечити безпеку будь-якої інформації компанії, а також управляти ризиками інформаційної безпеки. В політиці безпеки інформації визначаються основні принципи, цілі та обов'язки, пов'язані з захистом інформації в мережі. Вона охоплює такі аспекти, як управління доступом до інформації, захист від несанкціонованого доступу та вторгнень, шифрування даних, забезпечення цілісності та конфіденційності, а також політику використання паролів та інших ідентифікаторів. Політика безпеки інформації також включає процедури виявлення та реагування на інциденти безпеки, включаючи забезпечення резервного копіювання та відновлення даних, моніторинг та аналіз подій, аудит безпеки та навчання персоналу. Метою політики безпеки інформації є забезпечення високого рівня захисту інформації в мережі організації, зменшення ризиків безпеки та збереження довіри клієнтів та партнерів. Вона є основою для розробки та впровадження технічних, організаційних та правових заходів, спрямованих на забезпечення

безпеки інформації та виконання вимог стандартів та регуляторних вимог в сфері інформаційної безпеки. В кінцевому підсумку, політика безпеки інформації є важливим елементом управління ризиками та забезпеченням безпеки в корпоративній мережі. Вона створює умови для встановлення правил та практик, які допомагають організації ефективно захищати свою інформацію від загроз та потенційних атак.

Аудит безпеки. На початку створення ефективної системи безпеки, потрібно провести аудит безпеки корпоративної мережі, щоб виявити потенційні вразливості та слабкі місця в мережі. Це може включати перевірку конфігурації мережевих пристроїв, ідентифікацію потенційних точок входу для зловмисників, аналіз систем журналювання та виявлення аномалій. Результати аудиту допоможуть визначити основні проблеми та напрямки подальших заходів. Також Аудит системи захисту допоможе полипшити сприйняття безпекових норм серед користовачів КМ. Це означає для компанії те, що люди які працюють в мережі, усвідомлюють важливість затвердженої політики безпеки у компанії, правила користування тим чи іншим мережевим пристроєм. Проведення аудиту на регулярній основі також може значно покращити кіберзахист мережі завдяки виявленю нових потенційних вразливостей, загроз чи навіть спроб взлому системи через співробітників компанії (свідомих чи не свідомих агентів зловмисника).

Використання надійного антивірусного програмного забезпечення та системи виявлення/запобігання вторгненням (IDS/IPS). Антивірусне програмне забезпечення здатне виявляти та блокувати шкідливі програми, включаючи програми-кроти, віруси, тощо. IDS/IPS (системи виявлення та запобігання вторгнення) рекомендуються в корпоративних мережах з ряду причин. IDS/IPS дозволяють виявляти та реагувати на потенційні загрози безпеки в режимі реального часу. Вони аналізують мережевий трафік, виявляють аномалії та вразливості, що дозволяє своєчасно реагувати на інциденти та запобігати вторгненням. Також, IDS/IPS забезпечують

додатковий рівень захисту, доповнюючи інші механізми безпеки, такі як файрволи та антивірусне програмне забезпечення. Вони виявляють вторгнення, атаки і некоректну поведінку в мережі, що дозволяє оперативно реагувати та вживати відповідних заходів для мінімізації шкоди. Крім того, ще забезпечують збір і аналіз великої кількості інформації про мережеву активність та потенційні загрози. Це дозволяє виявляти тренди, аналізувати інциденти та здійснювати подальші вдосконалення системи безпеки на основі зібраних даних. Однією важливою особливістю IDS/IPS є їх гнучкість та можливість налаштування під конкретні потреби організації. Різноманітні правила та налаштування дозволяють пристосовувати систему до конкретних вимог безпеки, враховуючи специфіку мережі та видів загроз. Узагалінюючи, IDS/IPS рекомендуються в корпоративних мережах для постійного моніторингу та виявлення потенційних загроз, оперативного реагування на інциденти безпеки та забезпечення додаткового рівня захисту для корпоративної інформації та ресурсів.

Застосування файрвола. Файрвол дозволяє контролювати трафік, що входить в мережу та виходить з мережі, і блокувати небажані з'єднання. Це допомагає запобігати несанкціонованому доступу та зменшує ризик атак ззовні. Файрвол є важливим компонентом корпоративної мережі, оскільки забезпечує безпеку та захист інформації. Він виконує ряд функцій, які спрямовані на контроль трафіку в мережі та запобігання несанкціонованому доступу. Використання файрвола дозволяє обмежити права доступу користувачів що підвищує таким чином захист, а також виявляти та блокувати потенційні загрози безпеці, на приклад: віруси, шкідливі програми, хакерські атаки.

Файрвол виконує функцію фільтра мережевого трафіку, дозволяючи пропускати лише дозволений трафік та блокувати небажаний або потенційно небезпечний трафік. Він регулює доступ до різних ресурсів мережі залежно

від встановлених правил та політик безпеки. Окрім того, брандмауер забезпечує можливість моніторингу мережевої активності та виявлення аномалій. Він допомагає виявляти незвичайну поведінку, вразливості та спроби вторгнення, що дозволяє оперативно реагувати на потенційні загрози та забезпечувати безпеку мережі. Використання файрвола також сприяє виконанню вимог законодавства та регуляторних вимог, пов'язаних з захистом інформації. Він дозволяє встановлювати правила, що враховують ці вимоги та забезпечують відповідність встановленим стандартам та нормам. Загалом, файрвол є незамінним інструментом для забезпечення безпеки корпоративних мереж. Він допомагає запобігати несанкціонованому доступу, захищати інформацію від шкідливих впливів та забезпечувати безпеку даних організації.

Важливо забезпечити резервне копіювання даних. Регулярне створення резервних копій дозволяє відновити важливу інформацію у разі втрати або пошкодження даних в результаті інциденту. Методів резервного копіювання доволі багато, зовнішні жорсткі диски най надійніші та дешевші, проте вони не можуть робити автоматичне копіювання інформації компанії. Для цього потрібна присутність людини та ручне обирання типу інформації для копіювання. Є й автоматичні автоматичні програми копіювання важливої для компанії програми, якими не треба нехтувати. Проте, усе одно надійним методом резервного копіювання буде поєднання програми автокопіювання та сервера (SAN).

Навчання та свідомість персоналу. Компанія повинна забезпечити навчання співробітників щодо безпеки мережі, використання складних паролів, уникання підозрілих посилань та нехтуванням загрозами безпеці мережі. Це допоможе зменшити ризик внутрішніх загроз та помилок. Навчання та свідомість персоналу відіграють критичну роль у забезпеченні безпеки корпоративної мережі. Це означає, що всі працівники повинні мати

достатні знання та розуміння щодо правил та процедур безпеки, а також бути свідомими загроз, які можуть виникнути при роботі з інформацією. Навчання персоналу включає в себе проведення освітніх заходів, тренінгів, семінарів та інших форм навчання, які допомагають працівникам ознайомитися з політикою безпеки, процедурами реагування на інциденти, використанням захисних технологій тощо. Це допомагає підвищити їх усвідомлення ризиків та навички реагування на потенційні загрози. Гарная освідомленість персоналу означає, що кожен працівник повинен розуміти важливість безпеки інформації і приймати відповідальність за її збереження. Це включає своєчасне повідомлення про можливі загрози або інциденти безпеки, дотримання політик та процедур безпеки, обережне поводження з конфіденційною інформацією, використання сильних паролів та інших методів аутентифікації. Навчаність та свідомість персоналу сприяють зниженню ризику внутрішніх загроз, які можуть бути викликані недбалістю, помилками або зловмисними діями працівників. Вони також допомагають усвідомити важливість кожного працівника в системі загальної безпеки і покращують загальну реакцію на можливі інциденти безпеки.

Крім того, використання системи моніторингу та аналізу подій (SIEM) може покращити виявлення та реагування на потенційні загрози. SIEM система аналізує журнали подій, збирає та аналізує дані про активність в мережі, що дозволяє вчасно виявляти та реагувати на потенційні загрози безпеки. SIEM системи можуть бути ефективними як метод захисту корпоративної мережі з кількох причин.

— SIEM система здатна зібрати, проаналізувати та інтерпретувати великий обсяг інформації щодо подій та журналу подій, що відбуваються в мережі. Це дозволяє виявляти підозрілу активність, аномалії та потенційні загрози безпеки.

— SIEM система забезпечує централізоване управління та моніторинг подій безпеки в реальному часі. Це дозволяє оперативно виявляти та реагувати на загрози безпеки, спрощує процес виявлення інцидентів та полегшує подальший аналіз.
— SIEM система надає можливість здійснювати пошук, фільтрацію та кореляцію подій, що дозволяє виявляти складні зв'язки між різними подіями та виявляти потенційно шкідливі активності. Це допомагає знижувати кількість ложно-позитивних сигналів та концентрувати зусилля на реальних загрозах.
— SIEM система сприяє покращенню реагування на інциденти безпеки шляхом автоматизації процесу сповіщення, реагування та відновлення. Вона дозволяє швидко реагувати на загрози та вживати необхідні заходи для мінімізації впливу інциденту на мережу.

Загалом, SIEM система забезпечує цілісний погляд на безпеку корпоративної мережі, допомагає виявляти та вирішувати загрози безпеки, забезпечує швидке реагування на інциденти та полегшує процес аналізу та звітності, проте у SIEM системи вимагають гарних спеціалістів та значних грошових витрат.

Загалом, ефективна система захисту корпоративних мереж потребує комплексного підходу, який включає розробку політики безпеки, аудит безпеки, використання надійного програмного забезпечення та апаратних засобів, навчання персоналу та використання систем моніторингу. Тільки поєднання цих елементів допоможе забезпечити надійний рівень захисту та безпеки мережі організації.

Висновок

У даній дипломній роботі були розглянуті та проаналізовані різні механізми захисту інформації в корпоративних мережах. Дослідження показало, що захист інформації є надзвичайно важливим аспектом для будь-якої організації, оскільки цифрові загрози та кібератаки постійно зростають як за кількістю, так і за складністю.

Основною метою механізмів захисту інформації є забезпечення конфіденційності, цілісності та доступності даних. Для досягнення цих цілей були розглянуті різні технології та методи, такі як використання файрволів для контролю мережевого периметру, ідентифікація та аутентифікація користувачів, системи виявлення та запобігання вторгнень, шифрування даних, резервне копіювання та відновлення і аналіз наслідків взлому. Результати дослідження показали, що використання механізмів захисту інформації є важливим елементом у забезпеченні безпеки корпоративних мереж. Вони дозволяють ефективно виявляти та запобігати загрозам, а також швидко відновлювати нормальну роботу мережі у разі інциденту безпеки. Проте, слід зазначити, що неможливо створити абсолютно безпечну систему, і механізми захисту інформації мають свої обмеження та недоліки. Важливо розуміти, що захист інформації є постійним процесом, який вимагає постійного оновлення та вдосконалення з урахуванням нових загроз та технологій.

Отже, використання механізмів захисту інформації в корпоративних мережах є необхідним елементом для забезпечення безпеки даних та ділової організації. Це вимагає комплексного підходу, який включає в себе розробку та впровадження політик безпеки, навчання та свідомість персоналу, використання передових технологій та систем управління подіями та інформаційною безпекою. Тільки таким чином організації зможуть забезпечити надійний та безпечний захист своїх інформаційних ресурсів.

СПИСОК ЛІТЕРАТУРИ

1. "What is Network Security? Poda myre". *Forcepoint*. 2018-08-09. Retrieved 2020-12-05 [Електронний ресурс] – 2023 – Режим доступу: *https://www.forcepoint.com/cyber-edu/network-security*
2. A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco [Електронний ресурс] – 2023 – Режим доступу: *https://newsroom.cisco.com/c/dlls/2008/ts_010208b.html?sid=BAC-NewsWire*
3. *Rana, Shrikant (2021-12-01). The Learning Zone 8: A Textbook for Computer Science* [Електронний ресурс] – 2023 – Режим доступу: https://play.google.com/books/reader?id=jUaeEAAAQBAJ&pg=GBS.PA1&hl=uk
4. В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ [Електронний ресурс] – 2023 – Режим доступу: *https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf*
5. Луговой А.В., к.т.н., проф. ДО ПИТАННЯ ПРОВЕДЕННЯ АУДИТУ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ [Електронний ресурс] – 2023 – Режим доступу: *http://visnikkrnu.kdu.edu.ua/statti/2009-5-1(58)/62.PDF*
6. В.М. Франчук, Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних [Електронний ресурс] – 2023 – Режим доступу: *https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf*
7. М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук АСИМЕТРИЧНІ МЕТОДИ ШИФРУВАННЯ В ТЕЛЕКОМУНІКАЦІЯХ [Електронний ресурс] – 2023 – Режим доступу: *https://dut.edu.ua/uploads/l_491_94183247.pdf*

8. TLS vs SSL: Which Protocol Should You Use? By Haley Walden [Електронний ресурс] – 2023 – Режим доступу: *https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiPw9P0t57_AhUSwncKHUoAD44YABADGgJlZg&ohost=www.google.com&cid=CAESbeD2w21BU0S99LWhUvRd39fONzxd_hk5_L5QjZbp7HmXbI9cDiXBkv6rw3g216VLroaPoDXS860EghKe-evCEwM04HQcBgzKLD-40QnmZt70fUvzTuk54ia8ytdWBnSwL7iM_lOp7RpDHsgHLvo&sig=AOD64_0_8kom8nvFfURBuKSFCW2QYVEvYw&q&adurl&ved=2ahUKEwii5c30t57_AhVFg_0HHc8JBzkQ0Qx6BAgGEAE*
9. Андрій Білоконь ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ У ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ [Електронний ресурс] – 2023 – Режим доступу: *http://oldconf.neasmo.org.ua/node/563*
10. **Віртуальні приватні мережі (VPN)** [Електронний ресурс] – 2023 – Режим доступу: *https://compbest.com.ua/ua/virtualnye-chastnye-seti-vpn/*
11. Антивіруси [Електронний ресурс] – 2023 – Режим доступу: *https://sites.google.com/site/programnezabezpecenna/sistemne-programne-zabezpecenna/antivirusi*
12. Аутентифікація і авторизація: що це і в чому відмінність [Електронний ресурс] – 2023 – Режим доступу: *https://qagroup.com.ua/publications/autentyfikatciia-i-avtoryzatciia/*
13. Dave Dittrich, *Network monitoring/Intrusion Detection Systems (IDS)* Archived 2006-08-27 at the Wayback Machine, University of Washington. [Електронний ресурс] – 2023 – Режим доступу: *http://www.ticm.com/kb/faq/idsfaq.html*
14. Двофакторна автентифікація для безпеки [Електронний ресурс] – 2023 – Режим доступу: https://ssl.com.ua/blog/ukr/what-is-2fa/
15. Macfarlane, Richard; Buchanan, William; Ekonomou, Elias; Uthmani, Omair; Fan, Lu; Lo, Owen (2012). "Formal security policy implementations in network firewalls" [Електронний ресурс] – 2023 – Режим доступу:

https://www.sciencedirect.com/science/article/abs/pii/S0167404811001192?via%3Dihub

16. What is a denial of service attack (DoS) ? [Електронний ресурс] – 2023 – Режим доступу: *https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos*
17. Резервне копіювання даних і чому це важливо для бізнесу? [Електронний ресурс] – 2023 – Режим доступу: *https://itez.com.ua/data-backup-and-why-is-it-important-for-business.html*
18. Що таке зовнішні жорсткі диски [Електронний ресурс] – 2023 – Режим доступу *https://www.sysdevlabs.com/uk/articles/storage-devices/external-hard-drives/*
19. NAS-сховище — специфіка. [Електронний ресурс] – 2023 – Режим доступу *https://e-server.com.ua/uk/poradi/nas-shovishhe-specifika-i-4-kriterii-viboru*
20. Системи зберігання даних . [Електронний ресурс] – 2023 – Режим доступу *http://www.dtcenter.com.ua/component/spsimpleportfolio/item/88-sistemi-zberigannya-danikh*
21. Що таке відновлення даних? . [Електронний ресурс] – 2023 – Режим доступу *https://www.ufsexplorer.com/uk/articles/what-is-data-recovery/*
22. Security information and event management (SIEM) explained . [Електронний ресурс] – 2023 – Режим доступу https://www.ibm.com/topics/siem
23. БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ ТА ЇЇ ЗАБЕЗПЕЧЕННЯ [Електронний ресурс] – 2023 – Режим доступу *https://dut.edu.ua/repozitorii/ki/2022/%D0%9C%D1%96%D1%85%D0%B5%D1%94%D0%B2.pdf*