МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет комп’ютерних наук та технологій

Кафедра комп’ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Жуков А.І.

21.06.2023 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«БАКАЛАВР»

Тема: «Система захисту інформації в комп'ютерній мережі»

Студент: Михайловський Антон Віталійович

Керівник: Малярчук В.О.

Нормоконтролер: Журавель С.В

Київ 2023

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека;

КС – комп’ютерна система;

ТЗІ – технічний захист інформації;

ПРД – правила розмежування доступу;

НСД – несанкціонований доступ;

VPN – virtual private network (віртуальна приватна мережа);

SSH – secure shell (захищена оболонка);

DMZ – Demilitarized Zone (демілітаризована зона);

ВСТУП

У сучасному цифровому світі, комп'ютерні мережі стали невід'ємною складовою нашого повсякденного життя. Інтернет, корпоративні мережі, бездротові мережі - всі вони дозволяють нам спілкуватися, обмінюватися інформацією та отримувати доступ до різноманітних ресурсів. Однак, разом зі зручністю та доступністю, з'явилися і загрози безпеці інформації, що перебуває в цих мережах.

Забезпечення безпеки інформації є надзвичайно важливим завданням для будь-якої комп'ютерної мережі. Нестача відповідних заходів захисту може призвести до розголошення конфіденційних даних, крадіжки інтелектуальної власності, фінансових злочинів, пошкодження або втрати інформації, а також до розповсюдження шкідливих програм, які можуть шкодити як користувачам, так і системам.

Однак, системи захисту інформації розробляються та вдосконалюються, щоб протистояти цим загрозам. Сучасні технології та методи захисту інформації дозволяють створювати надійні системи, які забезпечують конфіденційність, цілісність та доступність даних.

Метою даної дипломної роботи є розгляд основних аспектів системи захисту інформації в комп'ютерних мережах та створення подібної системи. Ми розглянемо різні методи та засоби захисту, аналізуватимемо їх переваги та недоліки. Розуміння цих методів та засобів допоможе нам зрозуміти, як можна захистити інформацію в мережі від потенційних загроз.

У наступних розділах ми розглянемо основні загрози інформаційній безпеці, вимоги до систем захисту інформації, а також методи та засоби захисту, які можуть бути використані для створення надійної системи захисту інформації в комп'ютерній мережі.

1. АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

1.1 Аналіз термінології з ІБ корпоративних КС і мереж

Для отримання глибокого розуміння потенційних загроз, що виникають у комп'ютерних системах та мережах, а також для розробки методів боротьби з ними та захисту інформації, необхідно ознайомитися з термінологією, пов'язаною з інформаційною безпекою в організаціях. Перш за все, важливо зрозуміти сутність таких понять, як "інформація", "комп'ютерна мережа" та "комп'ютерна система", а також освоїти концепцію "вразливість-загроза-атака".

Термін "інформація" має різноманітні визначення, залежно від контексту його використання. Закон України "Про інформацію" надає найточніше пояснення, згідно з яким "інформація" охоплює будь-які дані або відомості, які можуть бути збережені на матеріальних носіях або представлені у формі електронних записів. Зазвичай, для зручного доступу до інформації та її використання створюються інформаційні системи, в яких вона обробляється та циркулює.

Інформаційна система, також відома як автоматизована система, є організаційно-технічною системою, що об'єднує комп'ютерну систему (апаратне та програмне забезпечення), фізичне середовище (зовнішнє середовище та контрольована зона), персонал (керівництво, адміністратори та користувачі) та оброблювальну інформацію.

Комп'ютерна система представляє собою інформаційно-технічний комплекс, який включає апаратне та програмне забезпечення і призначений для обробки, модифікації, введення та виведення інформації. Ця система є складовою частиною інформаційної системи.

Комп'ютерна мережа є сукупністю кінцевих (термінальних) та проміжних (комутуючих) пристроїв, а також середовища передачі інформації (провідне, безпровідне). Вона призначена для обробки інформації шляхом передачі даних у вигляді пакетів, що переносяться електромагнітними сигналами. Комп'ютерна мережа також є складовою частиною інформаційної системи, в якій кінцеві пристрої належать до комп'ютерної системи, а проміжні пристрої та середовище передачі інформації входять до складу телекомунікаційної системи.

Телекомунікаційна система включає в себе технічні та програмні засоби, які призначені для обміну інформацією шляхом передавання, випромінювання або приймання сигналів, знаків, звуків, рухомих або нерухомих зображень та інших даних.

Інформаційно-телекомунікаційна система є сукупністю інформаційних та телекомунікаційних систем, які взаємодіють між собою та діють як єдине ціле.

Отже, інформаційно-телекомунікаційна система складається з двох компонентів - інформаційної та телекомунікаційної систем. Комп'ютерна система виступає як складова частина інформаційної системи, а комп'ютерна мережа включає елементи інформаційно-телекомунікаційної системи.

У процесі створення та експлуатації будь-якої системи, де обробляється або циркулює інформація, можуть виникати вразливості, які загрожують нормальному функціонуванню такої системи. Вразливість системи відображає її нездатність протистояти певним загрозам. Це означає, що будь-яка інформаційна система може бути вразливою. Ця вразливість створює загрозу інформаційної безпеки, яка, у свою чергу, може призвести до атаки на систему.

Загроза - це обставини або події, які можуть порушити політику безпеки інформації та завдати шкоди автоматизованій системі. Спроба реалізації загрози називається атакою. Залежно від цілей зловмисника, атака може бути успішною (порушення інформаційної безпеки організації) або неуспішною.

Цей підхід типу "вразливість-загроза-атака" можна пояснити на прикладі корпоративної мережі. Уявімо собі, що в корпоративній мережі є певні вразливості. Зловмисник може намагатися використати ці вразливості (загроза), щоб отримати несанкціонований доступ до конфіденційної інформації організації. Ця спроба реалізується як атака на мережу.

При аналізі цих понять стає очевидним, що основні загрози, пов'язані з неправильним використанням та незаконним доступом до інформації, включають:

- Вразливості, що виникають під час обробки інформації в комп'ютерних системах та мережах, такі як вразливості апаратного та програмного забезпечення;
- Вразливості, що виникають під час передачі інформації в телекомунікаційних системах, комп'ютерних системах та мережах;
- Вразливості, пов'язані з халатністю та неналежною роботою персоналу.
- Вразливості, пов'язані з ненадійністю програмного та апаратного забезпечення та недосконалістю систем захисту інформації;
- Вразливості, пов'язані з порушенням організаційних заходів забезпечення безпеки;

Для ефективної обробки та обігу інформації в інформаційних системах необхідно забезпечити її належний рівень захисту. Захист інформації включає правові, адміністративні, організаційні, технічні та інші заходи, спрямовані на збереження цілісності інформації і контрольований доступ до неї [Закон України "Про інформацію"].

Зазвичай, основні принципи захисту інформації визначаються в політиці безпеки інформації. Політика безпеки організації є набором керівних принципів, правил, процедур і практичних прийомів, що регулюють управління, захист і розподіл цінної інформації. У короткій формі, це набір правил, які втілені у функціоналі програмного чи апаратного забезпечення, необхідного для використання в конкретній інформаційній системі.

З метою запобігання незаконному доступу, використанню або модифікації інформації, що циркулює в інформаційній системі організації, а також її неправомірному витоку за межі організації, розробляються комплексні системи захисту інформації. Комплексна система захисту інформації включає організаційні та інженерно-технічні заходи, спрямовані на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу [Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закон України "Про захист персональних даних"].

Окрім того, в контексті корпоративних мереж, важливо зазначити, що захист інформації також стосується корпоративних мереж. Корпоративна мережа - це мережа, яка об'єднує комп'ютери та інші пристрої в межах підприємства або організації. Забезпечення безпеки корпоративної мережі включає захист від несанкціонованого доступу, витоку конфіденційної інформації та інших загроз, що можуть виникнути у процесі її функціонування. Організація повинна приділяти належну увагу заходам захисту інформації в корпоративній мережі для забезпечення конфіденційності, цілісності та доступності даних.

1.2 Основні види загроз ІБ корпоративних КС і мереж

Кожна інформаційна система має забезпечувати механізми, методи, засоби та способи захисту інформації, що циркулює в системі, та процесів її обробки. Для забезпечення належного захисту важливо проводити регулярний аналіз на наявність вразливостей, які можуть підірвати конфіденційність, цілісність та доступність інформації.

Загрози безпеці комп'ютерних систем і мереж, а також інформації, що в них циркулює, розрізняються за властивостями інформації, яку може порушити кожна загроза. Такі властивості включають:

- Загроза порушення конфіденційності інформації.
- Загроза порушення цілісності інформації.
- Загроза порушення доступності інформації (порушення працездатності системи).

Конфіденційність означає, що інформація повинна бути захищена від несанкціонованого доступу. Незаконне розголошення конфіденційної, службової або таємної інформації, що належить або циркулює в комп'ютерних системах і мережах державних або комерційних організацій, становить порушення конфіденційності. Зловмисники можуть отримати несанкціонований доступ до цієї інформації шляхом здійснення інформаційних атак.

Цілісність означає, що інформація повинна бути захищена від несанкціонованого спотворення, руйнування або знищення. Порушення цілісності виникає при незаконній модифікації інформації з обмеженим доступом або відкритої інформації, що зберігається, обробляється або передається в комп'ютерних системах і мережах. Ця загроза може бути результатом зловмисних дій або зовнішнього впливу на систему. Часто це стає однією з найбільш поширених загроз інформації, особливо при передачі через комп'ютерні та телекомунікаційні мережі.

Доступність означає, що інформація повинна бути захищена від несанкціонованого блокування. Порушення доступності (працездатності системи) пов'язане з ситуаціями, що погіршують працездатність інформаційних систем і блокують доступ до їх ресурсів.

Додатково, важливо зазначити, що в контексті безпеки інформації також розглядаються аспекти, пов'язані з "Корпоративними мережами". Корпоративні мережі - це мережеві інфраструктури, що використовуються організаціями для забезпечення комунікації і обміну даними між різними вузлами та відділеннями в межах організації. Забезпечення безпеки інформації в корпоративних мережах включає застосування відповідних механізмів, методів і засобів для захисту інформації від можливих загроз, а також контроль доступу до ресурсів мережі та застосунків.

Наприклад, у разі успішної атаки на доступність інформаційної системи, користувач не може отримати санкціонований доступ до збереженої та оброблюваної в ній інформації, що призводить до відмови в обслуговуванні. Атаки на доступність можуть бути постійними або тимчасовими і зазвичай виконуються перед атаками на цілісність та конфіденційність інформації.

Порушення властивостей даних можуть виникати внаслідок різноманітних небезпечних впливів на інформаційну систему. Це зазвичай пов'язано зі складністю системи та вразливостями, які можуть виникнути через пошкодження або неналежну діяльність її складових елементів. Основними компонентами будь-якої інформаційної системи, які можуть мати вразливості, є програмне забезпечення, апаратно-технічний комплекс, персонал та інформація, що циркулює та обробляється.

В комп'ютерних мережах та системах небезпечні впливи можуть бути природними або створеними зловмисниками. Природні впливи виникають внаслідок природних катаклізмів або надзвичайних ситуацій, що стосуються апаратно-технічного комплексу, програмного забезпечення та персоналу, який обслуговує системи та мережі. Наприклад, це можуть бути помилки в роботі програмного забезпечення, помилки обслуговуючого персоналу або аварійні ситуації, спричинені стихійними лихами чи відключенням електричного живлення.

Штучні впливи або загрози виникають в результаті дій порушників, які можуть бути санкціонованими особами (персонал, що обслуговує інформаційні системи) або несанкціонованими особами (звичайні користувачі, відвідувачі організацій, конкуренти і т.д.). Зазвичай атаки на основі штучних загроз виникають після детального аналізу критичних елементів організації, на які можна здійснити успішну атаку. Наприклад, порушники можуть мати інформацію про організаційні та програмно-технічні принципи функціонування системи, бути ознайомленими з топологією мережі організації або зламати працівників з метою здійснення незаконних дій.

Приклади штучних загроз включають несанкціонований доступ сторонніх осіб до систем, ознайомлення обслуговуючого персоналу та користувачів з недоступною для них інформацією, незаконну модифікацію або копіювання програмного забезпечення та інформації, викрадення чи створення/зміну/знищення документів, викрадення матеріальних носіїв з обмеженим доступом, незаконне знищення інформації, фальсифікацію повідомлень, відмову від авторства, незаконне знищення або модифікацію даних та інше.

Крім того, варто додати інформацію про "корпоративні мережі". Корпоративні мережі є важливою складовою інформаційних систем організацій. Вони забезпечують обмін даними та комунікацію між різними вузлами в межах організації, дозволяючи спільний доступ до ресурсів та інформації. Однак, корпоративні мережі також стають об'єктом потенційних загроз безпеці. Небажані доступи, атаки на доступність, вразливості

програмного забезпечення, зловмисні дії персоналу або зовнішніх осіб - це лише деякі з проблем, які можуть виникнути в корпоративних мережах. Для забезпечення безпеки корпоративних мереж важливо використовувати заходи захисту, такі як мережева аутентифікація, шифрування, мережевий моніторинг та використання сучасних технологій безпеки.

1.3 Напрямки захисту інформації в корпоративних КС і мережах

1.3.1 НСД

Технічний захист інформації (ТЗІ) в корпоративних КС та мережах є важливим аспектом безпеки. Його розробка та використання здійснюються в рамках комплексних систем захисту інформації, спрямованих на вирішення різних аспектів безпеки організації. Основні завдання ТЗІ включають захист інформації від несанкціонованого доступу (НСД) та витоку технічними каналами.

Несанкціонований доступ означає нелегальне отримання доступу до інформації у комп'ютерних системах з використанням засобів, які порушують встановлені правила розмежування доступу (ПРД). Цей доступ може бути здійснений як за допомогою штатних засобів, програмного та апаратного забезпечення, внесених розробником або системним адміністратором, так і зловмисними програмно-апаратними засобами.

Наприклад, зловмисник може несанкціоновано використовувати комп'ютер локальної мережі для доступу до файлів, що належать іншим користувачам. Серед способів несанкціонованого доступу варто відзначити безпосереднє звертання до об'єктів для отримання доступу, створення програмно-апаратних засобів, які обходять захисні механізми, модифікацію існуючих засобів захисту або впровадження механізмів, що порушують структуру і функції системи для здійснення несанкціонованого доступу.

Захист від несанкціонованого доступу полягає у вжитті заходів для забезпечення виконання правил розмежування доступу шляхом створення і підтримки ефективної системи захисту інформації. Такі заходи включають в себе використання технологій ТЗІ в корпоративних мережах, мережеву аутентифікацію, шифрування даних та системи моніторингу. Дотримання правил розмежування доступу є ключовим для забезпечення безпеки корпоративних мереж та запобігання несанкціонованому доступу до важливої інформації.

1.3.2 Технічні канали витоку

Технічні канали витоку інформації є однією з ключових проблем, з якими стикаються корпоративні мережі. Вони можуть бути використані для незаконного витоку конфіденційних даних або незадуманого розголошення цінної інформації. Технічні канали витоку інформації виникають через недоліки або уразливості в апаратних пристроях, програмному забезпеченні, мережевих протоколах або конфігураційних параметрах.

Один з таких технічних каналів витоку інформації в корпоративних мережах - це "канал бічного каналу" (side channel). Цей тип каналу використовується для витоку інформації шляхом аналізу побічних ефектів, що виникають під час функціонування системи. Наприклад, можна аналізувати споживання енергії, електромагнітне випромінювання, час відгуку або шумові сигнали, щоб вилучити цінну інформацію.

Інший приклад технічного каналу витоку інформації - це "канал електронних перешкод" (TEMPEST). Цей тип каналу використовує можливості перехоплення електромагнітних сигналів, що генеруються пристроями, такими як комп'ютери, монітори, клавіатури тощо. Атакувач може використовувати спеціальне обладнання для перехоплення та аналізу цих електромагнітних сигналів, отримуючи доступ до конфіденційної інформації.

Для захисту від технічних каналів витоку інформації в корпоративних мережах застосовуються різні заходи. Одним з них є використання захисних пристроїв, які мінімізують побічні ефекти і зменшують можливості аналізу. Також важливо ретельно налаштувати мережеві протоколи та параметри, щоб уникнути недоліків, які можуть бути використані зловмисниками.

Подальша розробка і впровадження ефективних технологій та стратегій захисту від технічних каналів витоку інформації є невід'ємною частиною розвитку корпоративних мереж. Тільки шляхом поєднання технічного захисту інформації з адекватними політиками безпеки та постійним моніторингом можна забезпечити надійний рівень безпеки в корпоративному середовищі.

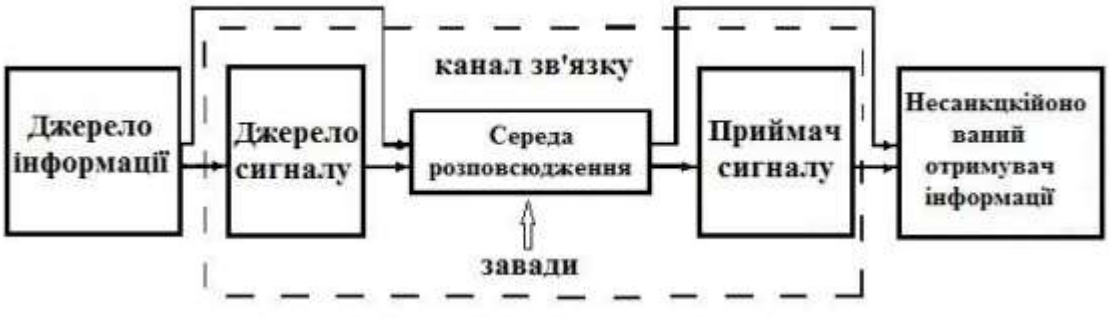

Рис.1.1 Структура технічного каналу витоку інформації

1.4 Організаційні та організаційно-технічні заходи захисту інформації

Організаційний захист інформації забезпечує безпеку шляхом регулювання доступу до ресурсів інформаційної системи за допомогою організаційних заходів. Цей вид захисту вимагає від персоналу, що обслуговує корпоративні мережі і комп'ютерні системи, дотримання правил експлуатації з метою забезпечення потрібного рівня безпеки.

Організаційні заходи захисту інформації включають:

- Контроль доступу до приміщень та обмеження входу до приміщень із обмеженим доступом (конфіденційних, службових, таємних). Доступ надається лише спеціальним посадовим особам, які мають відповідні повноваження, та лише тим працівникам, які мають необхідність в роботі з цією інформацією. У державних установах такі обов'язки покладені на режимно-секретні підрозділи;
- Збереження матеріальних носіїв даних у спеціальних, захищених, вогнестійких металевих шафах або приміщеннях;
- Виділення окремих персональних електронно-обчислювальних машин для обробки інформації з обмеженим доступом;
- Використання пристроїв введення та виведення інформації таким чином, щоб уникнути несанкціонованого доступу та використання інформації.
- Постійний контроль адміністратора безпеки організації або підрозділу за роботою принтера та інших пристроїв виведення для запобігання витоку інформації за межі організації;
- Здійснення процедур належної утилізації та знищення матеріалів, що містять важливу інформацію для організації. Наприклад, в державних установах використовуються шредери для знищення непотрібних паперових документів, а залишки паперу спалюються в спеціальних печах;
- Заборона обговорення змісту інформації з обмеженим доступом;
- Заборона використання незареєстрованих мобільних телефонів, планшетів, комп'ютерів та інших пристроїв для читання інформації під час роботи з інформацією з обмеженим доступом.

Організаційно-технічний захист інформації має схожі принципи з організаційним захистом, за винятком використання технічних засобів захисту інформації.

Організаційно-технічні заходи захисту інформації включають:

- Обмеження доступу до внутрішнього простору корпусу персональних електронно-обчислювальних машин за допомогою механічних запірних пристроїв;
- Процедура знищення інформації на жорстких дисках персональних електронно-обчислювальних машин, якщо потрібно відправити їх на ремонт. Знищення інформації має бути проведене за допомогою засобів низькорівневого форматування;
- Живлення персональних електронно-обчислювальних машин від окремих джерел живлення, або використання стабілізатора напруги (мережевого фільтру), якщо окремих джерел немає;
- Використання рідкокристалічних або плазмових дисплеїв для відображення інформації і струменевих або лазерних принтерів для друку;
- Розміщення системного блоку, пристроїв введення та виведення інформації на відстані не менше 2,5-3,0 метра від освітлювальних пристроїв, кондиціонерів, засобів зв'язку (телефонів), металевих труб, телевізійних та радіоапаратур, а також від інших персональних електронно-обчислювальних машин, які не використовуються для обробки конфіденційної інформації;
- Відключення персональних електронно-обчислювальних машин від глобальної мережі Інтернет під час обробки інформації з обмеженим доступом;
- Встановлення принтера і клавіатури на м'які прокладки з метою зменшення витоку інформації по акустичному каналу;
- Включення додаткових пристроїв, які створюють шумовий фон (кондиціонери, вентилятори) під час обробки цінної інформації на персональних електронно-обчислювальних машинах;
- Знищення інформації після того, як вона стала непотрібною або втратила свою актуальність.

1.5 Канали витоку інформації

Канали витоку інформації в корпоративній мережі є однією з важливих проблем, з якими стикаються організації у сучасному цифровому світі. Вони можуть призвести до небажаних наслідків, таких як втрата конфіденційності, розкриття комерційної інформації, порушення правил безпеки та навіть фінансових збитків.

Канали витоку інформації можуть бути різного характеру і включати як технічні, так і соціальні аспекти. Технічні канали можуть включати незахищені

мережеві з'єднання, недостатньо захищені сервери, вразливості в програмному забезпеченні та недостатню контрольованість даних.

Соціальні канали витоку інформації можуть включати недосконалу політику безпеки, недостатню усвідомленість співробітників щодо ризиків і важливості захисту інформації, а також можливість шпигунства або підманування співробітників.

Для запобігання каналам витоку інформації в корпоративній мережі важливо приділяти належну увагу політиці безпеки, забезпечувати належний рівень захисту мережі та систем, регулярно оновлювати програмне забезпечення і використовувати надійні антивірусні програми.

Крім того, необхідно навчати співробітників правилам безпеки, усвідомлювати їх щодо важливості обережності при роботі зі зв'язками та обмежувати доступ до конфіденційної інформації лише необхідним особам.

Запобігання каналам витоку інформації є постійним процесом, який вимагає постійного оновлення технологій та підвищення уваги до безпеки. Відповідальне ставлення до цієї проблеми допоможе забезпечити захист конфіденційності та цілісності даних в корпоративній мережі.

Найбільш поширені та відомі канали витоку інформації в корпоративній мережі включають наступні:

- Незахищені мережеві з'єднання: Використання незахищених мереж, таких як відкриті Wi-Fi мережі або недостатньо захищені VPN з'єднання, може призвести до перехоплення інформації зловмисниками;
- Фішинг: Це метод, коли зловмисники намагаються обманом отримати конфіденційну інформацію, таку як паролі або номери кредитних карт, шляхом відправки підроблених електронних листів або створення фальшивих веб-сайтів;
- Вразливості в програмному забезпеченні: Наявність незакритих уразливостей у програмному забезпеченні, яке використовується в корпоративній мережі, може стати причиною витоку інформації. Зловмисники можуть експлуатувати ці вразливості, щоб отримати несанкціонований доступ до системи та конфіденційних даних;
- Недосконала політика безпеки: Якщо в організації відсутня належна політика безпеки, то можуть відсутні правила та процедури щодо захисту інформації, що може сприяти витоку даних;
- Зловживання привілеями співробітників: Внутрішні зловживання можуть бути одним з найбільш серйозних каналів витоку інформації. Співробітники, які мають привілеї доступу до конфіденційної

інформації, можуть використовувати свої права недобросовісно і передавати цю інформацію третім особам;

- Фізичний доступ до систем: Якщо фізичний доступ до серверних кімнат або інших приміщень, де зберігаються сервери та мережеві пристрої, недостатньо захищений, зловмисники можуть фізично зламати систему та отримати доступ до конфіденційної інформації;
- Канали витоку:
  - Електромагнітний канал. Даний канал створюється внаслідок виникнення електромагнітного поля, яке пов’язе з проходженням електричного струму в технічних засобах обробки інформації. Також, дане поле створювати (індукувати) струми в неподалік розташованих дротяних лініях, так звані наводки. Основними видами електромагнітного каналу є низькочастотний, мережевий, радіоканал, канал заземлення, лінійний канал;
  - Акустичний канал. Він пов'язаний з поширенням звукових хвиль в повітрі або пружних коливань в інших середовищах, що виникають при роботі пристроїв відображення інформації;
  - Канал несанкціонованого копіювання;
  - Канал несанкціонованого доступу.

1.6 Методи захисту інформації по електромагнітним каналам

Методи захисту інформації по електромагнітним каналам використовуються для запобігання несанкціонованому перехопленню та доступу до електромагнітних сигналів, які передаються через комунікаційні канали. Основна мета цих методів полягає в забезпеченні конфіденційності, цілісності та доступності передаваної інформації.

Ось кілька методів захисту інформації по електромагнітним каналам:

- Криптографічне шифрування: Це один з найбільш ефективних методів захисту інформації. Він використовує математичні алгоритми для шифрування даних перед їх передачею через електромагнітний канал. Тільки особи з належними ключами можуть розшифрувати дані, забезпечуючи конфіденційність передаваної інформації;
- Захист електромагнітних випромінювань (TEMPEST): Цей метод полягає в застосуванні технологій та заходів, що допомагають знизити електромагнітні випромінювання, які можуть бути перехоплені зовнішніми атакуючими. Використання екранування, фільтрації та інших технологій допомагає зменшити можливість перехоплення електромагнітних сигналів;

- Фізична ізоляція: Цей метод передбачає фізичне відокремлення електромагнітних компонентів та каналів передачі інформації від потенційних атакуючих. Це може включати використання екранування, спеціальних контейнерів або приміщень з електромагнітною ізоляцією;
- Аналіз та виявлення електромагнітних атак: Для захисту від потенційних загроз електромагнітними атаками використовуються спеціальні системи аналізу та виявлення. Ці системи виявляють аномалії в електромагнітних сигналах, що можуть свідчити про спробу несанкціонованого доступу до інформації;
- Фізичний контроль доступу: Для запобігання фізичному доступу до електромагнітних каналів та обладнання використовуються методи фізичного контролю доступу. Це може включати встановлення системи контролю доступу, використання біометричних ідентифікаторів, фізичні бар'єри та інші заходи безпеки.

Ці методи захисту інформації по електромагнітним каналам допомагають забезпечити безпеку передаваної інформації та запобігти несанкціонованому доступу до неї. Ретельне впровадження цих заходів в комунікаційні системи допомагає зберегти конфіденційність та цілісність даних.

Основними сервісами, що забезпечують інформаційну безпеку організації є:

- Протоколювання і аудит;
- Криптографія;
- Екранування.
- Управління доступом;

1.6.1 Протоколювання і аудит

Протоколювання і аудит в корпоративних мережах є важливим методом захисту інформації, який дозволяє забезпечити контроль, моніторинг та аналіз діяльності в мережевому середовищі. Цей метод дозволяє виявити потенційні загрози безпеці, виявити аномалії, а також відновити події, що сталися в мережі.

В кожному сервісі виникає певний набір подій, які можна поділити на:

- Зовнішні – події, що створені діями інших сервісів;
- Внутріші – події, що створені діями самого сервісу;

- Клієнтські – події, що створені діями адміністраторів чи користувачі інформаційної системи.

Протоколювання включає запис та збереження інформації про події, що відбуваються в корпоративній мережі, такі як вхід та вихід з системи, зміни конфігурацій, аутентифікація користувачів, передача даних тощо. Ці дані відображаються у формі журналів (лог-файлів), які можуть бути використані для подальшого аналізу та перевірки безпеки мережі.

Аудит включає процес перевірки та аналізу протоколів, щоб виявити можливі проблеми безпеки, аномальну активність або порушення політик безпеки. Цей процес може бути автоматизованим або виконуватися фахівцями з безпеки. Шляхом аналізу протоколів і аудиту можна виявити атаки, незвичайну поведінку користувачів, пошукати слабкі місця у мережі та приймати відповідні заходи безпеки.

Переваги методу протоколювання і аудиту включають:

- Виявлення загроз безпеці: Шляхом протоколювання і аудиту можна виявити незвичайну або підозрілу активність в мережі, що може бути пов'язана зі зловмисними діями або атаками. Це дозволяє оперативно реагувати на потенційні загрози та запобігти їх подальшому поширенню;
- Відновлення подій: Журнали протоколювання дозволяють відновити події, що сталися в мережі, і проаналізувати їх. Це корисно для виявлення причин і наслідків подій, виявлення помилок або порушень політик безпеки та вжиття заходів для їх усунення;
- Виконання вимог регуляторних органів: Протоколювання і аудит є важливими компонентами для виконання вимог регуляторних органів і стандартів безпеки даних. Ці дані можуть використовуватися для аудиту безпеки, звітності та дотримання вимог;
- Покращення безпеки мережі: Аналіз журналів протоколювання дозволяє виявити слабкі місця в мережі та вжити відповідних заходів для покращення безпеки. За допомогою аудиту можна виявити проблеми безпеки, недостатню конфігурацію систем та вразливості, які потребують уваги та захисту.

Застосування методу протоколювання і аудиту допомагає підвищити безпеку корпоративних мереж, забезпечити виявлення загроз безпеці та вжити відповідних заходів для їх запобігання. Він є важливою складовою стратегії безпеки інформації в організації.

1.6.2 Криптографія

Криптографія є одним із основних методів захисту інформації в корпоративних мережах. Вона використовує математичні алгоритми для шифрування та розшифрування даних з метою забезпечення конфіденційності, цілісності та аутентичності інформації.

Основні принципи криптографії в корпоративних мережах включають:

- Шифрування даних: Криптографія дозволяє зашифровувати дані перед їх передачею через мережу. Шифрування перетворює звичайний текст у незрозумілий для сторони, яка не має ключа для розшифрування. Це забезпечує конфіденційність інформації та запобігає несанкціонованому доступу до даних.
- Аутентифікація: Криптографія дозволяє перевірити автентичність користувача або пристрою в мережі. Це досягається за допомогою цифрових підписів, сертифікатів або інших методів, що гарантують, що сторона, з якою взаємодіється користувач або пристрій, є справжньою та не підробленою.
- Цілісність даних: Криптографія дозволяє перевірити цілісність даних, тобто впевнитися, що дані не були змінені під час передачі по мережі. Це досягається за допомогою хеш-функцій або кодування повідомлень, які дозволяють виявити будь-які зміни в даних.
- Керування ключами: Криптографія вимагає використання ключів для шифрування та розшифрування даних. Ефективне керування ключами є важливою складовою безпеки криптографічних систем. Це включає генерацію безпечних ключів, збереження їх у безпечному місці, обмін ключами між сторонами та періодичну зміну ключів.

Основні методи криптографічного шифрування включають симетричне шифрування і асиметричне шифрування. Кожен з цих методів має свої особливості і використовується для різних цілей.

- Симетричне шифрування: У симетричному шифруванні використовується один і той самий ключ для шифрування та розшифрування даних. Цей ключ має бути обміненим між взаємодіючими сторонами перед передачею зашифрованої інформації. Одним з найпоширеніших алгоритмів симетричного шифрування є Advanced Encryption Standard (AES). Він забезпечує високий рівень безпеки і швидкодію шифрування.

- Асиметричне шифрування: У асиметричному шифруванні використовується пара ключів - публічний ключ і приватний ключ. Публічний ключ використовується для шифрування даних, тоді як приватний ключ використовується для розшифрування даних. Ця пара ключів взаємно пов'язана, тобто дані, зашифровані за допомогою публічного ключа, можуть бути розшифровані лише за допомогою відповідного приватного ключа. Асиметричне шифрування також використовується для цифрових підписів, які забезпечують аутентичність та цілісність даних. Найпоширенішим алгоритмом асиметричного шифрування є RSA (Rivest-Shamir-Adleman).
- Хеш-функції: Хеш-функції використовуються для створення хеш-коду, який є унікальним представленням вихідних даних фіксованої довжини. Цей хеш-код може бути використаний для перевірки цілісності даних, оскільки будь-яка незначна зміна в початкових даних призведе до зміни хеш-коду. Хеш-функції, такі як SHA-256 (Secure Hash Algorithm 256-bit), використовуються для захисту від модифікації даних та встановлення їх автентичності.

Застосування криптографії в корпоративних мережах дозволяє забезпечити конфіденційність даних, запобігти несанкціонованому доступу та зміні даних, а також забезпечити автентичність взаємодіючих сторін. Вона відіграє важливу роль у забезпеченні безпеки інформації та захисті корпоративних мереж від зловмисних дій.

1.6.3 Екранування

Екранування є одним з методів захисту в корпоративних мережах і використовується для зменшення електромагнітного випромінювання та експозиції до зовнішніх електромагнітних сигналів. Його основна мета - запобігти несанкціонованому доступу до електромагнітної інформації, яка може бути витягнута з мережі через радіоелектронні канали.

Для досягнення ефективного екранування використовуються наступні методи:

- Фізичне екранування: Цей метод полягає у використанні спеціальних матеріалів, які здатні блокувати або зменшувати проникнення електромагнітних сигналів. Наприклад, металеві екрануючі контейнери або кабельні канали з екраном можуть запобігти витоку електромагнітної інформації. Фізичне екранування вимагає належної конструкції і установки обладнання для забезпечення ефективності;

- Електричне екранування: Цей метод передбачає використання електричних екранів для блокування електромагнітних сигналів. Шари електропровідних матеріалів, таких як фольга або провідники, використовуються для створення електричного бар'єру навколо електронних пристроїв або кабелів. Це допомагає знизити перехід електромагнітних сигналів через пристрої і кабелі, тим самим запобігаючи витоку інформації;
- Акустичне екранування: Цей метод використовує звукові хвилі для маскування електромагнітних сигналів. Шумові генератори або спеціально розроблені акустичні матеріали використовуються для створення звукового поля, яке заважає проникненню електромагнітних сигналів і витоку інформації;
- Скрінінг електромагнітних сигналів: Цей метод включає в себе використання електромагнітних фільтрів і засобів підавлення для блокування або зменшення рівня електромагнітного шуму та інтерференції. Це може включати використання спеціальних компонентів, феритових кілець, екранів на кабелях і фільтрів для блокування або фільтрації небажаних електромагнітних сигналів;

Ефективне екранування в корпоративних мережах допомагає запобігти несанкціонованому доступу до електромагнітної інформації та забезпечити конфіденційність даних. При впровадженні екранування необхідно враховувати фізичну структуру мережі, типи пристроїв та кабелів, а також відповідні стандарти безпеки.

1.6.4 Управління доступом

Управління доступом є важливим методом захисту інформації в корпоративних мережах і використовується для контролю та обмеження доступу користувачів до різних ресурсів та сервісів в мережі. Його основна мета - забезпечити конфіденційність, цілісність та доступність даних шляхом встановлення правил і обмежень для кожного користувача чи групи користувачів.

Найпоширеніші методи управління доступом в корпоративних мережах включають:

- Аутентифікація користувачів: Цей метод передбачає перевірку ідентичності користувача перед наданням доступу до мережевих ресурсів. Це може включати введення логіна та пароля, використання

біометричних даних (відбитки пальців, розпізнавання обличчя) або використання токенів або смарт-карток.

- Авторизація користувачів: Після аутентифікації користувача система виконує процес авторизації, де встановлюються права доступу для користувача до конкретних ресурсів. Це забезпечує контроль над тим, які операції може виконувати користувач і які дані він може переглядати, редагувати чи видаляти.
- Ролева модель доступу: Цей метод використовує концепцію ролей для управління доступом. Кожен користувач призначається до певної ролі, яка визначає його права доступу до різних ресурсів. Наприклад, можуть бути визначені ролі адміністратора, менеджера, співробітника, і кожна роль матиме свої обмеження та повноваження.
- Аудит доступу: Цей метод включає в себе запис і аналіз дій користувачів в мережі. Журнали аудиту фіксують дії користувачів, такі як вхід в систему, доступ до ресурсів, зміни конфігурації тощо. Аналіз журналів аудиту дозволяє виявити незвичайну або підозрілу активність, що може вказувати на потенційне порушення безпеки.
- Використання вогнезахисних систем: Вогнезахисні системи допомагають захистити корпоративну мережу від несанкціонованого доступу, шкідливих програм та інших загроз. Вони можуть виявляти та блокувати небезпечний трафік, моніторити події в мережі та сповіщати про потенційні загрози.

Ці методи управління доступом спільно забезпечують збалансований підхід до захисту інформації в корпоративних мережах, дозволяючи забезпечити необхідну конфіденційність та доступність даних, а також контролювати та обмежувати права користувачів для забезпечення безпеки мережі.

1.7. Проблема захисту корпоративної інформації

1.7.1 Типи корпоративних мереж

Критично важливі підприємства, такі як ракетно-космічні комплекси, металургічна та хімічна промисловість, транспортні галузі, а також енергетичні підприємства, включаючи теплові та атомні електростанції, є прикладами *підприємств критичного призначення в корпоративних мережах*. Вони ставлять особливі вимоги до системи захисту інформації.

Системи реального часу в корпоративних мережах є невід'ємною частиною підприємств критичного призначення. Ці системи вимагають негайної реакції на події або вплив на зовнішнє середовище в межах встановлених обмежень часу. Вони повинні працювати безперервно, навіть у найскладніших умовах, таких як хімічне, бактеріологічне або інше забруднення, електромагнітне або радіаційне опромінення.

У *системах м'якого реального часу* допускаються певні затримки реакції, які вважаються відновлювальними помилками. Наприклад, якщо система не встигла опрацювати прийнятий пакет даних, це може призвести до перерви у передачі та повторної відправки. Проте, дані не втрачаються, а продуктивність системи не зменшується.

Насупротив, *системи жорсткого реального часу* не терплять жодних затримок реакції незалежно від умов. Випадки запізнення можуть мати катастрофічні наслідки або призвести до марнотратства ресурсів. У таких ситуаціях система повинна негайно зупиняти операцію та блокувати її, щоб забезпечити надійність інших частин системи.

Одним з важливих аспектів *інформаційно-обчислювальних та управляючих корпоративних мереж* є їх здатність працювати в реальному часі. Це вимагає використання систем реального часу, щоб забезпечити оперативність обробки і передачі інформації. Для підприємств загального призначення може бути достатнім м'який режим реального часу, що дозволяє реагувати на події протягом 24 годин. Однак, для підприємств критичного призначення обов'язковим є жорсткий режим реального часу, де негайна реакція на події є критично важливою.

Таким чином, корпоративні мережі, особливо ті, що обслуговують підприємства критичного призначення, вимагають використання систем реального часу для забезпечення безперебійної та надійної роботи. Це дозволяє досягти високого рівня захисту інформації та ефективності в умовах змінюючогося середовища та строгих вимог щодо реагування на події.

1.7.2 Основні принципи захисту в комп’ютерних корпоративних мережах

Інформація є надзвичайно важливим поняттям, тісно пов'язаним з комп'ютерними технологіями, системами зв'язку та мережами. Охорона інформації в цих сферах стає пріоритетом. У чесній конкуренції, основою є дотримання закону та моральних норм. Проте, зустрічаються випадки, коли підприємці порушують ці правила, намагаються отримати інформацію, яка може завдати шкоди іншій стороні та використати її для власної користі. Недостатній контроль з боку держави та недосконаліть правоохоронної системи змушують підприємців, виробництва та бізнесу самостійно боротися з негативними процесами, щоб запобігти витоку важливої конфіденційної інформації.

Існує багато причин, які призводять до зростання комп'ютерних злочинів і спричиняють значні економічні, матеріальні та репутаційні збитки. Серед них можна виділити наступні:

- Поступове відмовлення від паперової технології передачі та збереження інформації і зростання використання електронних носіїв, при цьому розвиток технологій захисту на таких носіях на даний момент є недостатнім.
- Розгортання глобальних мереж та збільшення доступу до інформаційних ресурсів.
- Зростання складності програмних засобів.

У сучасному світі спостерігається тенденція до збільшення кількості випадків комп'ютерних злочинів. З урахуванням численних загроз у сучасних мережах, забезпечення безпеки вимагає широкого спектру знань та досвіду у різних спеціалізаціях. Поширеною загрозою є спеціальне використання шкідливого програмного коду, такого як віруси, троянські програми, хробаки, а також атаки DoS (відмова в обслуговуванні) та DDoS (розподілена відмова в обслуговуванні).

Ключовими складовими безпеки, які повинні бути враховані в створенні інфраструктури захисту, є моніторинг, управління доступом, управління прогнозуванням, ведення контрольних журналів та управління конфіденційністю.

У контексті корпоративних мереж, виявлення небезпечних атак та розробка систем виявлення та протидії є ключовими аспектами для захисту інформації.

1.7.3 Класифікація та системи виявлення комп’ютерних атак

Необхідно докладно класифікувати мережеві атаки для ефективного захисту від них. Зараз існує багато різних типів класифікаційних ознак, таких як пасивні і активні, зовнішні і внутрішні атаки, свідомі й несвідомі. В державних організаціях з захисту конфіденційної інформації використовують таку класифікацію комп'ютерних атак:

- Віддалене проникнення - атака, яка здійснюється дистанційно через мережу для отримання контролю над комп'ютером.
- Локальне проникнення - атака, яка дозволяє несанкціонований доступ до конкретного вузла.
- Віддалена відмова в обслуговуванні - атака, спрямована на заваду нормальному функціонуванню системи в рамках глобальної мережі.
- Локальна відмова в обслуговуванні - атака, яка порушує функціонування системи в межах локальної мережі.
- Атаки з використанням мережних сканерів - базуються на програмах, що визначають доступні сервіси для атаки.
- Атаки з використанням сканерів вразливостей - полягають у пошуку вразливостей на вузлах, які потім використовуються для атаки.
- Атаки з використанням зламувачів паролів - програми, які намагаються підібрати паролі користувачів.
- Атаки з використанням аналізаторів протоколів - засновані на прослуховуванні мережного трафіку з метою зловживання.

Ця класифікація майже повністю охоплює можливі атаки, але сама по собі не забезпечує визначення елементів мережі, які можуть стати об'єктом атаки, або наслідки успішної атаки. Для побудови моделі загроз безпеки та організації захисту інформації в корпоративній мережі необхідно враховувати цей аспект.

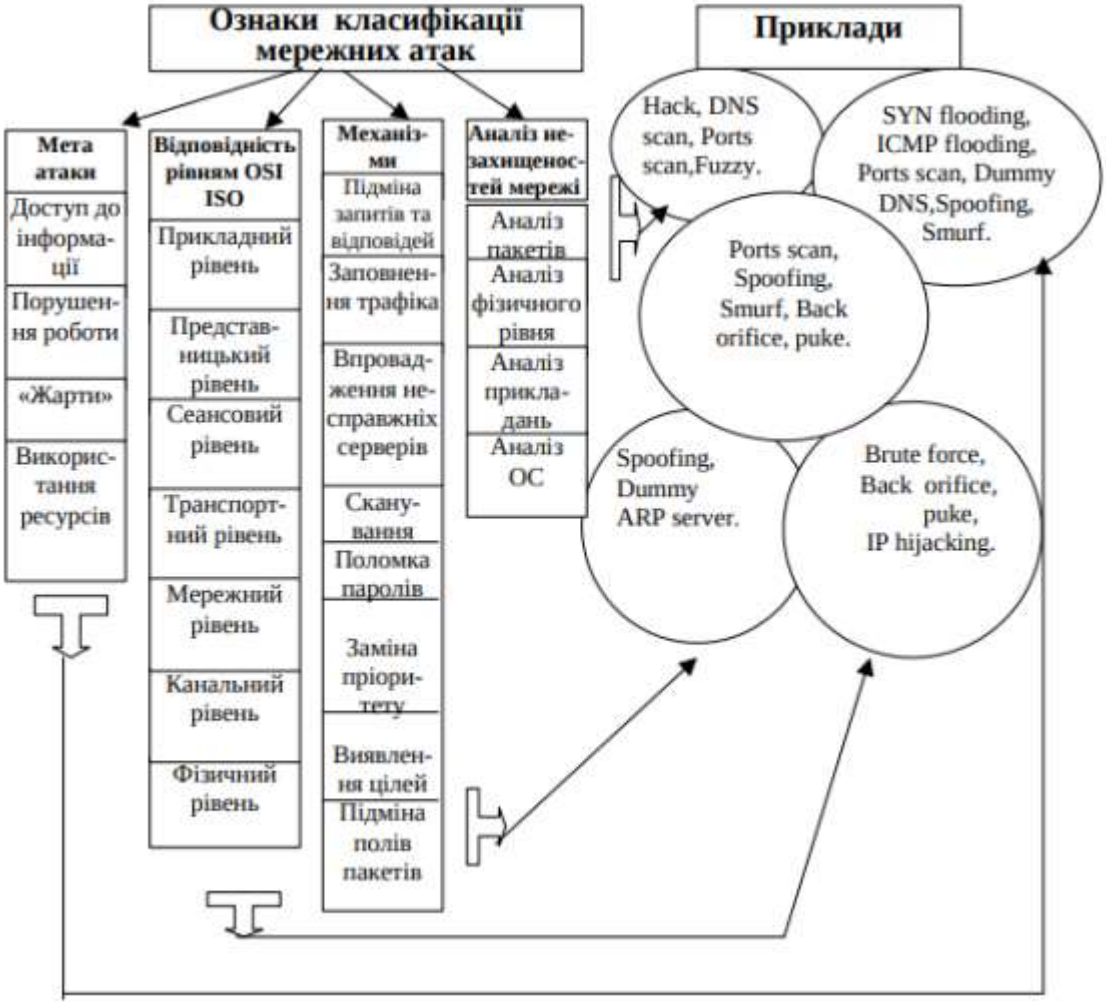

Рис.1.2 Класифікація атак різних рівнів

Загрози для корпоративних мереж також можуть включати аналіз трафіку. Аналіз трафіку є методом отримання паролів та інших особистих даних користувачів мережі. Для цього використовуються спеціалізовані аналізатори, такі як "sniffer", які перехоплюють всі пакети і визначають ті пакети, які містять паролі та важливі особисті дані.

Наразі деякі протоколи передачі даних, наприклад FTP, TELNET, HTTP, SMTP, POP3, IMAP, NNTP і IRC, передають дані в незахищеному вигляді, що дозволяє зловмисникам перехопити паролі, номери кредитних карток та іншу конфіденційну інформацію. Хоча існують протоколи, які дозволяють захищати мережу і шифрувати трафік, вони ще не стали загальноприйнятими стандартами і не використовуються кожним користувачем. Це пов'язано з обмеженнями на експорт сильної криптографії, які існують у деяких країнах, і частково обмежує їх поширення і використання.

Аналіз трафіку надає можливість:

- Розуміти принципи роботи комп'ютерної системи і встановлювати зв'язок між подіями та командами, які відбуваються в системі. Це досягається шляхом перехоплення та аналізу пакетів на канальному рівні. Розуміння принципів роботи дозволяє моделювати типові атаки на практиці.
- Перехоплювати потік даних, якими обмінюються об'єкти розподіленої системи. Така атака полягає в отриманні доступу до інформації, яку об'єднує користувачів. У цьому випадку можливість модифікувати трафік відсутня, і аналіз можливий лише в межах одного сегмента. Часто таким чином перехоплюють імена та паролі користувачів, якщо вони передаються через незахищену мережу.

Аналіз мережевого трафіку є пасивним впливом на мережу, і його виконання може порушити конфіденційність інформації всередині одного сегмента мережі на канальному рівні моделі OSI.

У корпоративних мережах також існує проблема недостатньої ідентифікації та аутентифікації віддалених об'єктів. Однією з головних проблем є неоднозначність ідентифікації повідомлень, що передаються між об'єктами та суб'єктами взаємодії. У розподілених системах ця проблема зазвичай вирішується шляхом "рукостискання" (handshake) під час встановлення віртуального каналу між об'єктами. Однак, існують випадки, коли окремий канал не розробляється і повідомлення відправляються без підтверджень.

Для адресації повідомлень у розподілених системах використовується мережева адреса, яка унікальна для кожного об'єкта і використовується для ідентифікації об'єктів у системі. Проте ця адреса може бути підроблена, тому не можна покладатися лише на неї для забезпечення безпеки.

При побудові системи захисту корпоративної мережі завжди слід враховувати такі фактори:

- атаки на мережу можуть бути різноманітними;
- більшість атак мають спрямований характер;
- випадкові атаки найнебезпечніші для системи захисту;
- силова протидія автономним атакам зазвичай не дає результатів.

Ці фактори впливають як на мережі загального призначення, так і на корпоративні мережі. Однак система захисту корпоративної мережі

підприємства має свої особливості, які випливають з унікальних вимог системи. Однією з найважливіших відмінностей є час. Корпоративні мережі повинні бути захищені в режимі реального часу, особливо у підприємствах критичної інфраструктури, де використовуються системи жорсткого часу.

Ключовим аспектом інформаційної безпеки є наявність або відсутність віддалених філій та підрозділів. Зазвичай головне підприємство має більш розвинуту систему захисту інформації, ніж регіональні підрозділи. Однак, якщо підрозділи та філії мають подібну архітектуру, це надає можливість покращити систему захисту. Важливу роль у цьому відіграють організаційні заходи, на які слід звернути особливу увагу.

Системи виявлення вторгнень (IDS) стали невід'ємною частиною стратегії мережевого захисту, що швидко набувають популярності в корпоративних мережах. Вони виконують головну функцію виявлення несанкціонованих вторгнень, забезпечуючи аналіз кожного пакету, щоб визначити його шкідливість. IDS використовують різні методи, які мають свої переваги і недоліки.

Одним з методів IDS є аналіз мережевого трафіку, який охоплює як вхідний, так і вихідний трафік у корпоративних мережах. IDS шукають недобросовісний трафік, не змінюючи його потік, і сповіщають системного адміністратора про можливі напади або неправомірне використання.

Інший метод IDS передбачає аналіз даних та протоколів мережі. IDS використовує RFC (Стандартні технічні вимоги) для перевірки очікуваних значень протоколів. Якщо значення відрізняється, IDS виявляє можливі вторгнення.

IDS докладно розглядає кожне поле IP, TCP і UDP протоколів у вхідних пакетах і сповіщає про будь-яке порушення протоколу. Технології IDS розвиваються, та вони стають складнішими для обходу. Аналіз протоколів відрізняється від аналізу сигнатур, який базується на відомих характеристиках атак для виявлення вторгнень.

Системи аналізу сигнатур мають свої переваги, такі як швидкість обробки пакетів та простота написання правил. Вони також підтримують швидку генерацію сигнатур для нових загроз. Але з часом швидкість роботи знижується через зростання кількості сигнатур, що перевіряються. Це впливає на продуктивність системи.

Аналіз протоколів має свої переваги і недоліки. Він часто є повільним і вимагає складнішого написання та налаштування правил. Залежність від виробника може створювати проблеми, оскільки виробники додають нові

правила, які можуть порушувати загальні стандарти і протоколи, внаслідок чого зловмисники мають більше можливостей.

У контексті корпоративних мереж, IDS є важливим елементом системи безпеки, який допомагає виявляти потенційні загрози та захищати мережу від несанкціонованого доступу та атак.

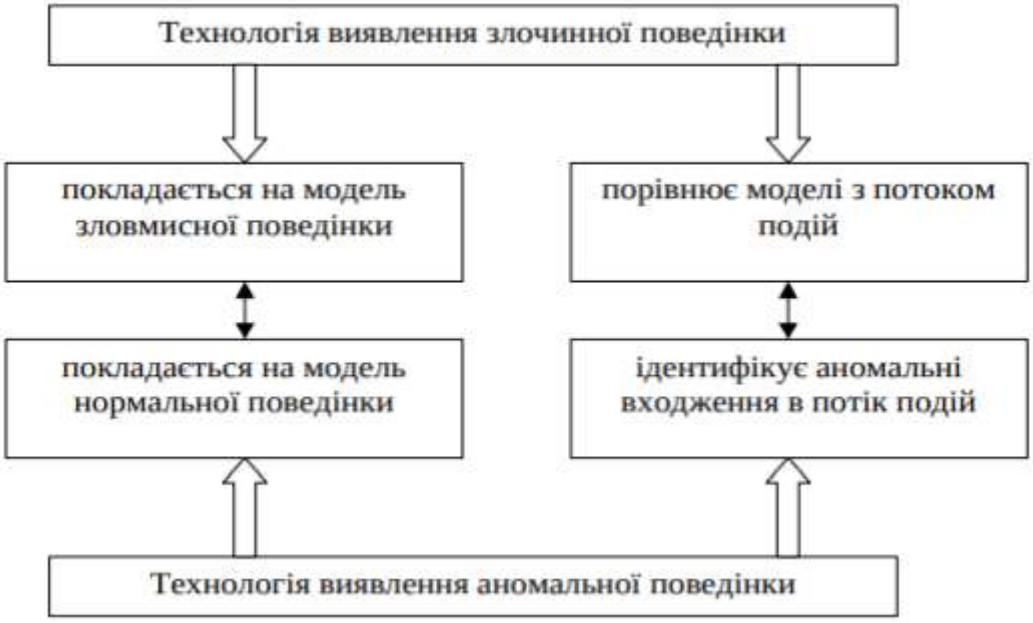

Рис. 1.3 Підходи до побудови системи виявлення атак

2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ КОРПОРАТИВНОЇ СИСТЕМИ ПІДПРИЄМТСВА

2.1 Структурна схема комплексу технічних засобів системи

Структурна схема комплексу технічних засобів демонструє основні компоненти комп'ютерної системи підприємства синтетичних виробів «Fenrir», включає мережеве обладнання. Представлені ієрархічні рівні моделі організації мережі та підмереж, що становлять корпоративну мережу підприємства.

Впровадження комп'ютерної системи на «Fenrir» забезпечує такі можливості: доступ фахівців з різних підрозділів підприємства до спільних ресурсів; централізоване управління, адміністрування та технічне обслуговування інформаційно-комунікаційних ресурсів; доступ до структурованої інформації в режимах on-line та off-line; впровадження єдиної системи електронної пошти та електронного документообігу; співпрацю з бізнес-системами інших організацій, обчислювальними мережами державних установ та фінансово-кредитними органами; функціональну масштабованість, що дозволяє розширювати корпоративну мережу.

Рівень ядра, де здійснюється комутація трафіку, складається з п'яти маршрутизаторів, які підключені до мереж WAN. Віддалений доступ до мережі "Відділ роботи з кадрами" реалізований за допомогою технології VPN. Підключення проектованої мережі до Інтернет здійснюється через маршрутизатор рівня ядра.

Рівень доступу до середовища передачі даних включає дев'ять комутаторів, які формують підмережі LAN та VLAN.

Основні пристрої, які виділені на структурній схемі, включають:

- Кінцеві мережні пристрої, такі як персональні комп'ютери з налаштованою IP-адресою та необхідним програмним забезпеченням для роботи персоналу та віддаленого адміністрування, мережні принтери з інтерфейсом для підключення до мережі, а також сервери, зокрема файловий сервер TFTP, веб-сервер HTTP та DNS-сервер;
- Комутатори рівня доступу, які використовуються для з'єднання вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатори передають дані безпосередньо отримувачеві, що підвищує продуктивність і безпеку мережі. На фабриці синтетичних виробів «Fenrir» в підмережі "Підрозділ маркетингу" встановлено 3 комутатори, які об'єднують три організаційні структурні відділи з використанням технології VLAN. В підмережі "Відділ роботи з кадрами" встановлено 3

комутатори, які об'єднані за допомогою технології агрегації каналів. У інших підмережах встановлено по одному комутатору для робочих груп.

- Маршрутизатор, який на основі інформації про топологію мережі та правилах приймає рішення щодо маршрутизації пакетів мережевого рівня між різними сегментами мережі. В мережі підприємства синтетичних виробів «Fenrir» рівень ядра та розподілу об'єднані в маршрутизаторах. Підключення проектованої мережі до Інтернет здійснюється через маршрутизатор рівня ядра.
- Середовище передачі даних, яке включає кабельну розводку всередині будівлі адміністрації відповідно до обраної технології мережі.

Ця комп'ютерна система підприємства синтетичних виробів «Fenrir» забезпечує реалізацію доступу фахівців з різних підрозділів підприємства до спільних ресурсів, централізоване управління, адміністрування та технічне обслуговування інформаційно-комунікаційних ресурсів, доступ до структурованої інформації в режимах on-line та off-line, єдину систему електронної пошти та електронного документообігу, взаємодію працівників з бізнес-системами інших організацій, обчислювальними мережами державних установ та фінансово-кредитними органами, а також функціональну масштабованість для побудови корпоративної мережі.

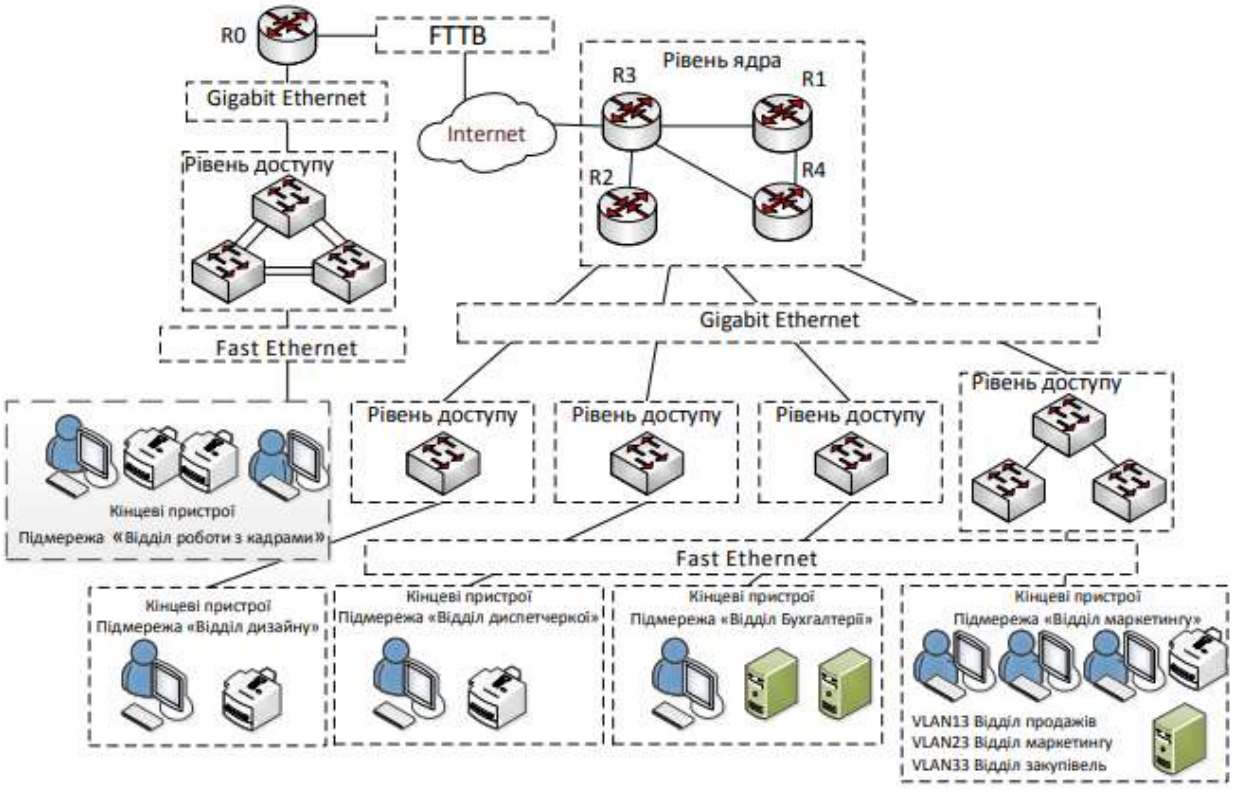

Рис.2.1 Структурна схема комплексу технічних засобів підприємства синтетичних виробів «Fenrir»

2.2 Апаратні засоби КС

При формуванні мережевого обладнання для корпоративної мережі підприємства синтетичних виробів «Fenrir» були враховані вимоги та потреби системи.

Для активного обладнання вибрано відповідні комутатори та маршрутизатори, враховуючи їх характеристики та вимоги до мережі. При виборі активного мережного обладнання враховувалися такі фактори, як кількість та типи інтерфейсів, підтримувані протоколи та пропускна здатність.

У конкретному випадку було обрано наступне обладнання:

- Маршрутизатори мережі, зокрема Cisco 2901-SEC/K9 серії 2911, які мають можливості розширення та забезпечують високопродуктивне підключення до мережі Інтернет зі швидкістю маршрутизації до 75 мегабіт за секунду. Вони підтримують гігабітні Ethernet порти, слоти розширення EHWIC та технологію Services Ready Engine (SRE) для розгортання апаратних і програмних сервісів.
- Комутатори робочих груп (підрозділів), такі як Cisco SB SF200-24FP, які підтримують технологію DHSP, мають достатню кількість портів для підключення кінцевих пристроїв та забезпечують швидкість передачі даних не менш як 100 Мбіт/с. Вони підтримують VLAN, Power over Ethernet (PoE) та інші функції.

Обране обладнання від компанії Cisco Systems було вибрано через його надійність, технічну підтримку та постійні оновлення програмного забезпечення.

Це обладнання дозволяє забезпечити ефективну роботу корпоративної мережі підприємства синтетичних виробів «Fenrir» з високою швидкістю передачі даних, безперебійним з'єднанням та підтримкою необхідних функцій і протоколів.

Крім того, у будівлі адміністрації фабрики необхідно встановити шість комутаторів, які також повинні підтримувати технологію DHSP і забезпечувати швидкість передачі даних не менше як 100 Мбіт/с. Для цього використовується комутатор Cisco SB SF200-24FP з 24 портами (100 Мбіт/с) та 2 портами Gigabit Ethernet.

Таким чином, обране обладнання Cisco забезпечує ефективну роботу корпоративної мережі підприємства синтетичних виробів «Fenrir», забезпечуючи надійність, швидкість та підтримку необхідних функцій.

Комутатори та маршрутизатори ретельно відповідають потребам та вимогам фабрики для побудови корпоративної мережі.

Позиція	Найменування	Марка	Кількість
1	2901-SEC/K9 4 EHWIC slots, IP Base, 10/100/1000Base-T, Gigabit Ethernet	Anton_R1 Anton_R2 Anton_R3 Anton_R4 Anton _R5	5
3	Cisco SB SF200-24FP Ethernet Switch 24 x Fast Ethernet Network;2 x Gigabit Ethernet Uplink;Fast Ethernet 10Base-T	Anton_Sw1.1 Anton_Sw1.2 Anton_Sw1.3 Anton_Sw2 Anton_Sw3 Anton_Sw5 Anton_SW0 Anton_SW1 Anton_SW2	9

Таблиця 2.1 Обладнання

2.3 Архітектура мережі

При проектуванні корпоративних мереж застосовується ієрархічна структура, яка допомагає організувати об'єкти на рівнях, встановити зв'язки між ними та визначити їх функції. Відповідно до підходу, запропонованого компанією Cisco Systems, комп'ютерні мережі розглядаються як трирівнева ієрархічна модель. З урахуванням невеликого розміру мережі підприємства синтетичних виробів «Fenrir», рівні ядра і розподілу будуть об'єднані в маршрутизаторах, а рівень доступу буде представлений комутаторами робочих груп.

Для впровадження корпоративної мережі підприємства синтетичних виробів «Fenrir» була обрана логічна топологія «ієрархічна зірка». Ця топологія є найшвидкодіючою серед усіх топологій обчислювальних мереж, оскільки передача даних між робочими станціями відбувається через центральний вузол за допомогою окремих ліній, використовуваних тільки цими робочими станціями.

Основною технологією мережі є Ethernet, яка була обрана як базова технологія. Ethernet може забезпечити найвищу швидкість, надійність і якість передачі даних, і вона є найпоширенішою технологією. На рівні доступу для підключення робочих груп використовується технологія Fast Ethernet, а між маршрутизатором і комутатором використовується GigabitEthernet.

Таким чином, впровадженням ієрархічної структури зі зв'язкою типу "зірка" та використанням технологій Ethernet, Fast Ethernet та GigabitEthernet, підприємства синтетичних виробів «Fenrir» забезпечить надійну, швидку та ефективну корпоративну мережу.

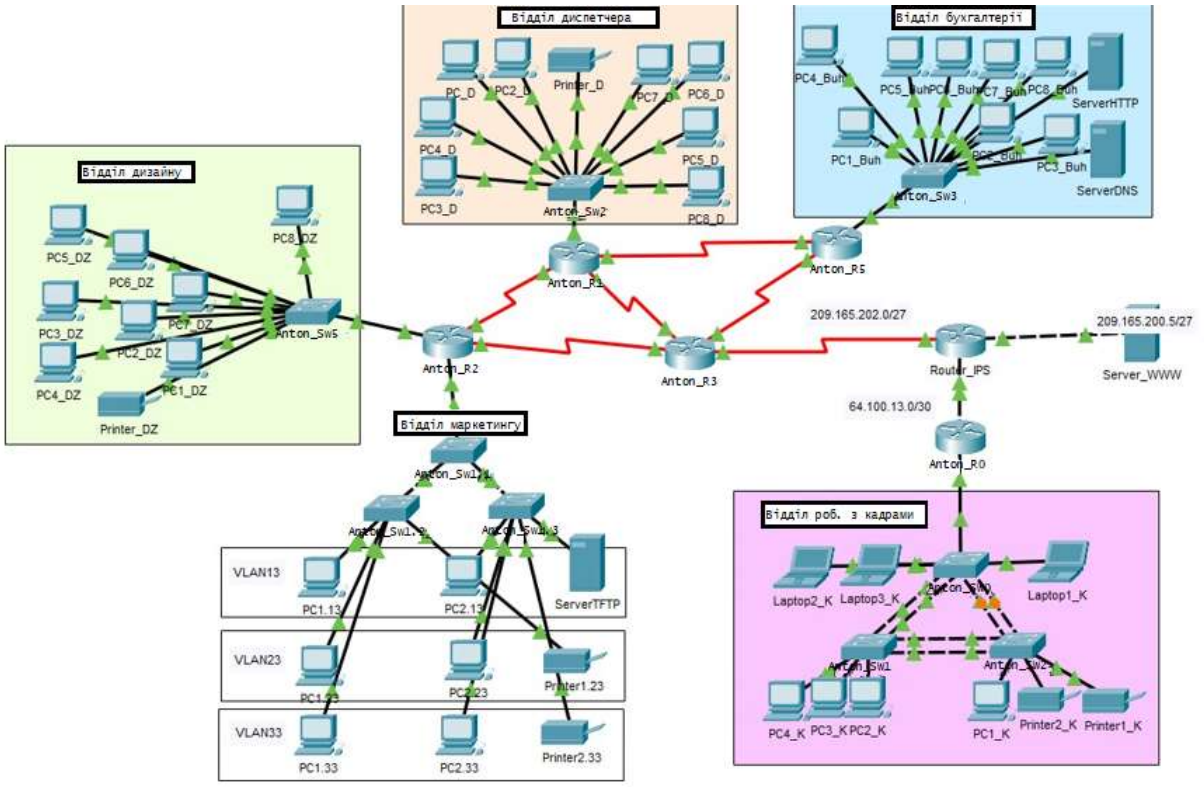

Рис.2.2 Архітектура мережі підприємства синтетичних виробів «Fenrir»

Мережа корпорації використовує одну IP-адресацію простору 192.168.24.0.0/21. Шляхи міжмережевого середовища (IP-підмережі) розподілені маршрутизаторами на п'ять підмереж. В цій мережі використовується адресація IP версії 4, що вимагає використання технології NAT для доступу до Інтернету. Адреса мережі для підключення до Інтернету - 209.165.202.0/27. Для маршрутизації використовується протокол OSPF. Маршрутизатор Anton_R2 використовує технологію інкапсуляції 802.1Q для маршрутизації між VLAN. Для каналів між маршрутизаторами використовується адресний блок 10.0.3.0/24. В VLAN мережах використовується адресація кінцевих пристроїв з використанням протоколу DHCP.

У віддаленій мережі "Відділ роботи з кадрами" для покращення швидкості передачі даних використовується технологія PAgP для агрегації каналів передачі даних.

Кінцеві мережні пристрої розподілені на чотири підмережі, враховуючи функціонал та напрямок підрозділів підприємства. Підмережа №2 "Відділ диспетчеркої" призначена для підключення 50 абонентів. Підмережа №3

"Відділ бухгалтерії" призначена для підключення 39 абонентів. Підмережа №5 "Відділ дизайну" призначена для підключення 40 абонентів. Підмережа №4 "Відділ роботи з кадрами" призначена для підключення 10 абонентів. Найбільша підмережа "Відділ маркетингу" нараховує 120 абонентів і, з міркувань безпеки даних, поділена на три віртуальні мережі - VLAN13, VLAN23, VLAN33. Комутатори Cisco Catalyst 2960 та маршрутизатор Cisco 2911 підтримують функціонал віртуальних мереж.

Таким чином, використання "Корпоративних мереж" дозволяє організації створити складну ієрархічну структуру мережі, що дозволяє ефективно розподілити об'єкти за рівнями, встановити зв'язки між об'єктами і виконувати необхідні функції.

3. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Схема адресації

Для побудови мережі підприємства синтетичних виробів «Fenrir» був використаний адресний простір 192.168.24.0/21 відповідно до технічних вимог. Розподіл адреси мережі на підмережі здійснюється з використанням технологій CIDR і VLSM. При проектуванні корпоративної мережі враховувалися критерії найкращої суммаризації та мінімальної витрати адрес.

Для забезпечення мінімальної витрати адрес та найкращої суммаризації використовувався метод VLSM. Він дозволяє розділити простір мережі на нерівні частини, де довжина маски підмережі залежить від кількості бітів, запозичених для кожної підмережі. Таким чином, мережа спочатку розбивається на підмережі, а потім ці підмережі також розбиваються на підмережі, що дозволяє створити підмережі різних розмірів.

У відповідності до технічних вимог до КС підприємства синтетичних виробів «Fenrir» було об'єднано 5 підмереж з хост-вузлами, 5 мереж маршрутизаторів, а також 2 мережі зовнішнього шлюзу з заданими адресами 209.165.202.0/27 та 64.100.13.0/30. Кожна мережа маршрутизаторів та зовнішнього шлюзу вимагає використання 2 IP-адрес.

При розрахунку схеми адресації мережі було використано наступні блоки адрес: 192.168.24.0/21 для виділення підмереж, 10.0.3.0/24 для каналів між маршрутизаторами. Кількість вузлів в підмережах складає: LAN1 - 120 вузлів, LAN2 - 40 вузлів, LAN3 - 50 вузлів, LAN4 - 39 вузлів, LAN5 - 10 вузлів.

В таблиці 5.1 наведена схема IP-адресації мережі КС підприємства синтетичних виробів «Fenrir», розрахована з використанням методу VLSM.

Таким чином, застосування "Корпоративних мереж" дозволяє ефективно розподілити адресний простір, забезпечити найкращу суммаризацію та мінімізувати витрати адрес.

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN1 «Відділ маркетингу»	120	192.168.24.0	255.255.255.128	192.168.24.1 - 192.168.24.126
LAN2 «Відділ диспетчерської»	50	192.168.24.128	255.255.255.192	192.168.24.129 - 192.168.24.190
LAN5 «Відділ дизайну»	40	192.168.24.192	255.255.255.192	192.168.24.193 - 192.168.24.254
LAN3 «Відділ Бухгалтерії»	39	192.168.25.0	255.255.255.192	192.168.25.1 - 192.168.25.62
LAN4 «Відділ роботи з кадрами»	10	192.168.25.64	255.255.255.240	192.168.25.65 - 192.168.25.78

VLAN13	20	192.168.24.0	255.255.255.224	192.168.24.1 - 192.168.24.30
VLAN23	20	192.168.24.32	255.255.255.224	192.168.24.33 - 192.168.24.62
VLAN33	20	192.168.24.64	255.255.255.224	192.168.24.65 - 192.168.24.94
VLAN99	20	192.168.24.96	255.255.255.224	192.168.24.97 - 192.168.24.126
WAN1	2	10.0.3.0	255.255.255.252	10.0.3.1 - 10.0.3.2
WAN2	2	10.0.3.4	255.255.255.252	10.0.3.5 - 10.0.3.6
WAN3	2	10.0.3.8	255.255.255.252	10.0.3.9 - 10.0.3.10
WAN4	2	10.0.3.12	255.255.255.252	10.0.3.13 - 10.0.3.14
WAN5	2	10.0.3.16	255.255.255.252	10.0.3.17 - 10.0.3.18

Табл.3.1 Схема адресації мережі

Відповідно до вимог, потрібно налаштувати IP-адреси для комп'ютерів, серверів, мережевих пристроїв та інтерфейсів. У таблиці 5.2 наведена адресація всіх пристроїв, що використовуються у мережі підприємства синтетичних виробів «Fenrir». Ця таблиця складається на основі даних з таблиці 4.1 та відповідає логічній топології корпоративної мережі підприємства синтетичних виробів «Fenrir».

Застосування "Корпоративних мереж" дозволяє належним чином налаштувати IP-адреси для різних пристроїв у мережі підприємства синтетичних виробів «Fenrir» з урахуванням їх функціональності та розташування у мережевій топології.

Ім'я пристрою	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Відділ диспетчерської						
Anton_R1	G0/1	192.168.24.129	/26	-	-	G0/1
	S0/1/0	10.0.3.9	/30	-	-	S0/0/1
	S0/0/0	10.0.3.1		-	-	S0/0/0
	S0/0/0	10.0.3.13	/30	-	-	S0/0/0
Anton_Sw2	Vlan1	192.168.24.130	/26	192.168.24.129	-	G0/1
PC1_D- PC8_D	NIC	192.168.24.190-192.168.24.182	/26	192.168.24.129		Fa0/1- Fa0/8
Printer_D	NIC	192.168.24.139	/26	192.168.24.129	-	Fa0/24
Відділ дизайну						
Anton_R2	G0/1	192.168.24.193	/26	-	-	G0/1
	S0/0/0	10.0.3.2	/30	-	-	S0/0/0
	S0/0/1	10.0.3.5	/30	-	-	S0/0/1
Anton_Sw_Ing	G0/1	192.168.24.194	/26	192.168.24.193	-	G0/1
Printer_DZ	NIC	192.168.24.133	/26	192.168.24.193	-	Fa0/24
PC1_DZ – PC8_DZ	NIC	192.168.24.254-192.168.24.246	/26	192.168.24.193		F0/0-F0/8

Відділ Бухгалтерії						
Anton_R2	S0/0/1	10.0.3.14	/30	-	-	S0/0/1
	S0/1/1	10.0.3.17	/30	-	-	S0/1/1
	G0/1	192.168.25.1	/26	-	-	G0/2
Anton_Sw_Buhg	Vlan1	192.168.2.2	/26	192.168.25.1	-	G0/1
ServerDNS	NIC	192.168.25.9	/26	192.168.25.1	-	Fa0/23
Server_HTTP	NIC	192.168.25.10	/26	192.168.25.1	-	Fa0/24
PC_B1- PC_B8	NIC	192.168.25.62 - 192.168.25.54	/26	192.168.25.1	-	Fa0/1- Fa0/8
PrinterB	NIC	192.168.25.8	/26	192.168.25.1	-	Fa0/22
Відділ маркетингу						
Anton_R2	G0/1	-	-	-	-	-
	G0/1.13	192.168.24.1	/27	-	13	G0/1
	G0/1.23	192.168.24.33	/27	-	23	G0/1
	G0/1.33	192.168.24.65	/27	-	33	G0/1
	G0/1.99	192.168.24.97	/27	-	99	G0/1
ServerTFTP	NIC		/27	192.168.24.1	-	Fa0/20
PC13.1-PC13.4	NIC	192.168.24.30-192.168.24.27	/27	192.168.24.1	13	F15-24
PC23.1-PC23.4	NIC	192.168.24.62-192.168.24.59	/27	192.168.24.33	23	F10-14
PC33.1-PC33.4	NIC	192.168.24.94-192.168.24.90	/27	192.168.24.65	33	F5-9
Anton_Sw1.1	G0/1	192.168.24.98	/27	192.168.24.97	99	-
Anton_Sw1.2	F0/12	192.168.24.99	/27	192.168.24.97	99	-
Anton_Sw1.3	F0/11	192.168.24.10	/27	192.168.24.97	99	-
Відділ роботи з кадрами						
Anton_R0	G0/1	192.168.24.65	/28	-	-	G0/1
	G0/2	64.100.13.2	/30	-	-	G0/2
Anton _SW0	Vlan1	192.168.24.66	/28	192.168.24.65	-	F0/1
Anton_SW1	Vlan1	192.168.24.67	/28	192.168.24.65	-	F0/2
Anton_SW2	Vlan1	192.168.24.68	/28	192.168.24.65	-	F0/3
PC1_K- PC7_K	NIC	192.168.25.78-192.168.25.69	/28	192.168.24.65	-	Fa0/1- Fa0/7
Printer1_K	NIC	192.168.25.68	/28	192.168.24.65		Fa0/24
IPS						
Anton_IPS	S0/0/0	209.165.202.1	/27	-	-	S0/0/0
	G0/2	64.100.13.1	/30	-	-	G0/2
Server_WWW	NIC	209.165.200.5	/25	209.165.200.5	-	G0/0

Табл.3.2 Схема адресації пристроїв мережі

3.2 Налаштування комп’ютерної корпоративної системи

3.2.1 Налаштування пристроїв

Відповідно до вимог технічних налаштувань, було виконано базову конфігурацію активних мережних пристроїв у комп'ютерній системі. При цьому були вжиті додаткові заходи:

- Налаштовано паролі для привілейованого режиму, консолі і vty з метою забезпечення безпеки.
- Всі паролі, що зберігаються у відкритому вигляді, були зашифровані.
- Було налаштовано банер MOTD, який відображає повідомлення при вході до пристрою.

- На всіх лініях vty було налаштовано використання протоколу SSH і локальних облікових записів. Для цього був створений користувач "Anton" з паролем "admin". В якості імені домена були використані назви пристроїв. Також було створено RSA-ключ завдовжки 1024 біт для шифрування даних.
- Були налаштовані IPv4-адреси відповідно до таблиці 4.2, що включає адреси пристроїв у корпоративній мережі.
- На DCE-інтерфейсах маршрутизаторів було встановлено значення тактової частоти 128000.

Нижче наведено приклад налаштування на маршрутизаторі Anton_R2. З метою уникнення неправильного інтерпретування некоректно введених слів у командному рядку, на маршрутизаторі було заборонено пошук DNS:

Router(config)#no ip domain-lookup

Задання пристрою унікального імені:

Router(config)#hostname Anton_R2

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

Anton_R2(config)#service password-encryption

Встановлення паролю на віхд до привілейованого режиму:

Anton_R2(config)#enable secret class

Налаштування запиту пароля при вході:

Anton_R2(config-line)#login

Anton_R2(config-line)#exit

Налаштування банера MOTD:

Anton_R2(config)#banner motd # 123-16

Anton zone is password protected # Anton_R2(config)#exit

Налаштування протоколу SSH, Створення користувача Anton з паролем admin:

Anton_R2(config)#username 12316_Anton password admin;

Створення домену:

Anton_R2(config)#ip domain-name Anton_R2

Для шифрування даних створено ключ RSA довжиною 1024 біт:

Anton_R2(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Налаштування лінії VTY:

Anton_R2(config)#line vty 0 4 Anton_R2(config-line)# password cisco

Встановлення необхідності введення логіну та пароля для входу лінії:

Anton_R2(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Anton_R2(config-line)#transport input ssh Anton_R2(config-line)#exit

Встановлення IPv4-адрес:

Anton_R2(config)#interface g0/1

Anton_R2(config-if)# ip address 192.168.2.1 255.255.255.0

3.2.2 Налаштування маршрутизаторів та роботи Інтернету

Відповідно до вимог технічних налаштувань, в корпоративній мережі підприємства використовується протокол OSPF (Open Shortest Path First) для динамічної маршрутизації. Цей протокол забезпечує загальну політику маршрутизації для всіх маршрутизаторів, що входять до автономної системи під єдиним адміністративним керуванням. Номер автономної системи, яку використовує OSPF, становить 3.

OSPF базується на технології відстеження стану каналу (link-state technology) і використовує алгоритм Дейкстри для пошуку найкоротших шляхів. Цей протокол є внутрішнім шлюзовим протоколом (Interior Gateway Protocol - IGP), і він розповсюджує інформацію про доступні маршрути між маршрутизаторами в межах однієї автономної системи.

Протокол OSPF має декілька переваг, зокрема:

- Швидка збіжність порівняно з іншими протоколами маршрутизації, що використовують дистанційно-векторний підхід.
- Підтримка мережевих масок змінної довжини (VLSM), що дозволяє ефективно використовувати IP-адресацію.
- Оптимальне використання пропускної здатності мережі за допомогою побудови дерева найкоротших шляхів.

У кожного маршрутизатора оголошені безпосередньо підключені мережі, і вимкнуте поширення оновлень маршрутизації на інтерфейсах, що належать до локальних мереж. На маршрутизаторі Anton_R3 налаштований маршрут за замовчуванням до Інтернету (ISP), і цей маршрут розповсюджується через оновлення OSPF.

Для serial-інтерфейсів встановлені наступні параметри відповідно до технічних вимог: пропускна спроможність - 128 Кб/с і вартість метрики - 7500. На DCE-інтерфейсі маршрутизатора встановлено значення тактової частоти 128000.

Anton_R1(config)#interface s0/0/0, s0/0/1

Anton_R1(config-if)#bandwidth 128

Anton_R1(config-if)#ip ospf cost 7500

Anton_R1(config-if)#clock rate 128000

NAT є механізмом, який змінює мережеві адреси в IP датаграмах під час їх проходження через маршрутизатор, з метою перетворення одного адресного простору на інший. Застосування NAT у корпоративних мережах дозволяє підключити до мережі значну кількість комп'ютерів, використовуючи обмежену кількість зовнішніх IP-адрес, які надає провайдер. Більшість маршрутизаторів підтримують функцію трансляції адрес, що дозволяє їх використання для з'єднання невеликих мереж з Інтернетом, використовуючи лише одну зовнішню IP-адресу.

У корпоративній мережі налаштовано NAT на прикордонному маршрутизаторі згідно вимог. Параметри NAT включають:

- Пул адрес, який охоплює діапазон від 209.165.202.1 до 209.165.202.30.
- Адресу Server HTTP - 192.168.24.10/26.
- Номер списку доступу - 3.
- Назву пулу - Internet.

На маршрутизаторі Anton_R3 налаштовано NAT за допомогою наступних команд:

Anton_R3(config)# access-list 3 permit 192.168.24.0 0.0.7.255

Anton_R3(config)# ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

Anton_R3(config)# ip nat inside source list 3 pool Internet

Anton_R3(config)# ip nat inside source static 192.168.24.10 209.165.202.2

Anton_R3(config)# interface Serial0/0/0

Anton_R3(config-if)# ip nat outside

Anton_R3(config-if)# interface Serial0/1/1

Anton_R3(config-if)# ip nat inside

Ці команди встановлюють правила NAT, включаючи заміну адрес внутрішньої мережі на адреси Інтернету та статичний NAT для сервера. Коли пакет надходить на порт Serial0/0/0, відбувається заміна зовнішньої IP-адреси на адресу внутрішньої мережі, а при надходженні пакету на порт Serial0/1/1 відбувається заміна адреси внутрішньої мережі на зовнішню IP-адресу.

NAT Table for Anton_R3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.17:12	192.168.24.11:12	209.165.202.1:12	209.165.202.1:12
icmp	209.165.202.16:1	192.168.24.140:1	209.165.200.5:1	209.165.200.5:1
icmp	209.165.202.16:2	192.168.24.140:2	209.165.200.5:2	209.165.200.5:2
icmp	209.165.202.16:3	192.168.24.140:3	209.165.202.1:3	209.165.202.1:3
icmp	209.165.202.16:4	192.168.24.140:4	209.165.202.1:4	209.165.202.1:4
icmp	209.165.202.13:11	192.168.24.205:11	209.165.202.1:11	209.165.202.1:11
icmp	209.165.202.15:1	192.168.25.11:1	209.165.202.1:1	209.165.202.1:1
---	209.165.200.5	192.168.25.10	---	---

Рис.3.1 Таблиця перетворюань на Anton_R3

3.2.3 Налаштування VPN site-to-site

У корпоративній мережі необхідно налаштувати site-to-site VPN з використанням IPsec для забезпечення безпечного трафіку між підмережами "Відділ роботи з кадрами" та "Відділ Бухгалтерії" через Інтернет.

На маршрутизаторі Anton_R0 необхідно налаштувати наступні параметри:

- Налаштування access-list для визначення дозволених IP-адрес трафіку:

Anton_R0(config)# access-list 110 permit ip 192.168.24.64 0.0.0.15 192.168.25.0 0.0.0.63

- Налаштування параметрів першої фази ISAKMP:

Anton_R0(config)# crypto isakmp policy 10

Anton_R0(config-isakmp)# encryption aes

Anton_R0(config-isakmp)# authentication pre-share

Anton_R0(config-isakmp)# group 2

Anton_R0(config-isakmp)# exit

- Налаштування ключа ISAKMP для обміну даними з віддаленим підключеним пристроєм:

  Anton_R0(config)# crypto isakmp key cisco address 64.100.13.2

- Налаштування параметрів другої фази ISAKMP:

  Anton_R0(config)# crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac

  Anton_R0(config)# crypto map VPN-MAP 10 ipsec-isakmp

  Anton_R0(config-crypto-map)# description VPN connection to Anton_R4

  Anton_R0(config-crypto-map)# set peer 64.100.13.2

  Anton_R0(config-crypto-map)# set transform-set VPN-CONF

  Anton_R0(config-crypto-map)# match address 110

  Anton_R0(config-crypto-map)# exit

- Налаштування криптографічного відображення на інтерфейсі Serial 0/1/1:

  Anton_R0(config)# interface Serial 0/1/1

  Anton_R0(config-if)# crypto map VPN-MAP

Ці налаштування дозволять забезпечити безпечний обмін даними між відділами за допомогою VPN у корпоративній мережі.

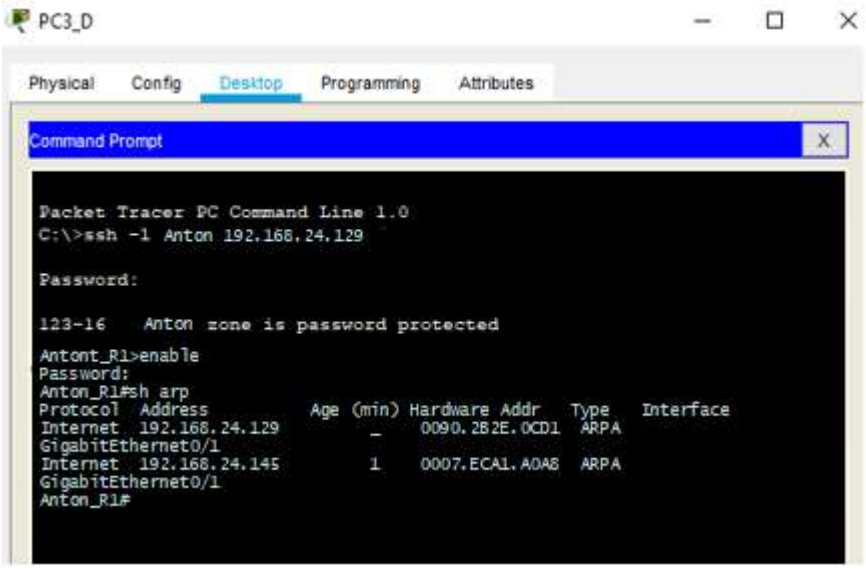

Рис.3.2 Перевірка підключення до маршрутизатора (SSH)

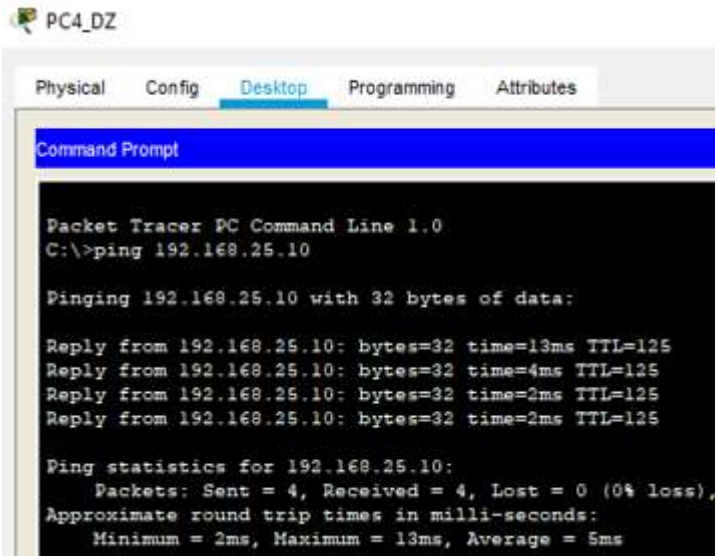

Рис.3.3 Доступність до вузлів мережі

4. ЗАХИСТ ІНФОРМАЦІЇ В КОМП`ЮТЕРНІЙ КОРПОРАТИВНІЙ СИСТЕМІ

4.1 Метод захисту AAA та RADIUS

У корпоративних мережах використовуються сервіси AAA (Authentication Authorization and Accounting) для авторизації користувачів під час підключення до мережевих пристроїв. AAA є системою аутентифікації, авторизації і обліку подій, яка вбудована в операційну систему Cisco IOS і забезпечує безпечний віддалений доступ користувачів до обладнання Cisco. Ця система дозволяє централізовано керувати доступом користувачів до мережевого обладнання і пропонує різні методи ідентифікації, авторизації та обліку подій.

На маршрутизаторі Anton_R3 необхідно налаштувати наступні параметри:

- Запуск служби AAA:

  Anton_R3(config)# aaa new-model

- Налаштування методу аутентифікації за замовчуванням з використанням локальної бази користувачів:

  Anton_R3(config)# aaa authentication login default local

- Налаштування методу аутентифікації Login з використанням сервера RADIUS, а при його недоступності - локальної бази користувачів:

  Anton_R3(config)# aaa authentication login Login group radius local

- Застосування методу аутентифікації Login на консольній лінії:

  Anton_R3(config)# line console 0

  Anton_R3(config-line)# login authentication Login

- Застосування методу аутентифікації за замовчуванням на vty-лінії:

  Anton_R3(config)# line vty 0 4

  Anton_R3(config-line)# login authentication default

- Налаштування RADIUS-сервера з визначенням його IP-адреси, порту аутентифікації та ключа:

  Anton_R3(config)# radius-server host 10.20.1.7 auth-port 1645

  Anton_R3(config)# radius-server key radius

В якості облікового запису користувача використовується ім'я пристрою з паролем admin.

```
123-16 Anton zone is password protected

User Access Verification

Username: Anton_R3
Password:
Anton_R3>en
Password:
Anton_R3#
```

Рис.4.1 Аутентифікація на маршрутизаторі

Для перевірки роботи аутентифікації можна підключитись до маршрутизатора Anton_R3 через консоль і провести аутентифікацію через сервер RADIUS. Для цього потрібно ввести ім'я користувача та пароль, які були налаштовані на сервері RADIUS.

4.2 Мережа VLAN

У корпоративних мережах, відомих як VLAN (Virtual Local Area Network), використовується віртуальна локальна обчислювальна мережа, яка дозволяє групувати хостів із загальним набором вимог, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але забезпечує можливість групування кінцевих станцій навіть у випадку, коли вони знаходяться в різних фізичних мережах. Це досягається за допомогою програмного забезпечення, що дозволяє перерозподілити пристрої в мережі без їх фізичного переміщення.

У пристроях Cisco використовується протокол VTP (VLAN Trunking Protocol), який спрощує адміністрування VLAN-доменів. VTP також здійснює фільтрацію трафіку, направляючи його лише на комутатори, що мають цільові порти для відповідного VLAN. Cisco комутатори часто використовують протокол ISL (Inter-Switch Link) для забезпечення сумісності інформації між комутаторами.

У відповідності до вимог підмережі "Відділ маркетингу" було створено чотири VLAN. В рамках мережевої архітектури в КС підприємства синтетичних виробів «Fenrir» були створені VLAN з унікальними назвами для кожного з них.

Для налаштування VLAN на комутаторах необхідно встановити порти, до яких підключені користувачі, у режим доступу (access), а порти, до яких підключені мережеві пристрої, такі як маршрутизатори та комутатори, у режим транка (trunk). Також рекомендується вимкнути всі невикористані фізичні порти на комутаторах.

Для перевірки налаштування можна відображати загальну інформацію про налаштування VLAN на комутаторах та відповідні порти.

```
Anton_Sw1.1#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Gig0/2
13   Sales_department                    active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24
23   Marketing-department                active    Fa0/10, Fa0/13, Fa0/14
33   Purchasing_department               active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9
99   Management                          active
100  Native                              active
```

Рис.4.2 VLAN на Anton_Sw1.0

Port Status Summary Table for Anton_Sw.1.1

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0050.0F75.EB01
FastEthernet0/2	Down	1	--	0050.0F75.EB02
FastEthernet0/3	Down	1	--	0050.0F75.EB03
FastEthernet0/4	Down	1	--	0050.0F75.EB04
FastEthernet0/5	Down	33	--	0050.0F75.EB05
FastEthernet0/6	Down	33	--	0050.0F75.EB06
FastEthernet0/7	Down	33	--	0050.0F75.EB07
FastEthernet0/8	Down	33	--	0050.0F75.EB08
FastEthernet0/9	Down	33	--	0050.0F75.EB09
FastEthernet0/10	Down	23	--	0050.0F75.EB0A
FastEthernet0/11	Up	--	--	0050.0F75.EB0B
FastEthernet0/12	Up	--	--	0050.0F75.EB0C
FastEthernet0/13	Down	23	--	0050.0F75.EB0D
FastEthernet0/14	Down	23	--	0050.0F75.EB0E
FastEthernet0/15	Down	13	--	0050.0F75.EB0F
FastEthernet0/16	Down	13	--	0050.0F75.EB10
FastEthernet0/17	Down	13	--	0050.0F75.EB11
FastEthernet0/18	Down	13	--	0050.0F75.EB12
FastEthernet0/19	Down	13	--	0050.0F75.EB13
FastEthernet0/20	Down	13	--	0050.0F75.EB14
FastEthernet0/21	Down	13	--	0050.0F75.EB15
FastEthernet0/22	Down	13	--	0050.0F75.EB16
FastEthernet0/23	Down	13	--	0050.0F75.EB17
FastEthernet0/24	Down	13	--	0050.0F75.EB18
GigabitEthernet0/1	Up	--	--	0050.0F75.EB19
GigabitEthernet0/2	Down	1	--	0050.0F75.EB1A
Vlan1	Down	1	<not set>	0009.7C51.371E
Vlan99	Up	99	192.168.24.98/27	0009.7C51.3701

Port Status Summary Table for Anton_Sw.1.2

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	--	--	0001.4282.6D01
FastEthernet0/2	Down	1	--	0001.4282.6D02
FastEthernet0/3	Down	1	--	0001.4282.6D03
FastEthernet0/4	Down	1	--	0001.4282.6D04
FastEthernet0/5	Up	33	--	0001.4282.6D05
FastEthernet0/6	Up	33	--	0001.4282.6D06
FastEthernet0/7	Down	33	--	0001.4282.6D07
FastEthernet0/8	Down	33	--	0001.4282.6D08
FastEthernet0/9	Down	33	--	0001.4282.6D09
FastEthernet0/10	Up	23	--	0001.4282.6D0A
FastEthernet0/11	Down	23	--	0001.4282.6D0B
FastEthernet0/12	Down	23	--	0001.4282.6D0C
FastEthernet0/13	Down	23	--	0001.4282.6D0D
FastEthernet0/14	Down	23	--	0001.4282.6D0E
FastEthernet0/15	Up	13	--	0001.4282.6D0F
FastEthernet0/16	Down	13	--	0001.4282.6D10
FastEthernet0/17	Down	13	--	0001.4282.6D11
FastEthernet0/18	Down	13	--	0001.4282.6D12
FastEthernet0/19	Down	13	--	0001.4282.6D13
FastEthernet0/20	Down	13	--	0001.4282.6D14
FastEthernet0/21	Down	13	--	0001.4282.6D15
FastEthernet0/22	Down	13	--	0001.4282.6D16
FastEthernet0/23	Down	13	--	0001.4282.6D17
FastEthernet0/24	Up	13	--	0001.4282.6D18
GigabitEthernet0/1	Down	1	--	0001.4282.6D19
GigabitEthernet0/2	Down	1	--	0001.4282.6D1A
Vlan1	Down	1	<not set>	0030.A3B2.B735
Vlan99	Up	99	192.168.24.100/27	0030.A3B2.B701

Рис.4.3-4.4 VLAN на Anton_Sw1.1 і Anton_Sw1.2

4.3 Безпека комутаторів

У Корпоративних мережах, на комутаторах, що підключені до серверів, була використана функція безпеки портів з такими характеристиками:

- Доступ до порту дозволяється лише одному вузлу.
- MAC-адрес пристрою статично додається до поточної конфігурації.
- У разі порушення системи безпеки порт буде відключений.

Команди, використані на комутаторах Anton_Sw3 і Anton_Sw.3, відповідають технічним вимогам:

Вхід до інтерфейсу:

Anton_Sw3(config)#int fa0/24

Режим доступу до порту:

Anton_Sw3(config-if)#switchport mode access

Включення засобів безпеки:

Anton_Sw3(config-if)#switchport port-security

Обмеження доступу до порту для одного вузла:

Anton_Sw3(config-if)#switchport port-security maximum 1

MAC-адреса першого вузла для доступу до порту:

Anton_Sw3(config-if)#switchport port-security mac-address 0001.6300.BABD

На маршрутизаторі Anton_R2, для забезпечення маршрутизації між VLAN за допомогою технології "router on a stick", використовується інкапсуляція 802.1Q на підінтерфейсі G0/0.

Anton_R2(config)#interface g0/1

Anton_R2(config-if)#no shutdown

Налаштування підінтерфейсу для маршрутизації трафіку між VLAN:

Anton_R2(config)#interface g0/1.13

Тегування пакетів для даного підінтерфейсу:

Anton_R2(config-subif)#encapsulation dot1Q 13

Anton_R2(config-subif)#ip address 192.168.24.1 255.255.255.224

Port Status Summary Table for Anton_R2

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Down	--	<not set>	<not set>	000A.F368.6A01
GigabitEthernet0/1	Up	--	<not set>	<not set>	000A.F368.6A02
GigabitEthernet0/1.13	Up	--	192.168.24.1/27	<not set>	000A.F368.6A02
GigabitEthernet0/1.23	Up	--	192.168.24.33/27	<not set>	000A.F368.6A02
GigabitEthernet0/1.33	Up	--	192.168.24.65/27	<not set>	000A.F368.6A02
GigabitEthernet0/1.99	Up	--	192.168.24.97/27	<not set>	000A.F368.6A02
GigabitEthernet0/2	Up	--	192.168.24.193/26	<not set>	000A.F368.6A03
Serial0/0/0	Up	--	10.0.3.2/30	<not set>	<not set>
Serial0/0/1	Up	--	10.0.3.5/30	<not set>	<not set>
Serial0/1/0	Down	--	<not set>	<not set>	<not set>
Serial0/1/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	00E0.F9E7.3507

Рис.4.5 VLAN на Anton_R2

4.4 Протоколювання та аудит

У корпоративних мережах широко використовуються протоколювання і аудити для моніторингу та аналізу роботи мережі. Ось приклади протоколів і методів аудиту, що застосовуються:

Протоколювання:

- Система журналювання подій (Event Logging): Цей протокол дозволяє реєструвати події, які відбуваються в мережі, такі як з'єднання, відключення, помилки, аварії і т.д. Журнали подій надають історичні дані, які можна використовувати для виявлення проблем і розв'язання інцидентів.

Аудит:

- Аудит доступу (Access Audit): Цей метод включає в себе реєстрацію всіх спроб доступу до мережевих ресурсів, включаючи авторизований і неавторизований доступ. Інформація про доступ зберігається в аудитних журналах і використовується для виявлення потенційних загроз безпеці та встановлення політик доступу.

- Аудит мережевого трафіку (Network Traffic Audit): Цей метод передбачає моніторинг і аналіз мережевого трафіку з метою виявлення аномалій, зловживань або вразливостей у мережі. Широко використовується системи інтрузії (Intrusion Detection Systems) і системи запобігання вторгненням (Intrusion Prevention Systems) для виявлення та реагування на вторгнення і зловживання в мережі.
- Аудит безпеки (Security Audit): Цей вид аудиту передбачає перевірку відповідності мережевих систем і політик безпеки. Аудит безпеки включає перевірку конфігурації мережевих пристроїв, виявлення потенційних вразливостей, перевірку дотримання політик безпеки і рекомендації щодо подальших покращень.

В корпоративній мережі ми можемо через сервер під’єднати усі пристрої та адміністратор зможе слідкувати та бачити, що робить кожний пристрій та блокувати або налаштовувати доступ до деяких відповідних параметрів або ПЗ кожному пристрою:

Рис.4.6 Логування подій (Event logging)

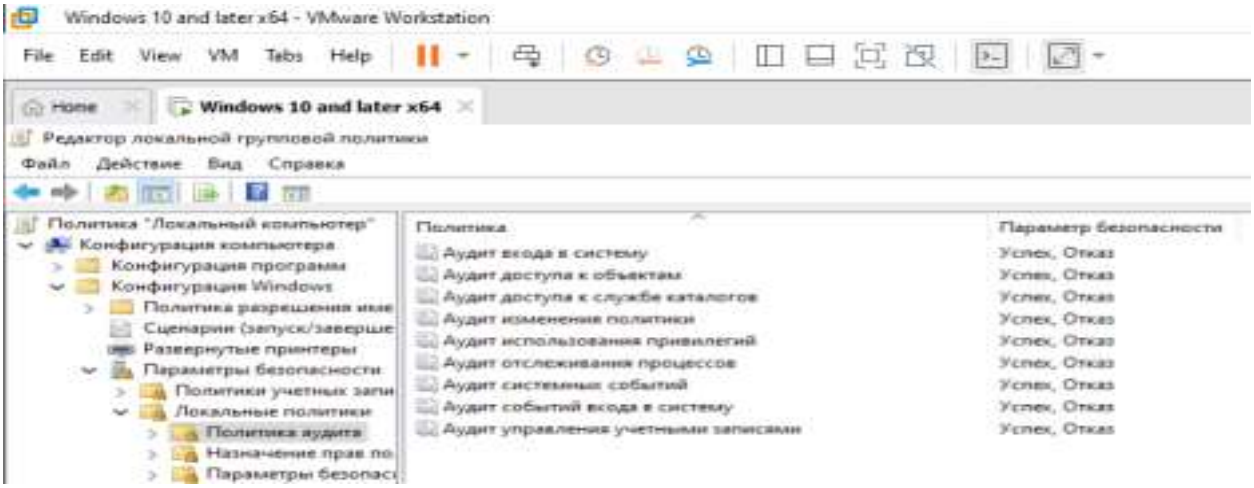

Рис.4.7 Увімкнення всіх аудитів безпеки

4.5 Firewall

Firewall (брандмауер) є невід'ємною складовою частиною корпоративних комп'ютерних мереж. Він є захисним пристроєм, який має на меті контролювати та регулювати потік інформації, що входить та виходить з мережі. Основна функція брандмауера полягає у встановленні правил доступу та фільтрації мережевого трафіку з метою захисту мережевої інфраструктури від несанкціонованого доступу, зловживань, вторгнень та інших загроз.

В корпоративних комп'ютерних мережах брандмауер виконує ряд важливих завдань. Він забезпечує контроль доступу до мережі шляхом перевірки пакетів даних, що проходять через нього, на відповідність заданим правилам. Брандмауер може блокувати небажаний трафік, такий як шкідливі програми, віруси, спам, зловживання та інші загрози, що можуть негативно вплинути на безпеку мережі.

Крім того, брандмауер може забезпечувати розділення мережі на сегменти (сегментацію), що дозволяє зменшити ризики випадкового поширення загроз усередині мережі. Він також може здійснювати переклад мережевих адрес (NAT), що дозволяє приховати внутрішню адресування мережі від зовнішнього середовища.

Багатофункціональний пристрій безпеки ASA Cisco (Adaptive Security Appliance; ASA) — це вдосконалений пристрій мережної безпеки, що включає міжмережевий екран зі збереженням стану, VPN та інші можливості. У цій статті для створення міжмережевого екрану та захисту внутрішньої корпоративної мережі від зовнішнього проникнення, а також організації доступу до Інтернету для внутрішніх користувачів використовується ASA 5505.

ASA створює три інтерфейси безпеки: зовнішній, внутрішній та DMZ. Цей пристрій надає зовнішнім користувачам обмежений доступ до DMZ і блокує доступ до внутрішніх ресурсів. Тоді як внутрішні користувачі мають доступ до DMZ та зовнішніх ресурсів.

Основний упор робиться на налаштуванні ASA як основний міжмережевий екран. На інших пристроях необхідно виконати мінімальне налаштування для підтримки роботи ASA. Для налаштування основних параметрів пристрою та безпеки використовується ASDM та графічний інтерфейс користувача (GUI) в ASA.

ASA – це граничний пристрій безпеки, що підключає внутрішньокорпоративну мережу та DMZ до ISP і одночасно надає сервіси NAT та DHCP внутрішнім хостам. ASA необхідно налаштувати для керування адміністратором як у внутрішній мережі, так і для віддаленого адміністратора.

Інтерфейси VLAN третього рівня надають доступ до трьох зон, створених під час налаштування: внутрішньої, зовнішньої та DMZ. При цьому ISP призначає простір загальнодоступних IP-адрес 209.165.200.224/29, який буде використовуватися для перетворення адрес на ASA.

Базове налаштування ASA:

enable

configure terminal

hostname CCNA-ASA

domain-name ccnasecurity.com

enable password 9D8jmmmgkfNZLETh encrypted

interface Ethernet0/0

switchport access vlan 2

interface Ethernet0/2

switchport access vlan 3

interface Vlan1

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

interface Vlan2

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

http server enable

http 192.168.1.0 255.255.255.0 inside

end

4.6 Екранування

Екранування корпоративної комп'ютерної системи є важливим кроком для забезпечення безпеки і захисту від зовнішніх загроз. Деякі заходи ми вже зробили, а деякі виконуються при деяких умовах:

- Встановлення брандмауера (firewall): Брандмауер встановлюється між корпоративною мережею і зовнішніми мережами з метою контролю трафіку і фільтрації пакетів. Він може блокувати небажані з'єднання, атаки з мережі, шкідливі програми і багато іншого.
- Використання віртуальної приватної мережі (VPN): VPN дозволяє створювати зашифровані з'єднання між віддаленими комп'ютерами через ненадійну мережу, таку як Інтернет. Він забезпечує конфіденційність трафіку і захищає його від перехоплення.
- Застосування системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS): IDS виявляє небезпечну активність у мережі і повідомляє про можливі загрози. IPS вживає заходів для запобігання таким загрозам і блокує їх.
- Регулярне оновлення програмного забезпечення: Важливо оновлювати всі програми та операційну систему до останніх версій і патчів. Це допоможе заповнити вразливості, які можуть бути використані зловмисниками.
- Використання сильних паролів і багатофакторної автентифікації: Важливо встановити складні паролі для всіх облікових записів і використовувати багатофакторну автентифікацію для додаткового рівня захисту.
- Заборона використання небезпечних сервісів і протоколів: Закриття небезпечних портів і блокування небажаних протоколів може зменшити ризик атак і неправомірного використання ресурсів мережі. Приклад::

  netsh advfirewall firewall add rule name="Block Port 1234" dir=in action=block protocol=TCP localport=1234

  Додавання правила до фаерволу, щоб заблокувати порти 1234.

- Шифрування даних: Шифрування даних забезпечує їх конфіденційність при передачі і зберіганні. Важливо шифрувати конфіденційну і чутливу інформацію, щоб запобігти її неправомірному доступу. Типу як у нас було RSA шифрування для пристроїв Cisco.

4.7 IDS та IPS системи

4.7.1 Визначення IDS та IPS

IDS

IDS є програмною чи апаратно-програмною пасивною системою, яка сканує трафік і повідомляє про загрози. IDS жодним чином не змінює мережні пакети, тоді як IPS запобігає доставці пакета в залежності від вмісту пакета, подібно до того, як ME запобігає трафіку за IP-адресою.

IDS відстежує трафік, порівнюючи його з власною базою даних можливих мережевих атак та базовою мережевою активністю. Такий механізм роботи дозволяє виявляти:

- мережеві атаки;
- неавторизований доступ до даних;
- дії шкідливих скриптів та програм;
- функціонування сканерів портів;
- порушення політик безпеки;
- звернення до центрів управління бот-мережами та майнінг-пулам;
- аномальну активність.

Виявити порушення політик безпеки можна за рахунок написання власних програм детектування. Це допомагає відстежувати певну поведінку у мережі. З цього слідує, що IDS-система не відображає атаки, а лише виявляє їх і повідомляє адміністратору, допомагаючи знайти причину та усунути її.

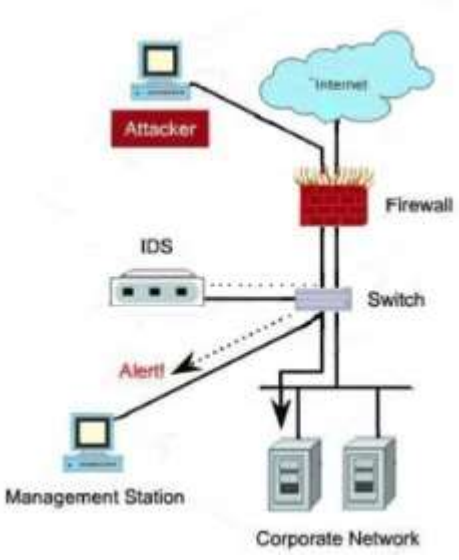

Рис.4.8 Схема IDS

IPS

IPS – це програмно або апаратний активний засіб безпеки для запобігання мережевим загрозам. Система досліджує мережевий трафік, потоки для запобігання exploit, зловмисних дій з цільовим додатком або службою. Все для того, щоб зловмисники не змогли перервати роботу компанії та отримати контроль над програмою або кінцевою точкою. Фактично IPS виступає другим стінкою захисту, що знаходиться за firewall або входить до його складу. Конкретні функції IPS залежать від типу рішення, але загалом наявність IPS корисно для автоматизації дій і стримування загроз без необхідності адміністратора.

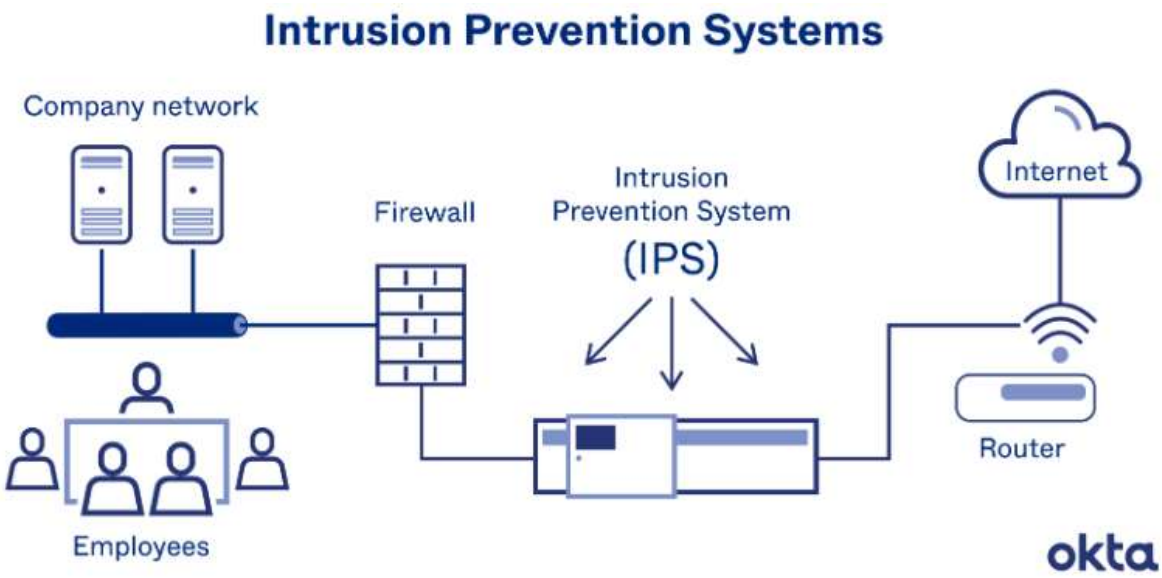

Рис.4.9 Схема IPS

IPS виконує зіставлення трафіку відомими мережевими атаками для виявлення:

- зміни тенденцій мережевого трафіку;
- спроб несанкціонованого доступу;
- спроб звернення до небезпечних ресурсів із мережі організації.

IPS здатна не тільки виявляти ризики на різних рівнях, а й автоматично відповідати на них:

- блокувати небезпечний трафік;
- генерувати подію ІБ для адміністратора.

4.7.2 Можливості систем

IPS та IDS-системи мають ряд корисних можливостей:

- Виявлення на основі сигнатур: рішення IDS на основі сигнатур сповіщають адміністраторів на основі вже існуючих сигнатур, які вказують на тип атаки або зловмисну поведінку. Це забезпечує точне й автоматичне сповіщення, оскільки система посилається на існуючу базу даних сигнатур. Така система часто шукає ознаки компрометації, такі як сканування хешів файлів, трафік, що йде до відомих шкідливих доменів, зловмисні послідовності байтів і навіть рядки теми електронних листів, які є відомими fishing атаками;
- Виявлення аномалій: рішення IDS на основі аномалій вважаються більш ефективними, ніж рішення на основі сигнатур, оскільки вони відстежують зловмисні або підозрілі моделі поведінки. Це дозволяє їм виявляти нові види загроз, що майже неможливо для систем на основі сигнатур. Виявлення на основі аномалій часто шукає поведінку, яка відрізняється від встановленого базового рівня. Наприклад, якщо ви встановили звичайний робочий час для співробітників, IDS на основі аномалій може позначити вхід у вихідні дні. Система також може попереджати вас на основі обсягу трафіку, що підключається до вашої мережі, або нових пристроїв, які додаються без належного авторизації;
- Спостереження за користувачами в реальному часі – алгоритми збирають дані про трафік та комплексно аналізують його. Це дозволяє не лише знаходити проблеми, а й точно ідентифікувати їх: звідки була загроза, коли та яким чином.

4.7.3 Під’єднання к нашій системі

Для нашої системи може підійти одна з двух популярних систем: Snort або Suricata.

Snort

Snort є вільно розповсюджуваною програмою з відкритим вихідним кодом під ліцензією GPL. Спочатку Snort був створений одним з найвідоміших людей у світі інформаційної безпеки, автором багатьох книг Мартіном Рошем у 1998 року. Основною причиною створення цієї IDS була відсутність на той момент досить ефективного, тим більше безкоштовного, інструменту оповіщення про атаках. На теперішній момент це система NIDS.

Snort є мережевою системою виявлення (IDS) і запобігання вторгненням (IPS) з відкритим вихідним кодом, здатна виконувати реєстрацію пакетів і в реальному часі здійснювати аналіз трафіку в IP-мережах, комбінуючи можливості зіставлення сигнатур, засоби для інспекції протоколів і механізми

виявлення аномалій. По суті, мова опису сигнатур Snort стала стандартом для багатьох систем виявлення вторгнень, які стали його використовувати у своїх двигунах.

Система Snort виконує протоколювання, аналіз, пошук за вмістом, а також широко використовується для активного блокування або пасивного виявлення цілого ряду нападів та зондувань. Snort здатний виявляти:

- Поганий трафік;
- Використання exploit (виявлення Shellcode);
- Сканування системи (порти, ОС, користувачі тощо);
- Атаки на такі служби як Telnet, FTP, DNS тощо;
- Атаки DoS/DDoS;
- Атаки пов'язані з Web серверами (cgi, php, frontpage, iss і т.д.);
- Атаки на бази даних SQL, Oracle і т.д.;
- Атаки за протоколами SNMP, NetBios, ICMP;
- Атаки на SMTP, imap, pop2, pop3;
- Різні Backdoors;
- Web-фільтри (порнографія);
- Віруси.

Додаткова ця IDS надає:

- Можливість написання власних правил;
- Розширення функціональності, використовуючи можливість підключення модулів;
- Гнучку систему оповіщення про атаки (Log файли, пристрої виведення, БД та ін.).

Snort може підтримувати такі інтерфейси для прослуховування:

- Ethernet;
- SLIP;
- PPP.

Основу Snort складає двигун, що складається з п'яти модулів:

- Sniffer пакетів: даний модуль відповідає за захоплення даних, що передаються по мережі, для подальшої їх передачі на декодер. Робить це за допомогою бібліотеки DAQ. Працювати даний sniffer може "в розрив" (inline), пасивному режимі або читати мережеві дані із заздалегідь підготовленого файлу;

- Декодер пакетів: даний модуль займається розбором заголовків захоплених пакетів, їх розбором, пошуком аномалій та відхилень від RFC, аналізом TCP-прапорів, виключенням окремих протоколів з подальшого аналізу та іншою аналогічною роботою. Фокусується цей декодер на стеку TCP/IP;
- Препроцесори: якщо декодер розбирав трафік на 2-му та 3-му рівні еталонної моделі, то препроцесори призначені для більш детального аналізу та нормалізації протоколів на 3-му, 4-му та 7-му рівнях. Серед найпопулярніших препроцесорів можна назвати frag3 (робота із фрагментованим трафіком), stream5 (реконструкція TCP-потоків), http_inspect_ (нормалізація HTTP-трафіку), DCE/RPC2, sfPortscan (застосовується для виявлення сканування портів) та різні декодери для протоколів Telnet, FTP , SMTP, SIP, SSL, SSH, IMAP тощо. Деякі розробники пишуть свої препроцесори і додають у власні системи IDS, побудовані з урахуванням Snort;
- Двигун виявлення атак: цей двигун складається з двох частин. Конструктор правил збирає безліч різних вирішальних правил (сигнатур атак) в єдиний набір, оптимізований для подальшого застосування підсистемою інспекції захопленого та обробленого трафіку у пошуках тих чи інших порушень;
- Модуль виведення: за фактом виявлення атаки Snort може видати, записати або відобразити відповідне повідомлення у різних форматах – файл, syslog, ASCII, PCAP, Unified2 (двійковий формат для прискореної та полегшеної обробки).

Рис.4.10 Консоль Snort

Suricata

Після трьох років розробки об'єднання OISF розпочало бета-тестування нової відкритої системи виявлення та запобігання атакам Suricata IDS/IPS, що базується на принципово нових механізмах роботи. Suricata створюється з метою створення нових ідей та технологій, а не просто розробки чергового нового інструменту, що дублює можливості інших продуктів галузі. Код проекту розповсюджується під ліцензією GPLv2.

Особливості системи:

- Багатопоточність - Snort з його одним потоком може використовувати тільки один процесор (ядро) одночасно. Suricata здатна запускати багато потоків, тому може задіяти переваги всіх доступних процесорів. Було багато суперечок про те, чи це вигідно, Snort каже, що «ні», а кілька контрольних показників кажуть, що «так»;
- Вбудоване апаратне прискорення – користувач може використовувати графічні карти для перевірки мережевого трафіку;
- Вилучення файлів – хтось встановлює шкідливе ПЗ? Користувач може захопити його за допомогою Suricata та вивчити;
- LuaJIT - це скриптовий двигун, який може бути використаний для перевірки інформації з пакетів. Це робить складне зіставлення даних ще простіше, і людина може об'єднати кілька правил в один скрипт;
- Ведення журналу — Suricata може захоплювати та реєструвати сертифікати TLS/SSL, HTTP та DNS запити;
- Постійна підтримка спільноти.

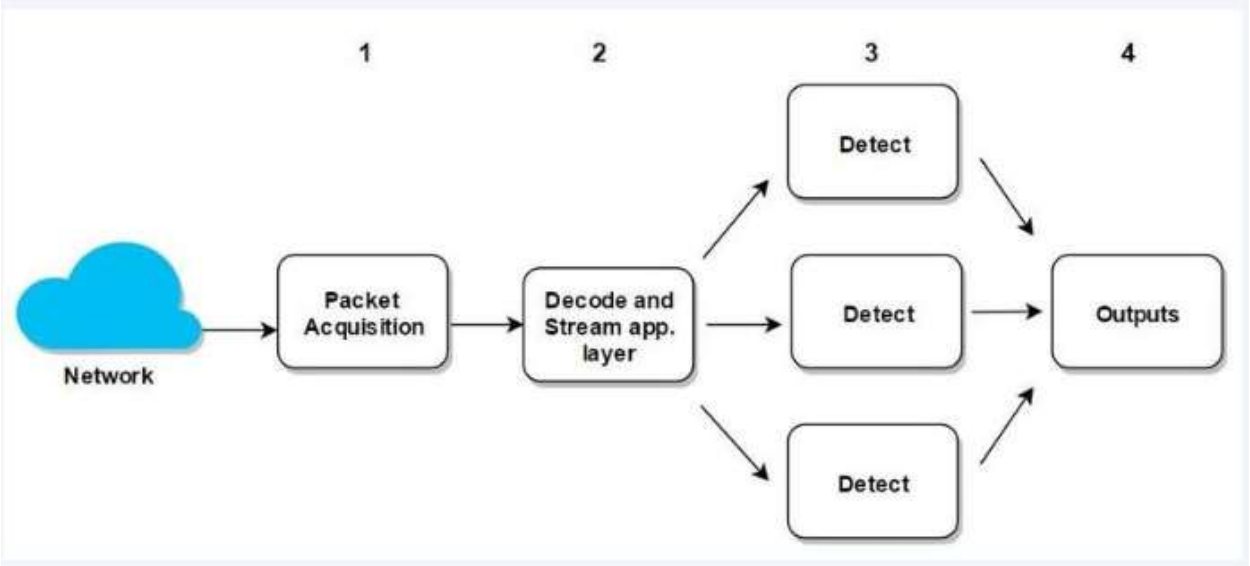

Рис.4.11 Робота Suricata

Беручи інформацію з сайту розробників, особливі риси системи включають:

- Висока продуктивність — багатопоточна, масштабована база кодів;
- Універсальний движок – NIDS, NIPS, NSM, автономний аналіз;
- Кросплатформову підтримку - Linux, Windows, macOS, OpenBSD та ін;
- Сучасну підтримку TCP/IP, включаючи масштабований механізм потоку, повний IPv4/IPv6, TCP-потоки та дефрагментацію IP-пакетів;
- Парсери протоколів — декодування пакетів;
- HTTP — реєстратор запитів, що містить ключові слова;
- Автоналаштування конфігурації;
- Сценарії Lua (LuaJIT);
- Ведення журналу та аналіз відповідного рівня, включаючи сертифікати TLS/SSL, HTTP та DNS-запити;
- Вбудоване апаратне прискорення (GPU для sniffer мережі);
- Залучення файлів.

Тестова група	Кількість тестів	Оцінка Suricata	Оцінка Snort
Поганий трафік	4	1	1
Роздроблені пакети	2	1	3
Шкідливі програми та віруси	14	9	7
Відмова в обслуговуванні (DoS)	3	3	3
Атака з боку клієнта	257	157	127
Оболонки	12	12	7
Продуктивність	0	2	1
Всього	297	185	149

Табл. 4.1 Порівняння Suricata та Snort

ВИСНОВКИ

У даній дипломній роботі було досліджено та розглянуто питання захисту інформації в корпоративній комп'ютерній системі. Основною метою дослідження було виявлення загроз безпеці інформації та розробка ефективних заходів для її захисту.

У процесі роботи були вивчені основні загрози, з якими зіштовхуються корпоративні комп'ютерні системи, такі як несанкціонований доступ до даних, втрата або пошкодження даних, атаки зламу, виток інформації тощо. Для кожної загрози було проаналізовано можливі наслідки та ризики для організації.

На основі проведеного аналізу були запропоновані та розроблені різноманітні заходи для захисту інформації. Серед них - встановлення фізичних та логічних заходів безпеки, використання міцних паролів, шифрування даних, впровадження системи контролю доступу, а також навчання персоналу з питань безпеки.

Крім того, було розглянуто питання захисту мережі та комунікацій, зокрема використання брандмауерів, віртуальних приватних мереж (VPN), контролю доступу до мережевих ресурсів, аудиту мережевої активності та виявлення інтрузій.

Результати проведеного дослідження та розробки заходів для захисту інформації підтверджують їхню ефективність та важливість у забезпеченні безпеки корпоративної комп'ютерної системи. Захист інформації є критично важливим завданням для будь-якої організації, оскільки від цього залежить успішність та стабільність її діяльності.

Отже, вироблення та впровадження комплексних заходів безпеки, що включають фізичні, логічні та мережеві аспекти, є необхідною умовою для забезпечення надійного захисту інформації в корпоративній комп'ютерній системі. Правильна стратегія захисту дозволить зменшити ризики витоку, втрати або пошкодження даних, забезпечити конфіденційність, цілісність та доступність інформації, а також зберегти репутацію та довіру клієнтів та партнерів.

Дослідження у цій області є постійно актуальним, оскільки з постійним розвитком технологій з'являються нові загрози та вразливості. Для подальшого вдосконалення систем захисту необхідно здійснювати моніторинг і аналіз загроз, вивчати нові методи атак та застосовувати відповідні технологічні та організаційні заходи.

У підсумку, успішний захист інформації в корпоративній комп'ютерній системі вимагає комплексного підходу, включаючи технологічні, організаційні

та людські аспекти. Правильне розуміння загроз, виявлення ризиків та впровадження відповідних заходів дозволить забезпечити надійну та безпечну роботу корпоративної комп'ютерної системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Новаківський, І. І. Вплив процесів інформатизації на організаційну структуру підприємств [Текст] / І. І. Новаківський // Вісник Національного університету «Львівська політехніка». – 2014. – № 425. – С. 285-286.
2) Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2020. – 69 с.
3) Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
4) The Great IDS Debate: Signature Analysis Versus Protocol Analysis by Matt Tanase, Feb. 5, 2003/ Електронний ресурс: режим доступу: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b4c1f4bd-4199-4d9e- b61b486b3df2d76c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
5) Kurose J.F. Computer Networking: A Top-Down Approach, 7th Ed / James F. Kurose, Keith W. Ross. - Pearson Education, Inc., 2017. - 864 pp. 3. Stallings W. Computer Organization and Architecture, 10th Ed. / Pearson Education, Inc., Hoboken, NJ, 2016. - 864 pp. 4. Ng C.K. Honeypot Frameworks and their Applications: A New Framework /Chee Keong Ng, Lei Pan, Yang Xiang. - Springer Nature Singapore Pte Ltd., 2018. - 81 pp.
6) Whitman, M. E., & Mattord, H. J. (2019). Management of information security. Cengage Learning.
7) Vacca, J. R. (2013). Computer and information security handbook. Morgan Kaufmann.
8) Іванов В.М., Дмитрієв О.М. Безпека інформаційних систем: підручник. Київ: Видавництво "Центр учбової літератури", 2018.
9) Куліков А.В., Журін О.Г., Максименко А.Є. Інформаційна безпека в корпоративних системах. Київ: Видавничий дім "Пропорції", 2014.
10) Кириченко І.М., Сарапінський В.Г. Захист інформації в комп'ютерних мережах: навчальний посібник. Харків: Видавничий дім "Інжек", 2012.