**Міністерство освіти і науки України**

**«Київський національний університет імені Тараса Шевченка»**

**Факультет інформаційних технологій**

**Кафедра кібербезпеки та захисту інформації**

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«  » червня 2021р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

**дипломної роботи**
***бакалавра***
(назва освітнього рівня)

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)

**спеціальність** 125 Кібербезпека
(код і назва спеціальності)

**освітня програма** Кібербезпека
(назва освітньої програми)

**на тему:** Підсистема захисту корпоративної мережі з використанням програмно-апаратних засобів

**Виконавець:** студент IV курсу, групи КБ-41

_____ **Шалатонов Олег Русланович**
(підпис) (прізвище ім'я по-батькові)

| | **Прізвище, ініціали** | **Підпис** |
|---|---|---|
| **Керівник** | Пархоменко І.І. | |

| | | |
|---|---|---|
| **Нормоконтроль** | Даков С.Ю. | |

**Київ 2021**

**Міністерство освіти і науки України**

**«Київський національний університет імені Тараса Шевченка»**

**Факультет інформаційних технологій**

**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » 2020 р.

# ЗАВДАННЯ
## на виконання дипломної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньої програми)

**Студенту** **КБ-41** (група) **Шалатонову Олегу Руслановичу** (прізвище ім'я по-батькові)

**Тема дипломної роботи** Підсистема захисту корпоративної мережі з використанням програмно-апаратних засобів

**1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ**

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

**2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ**

Архітектура та класифікаційні ознаки корпоративних мереж, протоколи, служби, обладнання та технології захисту корпоративних мереж.

**3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ**

Характеристика та компоненти корпоративної мережі, нормативно-правова база інформаційної безпеки, типові загрози безпеці корпоративних мереж, програмно-технічні засоби безпеки, вразливості з боку безпеки даних, визначення можливих критичних активів організації та представлення спеціалізованих рішень для мінімізації шансу реалізації загроз із загальною схемою.

**4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ**

**Практична цінність** Поєднання засобів і механізмів захисту корпоративної мережі та розробка структури корпоративної мережі з їх використанням

**5. ДАТА ВИДАЧІ ЗАВДАННЯ**

Дата видачі завдання:12 жовтня 2020 року

| | | |
|---|---|---|
| Завдання видав | | І.І. Пархоменко |
| | (підпис) | (ініціали, прізвище) |
| Завдання прийняв до виконання | | О.Р. Шалатонов |
| | (підпис) | (ініціали, прізвище) |

**КАЛЕНДАРНИЙ ПЛАН**

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 25.01.2021 – 27.01.2021 | *виконано* |
| 2 | Аналіз літератури | 28.01.2021 – 07.03.2021 | *виконано* |
| 3 | Аналіз нормативно-правової бази | 08.03.2021 – 15.03.2021 | *виконано* |
| 4 | Функціональні особливості корпоративних мереж | 16.03.2021 – 31.03.2021 | *виконано* |
| 5 | Аналіз вразливостей та загроз інформаційної безпеки | 01.04.2021 – 11.04.2021 | *виконано* |
| 6 | Дослідження засобів за методів захисту корпоративних мереж | 12.04.2021 – 19.04.2021 | *виконано* |
| 7 | Розвертання демо-стенду локальної мережі з ключовою підсистемою захисту | 20.04.2021 – 19.05.2021 | *виконано* |
| 8 | Оформлення пояснювальної записки | 20.05.2021 – 04.06.2021 | *виконано* |
| 9 | Підготовка до захисту дипломної роботи | 05.06.2021 – 21.06.2021 | *виконано* |

| | | |
|---|---|---|
| Завдання видав | | І.І. Пархоменко |
| | (підпис) | (ініціали, прізвище) |
| Завдання прийняв до виконання | | О.Р. Шалатонов |
| | (підпис) | (ініціали, прізвище) |

Термін подання дипломної роботи до ЕК 08 червня 2021 року

# РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел та додатків. Основний текст займає 60 сторінок і містить 2 таблиці та 31 рисунок.

Метою роботи є компонування програмно-апаратних засобів для забезпечення ефективного захисту корпоративної мережі, інформації та інформаційних систем, що знаходяться в ній.

Об’єктом дослідження є процес захисту корпоративної мережі, інформації та інформаційних систем в ній.

Предметом дослідження є технології та програмно-апаратні засоби захисту інформації.

У роботі проаналізована існуюча література з теорії технічного захисту інформації, виконаний аналіз джерел та нормативно-правової бази, розроблено демо-стенд локальної мережі з вказаними у роботі програмно-технічними засобами захисту та побудована структурна схема корпоративної мережі.

Ключові слова: корпоративна мережа, захист інформації, тунелювання, міжмережевий екран, рольовий доступ, нульова довіра, система захисту.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| **IDS** | – | Intrusion Detection System |
| **IPS** | – | Intrusion Prevention System |
| **(D)DoS** | – | (Distributed) Denial-of-Service |
| **SIEM** | – | Security information and event management |
| **NGFW** | – | Next Generation Firewall |
| **WAF** | – | Web Application Firewall |
| **NAT** | – | Network Address Translation |
| **ACL** | – | Access Control List |
| **VLAN** | – | Virtual Local Area Network |
| **VPN** | – | Virtual Private Network |
| **MPLS** | – | Multi Protocol Label Switching |
| **MitM** | – | Man in the Middle |
| **APT** | – | Advanced Persistent Threat |
| **IGA** | – | Identity Governance Platform |
| **IAM** | | Identity Access Management |
| **ПЗ** | – | Програмне забезпечення |

# ЗМІСТ

# ВСТУП

*Актуальність* даної роботи визначається двома факторами. По-перше, показники у статистичних звітах успішних атак з кожним роком зростають. По-друге, існує проблема нестачі спеціалістів у сфері кібербезпеки, одним із факторів якої є бажання підприємств, організацій мати лише досвідченого фахівця. Більшості не хочеться брати початківця і навчати його у своїй команді. Тому позиції топ менеджменту залишаються відкритими довго.

Досвід у конфігуруванні та підтримці систем інформаційної безпеки завжди буде вимагатися у фахівців з кібербезпеки. Кандидат має розуміти, як встановлювати, налаштовувати, використовувати і підтримувати різні системи: IDS/IPS, SIEM, NGFW, WAF тощо.

В приклад світових лідерів в області рішень для захисту корпоративних даних і кібербезпеки для бізнесу можу навести: Trend Micro [9], SailPoint, Sophos, Micro Focus, Checkmarx, CyberArk, McAfee. Ці компанії (вендори) надають курси, матеріали для вивчення їх продуктів, проблем кібербезпеки, базової інформації (наприклад, криптографія) і взагалі принципів роботи класів систем захисту.

Апробація роботи була проведена на IV міжнародній науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS).

# РОЗДІЛ 1
# ХАРАКТЕРИСТИКА ТА КОМПОНЕНТИ КОРПОРАТИВНОЇ МЕРЕЖІ

## 1.1 Функціональні особливості корпоративної мережі

Ще як мінімум 10 років тому впевнено говорили, що комп'ютерні мережі займають дуже важливе місце в бізнесі. Для бізнесу дуже важливо використовувати новітні технології, оскільки вони забезпечують підвищену безпеку, збільшений об'єм пам'яті, високу швидкість передачі даних, передачу голосу і відео в режимі реального часу і багато іншого. Такі переваги вкрай необхідні зростаючій компанії або великому підприємству.

Куди зараз дивляться архітектори корпоративних мереж, думаючи про їх розвиток:

1. Забезпечення основи для сучасного цифрового підприємства: від мереж все частіше очікують підвищення безпеки, поліпшення користувацького досвіду і підтримки безлічі пристроїв, які виконують важливі бізнес-завдання. Добре спроектовані корпоративні мережі підтримують безліч користувачів, пристроїв, «розумних речей» і додатків для забезпечення постійного гарантованого обслуговування.

2. Використання мережевих контролерів: контролери, будучи командними і керуючими центрами сучасних корпоративних мереж, організовують всі функції мережі. Вони виконують такі завдання, як перетворення бізнес-цілей в політики, автоматизація роботи мережевих пристроїв, моніторинг продуктивності і усунення неполадок.

3. Розширення сфери застосування: Оскільки кількість мережевих транзакцій, що виходять або завершуються за межами традиційного корпоративного периметра, збільшується - у зв'язку з такими тенденціями, як розширення до декількох загальнодоступних хмар, мобільність і робота з дому - мережа повинна

розширювати видимість, контроль і безпеку, де б не знаходилися користувачі, речі і додатки.

У поточних реаліях поняття корпоративна мережа, мережева інфраструктура, IT інфраструктура дуже перетинаються між собою, але все ж несуть в собі різні за охопленням речі.

Так для мережі підприємства було виділено наступні ключові особливості:

- Швидкість зв'язку. Мережа дозволяє нам швидко і ефективно спілкуватися по мережі. Наприклад, можна проводити відеоконференції, обмінюватися повідомленнями по електронній пошті і т.д. через Інтернет. Таким чином, комп'ютерна мережа - це відмінний спосіб поділитися своїми знаннями та ідеями.
- Спільне використання файлів. Обмін файлами - одне з головних переваг комп'ютерної мережі. Комп'ютерна мережа дозволяє нам обмінюватися файлами один з одним.
- Створення резервних копій та відкат - це просто. Оскільки файли зберігаються централізовано на головному сервері. Тому легко зробити резервну копію з головного сервера.
- Спільне використання програмного та апаратного забезпечення. Можна встановити додатки на головному сервері, тому користувач може отримати доступ до додатків централізовано. Таким чином, не потрібно встановлювати програмне забезпечення на кожну машину. Аналогічно, апаратне забезпечення також може бути загальним.
- Безпека. Мережа забезпечує безпеку, гарантуючи, що користувач має право доступу до певних файлів і додатків.
- Масштабованість. Масштабованість означає, що можна додавати нові компоненти в мережу. Мережа повинна бути масштабованої, щоб була можливість розширювати мережу, додаючи нові пристрої. Але при цьому знижується швидкість з'єднання і швидкість передачі даних також знижується, що збільшує ймовірність виникнення помилок. Ця проблема може бути вирішена за допомогою пристроїв маршрутизації або комутації.

• Надійність. Комп'ютерна мережа може використовувати альтернативне джерело для передачі даних в разі будь-якого апаратного збою.

## 1.2 Сучасний стан безпеки інформаційно-комунікаційної інфраструктури

Не все з перерахованого вище досягається установкою мережевого апаратного обладнання (комутатори, маршрутизатори, точки доступу), прокладанням відповідних кабельних ліній і налаштуванням перших (NAT, ACL, VLAN, (SSL) VPN, доступ по SSH, RDP і т.д.). Для деяких цілей знадобляться і програмні продукти, за допомогою яких буде можливо контролювати апаратні.

Проектування безпеки мережі є важливою частиною проектування всієї мережі. Для того щоб мережа була добре захищена, необхідно, щоб всі вимоги були детально описані до початку проектування.

Мережева безпека - це розділ IT-безпеки, який дуже важливий для функціонування всієї корпорації. Одна успішна атака в одній корпоративної мережі може завдати великої шкоди, наприклад, вкрасти конфіденційну інформацію, шпигувати за всіма користувачами, маніпулювати інформацією і т.д.

Головне завдання перед мережевими інженерами полягає в зв'язку головного офісу з віддаленими офісами - філіями, надомними і мобільними працівниками. У той час, як фахівці з відділу інформаційної безпеки підприємства повинні забезпечити правильне розмежування доступу до інформаційних корпоративних ресурсів для зовнішніх і внутрішніх користувачів, де зовнішні - це ті, які повинні не мати доступ до ресурсів. І друге їх (спільно з мережевими інженерами) головне завдання - це підтримка надійності роботи та відмовостійкості всіх елементів мережі.

Сьогодні однією з головних проблем інформаційної безпеки підприємства чи головною для служби безпеки будь-якої організації є навчання персоналу. Більшість співробітників не мають обізнаності у сфері IT та захисту інформації.

Придбати засоби технічного захисту зараз легко, маючи гроші. Є різні цінові діапазони, різна ефективність. Скоріш за все при налаштуванні нової системи

безпеки в організації, відповідальний за її встановлення навчить майбутніх адміністраторів цієї системи в організації, проте все одно необхідно писати спеціальні матеріали для звичайних користувачів, менеджерів, адміністраторів. Іноді навчання від інтегратора системи не вистачає, і організація мусить придбати або додаткове навчання для свого співробітника, або оплатити службу підтримки, яка вже зможе надати компетентну допомогу.

Якщо не брати до уваги формалізацію бізнес вимог, то придбати, встановити систему відносно легко, - робота перекладається на інтегратора. Вона буде працювати і захищати, підтримувати її та користуватись нею – задача складніша.

### 1.3 Нормативно-правова база інформаційної безпеки

Нормативно-правову базу у технічному захисті інформації (ТЗІ) складає декілька десятків законів, постанов, стандартів та інших нормативних документів. В цій роботі загострена увага на недержавній інформації, яка не потребує впровадження комплексної системи захисту.

Декілька років назад панувала думка, що нормативне забезпечення у сфері ТЗІ не розвинуте. Сьогодні ж ситуація стала розрідженою – є багато документів зі схожою темою. Раніше був закон про захист інформації в автоматизованих системах. Зараз замінили це поняття на «інформаційно-телекомунікаційні системи», і сформувався новий закон. Проте як мінімум НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» все ще вміщує старе поняття, що і дозволяє його використовувати. Невідомо навіщо було змінювати закон.

Основні документи та їх статті перераховано нижче, проте це не вичерпний список [23]:

*Закон України «Про інформацію» [1]*

Описує загальні положення щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Стаття 1.

Захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Стаття 20.

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21.

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

*Закон України «Про захист персональних даних» [2]*

Вміщує в себе положення, пов’язані із захистом і обробкою персональних даних. Обробка може вестися як із застосування автоматизованих систем, тка і без них.

Стаття 5.

1. Об’єктами захисту є персональні дані.

2. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою.

Стаття 24.

1. Володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист персональних даних від випадкових втрати або знищення, від

незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

*Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [3]*

Цей закон вміщує в себе положення щодо захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Стаття 1.

Виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства

Технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 8.

Інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення

функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації.

*«Положення про технічний захист інформації в Україні» [4]*

Це Положення визначає правові та організаційні засади технічного захисту інформації, який здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ і організацій.

Конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

Цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

Доступність - властивість інформації бути захищеною від несанкціонованого блокування;

Технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

Інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;

Комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Основними завданнями інших суб'єктів системи технічного захисту інформації є:

- дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;
- створення та виробництво засобів забезпечення технічного захисту інформації;
- розроблення, впровадження, супроводження комплексів технічного захисту інформації;

- підвищення кваліфікації фахівців з технічного захисту інформації.

*«Концепція технічного захисту інформації в Україні» [5]*

Концепція створена з ціллю забезпечити єдність принципів формування і проведення політики, де ТЗІ виступає складовою національної безпеки України, в усіх сферах життєдіяльності особи, суспільства та держави і служити підставою для створення програм розвитку сфери ТЗІ.

Технічний захист інформації - це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

*ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення [6]*

Стандарт визначає перелік термінів у сфері технічного захисту інформації. Містить інші варіанти тлумачень, що мало б бути неприпустимим.

Технічний захист інформації - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

Витік інформації - неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання

Інформація - відомості про об'єкти, процеси та явища.

Конфіденційна інформація - інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

*Постанова «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомуніка-ційних системах» [7]* визначає загальні вимоги та організаційні засади забезпечення захисту інформації в інформаційно-телекомунікаційних системах.

## 1.4 Постановка завдання

Метою роботи є компонування програмно-технічних засобів для забезпечення ефективного захисту корпоративної мережі, інформації та інформаційних систем, що знаходяться в ній.

В цьому розділі було розглянуто вже функціональні особливості корпоративної мережі, сучасний стан безпеки інформаційно-комунікаційної інфраструктури та нормативно-правова база інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити ще такі *завдання*:

- дослідити актуальні кібернетичні загрози для підприємства;
- провести аналіз існуючих засобів захисту інформації для підприємницького сектору;
- розробити демо-стенд корпоративної мережі з ключовими інформаційними системами;
- визначити потенційно критичні активи для організації;
- скомпонувати одні з основних засобів захисту інформації в підсистему захисту корпоративної мережі.

## Висновки за розділом 1

Корпоративна мережа відіграє важливу роль у бізнесі. Архітектори розробляють її з думками про:

1. Забезпечення основи для сучасного цифрового підприємства.
2. Використання мережевих контролерів.
3. Розширення сфери застосування.

Ключові особливості мережі підприємства виділені нижче:

- Швидкість зв'язку.
- Спільне використання файлів.
- Створення і використання резервних копій та відкат.
- Спільне використання програмного та апаратного забезпечення.

- Безпека.
- Масштабованість.
- Надійність.

Оглянуті закони, стандарти, положення та інші нормативні документи містять базову інформацію щодо технічного захисту інформації. Вони не виступають як вимоги у Постанові №95, а як щось більш загальне.

# РОЗДІЛ 2
# БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ

## 2.1 Загрози безпеці корпоративної мережі

З плином часу ідеї кіберзлочинців стають все витонченішими. Доопрацьовуються нові віруси, модифікуються старі, віруси-вимагачі отримують новий функціонал від троянських коней. Управління зловмисним ПЗ переноситься в стандартні для нинішнього інформаційного суспільства канали комунікації - месенджери. Так, наприклад, на відповідних майданчиках в мережі Інтернет можна придбати доступ до трояну віддаленого доступу T-RAT, управління яким відбувається за допомогою відомого месенджера Telegram. Новий ToxicEye, що застосовувався в атаках з лютого по квітень 2021 року також використовує у своїх цілях Telegram.

Але перелік основних загроз приблизно залишається незмінним для корпоративної мережі. Тому в рамках цього дослідження представлено список частих загроз і потім надана статистика щодо способів атак.

Головні категорії загроз наступні:

- відмова в обслуговуванні (DoS/DDoS);
- людина посередині (MitM);
- соціальна інженерія;
- шкідливі програми і шпигунські програми;
- парольні атаки;
- просунуті постійні погрози (APT).

Мета атаки "відмова в обслуговуванні" (DoS) - перевантажити ресурси цільової системи і змусити її припинити роботу, позбавивши доступу до неї користувачів. Розподілена відмова в обслуговуванні (DDoS) - це варіант DoS, при якому зловмисники зламують велику кількість комп'ютерів або інших пристроїв і використовують їх в скоординованій атаці на цільову систему.

Атаки DDoS часто використовуються в поєднанні з іншими кіберзагрозами. Ці атаки можуть запускати відмову в обслуговуванні, щоб привернути увагу співробітників служби безпеки і створити замішання, в той час як вони здійснюють більш тонкі атаки, спрямовані на крадіжку даних або заподіяння іншої шкоди.

Методи DDoS-атак включають:

- Ботнети - системи під контролем хакерів, заражені шкідливим ПЗ. Зловмисники використовують цих ботів для проведення DDoS-атак. Великі бот-мережі можуть включати мільйони пристроїв і здатні проводити атаки руйнівного масштабу.
- Атака Smurf - відправка exo-запитів Internet Control Message Protocol (ICMP) на IP-адресу жертви. ICMP-запити генеруються з «підроблених» IP-адрес. Зловмисники автоматизують цей процес і виконують його в великих масштабах, щоб перевантажити цільову систему.
- Атака TCP SYN flood - атака закидає цільову систему запитами на з'єднання. Коли цільова система намагається завершити з'єднання, пристрій зловмисника не відповідає, змушуючи цільову систему взяти тайм-аут. Це швидко заповнює чергу з'єднань, не дозволяючи легітимним користувачам підключитися.

Наступні дві атаки сьогодні менш поширені, оскільки вони спираються на уразливості в інтернет-протоколі (IP), які були усунуті на більшості серверів і мереж.

- Атака Teardrop - викликає перекриття полів довжини і зміщення фрагментації в IP-пакетах. Цільова система намагається відновити пакети, але зазнає невдачі, що може привести до її краху.
- Атака "Ping of death" - відправка на цільову систему неправильно сформованих або надмірно великих IP-пакетів, що призводить до збою або зависання цільової системи.

Коли користувачі або пристрої отримують доступ до віддаленої системи через Інтернет, вони припускають, що спілкуються безпосередньо з сервером цільової системи. При атаці MitM зловмисники порушують це припущення, поміщаючи себе між користувачем і цільовим сервером.

Після перехоплення зв'язку зловмисник може скомпрометувати облікові дані користувача, вкрасти конфіденційні дані і повернути користувачеві різні відповіді.

MitM-атаки включають в себе:

- Перехоплення сеансу - зловмисник перехоплює сеанс між мережевим сервером і клієнтом. Атакуючий комп'ютер замінює свою IP-адресу на IP-адресу клієнта. Сервер вважає, що він спілкується з клієнтом, і продовжує сеанс.
- Атака на повтор - кіберзлочинець підслуховує мережеву взаємодію і відтворює повідомлення в більш пізній час, видаючи себе за користувача. Атаки повторного відтворення були в значній мірі пом'якшені шляхом додавання тимчасових міток в мережеві повідомлення.
- Підміна IP-адреси - зловмисник переконує систему, що вона взаємодіє з довіреним, відомим суб'єктом. Таким чином, система надає атакуючому доступ. Зловмисник підробляє свій пакет, використовуючи IP-адресу джерела довіреного вузла, а не свою власну IP-адресу.
- Атака підслуховування - зловмисники використовують небезпечні мережеві комунікації для отримання доступу до інформації, що передається між клієнтом і сервером. Ці атаки важко виявити, оскільки мережеві передачі виглядають як звичайні.

Атаки соціальної інженерії працюють шляхом психологічного маніпулювання користувачами, змушуючи їх виконувати дії, бажані для зловмисника, або розголошувати конфіденційну інформацію.

До атак соціальної інженерії відносяться:

- Фішинг - зловмисники розсилають шахрайську кореспонденцію, яка здається що виходить із законних джерел, зазвичай по електронній пошті. У листі користувача можуть попросити виконати важливу дію або перейти по посиланню на шкідливий веб-сайт, в результаті чого він передасть зловмисникові конфіденційну інформацію або піддасть себе завантаженню шкідливого файлу. Фішингові листи можуть містити вкладення, заражене шкідливим ПЗ.

- Spear phishing - варіант фішингу, при якому зловмисники спеціально вибирають людей з привілеями безпеки або впливом, наприклад, системних адміністраторів або керівників вищої ланки.

- Типові атаки - зловмисники створюють підроблені веб-сайти з адресами, дуже схожими на адреси законних веб-сайтів. Користувачі заходять на ці підроблені сайти, не помічаючи незначну різницю в URL, і можуть передати зловмисникові свої облікові дані або іншу конфіденційну інформацію.

Атаки використовують безліч методів для впливу шкідливого ПЗ на пристрій користувача. Користувача можуть попросити здійснити будь-яку дію, наприклад, перейти за посиланням або відкрити вкладення. В інших випадках шкідливі програми використовують уразливості в браузерах або операційних системах, щоб встановити себе без відома або згоди користувача.

Після установки шкідливе ПЗ може відстежувати дії користувача, відправляти конфіденційні дані зловмисникові, допомагати зловмисникові проникати в інші цілі в мережі і навіть змушувати призначений для користувача пристрій брати участь в ботнет, використовуваному зловмисником в зловмисних цілях.

Атаки соціальної інженерії включають в себе:

- Троянський вірус - обманює користувача, змушуючи його думати, що це нешкідливий файл. Троян може почати атаку на систему і створити чорний хід, яким можуть скористатися зловмисники.

- Програми-вимагачі - забороняє доступ до даних жертви і загрожує видалити або опублікувати їх, якщо не буде виплачений викуп.

- Шкідлива реклама - інтернет-реклама, контрольована хакерами, яка містить шкідливий код, що заражає комп'ютер користувача при натисканні або навіть просто перегляді реклами. Шкідлива реклама була виявлена в багатьох провідних інтернет-виданнях.

- Шкідливі програми-чистильники - спрямовані на знищення даних або систем шляхом перезапису цільових файлів або знищення всієї файлової системи. Шкідливі програми-чистильники зазвичай призначені для передачі політичного повідомлення або для приховування дій хакерів після витоку даних.

- Завантажуючі на шляху - хакери можуть зламувати веб-сайти і вставляти шкідливі скрипти в PHP або HTTP-код на сторінці. Коли користувачі відвідують сторінку, шкідливе ПЗ безпосередньо встановлюється на їх комп'ютер; або скрипт зловмисника перенаправляє користувачів на шкідливий сайт, який і здійснює завантаження. Drive-by завантаження спираються на уразливості в браузерах або операційних системах.

- Шахрайські програми безпеки - вдають, що сканують комп'ютер на наявність шкідливих програм, а потім регулярно показують користувачеві фальшиві попередження і виявлення. Зловмисники можуть попросити користувача заплатити за видалення підроблених загроз з його комп'ютера або за реєстрацію програмного забезпечення. Користувачі, які погоджуються, передають зловмисникам свої фінансові дані.

Хакер може отримати доступ до парольної інформації людини, «пронюхавши» про підключення до мережі, використовуючи соціальну інженерію, вгадавши або отримавши доступ до бази даних паролів. Зловмисник може «вгадати» пароль випадковим або систематичним чином.

Атаки на паролі включають:

- Вгадування пароля грубою силою - зловмисник використовує програмне забезпечення для перебору безлічі різних паролів в надії вгадати правильний. Програмне забезпечення може використовувати певну логіку для перебору паролів, пов'язаних з ім'ям людини, його роботою, сім'єю і т.д.

- Атака по словнику - для отримання доступу до комп'ютера і мережі жертви використовується словник поширених паролів. Один з методів полягає в копіюванні зашифрованого файлу з паролями, застосуванні того ж шифрування до словника регулярно використовуваних паролів і порівнянні отриманих результатів.

Коли людина або група отримують несанкціонований доступ до мережі і залишаються невиявленими протягом тривалого періоду часу, зловмисники можуть поширювати конфіденційні дані, навмисно уникаючи виявлення співробітниками служби безпеки організації. Для APT потрібні складні зловмисники і великі зусилля,

тому вони зазвичай спрямовані проти національних держав, великих корпорацій або інших дуже цінних цілей.

З кожним роком статистика по успішним атакам стає більш привабливою для хакерів. Під їх вплив потрапляють все нові і нові компанії, більш великі та відомі. Нижче виділено найбільш цікаві дані за останні роки і щодо майбутніх:

1. Середній розмір виплат за вимагання в 2020 році виріс на 33% в порівнянні з 2019 роком і склав $ 111 605. [12]

2. У 2018 році в середньому в день блокувалося 10 573 шкідливих мобільних додатків. [13]

3. 48% шкідливих вкладень в електронну пошту - це офісні файли. [13]

4. Кількість шкідливих скриптів PowerShell, заблокованих в 2018 році на кінцевих пристроях, збільшилася на 1000%. [13]

5. Виявлення Ransomware переважає в країнах з великою кількістю населення, підключеного до Інтернету, а США займають перше місце - 18,2% всіх атак ransomware. [14]

6. 65% груп використовували spear-phishing як основний вектор зараження. [14]

7. 1 з 13 веб-запитів призводить до появи шкідливого ПЗ. [14]

8. На фішингові атаки припадає понад 80% зареєстрованих інцидентів безпеки. [15]

9. Кожну хвилину через фішингову атаку втрачається 17 700 доларів. [15]

10. 94% шкідливого ПЗ доставляється по електронній пошті. [15]

11. Атаки на IoT-пристрої потроїлися в першій половині 2019 року. [15]

12. Середня вартість атаки ransomware на підприємства становить $ 133 000. [16]

13. Більшість шкідливих доменів, близько 60%, пов'язані зі спам-кампаніями. [18]

14. Близько 20% шкідливих доменів є дуже новими і використовуються приблизно через тиждень після їх реєстрації. [18]

15. До 2023 року загальна кількість DDoS-атак у світі складе 15,4 мільйона. [19]

16. У 30% випадків витоку даних беруть участь внутрішні суб'єкти. [20]

17. 90% атак з віддаленим виконанням коду пов'язані з криптомайнінгом. [21]

18. 69% організацій не вірять, що загрози, які вони спостерігають, можуть бути блоковані їх антивірусним ПЗ. [22]

## 2.2 Методи і засоби захисту інформаційних потоків та ресурсів корпоративних мереж

На сьогоднішній день сучасна корпоративна мережа зазвичай побудована на клієнт-серверній архітектурі, яка розподілена на декілька географічно незалежних місць, між котрими завжди може встряти представник третьої сторони - зловмисник.

Огляд корпоративної мережі з точки зору необхідних точок для захисту дав ще низку результатів:

1. Наявність одного або декількох підключень до мережі Інтернет.
2. У кожній мережі можуть бути критично важливі сервери, які необхідні для зовнішніх користувачів, співробітників та підрядчиків.
3. Розмаїття пристроїв для роботи охопило і смартфони з планшетами.
4. Середній бізнес наразі може налічувати більше 100 сервісів, необхідних для роботи різних підрозділів.
5. Аудит корпоративної мережі вміщує в себе збір великої кількості логів.
6. Зміна деяких складових мережі (програмних чи апаратних) несе за собою редагування інших складових.
7. Велику кількість інформаційних систем всередині організації необхідно підтримувати кваліфікованими спеціалістами, які виступають зовнішніми користувачами зазвичай.

Забезпечення безпеки тільки на периметрі давно вже сприймається керівниками внутрішніх служб інформаційної безпеки підприємства як недостатній рівень. Просунуті атаки задіюють унікальне шкідливе програмне забезпечення з

розрахунку на те, що система захисту організації не зможе детектувати дії порушника. За деякими дослідженнями кібератак відсоток атак, спричинених діями інсайдерів становив 47%, що є величезною долею.

Аналіз поточного ринку щодо захисту інформації в корпоративних мережах привів нас до наступної класифікації рішень, що відображена в таблиці. Вона була представлена на IV міжнародній науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS).

Таблиця 2.1

Класифікація рішень

| *Класи* | *Системи* |
|---|---|
| Безпека даних | Запобігання витоку інформації |
| | Безпека баз даних |
| | Моніторинг доступу до файлів |
| Безпека кінцевих пристроїв | Безпека хостів |
| | Управління мобільними пристроями |
| | Контроль цілісності |
| Мережева безпека | Брандмауер для веб-додатків |
| | Захист від сучасних мережевих загроз |
| | Безпека електронної пошти та веб-серфінгу |
| Захист від APT атак | Обманний підхід / Пастки |
| | Виявлення вторгнень |
| | Хмара як засіб захисту від невідомих загроз |
| Захист віртуальної інфраструктури | Захист віртуальної інфраструктури |
| | Резервне копіювання даних |
| Управління ідентифікаціями і правами доступу | Управління ідентифікацією користувачів |
| | Управління привілейованими обліковими записами |
| | Технологія єдиного входу |
| | Моніторинг дій користувачів |
| Управління ризиками та вразливостями | Управління інформацією і подіями безпеки |
| | Управління мережевими вразливостями |
| | Управління вразливостями додатків |
| Розвідка та розслідування | Розвідка на основі відкритих джерел |
| | Управління розслідуваннями |
| | Комп'ютерна криміналістика |

Рішення з безпеки даних здатні відслідковувати критично важливу інформацію у всіх трьох станах (в русі, спокої, дії). За допомогою перегляду усіх даних, які передаються по портах і протоколах організації, відслідковування IP

адрес, з яких відбувся запит на доступ до інформації, перегляду активних дій співробітників на робочому місці, маскування та шифрування конфіденційних даних, визначення права власності на дані, осіб, що мають доступ до конфіденційних даних, виявленню закономірностей активності, що свідчать про наявність шкідливих програм, таких як криптографічні програми, збору всіх або окремих файлових операцій досягається ціль класу рішень.

Безпека кінцевих пристроїв базується на наступних функціях:

• моніторинг і збір даних про діяльність з кінцевих точок, які можуть вказувати на загрозу;

• аналіз цих даних для виявлення характерних особливостей загрози;

• автоматичне реагування на виявлені загрози для їх усунення або стримування, а також повідомлення співробітників служби безпеки;

• засоби криміналістики і аналізу для вивчення виявлених загроз і пошуку підозрілих видів діяльності;

• централізоване управління конфігураціями пристроїв.

Рішення з мережевої безпеки включають такі функції:

• фільтрування трафіку на основі протоколів, IP адрес, портів, внутрішніх користувачів організації, баз Spam DNS;

• глибокий аналіз пакетів даних;

• дешифрування SSL/TLS. Зараз сертифікат TLS у сайту не є 100 відсотковим фактором довіри. Зашифровані пакети можуть пройти через брандмауер та містити щось шкідливе;

• контроль додатків;

• аналіз електронної пошти з підтримкою DKIM, DMARC, SPF, BATV;

• захист від DDoS;

• балансування трафіку.

Методи захисту електронної пошти:

• SPF повідомляє приймаючим поштовим серверам про електронну пошту, що надходить з певного домену або стверджує, що вона належить до певного домену, а також дає вказівки про те, як ці повідомлення повинні бути оброблені в

разі збою. На дуже базовому рівні запис SPF визначає всі місця, звідки пошта з домена може бути законно відправлена, а потім вказує результат, якщо пошта не виходить з одного з схвалених джерел. Ці перевірки виконуються для запису відправника конверта, а не для запису з заголовка листа.

• DKIM - це процес криптографічного підпису різних розділів електронного листа. При отриманні електронного листа можна буде використовувати ці криптографічні підписи для підтвердження того, що електронний лист було отримано з заявленого джерела і що воно не було розкрите і змінено при транспортуванні. При невдачі цих перевірок ви можете вказати бажану дію.

• DMARC об'єднує результати DKIM і SPF, одночасно забезпечуючи петлю зворотного зв'язку з доменом будь-якої системи, яка могла бути підроблена. Подібно SPF і DKIM, DMARC покладається на підроблений домен, який опублікував запис DMARC DNS. DMARC-запис власників домену переглядається після SPF і DKIM, щоб подивитися, які дії вони рекомендують зробити (скинути, помістити в карантин або дозволити).

Захист від APT атак побудований в основному на технології Sandbox. Абстрактно на рівні вище знаходяться пастки та обманки, ціль котрих заманити ПЗ порушника у контрольовану зону. Вона зазвичай відокремлена від насправді цінних ресурсів корпоративної мережі, проте дуже схожа на них. Всередині ПЗ піддається сигнатурному на поведінковому аналізу. Разом із штучним інтелектом та машинним навчанням дані технології можуть дати оцінку діям порушника.

Функції рішень із захисту віртуальної інфраструктури схожі на перераховані вже класи систем:

• брандмауер,

• використання списків Web Reputation,

• використання модулів Intrusion Prevention, Anti-Malware, Application Control,

• моніторинг цілісності й інше.

Особливістю є безагентний режим, котрий працює на рівні системи віртуалізації – кінцеві точки комунікують не з додатковим ПЗ, встановленим на

кожній операційній системі, а з додатком на гіпервізорі, що розвантажує кінцеві системи.

Управління ідентифікаціями і правами доступу – широка категорія рішень, котра спрямована більше на захист від інсайдерів, але завжди є ймовірність зламу акаунтів одного із співробітників зовнішнім порушником.

В основі лежить централізоване управління правами внутрішніх і зовнішніх співробітників організації, доступом до інформаційних систем підприємства, механізми авторизації та простеження активності користувачів в них.

Перша частина категорії управління ризиками та вразливостями відповідає за збір інформації від мережевих програмних, програмно-технічних систем, кінцевих пристроїв та систем і базовий аналіз на можливість здійснення атаки на корпоративну мережу.

Друга та третя частини шукають вразливості у мережах, програмних додатках сигнатурним методом та за допомогою скриптів Proof-of-Concept чи базових реалізацій payload'ів, що підтверджують наявність вразливостей.

Розвідка допомагає службі безпеки організації виявити можливих ворогів у бізнесі, які можуть нанести атаку на корпоративну мережу чи зробити вклад в її здійснення.

Відбувається пошук інформації в мережі Інтернет:

- загальна інформація про компанію,
- оприлюднені сервіси для користування,
- дані співробітників,
- інформація щодо внутрішньої мережі контрагента.

А рішення з розслідування кіберінцидентів привносять деталізацію та візуалізацію негативної ситуації, що трапилася.

## 2.3 Активи, загрози та пропозиції захисту

Нехай є підприємство ABC, яке спеціалізується на бронюванні квитків для автобусів, потягів, літаків, готелів та курортів. Воно має 2 офіси, штат налічує приблизно 5 тисяч працівників.

Створення моделі загроз допоможе визначити, що слід захищати і сфокусуватися на активах, які важливі на бізнесу. Модель загроз описує корпоративні активи, загрози, що можуть атакувати ті активи, як ресурси можуть бути скомпрометовані і як зменшити ризики (рис. 2.2).

При вивченні SAST від Micro Focus був проаналізований дуже цікавий момент, що не розповідають в університеті протягом чотирьох років, - наявність більше десятка признаних технологій побудови моделі загроз (рис. 2.1). Вони описані, для деяких є навіть спеціальні програмні додатки (наприклад, для STRIDE від Microsoft).

Таблиця 2.2

Особливості методів побудови моделі загроз [24]

| Методи побудови моделі загроз | Особливості |
|---|---|
| STRIDE | • Допомагає визначити відповідні методи пом'якшення наслідків<br>• Є найбільш зрілим<br>• Простий у використанні, але забирає багато часу |
| PASTA | • Допомагає визначити відповідні методи зниження ризику<br>• Вносить безпосередній внесок в управління ризиками<br>• Містить вбудовану функцію пріоритезації заходів щодо зниження загроз<br>• Трудомісткий, але має багату документацію |
| LINDDUN | • Допомагає визначити відповідні методи пом'якшення наслідків<br>• Містить вбудовані пріоритети щодо зниження загроз<br>• Може бути трудомістким і віднімати багато часу |
| CVSS | • Містить вбудовану систему визначення пріоритетів при усуненні загроз<br>• Має стійкі результати при повторенні<br>• Автоматизовані компоненти<br>• Непрозорі розрахунки балів ризику |

*Продовження таблиці 2.2*

| | |
|---|---|
| Attack Trees | • Допомагає визначити відповідні методи зниження загроз<br>• Має стійкі результати при повторенні<br>• Легко використовувати, якщо ви вже добре розбираєтеся в системі |
| Persona non Grata | • Допомагає визначити відповідні методи пом'якшення наслідків<br>• Вносить безпосередній внесок в управління ризиками<br>• Має стійкі результати при повторенні<br>• Має тенденцію до виявлення тільки деяких підмножин загроз |
| Security Cards | • Заохочує співробітництво між зацікавленими сторонами<br>• Націлений на нестандартні загрози<br>• Приводить до великої кількості помилкових спрацьовувань |
| hTMM | • Містить вбудовану функцію визначення пріоритетів при усуненні загроз<br>• Заохочує співробітництво між зацікавленими сторонами<br>• При повторному проведенні має стійкі результати |
| Quantitative TMM | • Містить вбудовану систему визначення пріоритетів при усуненні загроз<br>• Має автоматизовані компоненти<br>• Має стійкі результати при повторенні |
| Trike | • Допомагає визначити відповідні методи пом'якшення наслідків<br>• Містить вбудовану систему визначення пріоритетів для зниження загроз<br>• Має автоматизовані компоненти<br>• Має нечітку, недостатню документацію |
| VAST Modeling | • Допомагає визначити відповідні методи зниження ризиків<br>• Має автоматизовані компоненти<br>• Явно розрахована на масштабованість<br>• Має мало загальнодоступної документації |
| OCTAVE | • Допомагає визначити відповідні методи зниження ризиків<br>• Містить вбудовану функцію визначення пріоритетів для зниження загроз<br>• Має стійкі результати при повторенні<br>• Явно розрахована на масштабованість<br>• Вимагає багато часу і має нечітку документацію |

Компанія ABC надає онлайн-портали, що дозволяють клієнтам заздалегідь бронювати квитки, змінювати або скасовувати їх до певного часу. Компанія зберігає інформацію про бронювання, особисті та платіжні дані клієнтів. Компанія пишається своїм сервісом і протягом останніх п'яти років справно виконує рейси вчасно.

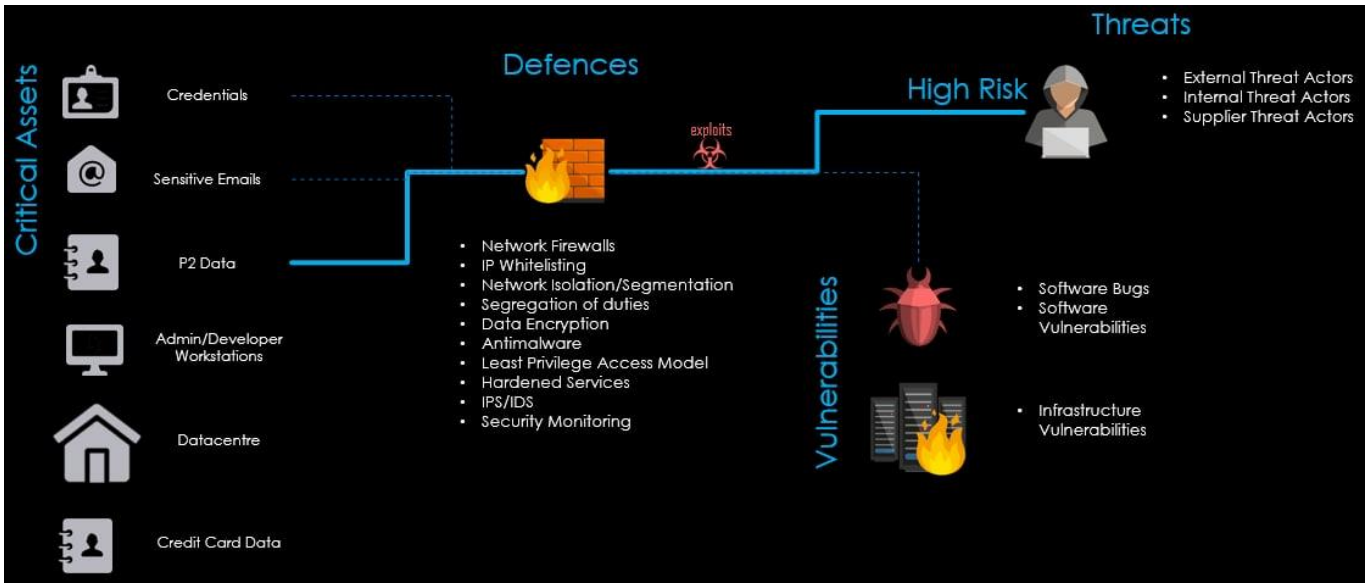



Рисунок 2.2. Важливі моменти при побудові моделі загроз

Модель загроз для цієї компанії повинна враховувати як матеріальні активи, такі як інформація про клієнтів, так і нематеріальні активи, такі як репутація. Також слід розглянути різні агенти загроз, такі як злочинці, конкуренти і іноземні уряди.

Клієнти довіряють компанії свої дані для оформлення платежів, включаючи дані про банківські картки.

Репутація для ABC – один із головних активів, чим вона пишається. Якщо відбудеться злам, витік конфіденційної інформації, то клієнти втратять довіру.

ABC необхідно, щоб їх сайт був доступний завжди для клієнтів, безперебійно. Якщо веб-сайт стане недоступним на декілька хвилин, то компанія втратить прибуток, а клієнти підуть до конкурентів.

Скоріш за все атакуюча сторона це злочинці, що зацікавлені у інформації про банківські картки, та конкуренти, що хочуть підставити під питання репутацію компанії чи тимчасово заблокувати онлайн портал.

Наступний крок у моделі загроз – зрозуміти, як активи можуть бути скомпрометовані. Зазвичай це робиться для всіх критичних активів. Проте в рамках цього дослідження – побудові підсистеми захисту – буде розглянуто тільки активи персональних даних клієнтів, банківських карт та ресурси мережі (інфраструктура з серверною, мережевою частиною, робочі місця та критична інформація). Останній широкий актив є важливим для бізнесу, і при втраті контролю над ним, організація понесе збитки. Тому захист корпоративної мережі – важливий пункт у забезпеченні головного інтересу бізнесу. Розглянуто декілька шляхів, як може статися витік:

- підкуп співробітників, інсайдерська атака;
- використання вразливостей на веб-сайті (SQLi, XSS, misconfiguration і т.д.);
- соціальна інженерія, фішинг.

Такі розповсюджені загрози та атаки можуть бути частиною APT атак, в життєвому циклі котрої скоріш за все буде розповсюдження по мережі, підняття привілеїв і як результат – дестабілізація усього бізнесу, особливо мережі організації.

Для протистояння таким атакам можна використати наступні рішення:

1. Перш за все використання Zero Trust, розподілення обов’язків, рольової моделі. Зазвичай базово це реалізується у Active Directory, але у нас 5000 співробітників, десятки додаткових інформаційних систем всередині мережі (IBM Notes/Domino, IBM Traveler, Exchange, SAP AMP, SAP Business Objects Enterprise, SAP BSP, SAP BWP, SAP UAP, 3DSECURE та інше), тому засіб з управління аккаунтами співробітників дуже допоможе контролювати права, доступи користувачів (не клієнтів).

2. Захист від атак на веб-сайт буде забезпечено за допомогою статистичного аналізу коду сайта.

3. Від фішингу буде використано Next-Generation Firewall (допоможе і з попереднім пунктом), спеціалізований захист електронної пошти.

## Висновки за розділом 2

Загрози безпеці корпоративної мережі не стоять на місці, вони розвиваються, деякі стають неактуальними (як Teardrop чи «Ping of death»). До головних категорій загроз виділено наступні:

- відмова в обслуговуванні (DoS/DDoS);
- людина посередині (MitM);
- соціальна інженерія;
- шкідливі програми і шпигунські програми;
- парольні атаки;
- просунуті постійні погрози (APT).

Методи і засоби для захисту від цих атак теж еволюціонують. Існує обширний список рішень інформаційної безпеки. Оглянувши корпоративну мережу компанії ABC вирішено організувати підсистему захисту, яка складається з брандмауера нового покоління, системи управління цифровими особистостями та тестування програмного коду веб-сайту компанії для проактивного захисту мережі.

# РОЗДІЛ 3
# РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА

## 3.1 Структура корпоративної мережі з підсистемою захисту

Як вже було сказано, організація має 2 територіально відокремлених офіси. Головний я назвав DC Main, іншого DC Read-only. Усе через те, що в кожній локальній мережі стоїть свій контролер домену (DC), проте у другій мережі – RODC. Він займається реплікацією даних з серверу у DC Main. Для легшого розуміння структури мережі вона була розділена на VLAN'и. У 101 VLAN'і, що зображений на рисунку 3.1, знаходяться робочі місця співробітників. Для меншого навантаження використано один Switch на схемі у кожному VLAN'і. Кольори ліній описані у відокремленій зоні схеми та продубльовані на рисунку 3.2.

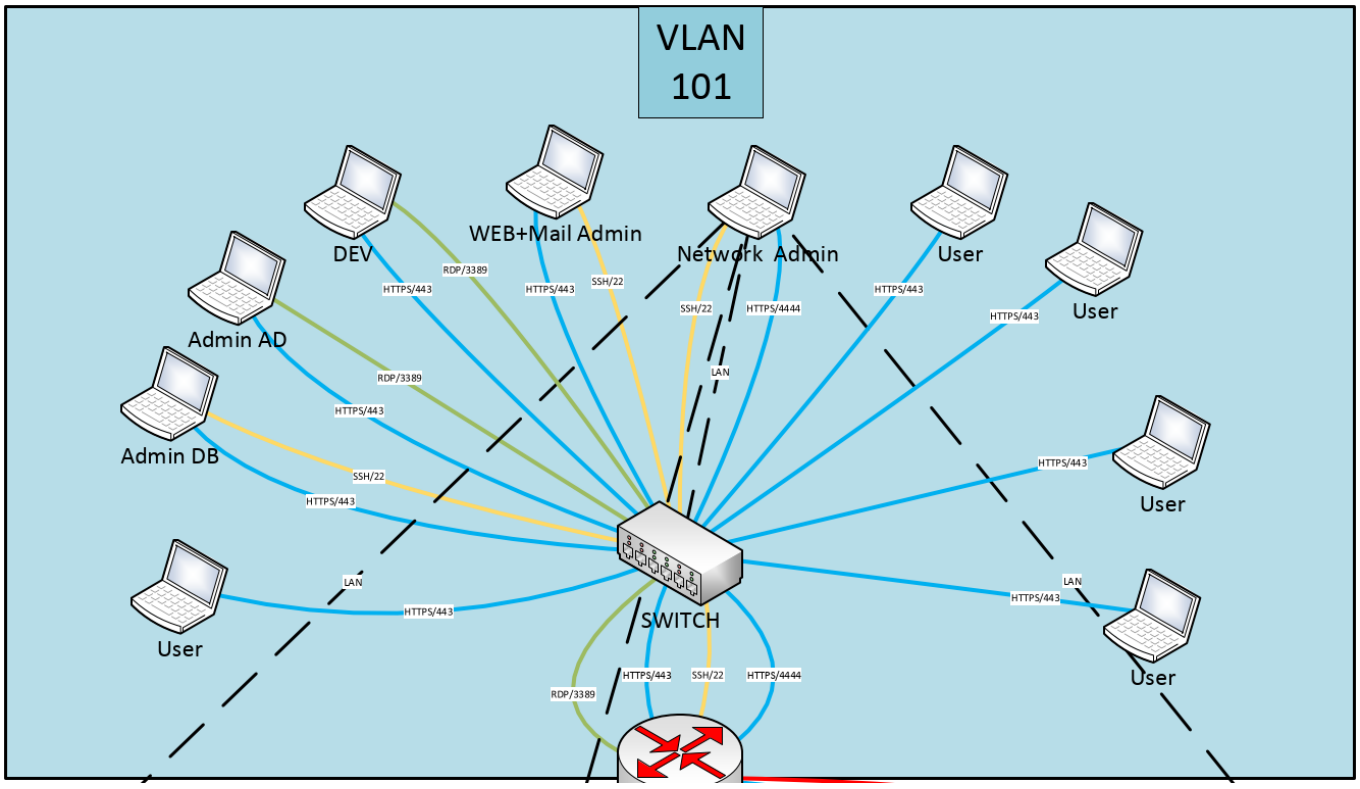



Рисунок 3.1. VLAN 101

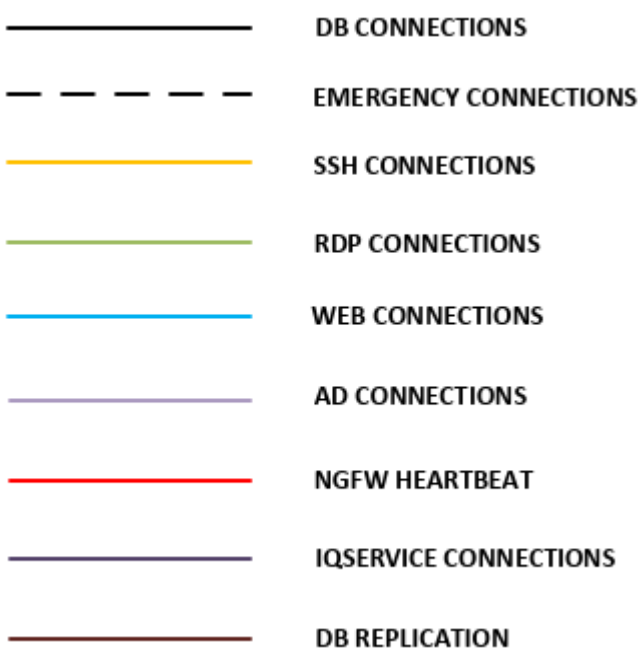



Рисунок 3.2. Опис схеми

Адміністратори AD, співробітники з критичними правами розробників мають можливість підключатися до деяких систем по RDP. Адміністратори баз даних, електронної пошти, мережі та веб-серверів мають можливість підключатись по SSH до своїх цільових машин. Усі співробітники можуть використовувати веб-доступ до кінцевих інформаційних систем. Мережеві адміністратори уповноважені підключатись напряму до мережевого обладнання по спеціально виділеному фізичному порту в ньому, цей зв’язок я відобразив пунктирними лініями. Вважається, що цей адміністратор може налаштовувати обладнання, не тільки до яких приведені лінії, а до усього.

Схожа ситуація стоїть з VLAN’ом 201 (у DC Read-only усі віртуальні локальні мережі в діапазоні з 201), що зображений на рисунку 3.3. Усі безіменні комп’ютери це звичайні користувачі, деякі ПК не підключені ніяк у схемі до систем – це лише знак, що доступ для співробітників ще не виділений.

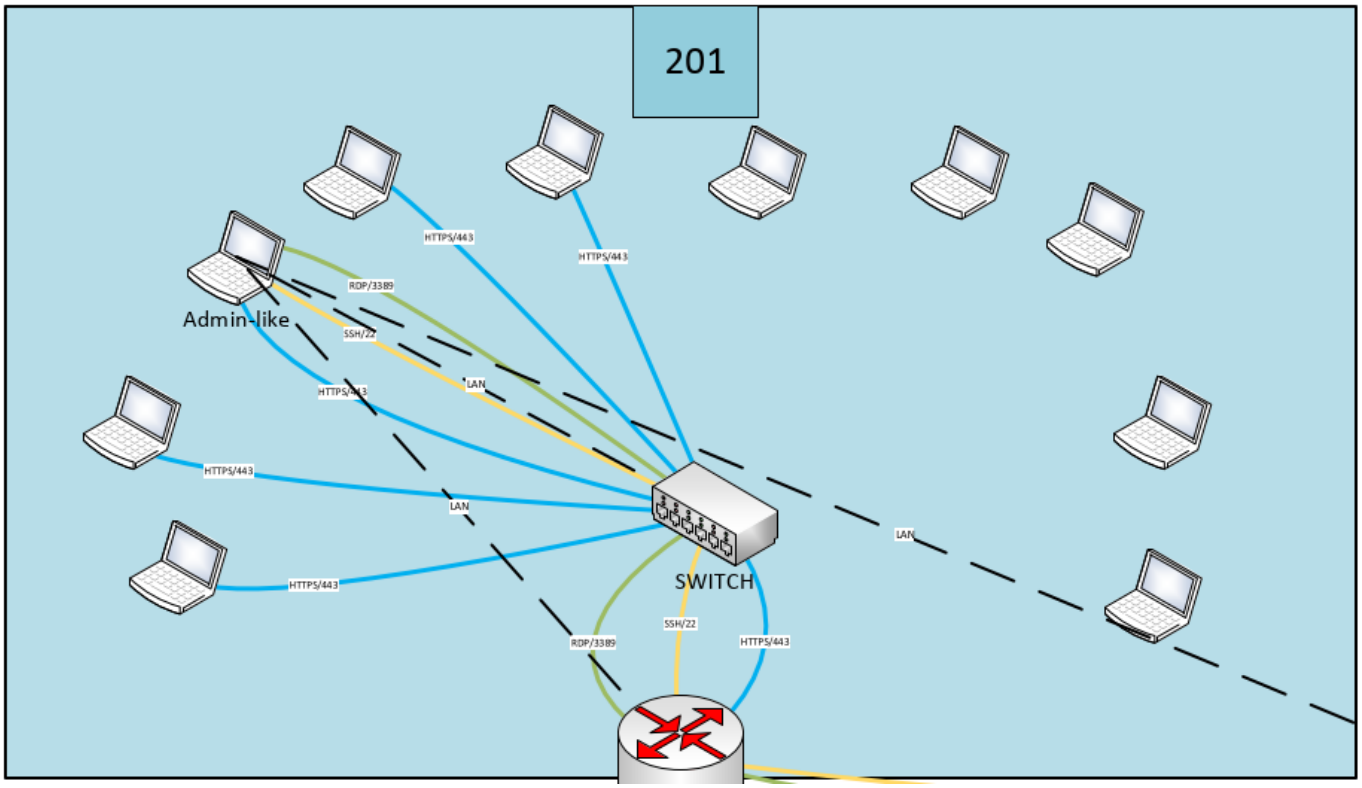



Рисунок 3.3. VLAN 201

У VLAN 103 (рис. 3.4) знаходяться AD DC, термінальний сервер, з якого можуть відбуватися допоміжні дії або дії, які небезпечно проводити безпосередньо на цільовій машині. Також тут знаходиться сервер SAP HR/HCM, в якій виконуються усі кадрові операції, сервери від IdentityIQ та балансувальник трафіку. IdentityIQ розвернута у розподіленому вигляді з відмовостійкістю. Тобто є окремо сервер бази даних та окремо сервер для виконання операцій з веб частиною. І копії цих машин стоять у VLAN 203 (рис. 3.5). Реплікація бази даних відбувається по захищеному порту, на якому й відкрита ця БД, тобто 1522. На термінальному сервері розвернутий IQService, зв'язок з яким від IdentityIQ Server здійснюється по захищеному порту 6060. IdentityIQ Server отримує інформацію з Global Catalog в AD по порту 3269. А основна реплікація DC відбувається по порту 636. Операційна система на серверах IdentityIQ – Red Hat 8, тому RDP там не потрібне. А от до DC та терміналу адміністратори отримують RDP доступ.

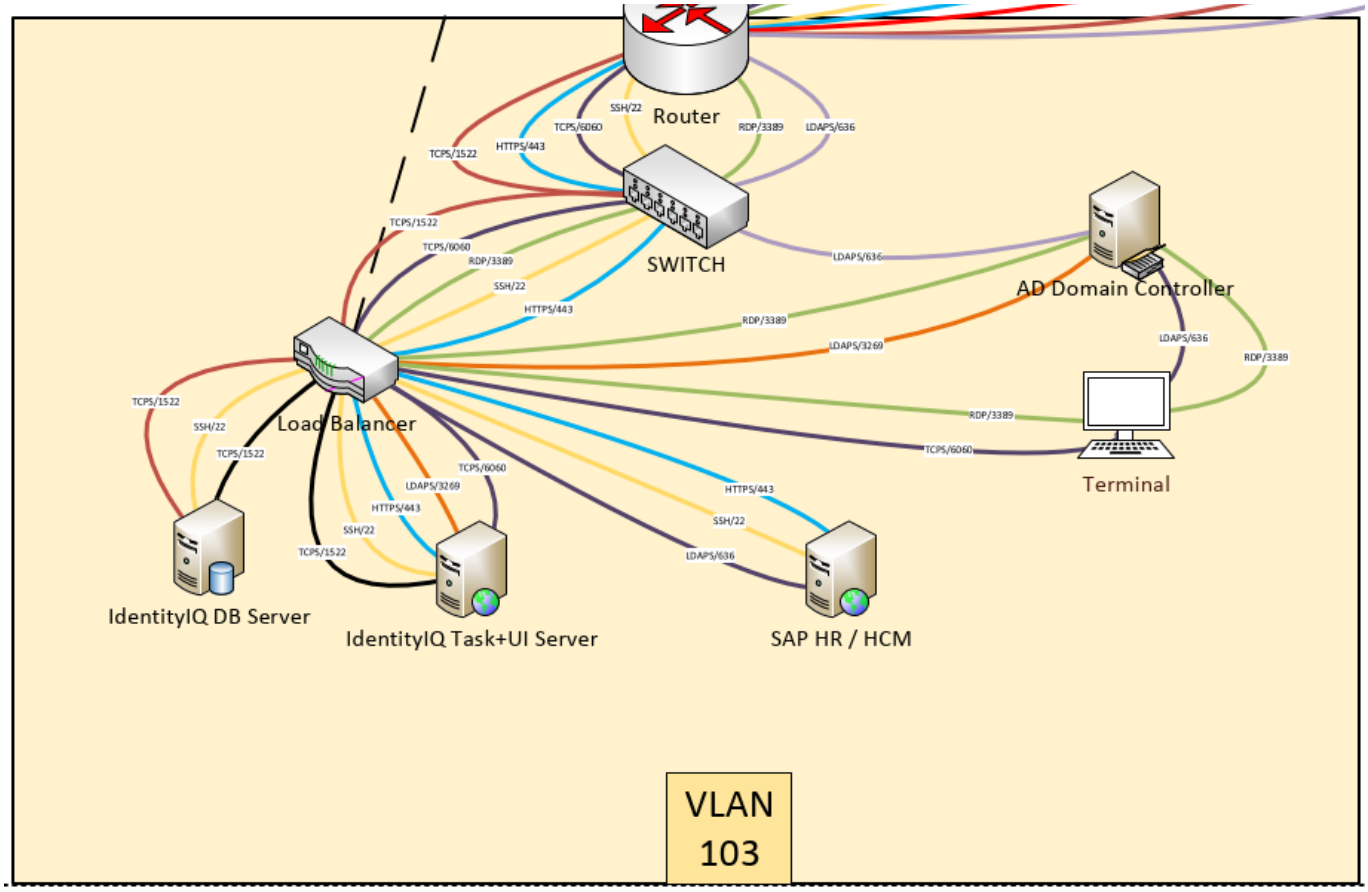



Рисунок 3.4. VLAN 103

У VLAN 203 зображені сервери, які йдуть після балансувальника.

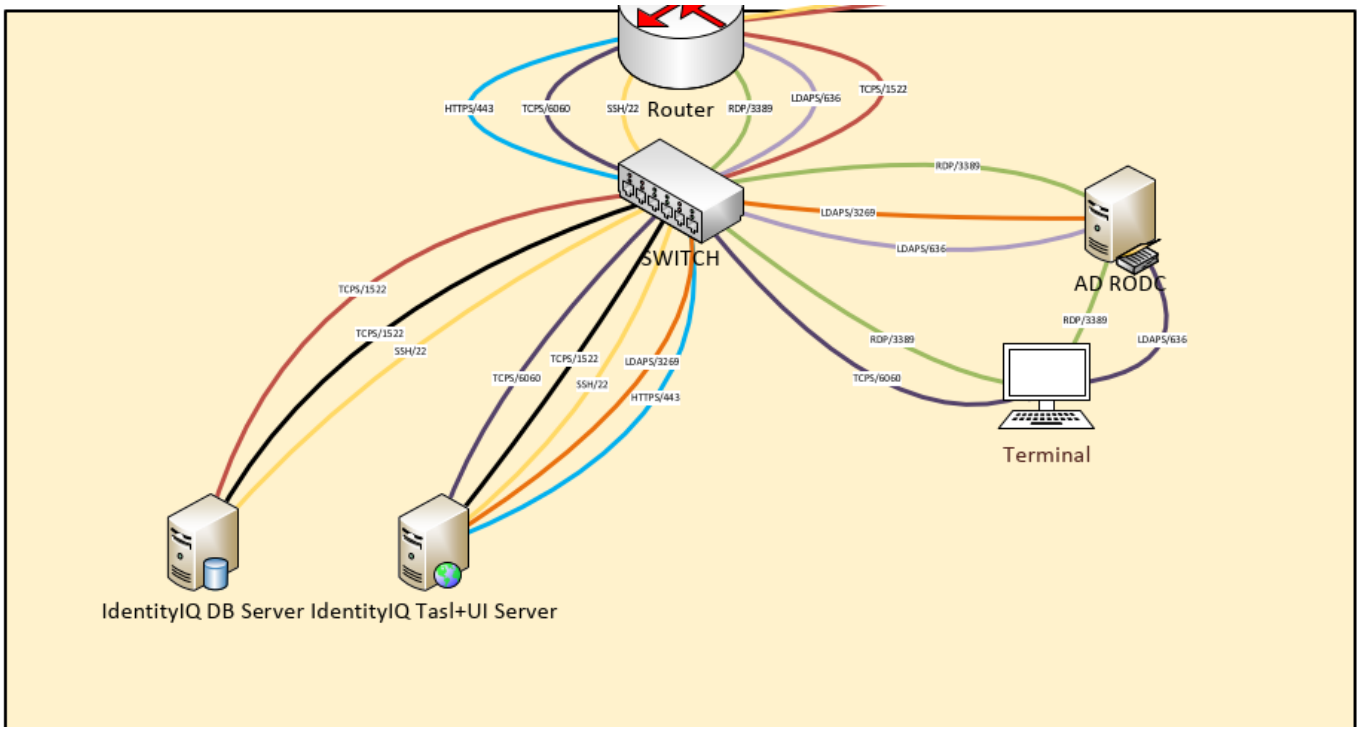



Рисунок 3.5. VLAN 203

Vlan 104, що зображений на рисунку 3.6, містить інші сервери, серед яких: для Fortify Application Security Testing систем, для розробників з налаштованим SDLC (середовище розробки, GitHub, Jenkins, Jira), база даних з-під веб-серверу у DMZ-зоні та інші.

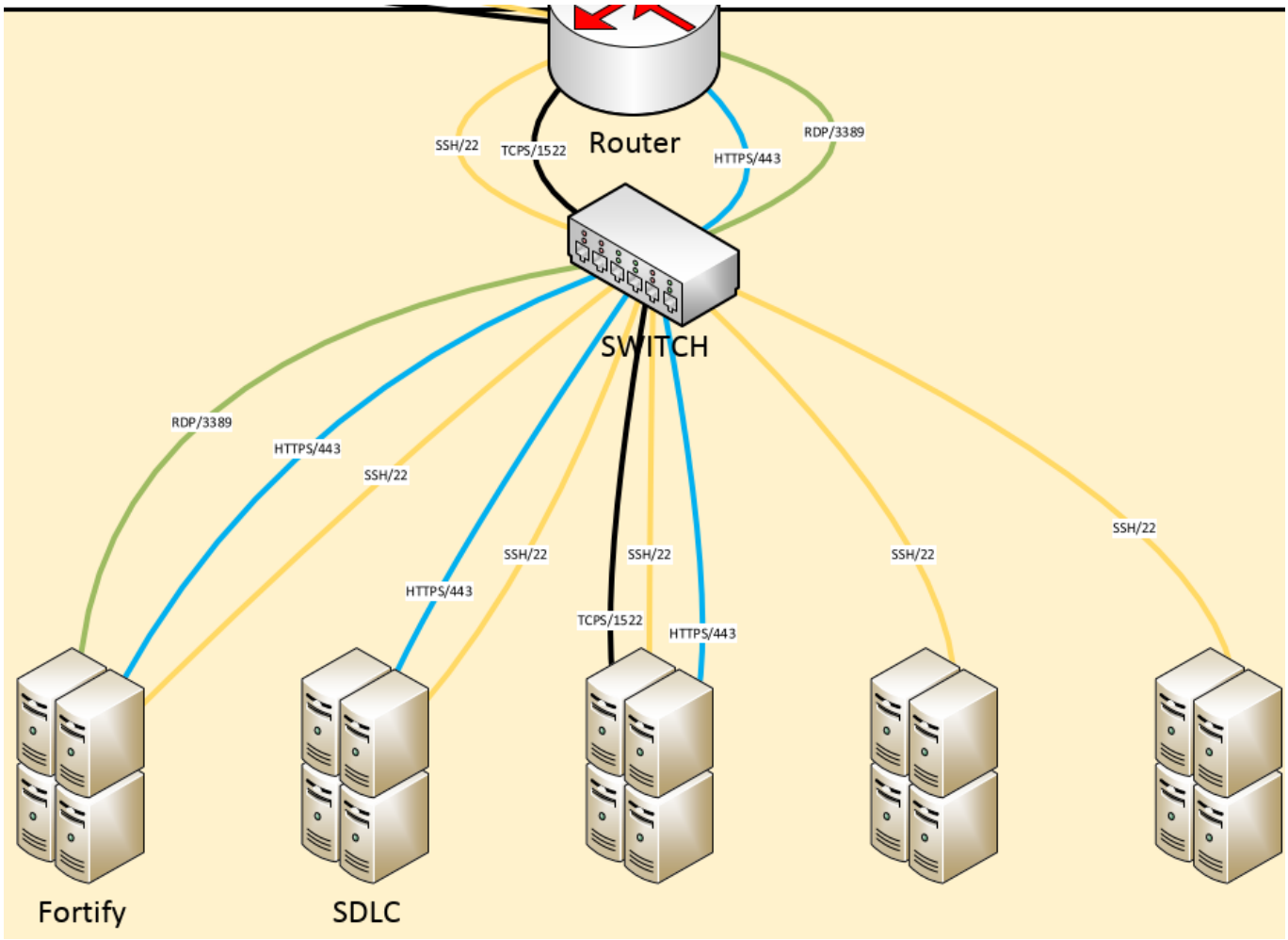



Рисунок. 3.6. VLAN 104

В DMZ (рис. 3.7) розташовані веб-сервер, поштовий сервер та термінальний, з якого відбуваються підключення до серверів. І на вході стоїть додатковий NGFW. Поштовий сервер контролює 2 домени, один локальний, а другий – для використання у мережі Інтернет.

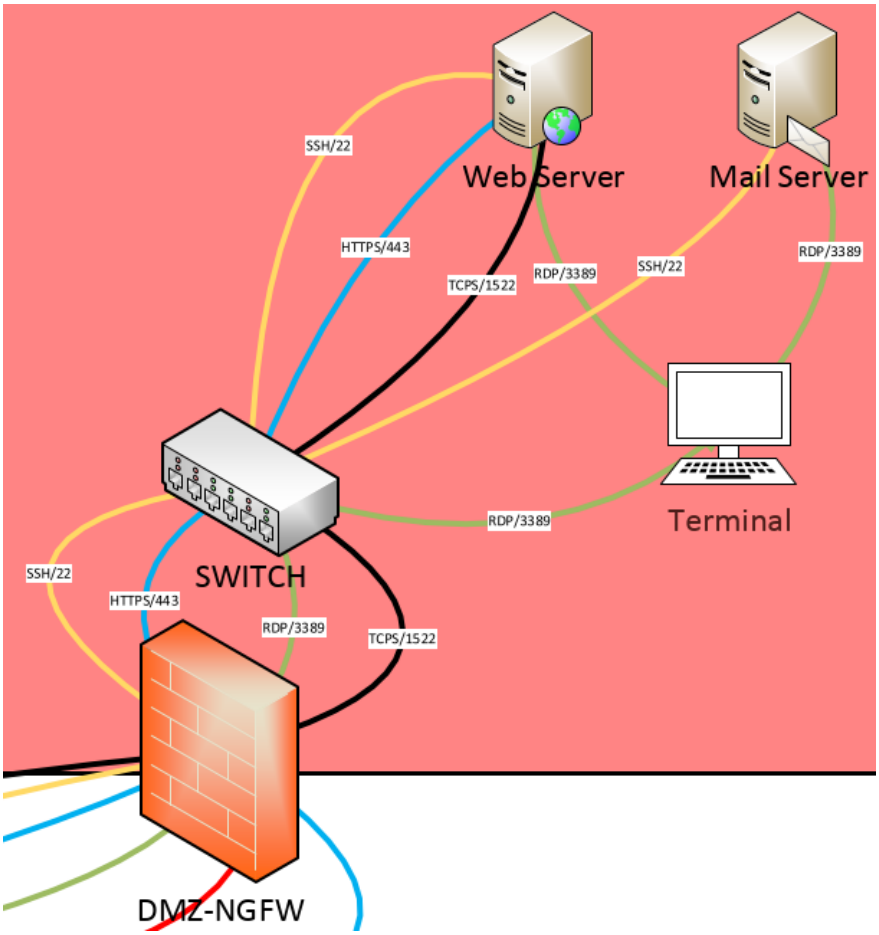



Рисунок 3.7. DMZ-зона

Ззовні знаходиться непідконтрольний користувач, що підключається на веб-сайт чи пересилає пошту. Між офісами налаштований MPLS. А на брандмауері для нього виділений окремий порт.

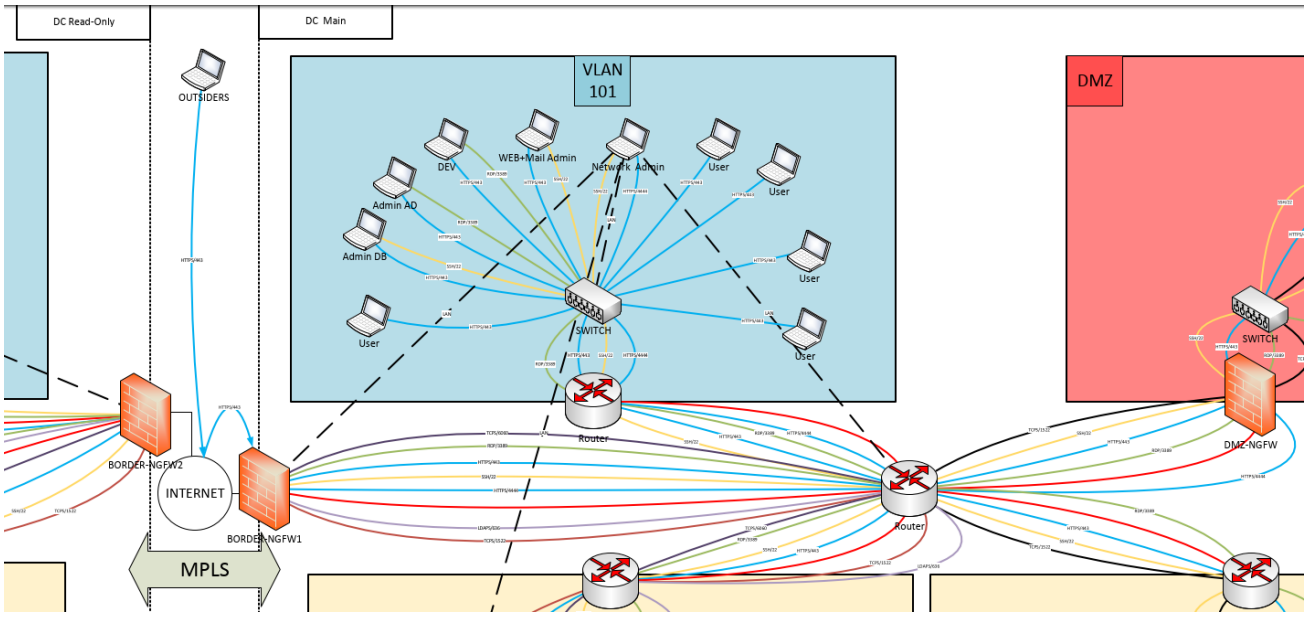



Рисунок 3.8. Зв’язність офісів

### 3.2 Управління привілеями, доступами співробітників

Напевно кожна мережа, що побудована на Windows архітектурі в основному, має розгорнуту службу каталогів Active Director (AD), яка вміщує в себе облікові записи співробітників, сервісні акаунти, групи, політики доступу і використання робочих місць та інше.

AD відповідає за загальну організаційну структуру підприємства, приклад якої зображено на рисунку 3.9. Можна створити групи в залежності від департаментів, відділів, посад і т.п. Надати цим групам різні політики, різний доступ до інформації та ресурсів корпоративної мережі.


Рисунок 3.9. Приклад організаційної структури організації у AD

На рисунку як раз зображено, що у кожному обліковому записі вказаний департамент, в якому знаходиться співробітник.

Частою практикою є створення двох або й більше акаунтів для одного співробітника, якщо він є розробником якоїсь системи або повинен мати права адміністратора. Як раз Кетрін Сімонс має додатковий обліковий запис з адміністративними правами csimmons-adm. Таким чином застосовується модель Zero Trust. Кетрін використовуватиме свій додатковий акаунт лише за необхідності.

Я додав її у різні групи, і анкета Кетрін виглядає приблизно так, як показано на рисунку 3.10.

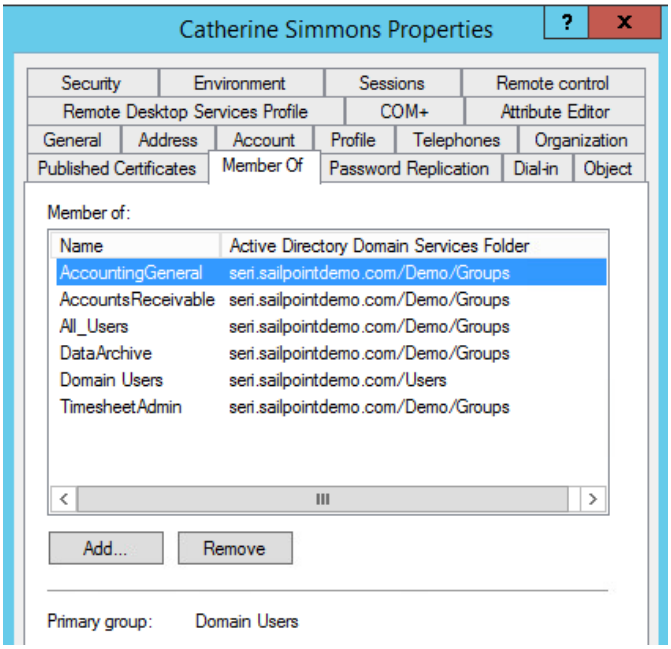



Рисунок 3.10. Приклад назначених груп, що буде надалі привілеями

В компанії ABC нараховується понад ста інформаційних систем. Зазвичай групи ще й створюються з урахуванням привілеїв у кінцевих системах. А отже, в AD буде величезна кількість привілеїв, які можна надати співробітникам. Для такої великої компанії  не дивно мати спеціалізований продукт SAP HR/HCM, який використовується для управління персоналом (прийняття на роботу, переміщення на посадах, між департаментами, звільнення, відпустки і т.д.), створення заявок на кожну дію з персоналом. В ньому ж пересилаються підписані документи, щодо організації бізнес-процесів, операцій з персоналом та вирахування заробітної плати.

В SAP HR величезна кількість привілеїв зазвичай зберігається. Але як я вже зазначив, великою кількістю систем та обліковими записами в них складно керувати. Саме для цього і рекомендується використовувати IGA систему. Про неї я розповім на прикладі Sailpoint IdentityIQ [10], що є лідером і на сьогодні на порталі Gartner Peer Insights за відгуками клієнтів.

SailPoint IdentityIQ - технологія управління обліковими записами і призначеним для користувача доступом. Служить для централізованого управління життєвим циклом облікових записів користувачів, їх правами доступу до інформаційних ресурсів організації на основі рольових моделей, політик і правил.

Технологія реалізує управління і контроль прав доступу (атестацію і сертифікацію) на предмет відповідності корпоративної моделі доступу всередині організації та оцінку / аналіз ризиків, пов'язаних з наданням цих прав.

SailPoint IdentityIQ допомагає відповісти на три головні питання:

1. У кого є доступ?
2. У кого повинен бути доступ?
3. Як цей доступ використовується?

У складі основних компонентів IdentityIQ:

1. IdentityIQ Compliance Manager (Модуль управління відповідністю) - систематизує контроль за виконанням процедур управління відповідністю і прискорює процес проведення аудиту за рахунок автоматизованої сертифікації / атестації доступу і централізованого управління політиками.

2. IdentityIQ Lifecycle Manager (Модуль управління життєвим циклом) управляє змінами прав доступу, зміною паролів і автоматизацією життєвого циклу подій за допомогою зручного порталу самообслуговування. Дозволяє гнучко підстроювати рішення для задоволення постійно мінливих потреб бізнес користувачів, одночасно відповідаючи вимогам ефективності.

3. IdentityIQ Password Manager (Модуль управління паролями) допомагає співробітникам самостійно управляти паролями в своїх акаунтах, делегувати таку можливість іншим або ж бере участь в автоматичній синхронізації паролів від акаунтів різних систем.

SailPoint IdentityIQ базується на платформі управління «особистостями» (Identity Governance Platform), яка складається з:

1. Сховище ідентифікаційних даних:

   - Формує єдине уявлення про всіх користувачів, облікові записи та привілеї, які містяться в усіх додатках.
   - Використовує зовнішні конектори і прості файли для імпорту даних з будь-якого ресурсу, в тому числі даних про облікові записи і привілеї з бізнес-додатків, баз даних, платформ, додатків SaaS і інших систем.

- Порівнює індивідуальні облікові записи та привілеї для створення багатовимірного «куба особистості», виділяючи кожного користувача і його доступ.
- Перекладає технічні дані про ролі та привілеї в зрозумілу для бізнесу інформацію, виділяючи важливий бізнес-контекст, в тому числі опис привілеїв, які використовуються в IAM-процесах.

2. Конектори ресурсів:

- Забезпечують інтеграцію з корпоративними додатками, такими як платформи, бази даних, каталоги і бізнес-додатки, які працюють в центрі обробки даних або в хмарі.
- Підтримують автоматичну агрегацію даних про користувачів, їх облікові записи і привілеї, що містяться у взаємозалежних системах.
- Автоматизує додавання облікових записів і паролів в систему.

3. Модель політик:

Модель політик IdentityIQ задає потужну структуру управління за рахунок ефективного визначення, перевірки і дотримання політик доступу на підприємстві. Використовуючи централізований арсенал політик, підприємства можуть ефективно застосовувати всі типи політик в області відповідності, провіжінінга і управління.

4. Рольова модель:

Рольова модель допомагає легко встановлювати відповідність між привілеями користувача і його робочими функціями - використовуючи простий підхід до адміністрування, запиту, перегляду і виконання призначеного для користувача доступу.

- Визначає гнучкі типи ролей з найменшим необхідним рівнем привілеїв.
- Виявляє бізнес та IT-ролі на основі атрибутів особистості і привілеїв.

5. Модель ризиків:

IdentityIQ містить модель ризиків, яка виявляє в організації зони ризику, що утворилися в результаті видачі користувачам конфліктних або надмірних привілеїв

доступу. Актуалізує ступінь ризику, грунтуючись на змінах в призначених для користувача привілеї та інших факторах.

6. Модель управління робочим процесом:

Модель управління робочим процесом SailPoint заснована на гнучких повторюваних бізнес-процесах, що дозволяє скоротити час і витрати на їх впровадження та реалізацію і спростити роботу кінцевого користувача.

Налаштування IdentityIQ починається з підключення існуючих кінцевих систем, у котрий зберігаються привілеї та облікові записи. Я маю з десяток підключених інформаційних систем, серед яких Active Directory, бази даних, прості файли та інше, що представлено на рисунку 3.11. Звертаю увагу на числові мітки біля «Name», «Host» і тому подібне. Їх немає бути насправді, це моя робота. SailPoint не підтримує українську мову, тому я перекладаю інтерфейс IdentityIQ, використовуючи ці мітки.

| 479__Name | 700__Host | 516__Type | 8321__Aggregation Types |
|---|---|---|---|
| Active Directory | seri.sailpointdemo.com | Active Directory - Direct | account, group |
| Enterprise Directory | seri.sailpointdemo.com | SunOne - Direct | account, group |
| ERP Portal | seri.sailpointdemo.com | SOAPConnector | account |
| File Access Manager | seri.sailpointdemo.com | SecurityIQ | group, alert, unstructured |
| Human Resources | seri.sailpointdemo.com | JDBC | account |
| JDBC PAM Application | localhost | JDBC | account, group |
| Mainframe | localhost | RACF | account, group |
| Microsoft SQL Server | seri.sailpointdemo.com | Microsoft SQL Server - Direct | account, group |
| Oracle EBS | localhost | Delimited File Parsing Connector | account, group |
| PRISM | seri.sailpointdemo.com | JDBC | account, group |
| Privileged Account Management | http://localhost:8080/identityiq/plugin/rest/scimPamBri... | Privileged Account Management | account, group |
| TRAKK | seri.sailpointdemo.com | JDBC | account |
| TRAKK-WS | seri.sailpointdemo.com | Web Services | account, group |

Рисунок 3.11. Список додатків або інформаційних систем

IdentityIQ містить декілька файлів зі списком усіх фраз та слів, що використовуються в інтерфейсі чи в шаблонах електронних листів. Файл, кусок якого представлений на рисунку 3.12, місить зліва порядковий номер рядка, назву змінної та значення на українській мові.

| | | | |
|---|---|---|---|
| 2106 | menu_label_my_work | = | Справи |
| 2107 | menu_label_identities | = | Особистості |
| 2108 | menu_label_identity_warehouse | = | Список особистостей |
| 2109 | menu_label_applications | = | Додатки |
| 2110 | menu_label_app_definition | = | Списк додатків |
| 2111 | menu_label_intelligence | = | Аналітика |
| 2112 | menu_label_setup | = | Система |
| 2113 | menu_label_global_settings | = | Глобальні налаштування |
| 2114 | menu_label_dash | = | Інформаційна панель |
| 2115 | menu_label_define | = | Define |
| 2116 | menu_label_apps | = | Додатки |
| 2117 | menu_label_debug | = | Діагностика |
| 2118 | menu_quick_links_aria_label | = | Інформаційні панелі та швидкі посилання. Натисніть клавішу Er |
| 2119 | menu_admin_aria_label | = | Адміністратор |
| 2120 | menu_desc_apps | = | Налаштовувати додатки, якими керує IdentityIQ. |
| 2121 | menu_label_roles | = | Ролі |
| 2122 | menu_desc_roles | = | Створювати та підтримувати ролі та профілі. |
| 2123 | menu_label_role_mining | = | Отримання ролей |
| 2124 | menu_desc_role_mining | = | Запланувати процес отримання ролей та аналіз результатів. |
| 2125 | menu_desc_identities | = | Список усіх особистостей у системі з використанням фільтрів. |
| 2126 | menu_label_entitlement_catalog | = | Каталог привілеїв |
| 2127 | menu_desc_entitlement_catalog | = | Налаштування привілеїв. |
| 2128 | menu_label_groups | = | Групи |
| 2129 | menu_desc_groups | = | Налаштування груп. |
| 2130 | menu_label_activity_target_cats | = | Категорії цільових активностей |
| 2131 | menu_desc_activity_target_cats | = | Налаштування категорій цільових активностей. |
| 2132 | menu_label_policies | = | Політики |
| 2133 | menu_desc_policies | = | Налаштування політик. |

Рисунок 3.12. Список фраз інтерфейсу

SailPoint офіційно не має свого представника в Україні, проте як мінімум 2 українські банки мають її всередині своєї мережі. Наразі немає підтримки навіть російської мови, не те що української. Тому один з цих банків отримає переклад IdentityIQ саме від мене. Я взяв англійську версію .properties файлу, завантажив її у Excel та розмістив у три колонки. Це додало зручності із копіюванням лише значень змінних.

Паралельно до цього я вже написав скрипт для додавання в кожне значення змінної номер рядка, на якому розміщена змінна. Код написаний на мові програмування Python третьої версії, що дуже важливо. Перш за все потрібно імпортувати необхідний модуль для роботи з файлами: import os. Далі пара змінних, перша з яких – це файл з якого будуть читатися усі фрази, а друга – файл, у який будуть записані змінені дані (рис. 3.13).

```
import os

filePath='test1.txt'
destPath='iiqCustom.properties.bk'
```

Рисунок 3.13. Робочі файли

Наступна функція, зображена на рисунку 3.14, зчитує усі рядки та організує їх у список

```
def reading(filePath):
    with open(filePath,encoding='utf-8', mode='r') as reader:
        return list(reader)
```

Рисунок 3.14. Функція зчитування

Після зчитування даних можна приступити до зміни. Функція setMarks() відкриває обов'язково новий файл з другої змінної у режимі запису, та в кожну змінну додає на початок значення число та два нижніх дефіси. Вона зображена на рисунку 3.15.

```
def setMarks():
    l = reading(filePath)
    with open(destPath,encoding='utf-8', mode='w') as writer:
        n=0
        for item in l:
            n+=1
            point = item.find('=')
            if point!=-1:
                writer.write(item[:point+1]+'{0}__'.format(n)+item[point+1:])
            else:
                writer.write(item)
```

Рисунок 3.15. Функція додавання міток

Функція deleteMarks(), що на рисунку 3.16, вертає стан оригінального файлу, без числових міток:

```
def deleteMarks():
    l = reading(filePath)
    with open(destPath, encoding='utf-8', mode='w') as writer:
        n=0
        for item in l:
            n+=1
            point = item.find('=')
            noPoint = item.find('__')
            if point!=-1:
                writer.write(item[:point+1]+item[noPoint+2:])
            else:
                writer.write(item)
```

Рисунок 3.16. Функція видалення міток

Остання функція створена через неможливість веб-серверу та Java (при поточних налаштуваннях кожного) відобразити правильно український алфавіт, як і французький з його «шапочками» зверху літер. Я зчитую файл після попередньої дії і відкриваю другий файл у режимі запису. Перевіряю кожну літеру в рядку на співпадіння з латинськими літерами, базовими знаками і цифрами. Конвертую з utf-8 у utf-16 лише українську мову. Алгоритм представлений на рисунку 3.17.

```
def unicoding():
    l = reading(destPath)
    with open(destPath, encoding='utf-8', mode='w') as writer:
        for item in l:
            writer.write(''.join(c if 0 < ord(c) <= 127
            else '\\u{:04x}'.format(ord(c)) for c in item))
```

Рисунок 3.17. Функція конвертування utf-8 у utf-16

І вкінці я викликаю потрібні функції, коментуючи зайві:

*#deleteMarks()*

*setMarks()*

*unicoding()*

Наступним кроком є агрегація облікових записів із підключених додатків (рисунок 3.18) та привілеїв (рисунок 3.19). Після першого запуску задачі на зчитування створюються цифрові особистості, так звані Identity Cubes. Кореляція атрибутів кінцевих додатків з атрибутами цього куба налаштовується власноруч.

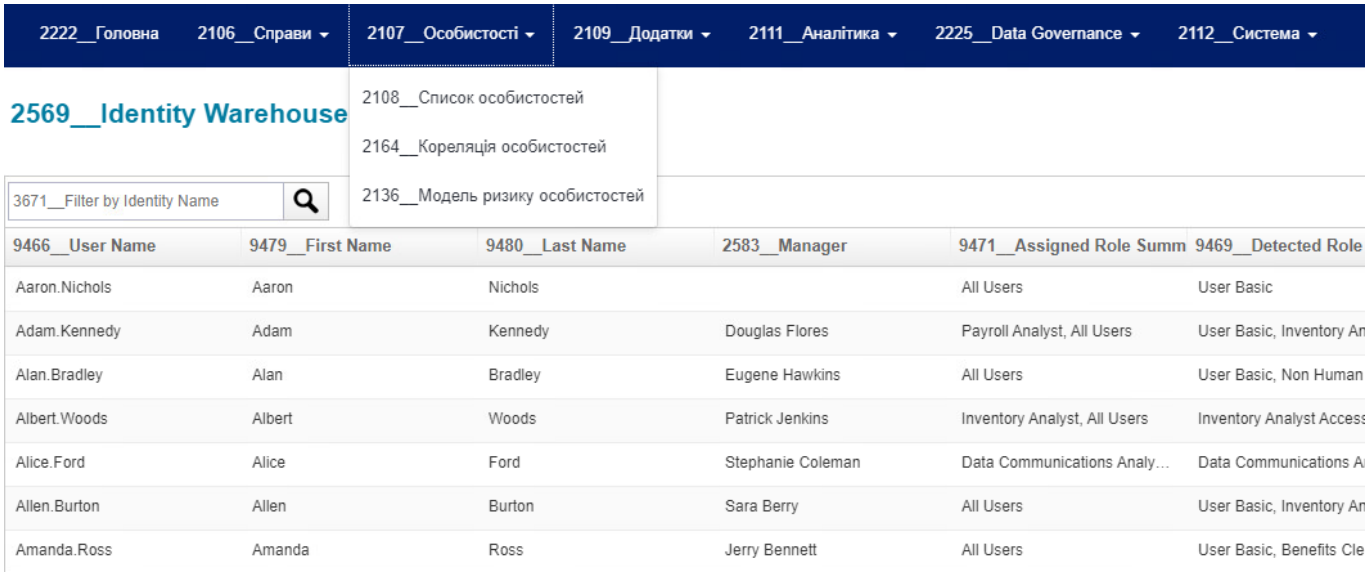



Рисунок 3.18. Список цифрових особистостей

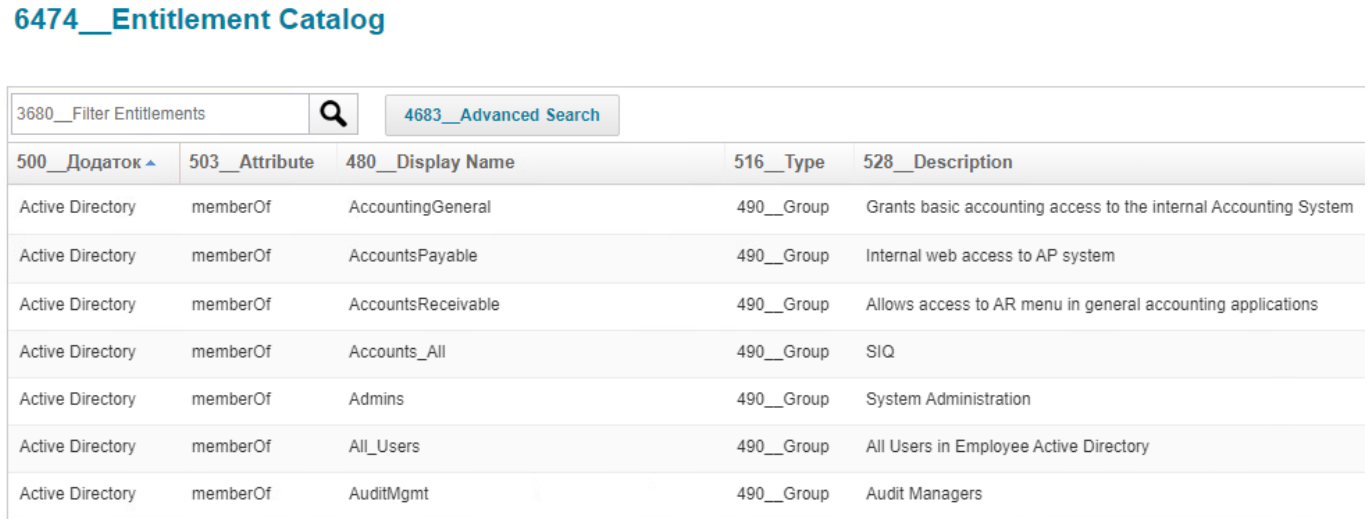



Рисунок 3.19. Список привілеїв

Для того, щоб провести зчитування даних з Active Directory, слід встановити на додатковій Windows-машині або прямо на domain controller IQService. Зареєструвати його як сервіс та завести новий сервісний акаунт, від лиця котрого будуть виконуватися дії в AD. Також слід наділити цей обліковий запис відповідними правами, щоб він мав можливість редагувати, додавати, видаляти користувачів, групи.

У IdentityIQ є політики розподілення обов'язків (рис. 3.20), які можна налаштувати в залежності від атрибутів цифрових особистостей, привілеїв або ж ролей, які також створюються всередині системи. Вони регулюють ситуації, коли співробітник може мати пару ролей чи привілеїв, які конфліктують між собою.

Наприклад, співробітник з правами адміністратора Windows машин не може виступати архітектором з питань безпеки мережі. Є 2 типи ролей: технічні та бізнес (більш зрозумілі для більшості співробітників).

| | |
|---|---|
| Oracle EBS Effective Entitlement SOD | EffectiveEntitlementSOD |
| Risk Demo Policy | Risk |
| SOD Policy Accounting General Access-Internal Auditor Access | SOD |
| SOD Policy Accounts Payable Access-Accounts Receivable Access | SOD |
| SOD Policy Internal Auditor Access-Oracle Administrator Access | SOD |
| SOD Policy Internal Auditor Access-Unix Administrator Access | SOD |
| SOD Policy Internal Auditor Access-Windows Administrator Access | SOD |
| SOD Policy Oracle Administrator Access-Security Architect Access | SOD |

Рисунок 3.20. Список політик розподілення обов’язків

Окрім цього можливо запускати перевірку поточних привілеїв у співробітників. Для цього виконуються або сертифікації, або, так і називаються, перевірки доступу. Менеджери, керівники підрозділів (зазвичай такі категорії) або конкретна інша особа отримують сертифікацію, яку мають виконати. За ними тепер закріплена робота з визначення необхідності прав співробітнику(ам). Є кнопки для погодження доступу або відкликання, вони показані на рисунку 3.21. Також ці сертифікації можуть знаходити порушення політик, про які я сказав вище.

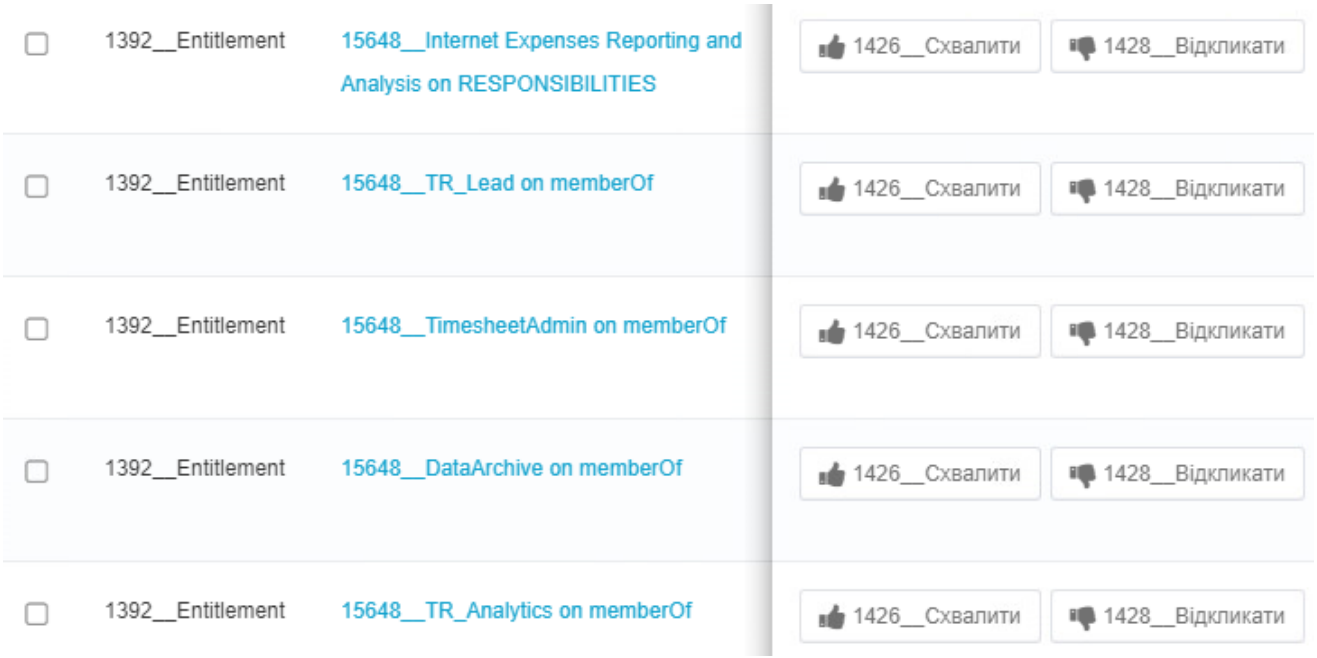



Рисунок 3.21. Перевірка доступів співробітника

Також IdentityIQ дозволяє блокувати, видаляти акаунти співробітників у кінцевих системах, як це показано на рисунку 3.22.

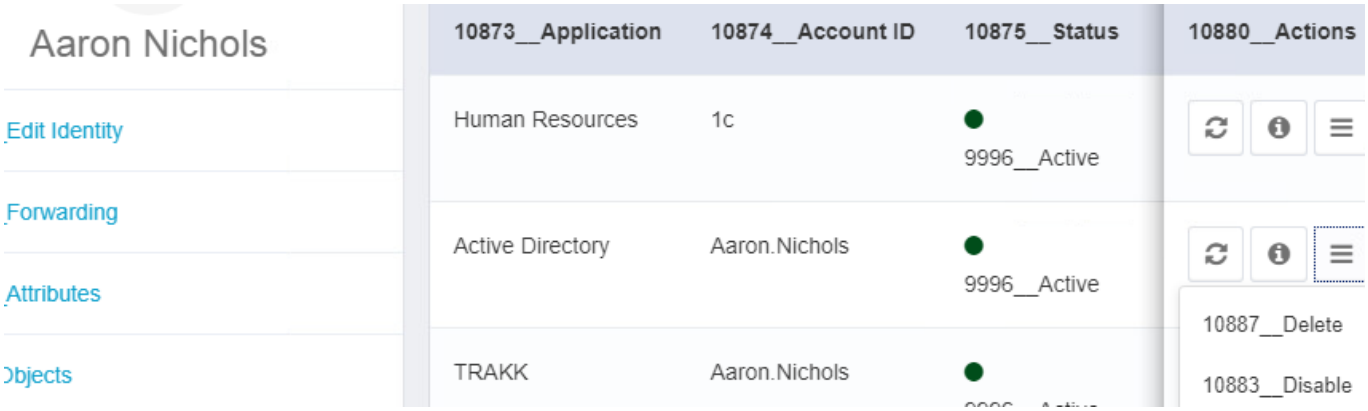



Рисунок 3.22. Операції з обліковими записами у кінцевих системах

### 3.3 Використання Next-Generation Firewall для захисту мережі

Міжмережеві екрани нового покоління, або NGFW - захисні програмно-технічні засоби , які включають в себе функції звичайних фаєрволів разом з додатковим функціоналом: глибоку інспекцію трафіку і систему проактивного виявлення загроз.

Gartner визначає визначив Sophos XG Firewall [8] як візіонер серед інших 18 вендорів цього забезпечення в минулі 2 роки. Я, як сертифікований інженер і вже дуже скоро архітектор по цьому продукту, можу впевнено сказати, що Sophos розробили дуже прозору і ефективну екосистему кібербезпеки всередині мережі для управління, видимості і захисту за допомогою хмарного управління Sophos Central і Synchronized Security. Вони дивляться у майбутнє і створюють новий передовий функціонал. Тому саме на прикладі міжмережевого екрану від цього вендора я захищу периметр, ключові точки нашої мережі та трафік всередині неї.

При конфігуруванні звичайних правил фаєрволу доступний ряд цікавих функцій. Першою я б виділив «Аналіз HTTP та розшифрованого HTTPS на шкідливий контент», також можна використовувати Sandstorm (хмарна пісочниця від Sophos) та функцію Deep Packet Inspection, принцип роботи якої зображений на рисунку 3.23.

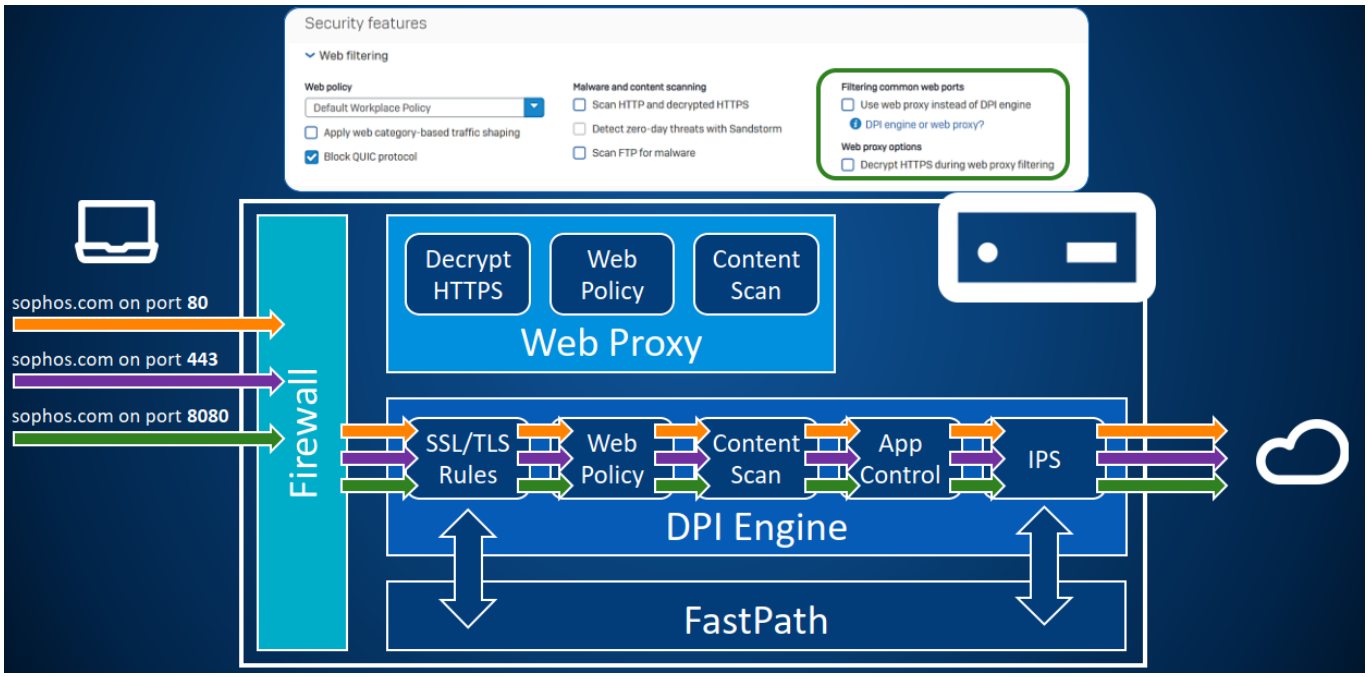



Рисунок 3.23. Deep Packet Inspection

SSL/TLS правила просто кажуть, як опрацьовувати трафік з конкретних адрес до якихось серверів (розшифровувати, пропускати, блокувати). Забезпечу захищений зв’язок між офісами за допомогою IPsec тунеля, налаштування показані

нижче на рисунку 3.24. Відкриваю доступ до AD, SAP HR та термінального сервера з філії.

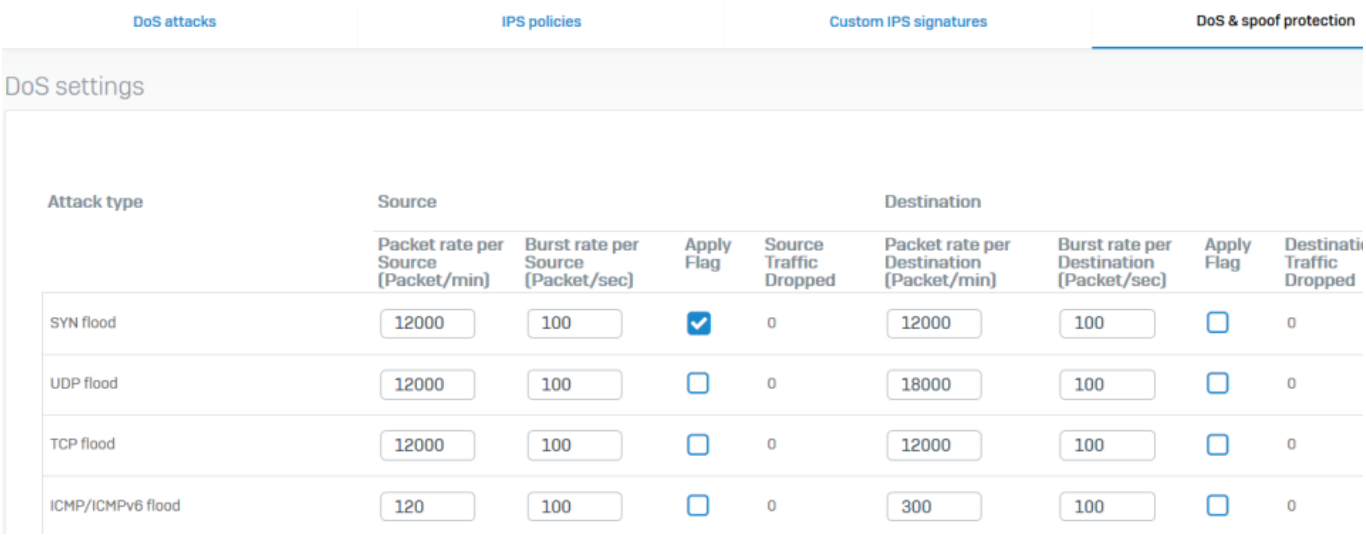



Рисунок 3.24. Захист від DoS атак

Модуль IPS налаштовується доволі легко. Створюються правила, використовуючи готові сигнатури чи розробляючи власні. Фільтрація категорій відбувається досить гнучка. Якщо якась категорія обрана, то за замовчуванням усі сигнатури з неї активуються у правилі. Потім це правило вибирається у секції правил фаєрвола. На рисунку 3.25, наприклад, створюється правило для веб-серверу головного. Також воно буде задіяне у внутрішніх веб-серверах, тобто тих, що необхідні для функціонування деяких інформаційних систем організації (SAP наприклад).

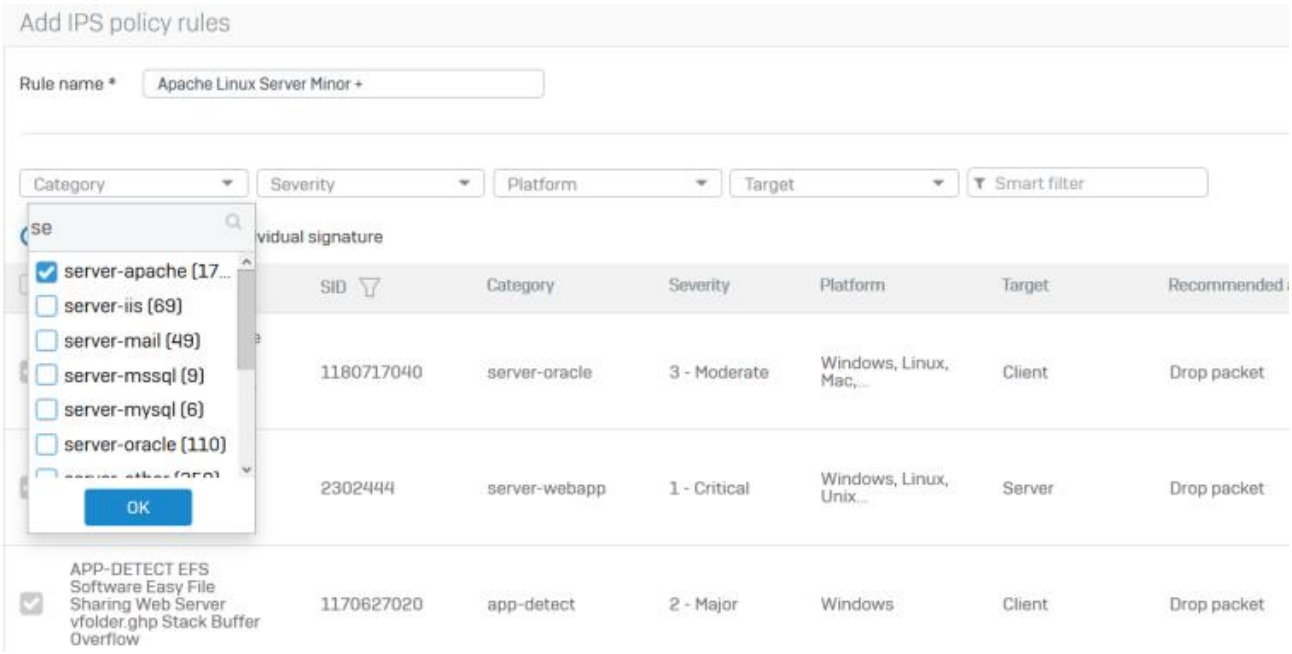



Рисунок 3.25. Правило IPS

Дуже корисною функцією, за яку неодноразово відмічали Sophos, є Security Heartbeat (рис. 3.26). На кінцеві системи встановлюється тонкий додаток. При виявленні на машині шкідливого ПЗ додаток сповіщає через сусіднє мережеве обладнання до головного NGFW, що є зараження. І в залежності від сповіщення виконується дія. Найкатегоричнішою є відключення повністю усього вузла мережі з іншими кінцевими точками, котрі вже потенційно могли заразитися. Це не допустить розповсюдження атаки. Така функція налаштована в компанії ABC. Вмикається легко - вибирається зона, на яку розповсюджується дія і все. Контроль відбувається через командний центр, який також є особливістю рішень від Sophos. Він є хмарним і контролює усі продукти з однієї панелі.

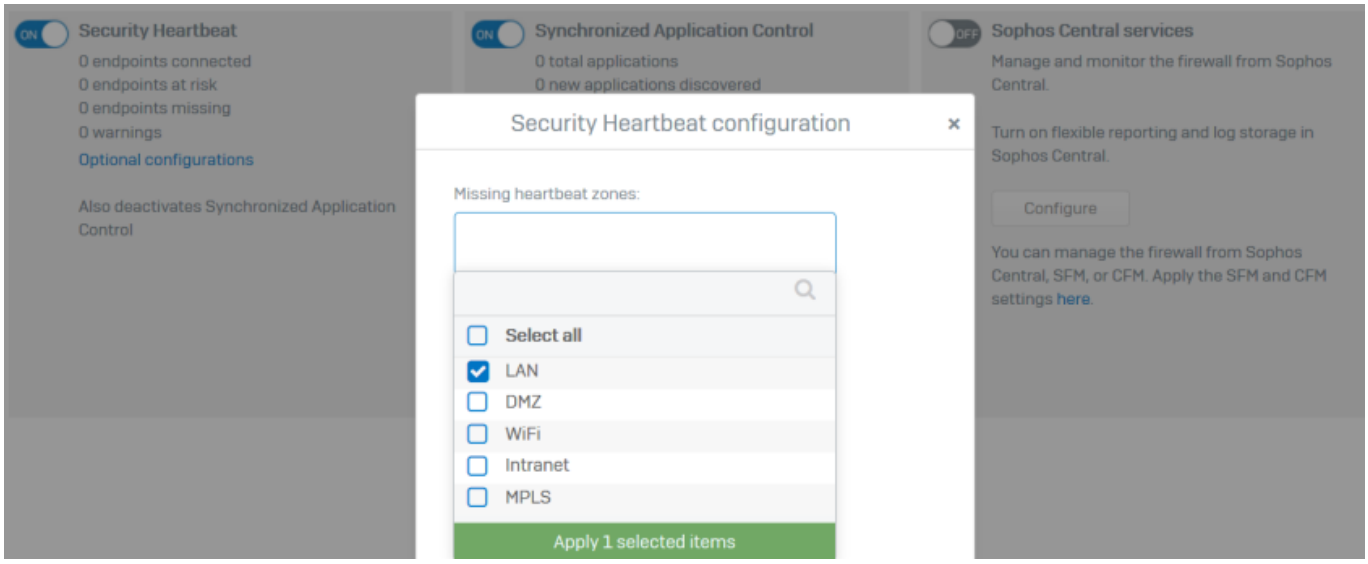



Рисунок 3.26. Включення Security Heartbeat

Захист електронної пошти базується на створенні проксі для поштового сервера і перевірці кожного листа. Є перевірки на спам (рис. 3.27), шкідливе ПЗ на формати файлів, які передаються поштою. У налаштуваннях шкідливого ПЗ я увімкнув «Детектування zero-day атак за допомогою Sandstorm» та «Використання двох двигунів для перевірки на віруси». Тобто Sophos XG Firewall надає 2 антивірусні двигуни.

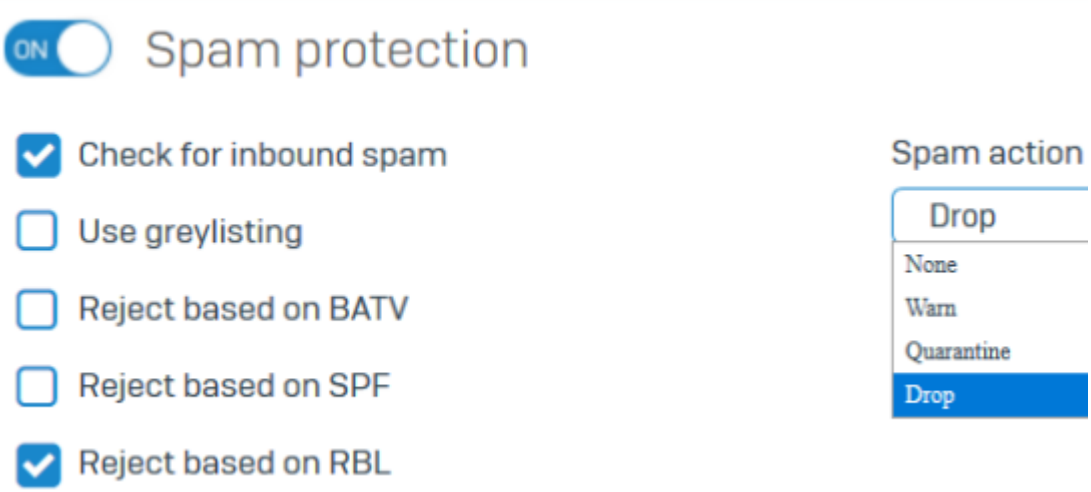



Рисунок 3.27. Перевірка на спам

Звісно були налаштовані правила для забезпечення зв’язку всередині локальної мережі, між LAN та WAN, DMZ та WAN, DMZ та LAN. Налаштована аутентифікація у систему Sophos User Portal, де співробітники можуть переглянути власну статистику по своїм електронним листам, можливим зараженням. Додавання

облікових записів я виконав через інтеграцію з AD, а не власноручним додаванням кожного співробітника.

### 3.4 Використання Application Security Testing засобів

Тестування безпеки додатків (AST) є найважливішим компонентом безпеки додатків і наріжним каменем будь-якої стратегії безпеки програмного забезпечення.

Статичне AST (SAST) - показує, де саме в коді можна знайти проблему. Це не просто пошук помилок безпеки, але і допомога розробникам у створенні більш безпечного коду. Статичний аналіз коду може бути повністю інтегрований в середу розробки, надаючи розробникам дані для створення кращого і більш безпечного програмного забезпечення.

Суттю динамічного AST (DAST) є моделювання атак в реальному світі на працюючий веб-додаток або сервіс для виявлення вразливостей, які можна використовувати (тому для цього не потрібен код і немає мовних обмежень). Ціль - виявити вразливості до того, як вони потраплять в виробничу середу.

Micro Focus [11] має рішення світового класу в рамках як SAST, так і DAST.

Як інженер по продуктам від двох найкращих вендорів (Checkmarx, Micro Focus) у цій сфері, можу стверджувати, що другий останніми роками плідно попрацював над покращенням своїх рішень, і саме його буду використовувати у корпоративній мережі.

На схемі, рисунку 3.6, зображений сервер під Micro Focus Fortify. На ньому встановлено:

1. Статичний аналізатор коду (SCA) - SAST.
2. WebInspect - DAST.
3. Software Security Center (SSC) - комплексна платформа безпеки додатків, що входить до складу локальних рішень для отримання повної видимості ризиків безпеки додатків.

SCA отримує код, що знаходиться на корпоративному github, де розробники оновлюють його при дописуванні веб-сайтів організації.

І при кожному новому зчитуванні і збірці запускається скрипт на Jenkins, що сканує весь код на вразливості. Зберігається результат у форматі .fpr, і його вже можна переглянути у 2 середах: Audit Workbench (тут можна і запустити сканування власноруч) та SSC.

Запустивши тестове сканування вразливостей, я отримав результат, який показаний на рисунку 3.28. На ньому показане вразливе відображення чутливої інформації, а саме – паролів.

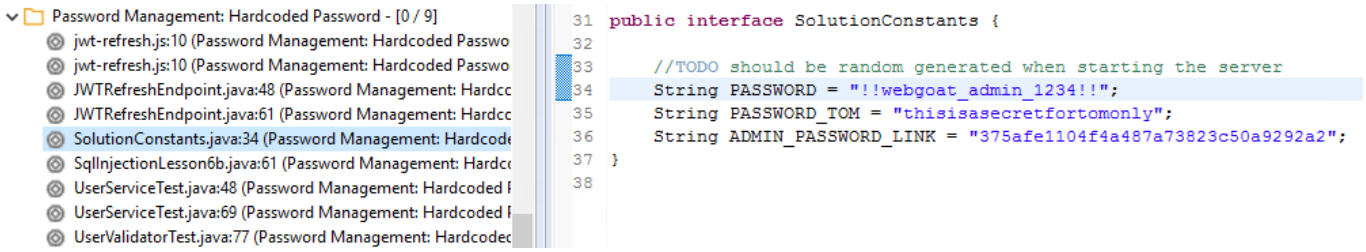
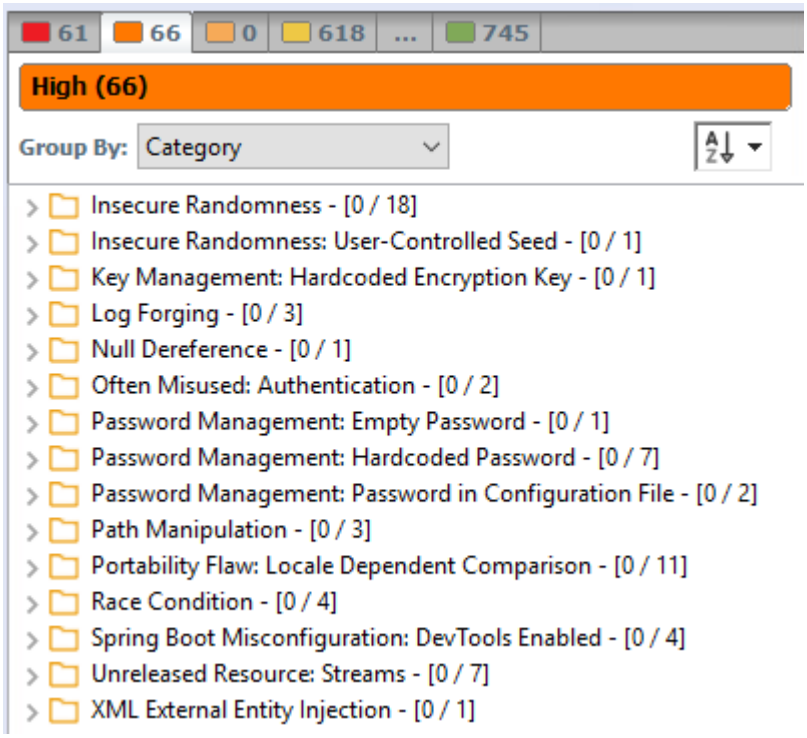



Рисунок 3.28. Приклад вразливості відкритого паролю

Виправленням вразливостей будуть займатися розробники та спеціальний аудитор, перевіряючий код на безпечність. Усього було виявлено 745 вразливостей різної важливості, список яких показано у відповідному вікні програми та на рисунку 3.29.




Рисунку 3.29. Список вразливостей

A Software Security Center розвертається як веб-додаток. У ньому аудитор проглядає так само інформацію по знайденим вразливостям, проте тут вже містяться рекомендації по усуненню (рис. 3.30), загальна статистика по сканованому проекту. Можна простерігати його еволюцію і деталі сканувань при кожній його перевірці.

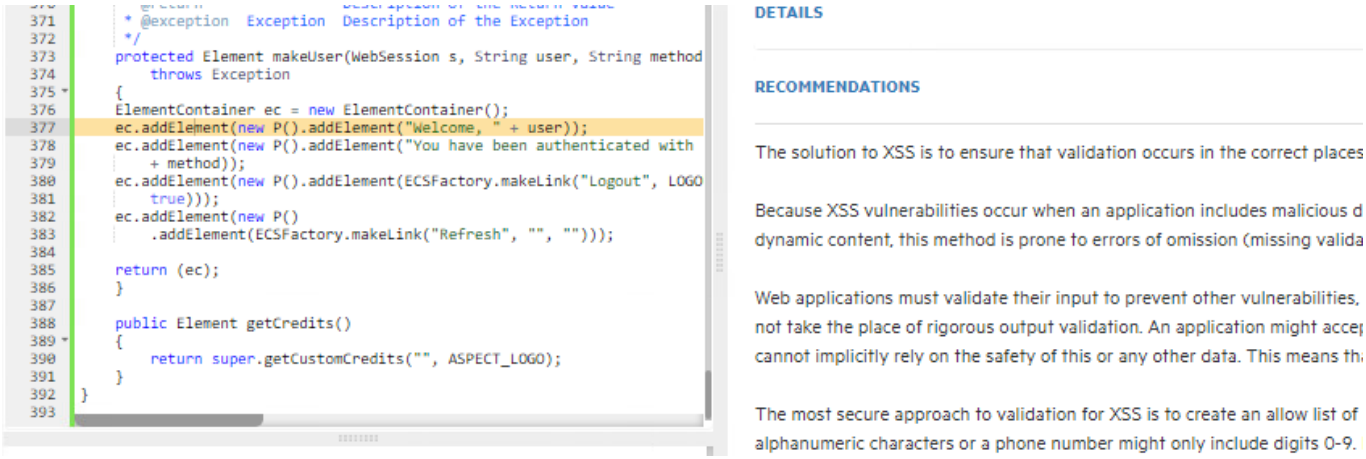



Рисунок 3.30. Приклад рекомендацій щодо усунення вразливостей

**Висновки за розділом 3**

Корпоративна мережа організації ABC містить вразливі активи, які необхідно захистити спеціалізованими програмно-технічними рішеннями. Було вирішено для безпеки персональних даних клієнтів, банківських карт та ресурсів мережі (інфраструктура з серверною, мережевою частиною, робочі місця та критична інформація) використати одні з найкращих засобів у своїх сферах: управління цифровими особистостями Sailpoint IdentityIQ, міжмережевий екран наступного покоління Sophos XG Firewall, тестування безпеки додатків Micro Focus Fortify.

Next-Generation брандмауер забезпечив безпечну комунікацію всередині корпоративної мережі, між офісами та з непідконтрольною глобальною мережею. Глибокий аналіз пакетів допоміг контролювати трафік краще, блокувати звернення на небажані сайти зсередини мережі, захищати електронну пошту (яка в свою чергу є головним способом передачі небезпечного ПЗ) та захист локального веб-серверу за допомого WAF модулю.

Система управління цифровими особистостями допомагає контролювати співробітників, їх облікові записи, права та можливості на інших цільових системах. Автоматизує процес надання привілеїв, допомагає на всіх етапах кадрового життя співробітника., контролює його доступи за політиками розділення обов’язків і zero-trust.

І для розробників корпоративних веб-додатків було інтегровано систему тестування безпеки веб-додатків. Яка допоможе детектувати вразливості ще до того, як кінцева версія додатку відобразиться у продуктивному середовищі.

Так було скомпоновано підсистему захисту корпоративної мережі, основуючись на критичні активи та вразливості безпеки компанії. Для наглядності була сформована схема мережі з включеним основним обладнанням.

# ВИСНОВКИ

У еру інформаційних технологій для бізнесу захист корпоративної мережі стоїть як критична задача. На плечах відділу інформаційної безпеки організації лежить вибір методів і засобів захисту. У цьому їм допомагають представники компаній-розробників програмно-технічних технологій інформаційної безпеки. Вони проводять презентації продуктів. І здатність обрати кращий і необхідний із багатьох пропозицій є необхідною для керівників відділу ІБ.

Еволюціонування засобів, способів і методів атаки на інформаційні системи зумовлює модернізацію технологій захисту від них. Щороку показники успішних атак зростають, компанії-гіганти теж потерпають, і кібербезпека підприємства стає все більш гострим питанням для керівництва.

У роботі описані кіберзагрози для корпоративної мережі у різних її місцях. Різні категорії загроз потребують свій спеціалізований захист. І для того, щоб розуміти, які засоби необхідні для безпеки підприємства, слід спочатку зрозуміти важливі активи, як і чому вони можуть бути скомпрометовані. Після цього вже можна обрати відповідний захист.

У роботі акцентувалась увага на персональних даних клієнтів, банківських картах та ресурсах мережі (інфраструктура з серверною, мережевою частиною, робочі місця та критична інформація). Відбувався захист інформаційної системи веб-сайтів підприємства, захист мережі від інсайдерів та захист інших активів за допомогою брандмауерів нового покоління.

Для досягнення поставленої мети у цій роботі були виконані наступні завдання:

- проаналізовано сучасний стан безпеки інформаційно-комунікаційної інфраструктури та нормативно-правової бази інформаційної безпеки;
- досліджено кібернетичні загрози для підприємства;
- проведено аналіз існуючих засобів захисту інформації для підприємницького сектору;

- розроблено демо-стенд корпоративної мережі з ключовими інформаційними системами;
- визначено потенційно критичні активи для організації;
- скомпоновано засоби захисту інформації в підсистему захисту корпоративної мережі;
- відображено результат на структурній схемі мережі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію [Електронний ресурс]: закон України від 16.07.2020 № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2657-12.

2. Про захист персональних даних [Електронний ресурс]: закон України від 23.04.2021 № 2297-VI. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2297-17.

3. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: закон України від 04.07.2020 № 80/94-ВР. – Режим доступу: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80.

4. Положення про технічний захист інформації в Україні [Електронний ресурс]: від 04.05.2008 № 1229/99. – Режим доступу: https://zakon.rada.gov.ua/laws/card/1229/99.

5. Концепція технічного захисту інформації в Україні [Електронний ресурс]: постанова КМУ від 13.10.2011 № 1126-97-п. – Режим доступу: https://zakon.rada.gov.ua/laws/card/1126-97-%D0%BF.

6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Чинний від 01.01.1998. – 11 с.

7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомуніка-ційних системах [Електронний ресурс]: від 10.02.2021 № 373-2006-п. – Режим доступу: https://zakon.rada.gov.ua/laws/card/373-2006-%D0%BF.

8. Sophos Partner Portal [Електронний ресурс]. – Режим доступу: https://partners.sophos.com/.

9. Trend Micro Partner Portal [Електронний ресурс]. – Режим доступу: https://community-trendmicro.force.com/Gpartner.

10. SailPoint Identity University [Електронний ресурс]. – Режим доступу: https://university.sailpoint.com.

11. Micro Focus Partner Portal [Електронний ресурс]. – Режим доступу: https://microfocuspartner.force.com.

12. Fintech News «The 2020 Cybersecurity stats you need to know» [Електронний ресурс]. – Режим доступу: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/.

13. Symantec, Internet security threat report, 2019 [Електронний ресурс]. – Режим доступу: https://docs.broadcom.com/doc/istr-24-2019-en.

14. Symantec, Internet security threat report, 2018 [Електронний ресурс]. – Режим доступу: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?/

15. CSO Online, Top cybersecurity facts, figures and statistics [Електронний ресурс]. – Режим доступу: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

16. Safe at Last, 22 Shocking Ransomware Statistics for Cybersecurity in 2021 [Електронний ресурс]. – Режим доступу: https://safeatlast.co/blog/ransomware-statistics/.

17. Cicso Annual Cybersecurity Report, 2018 [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?/.

18. Cisco Reports [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html.

19. Cisco Annual Internet Report (2018–2023) White Paper [Електронний ресурс].– Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

20. Verizoon, 2020 Data Breach Investigations Report [Електронний ресурс].– Режим доступу: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

21. Purplesec, 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends [Електронний ресурс]. – Режим доступу: https://purplesec.us/resources/cyber-security-statistics/.

22. Ponemon Institute’s Cost of Data Breach Study [Електронний ресурс]. – Режим доступу: https://www.ibm.com/security/data-breach.

23. AlterSign «Нормативна база у сфері ТЗІ» [Електронний ресурс]. – Режим доступу: http://altersign.com.ua/korysna-informacija/normatyvna-baza-u-sferi-tzi.

24. Nataliya Shevchenko, Timothy A. Chick, Paige O’Riordan, Thomas Patrick Scanlon, Carol Woody, Threat modeling: a summary of available methods [Електронний ресурс], 2018. – Режим доступу: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.

25. Gartner Peer Insights, Identity Governance and Administration Reviews and Ratings [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/identity-governance-administration.

# ДОДАТКИ

## Додаток А. Скрипт для SailPoint IdentityIQ

```
import os

filePath='test1.txt'
destPath='iiqCustom.properties.bk'
#filePath='iiqCustom.properties.bk'

def reading(filePath):
    with open(filePath,encoding='utf-8', mode='r') as reader:
        return list(reader)

def setMarks():
    l = reading(filePath)
    with open(destPath,encoding='utf-8', mode='w') as writer:
        n=0
        for item in l:
            n+=1
            point = item.find('=')
            if point!=-1:
                writer.write(item[:point+1]+'{0}__'.format(n)+item[point+1:])
            else:
                writer.write(item)

def deleteMarks():
    l = reading(filePath)
    with open(destPath, encoding='utf-8', mode='w') as writer:
```

```
        n=0
        for item in l:
            n+=1
            point = item.find('=')
            noPoint = item.find('__')
            if point!=-1:
                writer.write(item[:point+1]+item[noPoint+2:])
            else:
                writer.write(item)


def unicoding():
    l = reading(destPath)
    with open(destPath, encoding='utf-8', mode='w') as writer:
        for item in l:
            writer.write(''.join(c if 0 < ord(c) <= 127 else '\\u{:04x}'.format(ord(c)) for c in
item))

#deleteMarks()
setMarks()
unicoding()
```