Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

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: «Програмний засіб моніторингу подій в корпоративній мережі організації»

Виконавець: студент ІІІ (за скороченим терміном навчання) курсу, групи КБ-43мс

_____ **Іван БЕРЕГОВИЙ**
(підпис) (ім'я прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Іван ПАРХОМЕНКО	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-43мс** **Береговому Івану Геннадійовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Програмний засіб моніторингу подій в корпоративній мережі організації

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структури, представлення, види, топології, етапи проектування корпоративних мереж, методи та механізми моніторингу, алгоритми шифрування та хешування.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Структура корпоративної мережі та багатошарове представлення, її види та етапи створення, топології корпоративних мереж, вразливості корпоративних мереж, основні атаки на мережі, засоби та механізми захисту від загроз атаки «людина посередині», «відмови в обслуговуванні», інсайдерських атак, моніторинг подій.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Поєднання та програмна реалізація засобів і механізмів

захисту веб-додатків, включаючи моніторинг подій корпоративних мереж.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Іван БЕРЕГОВИЙ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 28.01.2022	*виконано*
2	Аналіз літератури	31.01.2022 – 01.03.2022	*виконано*
3	Дослідження структури та функціоналу корпоративних мереж	02.03.2022 – 31.03.2022	*виконано*
4	Дослідження основних вразливостей	01.04.2022 – 30.04.2022	*виконано*
5	Дослідження основних атак на корпоративну мережу	01.05.2022 – 15.05.2022	*виконано*
6	Огляд засобів та механізмів захисту корпоративної мережі	16.05.2022 – 22.05.2022	*виконано*
7	Вибір середовища створення програмного засобу	23.05.2022 – 25.05.2022	*виконано*
8	Проектування бази даних	26.05.2022 – 29.05.2022	*виконано*
9	Конструювання програмного засобу моніторингу подій корпоративної мережі організації	30.05.2022 – 01.06.2022	*виконано*
10	Оформлення пояснювальної записки	02.06.2022 – 06.06.2022	*виконано*
11	Підготовка до захисту	07.06.2022 – 14.06.2022	*виконано*

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Іван БЕРЕГОВИЙ (ім'я, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел. Основний текст займає 67 сторінки, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 24 рисунки.

Метою роботи є створення програмного засобу моніторингу подій в корпоративних мережах організації.

Для досягнення зазначеної мети поставлено наступні *завдання*:

– провести аналіз структури та функціональних можливостей корпоративних мереж;

– дослідити вразливості та загрози корпоративних мереж;

– проаналізувати існуючі системи моніторингу, їх можливості, переваги та недоліки;

– побудувати програмний засіб моніторингу подій в корпоративних мережах.

Об'єктом дослідження є процес виявлення загроз в корпоративних мережах.

Предметом дослідження є засоби та механізми моніторингу подій для виявлення загроз в корпоративній мережі.

Методом дослідження є аналіз літератури, дослідження впливу вразливостей на мережі та створення програмного засобу моніторингу подій.

Практичною цінністю отриманих результатів є поєднання та програмна реалізація засобів і механізмів захисту веб-додатків, включаючи моніторинг подій корпоративних мереж.

Ключові слова: корпоративна мережа, програмний засіб моніторингу, база даних, вразливості, кібератаки, захист інформації, кібербезпека, веб-застосунок.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

КМ	–	Комп’ютерна мережа
СУБД	–	Система управління базами даних
CAN	–	Campus Area Network
PSTN	–	Public Switched Telephone Network
ІС	–	Інформаційна система
ПЗ	–	Програмне забезпечення
ЛОМ	–	Локальна обчислювальна мережа
IPX	–	Internetwork Packet Exchange
SNA	–	Systems Network Architecture
BYOD	–	Bring Your Own Device
IoT	–	Internet of Things
MitM	–	Man-in-the-Middle
(D)DoS	–	(Distributed) Denial of Service
VPN	–	Virtual Private Network
SIEM	–	Security Information and Event Management
IDPS	–	Intrusion Detection and Prevention System
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
CSIRT	–	Computer Security Incident Response Team
DLP	–	Data Loss Prevention
UEBA	–	User and Entity Behavior Analytics
VA	–	Vulnerability Assessment
WAF	–	Web Application Firewall
ЦОД	–	Центр обробки даних
AFK	–	Away From Keyboard

ЗМІСТ

ВСТУП

При збільшені кількості компаній, які мають превеликий успіх на ринку та розширюються, зростає й важливість проблеми інформаційної безпеки корпоративних мереж підприємств. З кожним днем, у злочинців з'являється все більше інструментарію та можливостей задля нанесення удару на ласий шматок компанії, а також з'являється все більше методів атак на мережі. В зв'язку з цим, виникають вимоги стосовно забезпечення кібербезпеки підприємства, уникнення існуючих та запобігання нових загроз. Для вирішення таких потреб створюються спеціальні програмні забезпечення, системи моніторингу подій, розподілу ролей, розпізнавання втручання, покращуються функціональні можливості мережевих екранів, маршрутизаторів, комутаторів тощо.

Також, виникає проблема у спеціалізації програмного забезпечення під окрему організацію, так як кожна має свою структуру та інформаційну діяльність.

Таким чином, створення універсальних засобів забезпечення інформаційної безпеки в корпоративних мережах, а саме систем моніторингу подій, втручання, витоків даних тощо, які будуть доцільні для кожної організації, для більшості їх структур є актуальною задачею.

Метою роботи є створення програмного засобу моніторингу подій в корпоративних мережах організації.

Для досягнення зазначеної мети поставлено наступні *завдання*:

– провести огляд структури та функціональних можливостей корпоративних мереж;

– дослідити вразливості та загрози корпоративних мереж;

– проаналізувати існуючі системи моніторингу, їх можливості, переваги та недоліки;

– побудувати програмний засіб моніторингу подій в корпоративних мережах.

Об'єктом дослідження є процес виявлення загроз в корпоративних мережах.

Предметом дослідження є засоби та механізми моніторингу подій для виявлення загроз в корпоративній мережі.

Методом дослідження є аналіз літератури, дослідження впливу вразливостей на мережі та створення програмного засобу моніторингу подій.

Практичною цінністю отриманих результатів є поєднання та програмна реалізація засобів і механізмів захисту веб-додатків, включаючи моніторинг подій корпоративних мереж.

РОЗДІЛ 1
КОМПОНЕНТИ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1 Поняття та багатошарове представлення корпоративної мережі

На сьогодні, розробка комп'ютерної мережі відіграє важливу роль в діяльності майже кожного підприємства. За допомогою неї, здійснюється зв'язок між працівниками всередині офісу (підприємства, будівлі) та в рамках міжрайонного, міжміського або навіть міжнародного сполучення. Без безперервного відстеження інформаційних потоків й оперативної координації діяльності всіх підрозділів і співробітників неможливо ефективно керувати підприємством.

Корпоративна мережа (КМ) – це мережа, яка існує для підтримки роботи певного підприємства, яке володіє нею. Користувачами корпоративної мережі є лише співробітники окремо визначеної організації, наприклад, корпорації (головний офіс та віддалені філії), фінансові організації, банки, інформаційні підприємства та друкарські ЗМІ тощо. Дані мережі не надають послуг стороннім підприємствам чи користувачам, як, наприклад, оператори зв'язку. Залежно від розмірів підприємства, складності і різновидності вирішуваних завдань розрізняють мережі відділу, мережі кампусів і корпоративні мережі [1].

Корпоративна мережа працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також сервісні комплекси, що забезпечують доставку даних користувачам в ній [1].

Як правило, вона територіально розподілена, тобто об'єднує офіси, підрозділи і інші структури, що знаходяться на значній відстані один від одного. Принципи, побудови та проектування корпоративної мережі, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі [1]. Загальну схему корпоративної мережі зображено на рисунку 1.1.

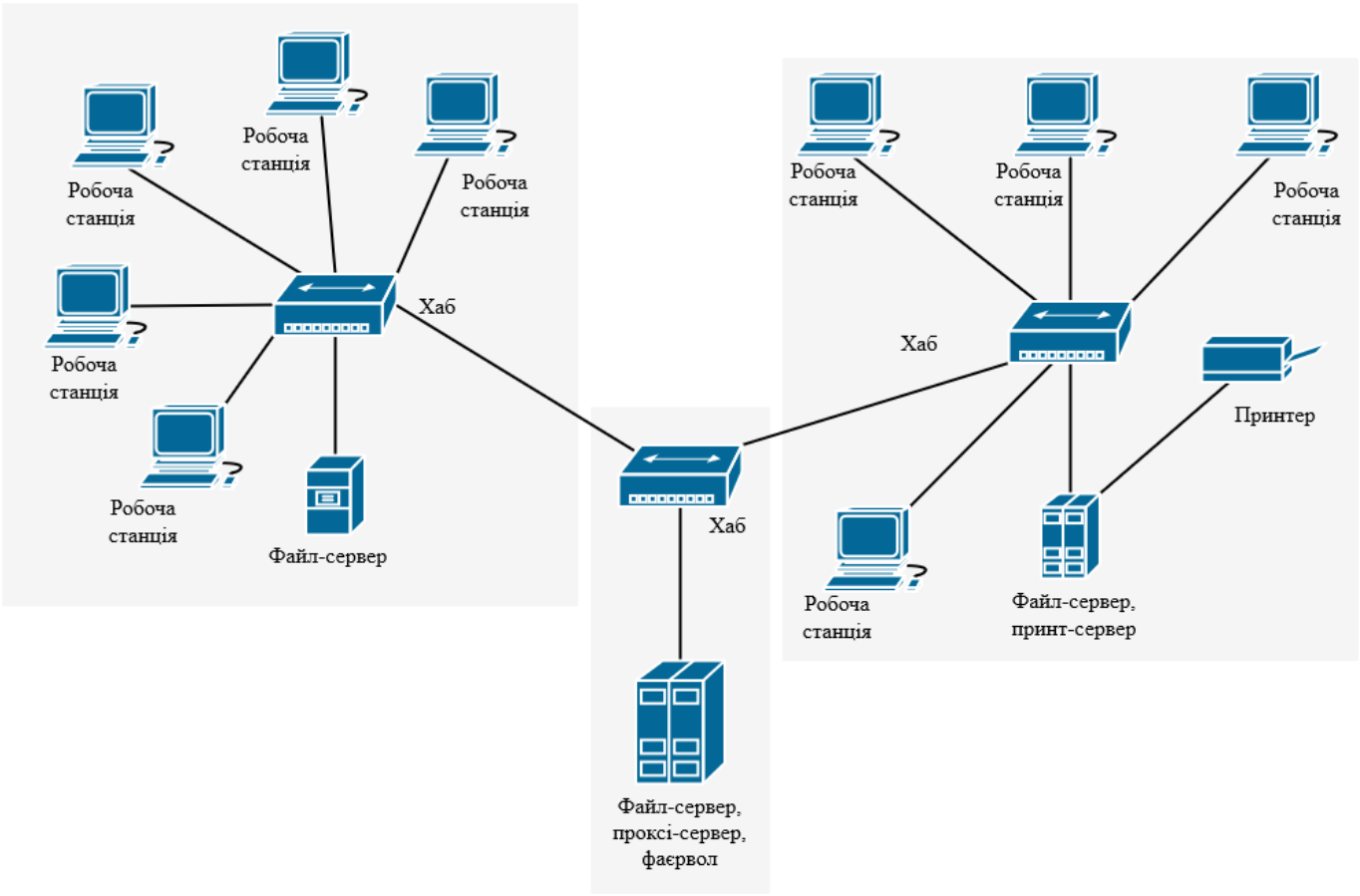

Рисунок 1.1 – Загальна схема корпоративної мережі

Сучасні мережі класифікуються за наступними ознаками: по віддаленості комп'ютерів, топології, призначенню, переліку послуг, принципами управління, методами комутації та доступу, видами середовища та швидкостями передачі даних.

В корпоративній мережі існують наступні можливості [2]:

– централізований доступ до мережі інтернет;

– відеоконференційний зв'язок в межах компанії;

– корпоративна електронна та голосова пошта, факси для підвищення ефективності та продуктивності роботи співробітників;

– єдиний електронний документообіг компанії;

– корпоративна IP-телефонія;

– загальні архіви документів;

– єдині корпоративні довідники та сервіси;

– автоматичний збір даних систем відеонагляду;

– комплексна автоматизація робочих місць;

– дистанційний режим доступу до файлів, серверів з базами даних, пристроїв друку;

– безпека передачі даних та захисту корпоративної інформації від несанкціонованого доступу.

Перевагами корпоративної мережі можна назвати наступні аспекти [2]:

– можливість централізованого дистанційного навчання;

– скорочення витрат на експлуатацію мереж та підвищення інвестицій в мережеву інфраструктуру;

– прозорість роботи компанії, контроль над мережевими ресурсами;

– повний контроль за діяльністю всіх служб та структурних підрозділів;

– автономність мережі та високий рівень безпеки;

– безперервне оновлення інформації між співробітниками підприємства дозволить приймати їм своєчасні та правильні рішення;

– гнучкість корпоративної мережі на внутрішні та зовнішні зміни в середині компанії;

– доступ до всіх інформаційних ресурсів підприємства в реальному часі, незалежно від місця знаходження співробітників: в офісі, в іншому місті, дома або в дорозі.

Корпоративну мережу також розглядають як складну систему, що містить у собі декілька взаємодіючих рівнів [3]. Для показу архітектури багатошарового представлення доволі часто використовують схему у вигляді піраміди, яка зображена на рисунку 1.2.

На першому рівні знаходяться комп’ютери, що є центрами зберігання та обробки інформації.

Далі, транспортна система, що забезпечує надійну передачу інформаційних пакетів між комп’ютерами.

Над транспортною системою працюють мережеві операційні системи, які організовують роботу додатків у комп’ютерах та надають через транспортну систему ресурси свого комп’ютера у спільне користування.

Рисунок 1.2 – Ієрархія шарів корпоративної мережі

Згодом, йде рівень систем управління базами даних (СУБД). Вони зберігають у впорядкованому вигляді основну корпоративну інформацію та виконують над нею базові операції пошуку.

Потім, йдуть системні сервіси, які, користуються СУБД, для пошуку потрібної інформації і надають кінцевим користувачам цю інформацію у зручній формі, а також виконують процедури обробки інформації. Такими сервісами можуть бути: служба WorldWideWeb, система електронної пошти, системи колективної роботи тощо.

На верхньому рівні корпоративної мережі знаходяться спеціальні програмні системи, що виконують завдання, спеціалізовані для даного підприємства чи підприємств даного типу. Прикладами є системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проектування, управління технологічними процесами тощо.

Кінцева мета корпоративної мережі втілена в прикладних програмах верхнього рівня, але для їхньої роботи необхідно, щоб підсистеми інших рівнів чітко виконували свої функції.

1.2 Види корпоративних мереж

Мережа кампусів (CAN — Campus Area Network) – це група деяких локальних мереж, розміщених на відносно невеликій території (кампусі) будь-якої організації, наприклад, підприємство, офіси, порт, університет, оптові склади, державні установи тощо. В такому випадку все мережеве обладнання і середовище передачі даних є власністю орендаря чи власника кампусу. Якщо коротко, то це велика багатосегментна локальна мережа, розміщена на території до декількох кілометрів в діаметрі і яка об’єднує між собою локальні мережі будівель, які близько розташовані між собою.

Діапазон дії становить від 1 км до 5 км. Якщо дві будівлі знаходяться в одному домені, і пов’язані спільною мережею, то це буде розглядатися лише як CAN. Причому канал передачі даних буде мати високу швидкість.

Така мережа включає взаємодію між мережами відділів, доступ до загальних баз даних підприємства, факс-серверів, високошвидкісних модемів і принтерів. У результаті, робітники кожного відділу підприємства мають доступ до деяких файлів і ресурсів мереж інших відділів. Важливим аспектом кампусної мережі є те, що у працівників є доступ до корпоративних баз даних незалежно від типів комп’ютерів, на яких вони розташовуються.

Із проблем можна визначити проблеми інтеграції неоднорідного апаратного і програмного забезпечення. Типи мережевих операційних систем, комп’ютерів, мережевого апаратного забезпечення можуть відрізнятися в кожному відділі. З цього виникають складнощі управління мережами кампусів. І, оскільки мережі відділів, які в кампусі, незалежні і побудовані на базі різних технологій, то об’єднуючою технологією зазвичай є IP.

Правильна кампусна мережа організації має ієрархічну структуру, яка складається з трьох рівнів:

– магістральний рівень (Core);

– рівень розподілу (Distribution);

– рівень доступу (Access).

Структура мережі кампусу зображена на рисунку 1.3.

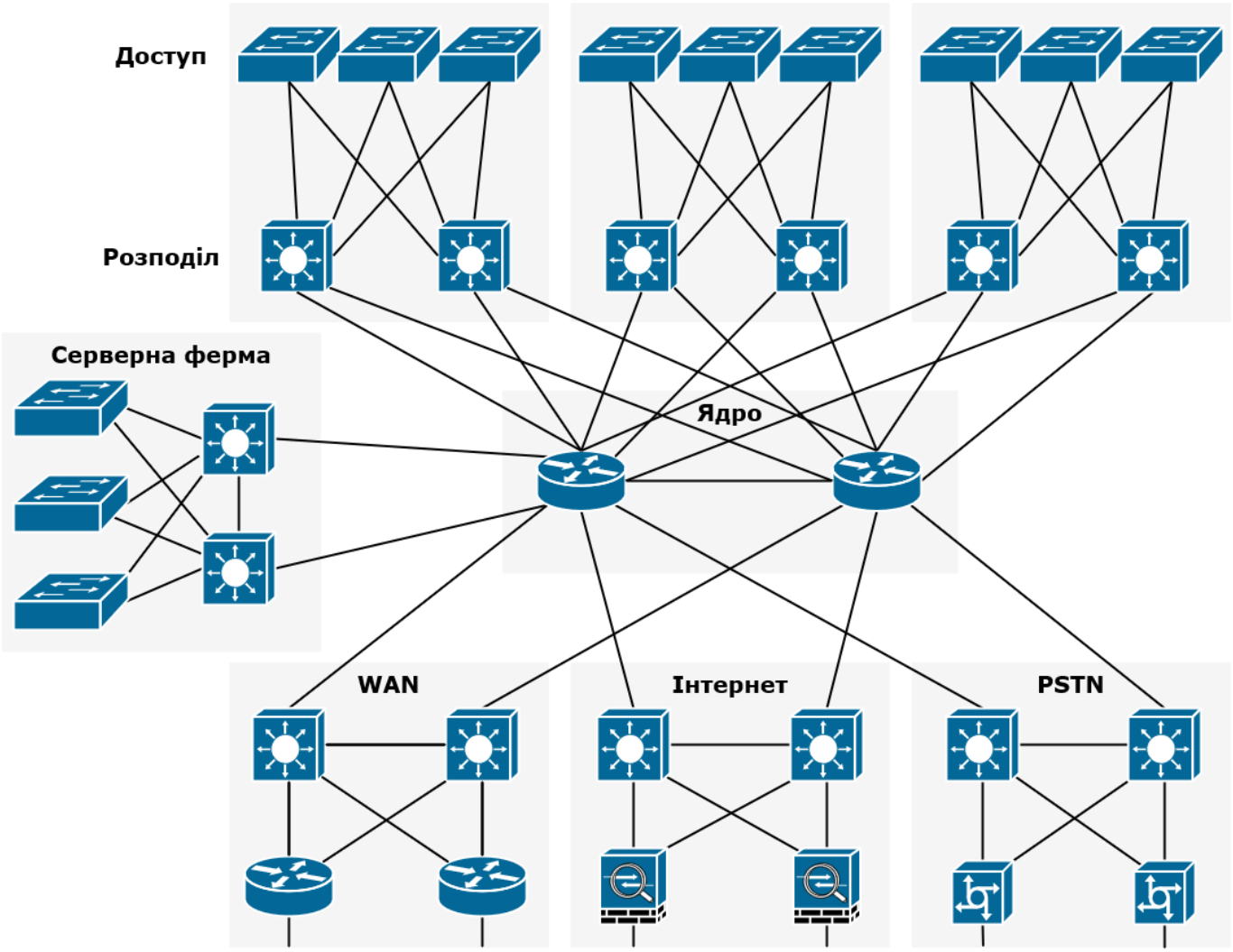

Рисунок 1.3 – Приклад структури мережі кампусів

Даний варіант опису мережі надає можливість обирати обладнання, що задовольняє функціональним потребам конкретної мережевої структури.

Магістральний рівень або ядро – це головний елемент мережі всього підприємства, що відповідає за основні магістральні канали зв’язку.

Характеристика ядра:

– висока надійність;

– адаптація до змін в мережевому середовищі;

– незначна затримка при передачі даних;

– передбачувана продуктивність;

– зручне керування.

На рівні розподілу виконується доступ до послуг та в різні частини мережі.

До нього відносяться наступні механізми:

– політика безпеки;

– політика доступу до інформаційних ресурсів;

– управління якістю послуг;

– середовища передачі даних;

– маршрутизація між логічними сегментами мережі;

– визначення мультимедійних доменів тощо.

Рівень доступу забезпечує доступність до корпоративних ресурсів для робочих груп і мережевих сегментів. У таких мережах рівень доступу визначається комутованим або розподіленим для користувачів відповідно до середовища передачі даних.

Мережі відділів – це мережі, які використовуються співробітниками, що працюють в одному відділі підприємства (приблизно 50-150 осіб), наприклад, кілька кімнат, залів або цілий поверх будівлі.

Її призначення полягає в розподілі локальних програм, даних, модемів тощо. Як правило, вони не поділяються на окремі підмережі, оскільки їх масштаби незначні. Такі мережі складаються з одного чи двох файлових серверів і приблизно тридцяти користувачів. Приблизна схема мережі відділу представлена на рисунку 1.4.

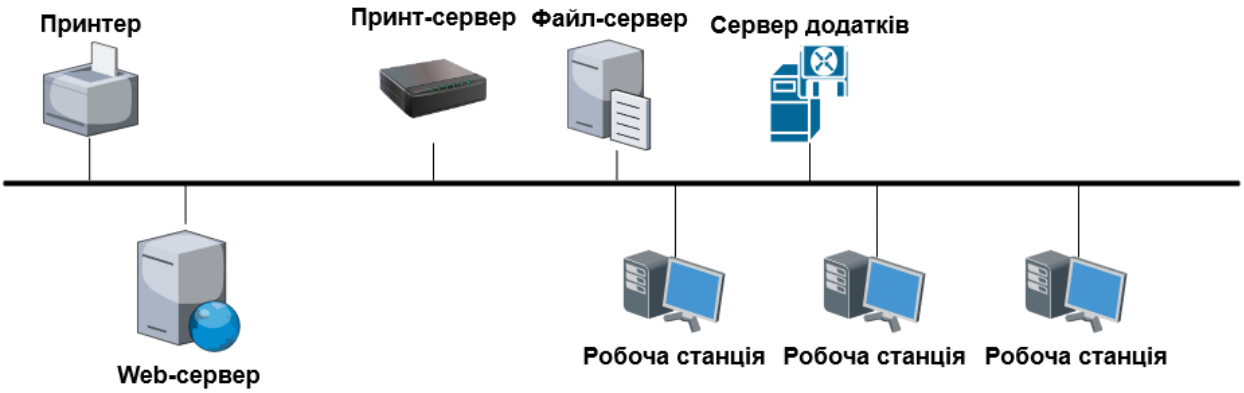

Рисунок 1.4 – Приклад структури мережі відділів

До задач мережевого адміністрування відноситься:

– встановлення нових вузлів;

– додавання нових користувачів;

– нових версій програмного забезпечення;

– усунення простих неполадок чи відмов.

Мережі робочих груп – це невеликі мережі, що включають в себе до 10-20 комп'ютерів. Принципи побудови і роботи мереж робочих груп практично не відрізняються від мереж відділів.

У даних мережах доволі часто використовуються технології локальних мереж на розподілених середовищах.

1.3 Етапи створення корпоративних мереж

Для створення корпоративної мережі підприємства виділяють три основні етапи:

1. інформаційна діагностика підприємства;

2. вибір архітектури системи та програмно-апаратних засобів для її реалізації, виходячи з результатів попереднього етапу;

3. після обстежень, обрати головні компоненти та розробити їх.

Кожному підприємству необхідна інформаційна система для підтримки її діяльності. Тому, потрібно проаналізувати цілі і задачі організації, щоб зрозуміти, де потрібна автоматизація.

До цілей інформаційного обстеження належить:

– визначення кількості робочих місць в кожному структурному підрозділі компанії, визначення функціонального складу технологій, опис функцій, які будуть виконуватися на кожному робочому місці;

– алгоритми проходження вхідних, внутрішніх і вихідних документів, опис головних шляхів і технології для їх обробки;

– опис і формулювання функцій всіх підрозділів компанії, а також задачі, які ними вирішуються;

– опис технології роботи кожної секції і їх потоків інформації.

У результаті з’являється модель діяльності компанії та її інформаційна інфраструктура. На її основі буде розроблятись проект корпоративної інформаційної системи (ІС), специфікації на розробку прикладного програмного забезпечення (ПЗ) та вимоги до апаратно-програмних засобів.

Далі, потрібно визначити, якою буде архітектура системи. Для корпоративних систем рекомендується клієнт-серверна архітектура.

Даний варіант є домінуючою концепцією у створенні розподілених мережних застосунків і передбачає взаємодію та обмін даними між ними. Така архітектура передбачає наступні основні компоненти:

– сервери, які надають інформацію або інші послуги програмам, які звертаються до них;

– клієнти, які використовують сервіси, що надаються серверами;

– мережа, яка забезпечує взаємодію між клієнтами та серверами.

Одним з основних завдань в розробці ІС є вибір системи управління базами даних (СУБД). Лише після обстеження і отримання інформаційних моделей діяльності можна визначити, яку краще використовувати на підприємстві.

Управління інформаційними ресурсами має для діяльності будь-якої установи особливе значення. Незалежно від правового статусу або організаційних форм

діяльності, установи покликані активно взаємодіяти з органами виконавчої та законодавчої влади, а також структурами, які беруть участь у регулюванні економіки. Все це в свою чергу породжує специфічний документообіг.

Система електронного документообігу (СЕД) – це система автоматизації роботи з документами протягом всього їх життєвого циклу, а також процесів взаємодії між співробітниками. Причому, документи є неструктуровані, наприклад файли Word, Excel тощо. Як правило, СЕД включає в себе електронний архів документів і систему автоматизації ділових процесів.

Ефективне управління документацією на основі СЕД засноване на трьох складових системи:

– технологія (на основі сучасних комп'ютерних комплексів);

– корпоративні правила створення і використання інформаційних ресурсів (і їх закріплення в розпорядчих документах);

– психологія користувачів та їх навчання (при необхідності індивідуальне).

1.4 Узагальнена структура корпоративної мережі

Узагальнену структуру корпоративної мережі, представлено на рисунку 1.5. Будь-яка корпоративна мережа містить в собі фрагменти узагальненої структури. Також, в межах даної мережі має бути реалізована система управління (СУ), яка вказана на рисунку 1.6.

Основу системи управління корпоративної мережі створюють наступні методи:

– адаптивне керування безпекою в межах системи безпеки;

– система автоматичного керування в межах керуючої системи. В системі повинна виконуватись автоматична обробка особливо важливих впливів для збільшення швидкості реакції системи керування на важливі події;

– розподілене чи централізоване адміністрування;

– експертна система для підвищення ефективності і надійності системи керування;

– поєднання адміністрування окремих функціональних підсистем (тобто, при зміні рівня безпеки змінюється і ефективність).

Спрощення структури мережі, полягає в зменшені складності віддалених фрагментів, з перенесенням відповідних функцій до елементів основного фрагмента [4]. Такими елементами є:

– інформаційні сервери;

– під’єднання до сервісів, які знаходяться в загальному доступі;

– адміністрування усіма підсистемами функціонального підсистемами, де використовується обмежена кількість додаткових засобів реалізації таких підсистем.

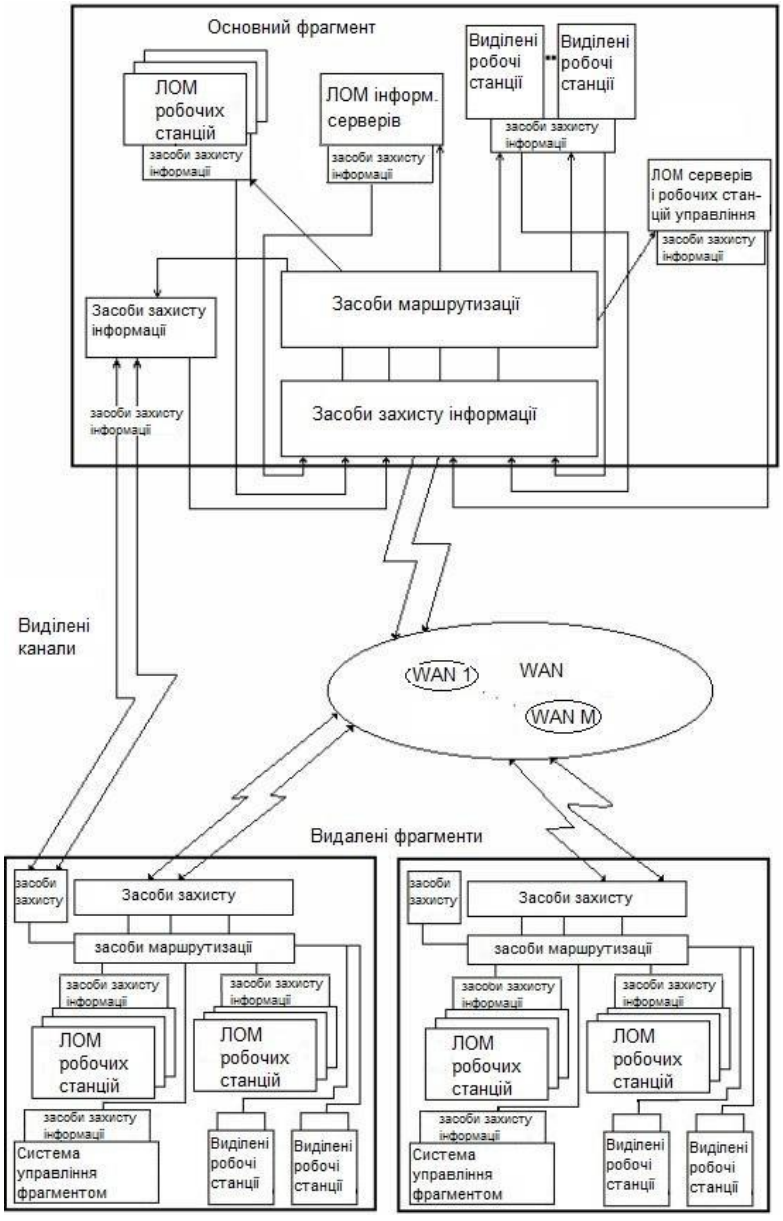

Рисунок 1.5 – Узагальнена структура корпоративної мережі

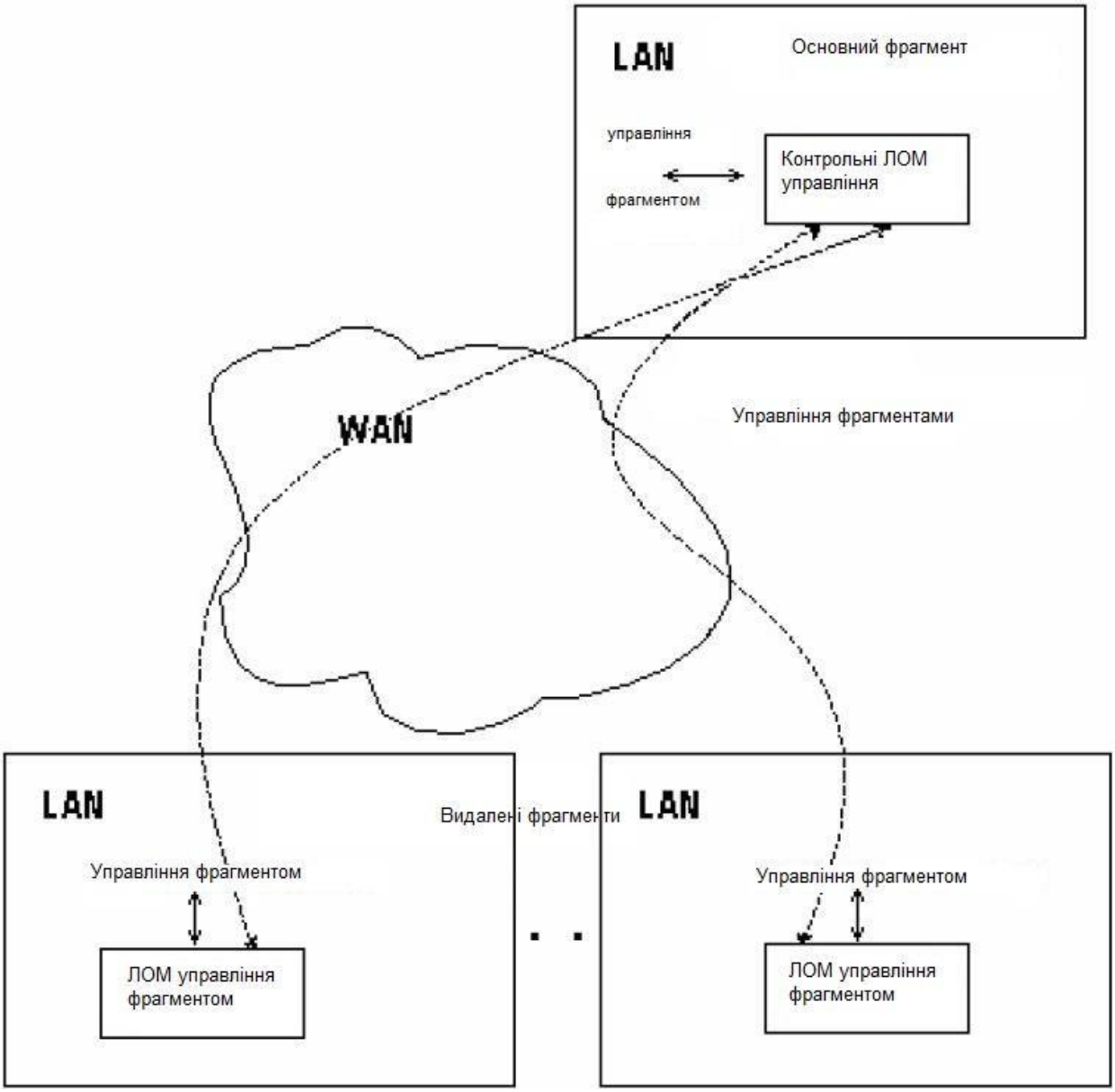

Рисунок 1.6 – Система управління корпоративною мережею

1.5 Обладнання корпоративних мереж

Корпоративна мережа – це досить складна структура, що використовує різні типи зв’язку, комунікаційні протоколи та способи підключення ресурсів.

Відносно зручності побудови та керованості мережі слід орієнтуватися на однотипне обладнання одного виробника. Робоча мережа завжди є результатом компромісу, тобто або це однорідна система, неоптимальна з точки зору ціни та можливостей, або складна у встановленні та налагоджувані комбінацій продуктів різних виробників.

Все обладнання мереж передачі даних поділяється на два великі класи:

– периферійне, яке використовується для підключення до мережі кінцевих вузлів;

– магістральне або опорне, що реалізує основні функції мережі (комутацію каналів, маршрутизацію тощо).

Особливість полягає в тому, що пристрої різних класів можуть використовуватися в різній якості або поєднувати ті й інші функції. Варто зауважити, що до магістрального обладнання зазвичай застосовуються підвищені вимоги щодо надійності, продуктивності, кількості портів і подальшої розширюваності.

Периферійне обладнання є необхідним компонентом будь-якої корпоративної мережі. Якщо їх брати для функцій магістральних вузлів, то вони будуть відповідати за глобальну мережу передачі, до якої підключаються ресурси.

Магістральні вузли у складі корпоративної мережі використовуються лише у випадках орендованих каналів зв'язку або створюються власні вузли доступу.

З точки зору виконуваних функцій, периферійне обладнання поділяється на два класи:

– маршрутизатори (routers);

– шлюзи (gateways).

Маршрутизатори, служать для об'єднання однорідних LAN, зазвичай, IP чи IPX (Internetwork Packet Exchange), через глобальні мережі. У мережах, що використовують IP або IPX як основний протокол, маршрутизатори використовуються як магістральне обладнання, що забезпечує поєднання різних каналів і протоколів зв'язку. Вони можуть слугувати як автономні пристрої, так і програмні засоби.

Шлюзи реалізують взаємодію додатків, що працюють у різних типах мереж. Повнофункціональний шлюз є програмно-апаратним комплексом, оскільки повинен забезпечувати програмні інтерфейси для додатків. У корпоративних мережах використовуються в основному шлюзи OSI, що забезпечують взаємодію локальних

мереж з ресурсами X.25 та шлюзи SNA, що забезпечують підключення до мереж IBM [3].

1.6 Топології корпоративних мереж

Для корпоративних мереж використовується два види топології:

– «Зірка»;

– «Змішана».

Топологія «Зірка» використовується для забезпечення керованості і надійності роботи мережі. Причому, необхідно враховувати те, що кожен промінь «зірки» повинен теж бути зіркою. Дана топологія дозволяє керувати сервером рівнем вище, відносно інших, що знаходяться нижче по ієрархії, що, в цілому, підвищує надійність і керованість мережі. Така методологія гарантує наявність «третьої сторони» при передачі повідомлень між користувачами, які мають сервери, що обслуговуються по-різному.

Наприклад, повідомлення від клієнта «Організації 3» надсилається користувачу «Організації 2» і проходить через сервер «Організації 1».

З одного боку, побудова мережі з великою кількістю вузлів збільшує експлуатаційні витрати і ускладнює обслуговування, але з іншого боку, зменшує навантаження на сервери мережі та спрощує роботу адміністратора.

Якщо говорити про «Змішану» топологію, то сервери, які розташовані на одному рівні, можуть передавати повідомлення безпосередньо один одному. Це зменшує навантаження на канали передачі даних, при цьому контроль мережі різко падає. До недоліків можна віднести відсутність «третьої сторони», яка працює контролером при виникненні спірних ситуацій між різними «Організаціями» та підрозділами «Організації» [1].

Висновки за розділом 1

У першому розділі проаналізовано структуру та компоненти корпоративної мережі, її види, етапи створення, топології та представлення.

Коли у компанії з’являється можливість розширення потужностей та бізнес-процесів, то виникає проблема збереження функціональної складової існуючої локальної мережі.

Для вирішення таких проблем створюється корпоративна мережа, яка дозволяє працювати співробітникам організації в минулій мережі, причому бути в різних офісах, будівлях тощо.

Корпоративну мережу доволі часто зображають у вигляді багатошарового представлення. Дане представлення екранізується пірамідою, рідше трапецією, в якій вказуються початкові та кінцеві рівні, але без існування хоча б одного, виключає існування такої мережі. Воно, по черзі, складається з: комп’ютерів, транспортної мережі, мережевої операційної системи, системи управління базами даних, системних сервісів та спеціалізованих, під сферу застосування підприємства, додатків.

До видів корпоративних мереж відносяться: мережі кампусів, відділів та робочих груп. Кожна з них, відрізняється своїм обсягом, безпекою, методами створення та процесами.

Для створення корпоративної мережі необхідно пройти через три етапи проектування, а саме: діагностика оперування інформації всередині підприємства, вибір архітектури та апаратно-програмних засобів для її реалізації і, згодом, обрати головні аспекти та компоненти після дослідження. Без послідовного виконання цих етапів неможливо створити оптимізовану та доцільну мережу.

Так як корпоративна мережа використовує різні типи зв’язку, комунікаційні протоколи та способи підключення ресурсів, то для створення їх взаємодії необхідне обладнання. Обладнання може бути як периферійним, так і магістральним, причому воно є взаємозамінним. Основними типами є маршрутизатори та шлюзи. В той час,

як роутери реалізують з’єднання локальних мереж компанії через глобальну, шлюзи – створюють взаємодію між додатками.

Щодо топології мережі, основними будуть «Зірка» та «Змішана». Причому, якщо використовується «Зірка», то варто зазначити, що на промені однієї повинна бути ще одна.

РОЗДІЛ 2
ВРАЗЛИВОСТІ ТА ЗАГРОЗИ В КОРПОРАТИВНИХ МЕРЕЖАХ

2.1 Вразливості корпоративних мереж

Відповідно до набору стандартів ISO/IEC 27005 [5], вразливості можна класифікувати в залежності від типу активів, до яких вони належать. Таким чином, ваше підприємство може мати справу з наступними вразливостями:

- програмного забезпечення;
- апаратного забезпечення;
- персоналу;
- організаційними;
- мережевими.

Мережева вразливість – це слабке місце у системі або її конструкції, яке використовується зловмисником для порушення безпеки компанії та організації кібератаки. Залежно від положення слабкого місця, мережеві вразливості поділяють на дві категорії: внутрішні і зовнішні [6].

Внутрішня мережева вразливість зазвичай спричинена неправильною конфігурацією, помилками, погано написаним кодом або навіть працівниками. Зовнішні вразливості мережі представлені пристроями або платформами, які компанія використовує щодня [6].

Виділяють наступні загрози корпоративної мережі:

- вразливі мобільні пристрої;
- відкриті/доступні пристрої інтернету речей;
- флеш-носії;
- неправильно налаштовані брандмауери;
- однофакторна автентифікація;
- прості або словникові паролі;
- погано налаштований Wi-Fi;

– не захищені послуги (сервіси) електронної пошти;

– застаріле програмне забезпечення;

– інсайдерська загроза.

Мобільні пристрої присутні в кіберсередовищі будь-якої компанії, чи то локальна, чи віддалена. Співробітники або приносять їх із собою в офіс, або використовують для роботи в рамках політики компанії BYOD (Bring Your Own Device – Принеси Власний Пристрій). На жаль, існує безліч способів, за допомогою яких смартфони та планшети можуть стати вразливими місцями у мережі [6].

Поширена проблема з мобільними пристроями пов’язана з їх викраденням. Коли співробітник підключає свій телефон або планшет до корпоративної мережі та використовує їх для доступу до конфіденційних даних – це відкриває світ можливостей для кібератак. Таким чином, крадіжка таких пристроїв – це можливість, якою скористаються деякі зловмисники. Деякі можуть навіть вдатися до більш витонченої стратегії, яка базується на використанні схожих програм, які обманом змушують користувача розкрити конфіденційну інформацію [6].

Інтернет речей складається з взаємозалежних обчислювальних пристроїв, що мають здатність передавати дані в мережі, але що знаходяться поза спектром того, що ми зазвичай вважаємо частиною системи. Місцевий офіс не є винятком, оскільки багато компаній мають такі пристрої IoT як розумні термостати, камери спостереження або навіть холодильники [6].

Ситуація стає складнішою, коли підприємство працює віддалено. У співробітників в будинку може бути безліч IoT-пристроїв, причому вони можуть бути як маленькими, наприклад, смарт-годинники, так і великими, як електропіч. Тому їх часто ігнорують як потенційні мережеві вразливості, але насправді безпека IoT дуже важлива для цифрової безпеки підприємства [6].

Хоча USB-накопичувачі можуть здатися цілком доброякісними, вони можуть містити шкідливі файли, які автоматично встановлюються, як тільки пристрій підключається до комп’ютера або ноутбука. Багато масштабних кібератак, наприклад, кібератака 2008 року на Міністерство оборони США, були спровоковані саме такою практикою [6].

На щастя, в сучасному офісі, підключеному до хмари, такі пристрої вже практично не використовуються. Тому, якщо помічено на робочому місці флеш-пам’ять USB, підключену до будь-якого пристрою, можна вважати, що його слід негайно видалити. Однак, перш ніж це зробити, краще порадитися з колегами [6].

Після маршрутизатора брандмауер є наступною лінією захисту даних від зловмисників, які намагаються використовувати вразливість мережі. Потужна система безпеки, що блокує несанкціонований доступ до комп’ютера або мережі, використовується багатьма організаціями та приватними особами, як частина загальної стратегії безпеки для захисту своїх даних та пристроїв від атак через Інтернет [6].

Саме тому неправильно налаштований брандмауер може стати фатальним для цифрової цілісності організації. Подібна ситуація зазвичай викликана помилкою мережевого адміністратора, однак, корінь проблеми також може полягати в неправильному виправленні або керуванні брандмауером [6].

Однофакторна автентифікація (ОФА) – це метод аутентифікації, який спирається лише на один фактор для перевірки особи користувача. Цей метод зазвичай використовується для автентифікації в онлайн-банкінгу, соціальних мережах та інших сервісах. Найбільш поширеною формою ОФА є ім’я користувача та пароль [6].

Однак ризики, пов’язані з однофакторною автентифікацією, полягають у тому, що її може обійти зловмисник, який скомпрометував пароль або дізнався його іншим способом. Двофакторна аутентифікація, з іншого боку, вимагає двох елементів для автентифікації користувача і тому забезпечує більшу безпеку, аніж однофакторна [6].

Багато співробітників створюють слабкі паролі, тому що не помічають або не усвідомлюють ризик безпеки, пов’язаний з цим. На жаль, це може стати великою проблемою, оскільки хакери можуть легко зламати робочі облікові записи та вкрасти приватну інформацію, надавши їм доступ до мережі компанії. Надійний та складний пароль – це перша лінія оборони підприємства від кібератаки [6].

Сучасний офіс та віддалені працівники значною мірою покладаються на використання інтернет-підключень Wi-Fi, оскільки вони дозволяють пристроям виходити до мережі без жодних дротів. Однак, погано налаштований маршрутизатор або навіть той, який не був оновлений із заводських налаштувань за замовчуванням, може дуже швидко стати вразливим місцем у мережі, дозволяючи зловмисникам проникнути у вашу корпоративну систему [6].

Безпечне Wi-Fi з'єднання досягається шляхом застосування шифрування WPA2, зміни паролю та імені мережі за замовчуванням, використанням надійного пароля та заборони доступу невідомих пристроїв до мережі [6].

Служби електронної пошти часто використовуються підприємствами для надсилання та отримання даних. Звичайно, іноді це стосується конфіденційних повідомлень, що містять фінансові дані, які стають легкою здобиччю на цих платформах завдяки таким методам, як соціальна інженерія, розсилання спаму та фішинг [6].

Хакери часто використовують сервіси електронної пошти для створення шлюзу в мережу компанії, що робить її вразливою для атак. Крім пошуку конфіденційних даних та перехоплення повідомлень, вони також створюють продумані кампанії, які переконують співробітників повідомити свої дані для входу в систему або стати неусвідомленими розповсюджувачами шкідливого програмного забезпечення в системі [6].

Раніше, компанії-розробники програмного забезпечення часто випускали нову версію свого програмного забезпечення кожні кілька років. Це робилося для того, щоб представити нові функції та покращити роботу користувачів. Проте, останніми роками вони випускають нові версії частіше, задля усунення помилок та вразливостей у системі безпеки, які виявляються після виходу [6].

Таким чином, ігнорування критичних оновлень може стати загрозою для безпеки підприємства. Проблема неоновленого програмного забезпечення полягає в створенні для системи вразливості до кібератак. Хакери, знаючи про них, використовують їх для крадіжки даних або зараження системи, тому необхідно стежити за тим, щоб усі програми були оновлені [6].

Іноді, інцидент кібербезпеки не з’являється із-за недоліків в архітектурі, погано написаним рядком коду, неправильно налаштованим програмним забезпеченням або навіть неоновленими програмами. В таких випадках, справжніми винуватцями інцидентів стають люди у вашій організації [6].

Інсайдерська загроза, безумовно, є найнебезпечнішою мережевою вразливістю через людський фактор, що лежить в її основі. Співробітники самі можуть стати загрозою для цифрового благополуччя вашого підприємства випадково чи навмисно [6].

2.2 Класифікація атак на мережу

До основних та розповсюджених атак на мережу, незважаючи на її різновид, відносяться:

- атака за допомогою шкідливого програмного забезпечення;
- фішинг;
- людина посередині;
- відмова в обслуговуванні (DoS – Denial of Service);
- SQL-ін’єкції;
- атака нульового дня;
- перебір паролей (Brute-force);
- міжсайтовий скриптинг;
- руткіти;
- атаки на Інтернет речей;
- атаки спрямовані на 5G.

Шкідливе програмне забезпечення використовує вразливість для проникнення в мережу, коли користувач натискає на «підкинуте» небезпечне посилання або вкладення електронної пошти, яке використовується для його встановлення всередині системи [7].

Всередині комп’ютерної системи воно може:

- заборонити доступ до критичних компонентів мережі;

– отримувати інформацію шляхом вилучення даних із жорсткого диска;

– порушити роботу системи чи навіть вивести її з ладу.

Найбільш поширеними типами є:

– віруси;

– трояни;

– хробаки;

– вимагачі;

– програми-шпигуни.

Фішингові атаки надзвичайно поширені і полягають у масовому розсиланні шахрайських електронних листів нічого не підозрюючим користувачам, замаскованих під листи з надійних джерел. Часто мають вигляд законних, але направляють одержувача на шкідливий файл або сценарій, призначений для надання зловмисникам доступу до пристрою для керування ним, збору розвідданих, встановлення шкідливих сценаріїв/файлів або вилучення даних, таких як інформація про користувача, фінансова інформація тощо [7].

Фішингові атаки можуть також здійснюватися через соціальні мережі та інші онлайн-спільноти за допомогою прямих повідомлень від інших користувачів із прихованими намірами. Злодії часто використовують соціальну інженерію та інші відкриті джерела інформації для збору відомостей про вашу роботу, інтереси та діяльність, що дає зловмисникам перевагу в переконанні вас у тому, що вони не ті, за кого себе видають [7].

Існує кілька різних типів фішингових атак:

– Spear Phishing – цільові атаки, спрямовані на конкретні компанії та/або окремих осіб.

– Whaling – атаки, спрямовані на вище керівництво та зацікавлених осіб в організації.

– Фармінг – використання отруєння кешу DNS для отримання облікових даних користувача через підроблену цільову сторінку входу до системи.

– Голосовий фішинг.

– SMS-фішинг.

Атака «Людина посередині», яка зображена на рисунку 2.1, відбувається, коли зловмисник перехоплює двосторонню транзакцію, вставляючи себе у середину. Після цього зловмисники можуть викрадати дані та маніпулювати ними, перериваючи трафік [7].

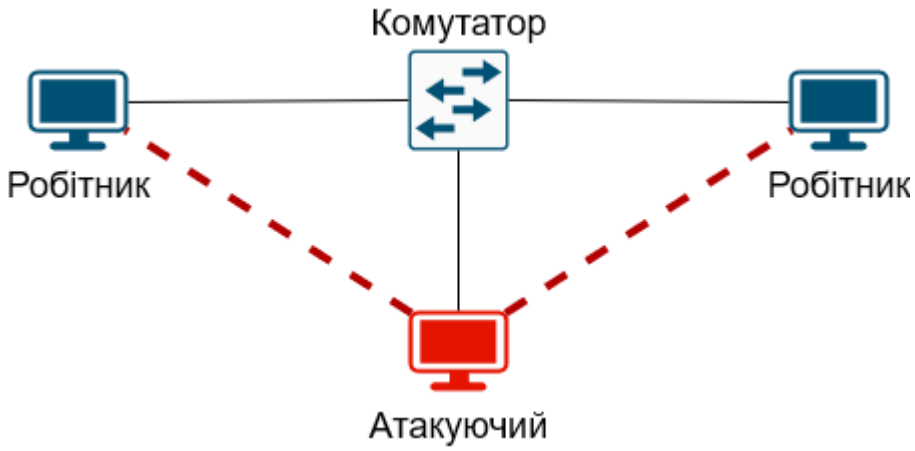

Рисунок 2.1 – Принцип атаки типу «Людина посередині»

Цей тип зазвичай використовує вразливість безпеки в мережі, наприклад незахищений громадський Wi-Fi, щоб вставити себе між пристроєм відвідувача і мережею. Проблема полягає в тому, що їх дуже важко виявити, оскільки жертва вважає, що інформація відправляється в законне місце. Для проведення такого нападу, часто використовуються атаки фішинга або шкідливого програмного забезпечення [7].

DoS-атаки працюють шляхом насичення систем, серверів та/або мереж трафіком, щоб перевантажити ресурси та пропускну спроможність. В результаті, система стає нездатною обробляти та виконувати законні запити. Окрім атак типу «відмова в обслуговуванні», існують також розподілені атаки – DDoS (Distributed Denial of Service) [7].

DDoS-атака запускається з декількох заражених хост-машин з метою домогтися відмови в обслуговуванні та вивести систему з мережі, тим самим підготувавши ґрунт для проникнення іншої атаки в мережу чи середовище [7].

SQL-ін’єкція відбувається, коли зловмисник вставляє шкідливий код сервера, використовуючи мову запитів до сервера (SQL), змушуючи його передати захищену інформацію. Цей тип атак зазвичай пов’язаний з введенням шкідливого коду в коментар або пошуковий рядок незахищеного веб-сайту. Ефективним способом запобігання SQL-ін’єкцій є безпечне кодування, наприклад, використання підготовлених операторів із параметризованими запитами [7].

Коли команда SQL використовує параметр замість безпосередньої вставки значень, це може дозволити бек-енду виконувати шкідливі запити. Більш того, інтерпретатор SQL використовує параметр лише як дані, не виконуючи його як код [7].

Атака нульового дня полягає у використанні мережевої вразливості, коли вона є новою та нещодавно створеною, тобто до випуску та/або впровадження оновлення. Атакуючі кидаються на розкриту вразливість у той невеликий проміжок часу, коли немає жодних рішень або запобіжних заходів. Таким чином, запобігання атакам нульового дня потребує постійного моніторингу, проактивного виявлення та гнучких методів управління загрозами [7].

Паролі є найбільш поширеним методом автентифікації доступу до захищеної інформаційної системи, що робить їх привабливою метою для кіберзлочинців.

Зловмисники використовують величезну кількість методів для визначення індивідуального пароля, включаючи соціальну інженерію, отримання доступу до бази даних паролів, перевірку з’єднання для отримання незашифрованих паролів або просте вгадування.

Останній із згаданих методів виконується систематично та відомий як «атака перебором». При даній атаці програма перебирає всі можливі варіанти та комбінації інформації, щоб вгадати пароль [7].

Іншим поширеним методом є атака за словником, коли зловмисник використовує список спільних паролів, щоб спробувати отримати доступ до комп’ютера та мережі користувача [7].

Для запобігання атаки з використанням пароля дуже корисні методи блокування облікового запису та двофакторна автентифікація. Функції блокування

облікового запису можуть блокувати обліковий запис після кількох спроб введення неправильного пароля, а двофакторна автентифікація додає додатковий рівень безпеки, вимагаючи від користувача, що входить до системи, ввести вторинний код, доступний лише на пристрої (пристроях) двофакторної автентифікації.

Атака міжсайтового скриптингу направляє шкідливі скрипти на вміст надійних веб-сайтів. Шкідливий код приєднується до динамічного контенту, який надсилається до браузера жертви. Зазвичай, цей шкідливий код складається з коду Javascript, що виконується браузером жертви.

Руткіти встановлюються всередині легального програмного забезпечення, де вони можуть отримати віддалений контроль та доступ до системи на рівні адміністратора. Потім, зловмисник використовує його для крадіжки паролів, ключів, облікових даних та отримання критично важливих даних [7].

Оскільки руткіти ховаються в легітимному програмному забезпеченні, як тільки програмі дозволяється внести зміни до вашої операційної системи (ОС), він встановлюється в систему і залишається в сплячому стані, доки зловмисник не активує його або він не запуститься через механізм збереження. Руткіти зазвичай розповсюджуються через вкладення електронної пошти та завантаження з небезпечних веб-сайтів [7].

2.3 Методи уникнення загроз

Для запобігання та уникнення загроз, з кожним днем створюються нові методики, від організаційних до технічних. Розглянемо основні з них.

Налаштування брандмауера. Брандмауери є передовою лінією оборони. В зв’язку зі збільшенням методів захисту зв’язку та шифрування даних, виникають складнощі в аналізі трафіку. Причому, злочинці, маючи аналогічні технології, можуть використовувати шкідливе програмне забезпечення, наприклад віруси, задля підміни даних, які практично не відрізнятимуться від оригіналу [10].

Брандмауер може допомогти запобігти несанкціонованому доступу до мережі, блокуючи вхідний трафік з ненадійних джерел. Крім того, брандмауери можуть бути

налаштовані на дозвіл лише певних типів трафіку, наприклад, веб-трафіку або електронної пошти [11].

Віртуальні приватні мережі (VPN). Ситуації, коли співробітникам потрібно отримати доступ до ресурсів компанії з громадських місць (Wi-Fi в аеропорту чи готелі) або з дому, особливо небезпечні для інформації компанії. Вони повинні бути захищені зашифрованим тунелем VPN.

До недоліків VPN можна віднести відносну складність розгортання, додаткову вартість ключів автентифікації та збільшену пропускну здатність Інтернет-тунелю. Ключі аутентифікації також можуть бути скомпрометовані. Викрадені корпоративні або службові мобільні пристрої (ноутбуки, планшети, смартфони) із попередньо налаштованими параметрами VPN-з'єднання можуть бути потенційною вразливістю для несанкціонованого доступу до корпоративних ресурсів [10].

Антивіруси. Вони є основним захистом більшості сучасних компаній.

Антивірусний захист спрямований на клієнтські пристрої та робочі станції. Комерційні версії включають можливості централізованого керування для доставки оновлень антивірусних баз на клієнтські пристрої, а також можливість централізовано налаштовувати політики безпеки. В асортименті антивірусних компаній є спеціалізовані серверні рішення [10].

Антивірусне програмне забезпечення може виявити та запобігти установці шкідливих файлів у систему, і його слід регулярно оновлювати, щоб включити останні сигнатури [11].

Білі списки. Перший метод передбачає, що операційна система за замовчуванням дозволяє запускати будь-яку програму, яка раніше не була в чорному списку. З іншого боку, другий метод передбачає, що тільки ті програми, які раніше були в білому списку, дозволено запускати, тоді як усі інші блокуються за замовчуванням [10].

Білі списки можна створювати за допомогою вбудованих інструментів операційної системи та стороннього програмного забезпечення. Антивірусне програмне забезпечення зазвичай передбачає цю функціональність у своєму складі. Однак, білий список безсилий проти атак, які використовують вразливості в

програмах, що в ньому знаходяться. Також, варто звернути увагу на найслабшу ланку будь-якого захисту: працівники можуть ігнорувати попередження антивірусів і додавати шкідливі програми в білий список [10].

Фільтрація спаму. При фішинг-атаках доволі часто використовуються спам-розсилки. Відфільтрувати спам-розсилку можна наступними способами: власно створене програмне забезпечення, послуги від зовнішніх постачальників або hardware-рішення в дата-центрі [10].

Підтримка та оновлення програмного забезпечення. Злодії завжди намагаються використати будь-яку помилку чи брак безпеки у мережах компаній. Саме тому розробники програмного забезпечення часто випускають нові оновлення для своїх програм у спробі усунути вразливості [12].

На жаль, більшість компаній не застосовують ці безкоштовні виправлення безпеки. Вони продовжують використовувати застарілі та неоновлені версії, оскільки їм простіше використовувати програму при необхідності, ніж на деякий час відключати її та оновлювати. Бувають також випадки, коли організації не знають, що можуть застосувати оновлення для усунення вразливостей. Це відбувається тому, що власники не мають точної інвентаризації програмного забезпечення, яке вони використовують у своїй бізнес-мережі [12].

У таких випадках слід розглянути можливість проведення аудиту та оцінки політики безпеки для створення картки мережі, інвентаризації всіх програмних додатків у ній та визначення того, чи оновлено ці програми оновленнями безпеки. Це дозволить активно вирішувати проблеми безпеки мережі, а також уникати будь-які вразливості до того, як вони будуть використані [12].

Фізична безпека корпоративної мережі є одним із найважливіших факторів. У більшості випадків, маючи фізичний доступ до мережевого пристрою, зловмисники можуть легко отримати доступ до вашої мережі. Іншою проблемою є вкрадений або занедбаний жорсткий диск після його заміни на сервері чи іншому пристрої. Оскільки знайдені там паролі можна розшифрувати. Серверні шафи та кімнати чи бокси з обладнанням завжди повинні бути захищені від злому [10].

Складні, захищені паролі. Пароль повинен складатися як мінімум з восьми символів і включати поєднання літер, цифр і символів. Їх також не повинно легко вгадати, наприклад, ім’я користувача або назва компанії [11].

Дотримання політики безпеки підприємства. Політики безпеки можуть допомогти захистити всі пристрої в мережі від вірусів та шкідливих програм, а також використання користувачами надійних паролів. Ці політики також можуть обмежувати доступ до деяких регіонів мережі та привілеїв користувачів [11].

Обмеження привілеїв. Багато засновників бізнесу не враховують внутрішні загрози, що є найбільшою помилкою.

Очевидно, що значна частина всіх загроз кібербезпеці походить від співробітників. Головний актив може швидко стати однією з найбільших проблем мережевої безпеки, незалежно від того, чи зловживають вони своїми привілеями доступу навмисно або наражають бізнес на ризик випадково [12].

Використання принципу найменших привілеїв для доступу користувачів обмежує доступ кожного лише тією інформацією, яка необхідна йому для виконання своєї роботи. Тобто, кожен співробітник організації не повинен мати необмежений доступ до конфіденційних активів. Таким чином, навіть якщо доступ буде зловживаний, то збиток буде мінімальним [12].

Резервні системи. У модулях безперервності бізнесу та аварійного відновлення є поняття «єдина точка відмови».

«Єдина точка відмови» – це термін, який описує, як відмова активу вплине на мережу, тобто, чи зможе мережа продовжувати працювати. Активом може бути будь-що у мережі, включаючи базу даних, точку доступу, сервер, пристрій маршрутизації трафіку тощо. Якщо будь-який актив може поставити мережу під загрозу у разі відмови, цей актив є єдиною точкою відмови [12].

Вирішенням проблеми одиничних точок відмови є надмірність, тобто наявність кількох додаткових активів, які виконують однакову роботу. Тому, якщо перший актив вийде з ладу, мережа зможе працювати як й раніше [12].

Наявність резервування дозволить захистити мережу від усіх видів проблем, особливо атак, спрямованих на ці точки в мережі [12].

Аналіз вразливих точок мережі. Під час проведення оцінки мережевої безпеки необхідно враховувати, наскільки важливим є кожен фактор ризику для вашого бізнесу [12].

Аналіз має враховувати наступне [12]:

– потенційні втрати під час збору рахунків.

– загальна вартість відновлення даних.

– втрата всіх записів про ділові операції штрафи за пропуск строків оплати кредиторської заборгованості.

– зниження продуктивності при спробі повернути бізнес у нормальне русло.

Вивчення всіх аспектів загроз безпеки допоможе створити структуровану відповідь. Це допоможе розставити пріоритети в порядку від найбільш значущих до найменш значимих і, згодом, працювати над їх усуненням.

Сегментація мережі – це чудовий спосіб контролювати проблеми мережевої безпеки та обмежувати їх вплив. Така стратегія поділяє велику комп'ютерну мережу на дрібніші підмережі. Потім, кожна з цих підмереж ізолюється одна від одної за допомогою внутрішніх брандмауерів та інших заходів безпеки [12].

Коли обмежується кожна пошукова мережа, зловмисникам – навіть тим, хто вже перебуває в організації – стає складніше проникнути з однієї системи до іншої [12].

Замість того, щоб обходити один набір захисних систем по периметру, кіберзлодіям доведеться прокладати шлях через захист кожної окремої підмережі. Це не лише уповільнить їхнє просування, але й полегшить команді IT-безпеки виявити та нейтралізувати злам до того, як буде завдано істотних збитків [12].

Тестування співробітників. Робітники повинні знати про ризики кібератак, що зростають. Для їх усвідомлення, наскільки вони впливають на безпеку організації, необхідно забезпечити належне навчання і заохочувати їх до участі в програмах підвищення обізнаності [12].

Належне навчання кожного співробітника допоможе знизити рівень загроз і клопоту вашого бізнесу, що, у свою чергу, дозволить запобігти атак [12].

Спостереження за активністю в мережі. Журнали відстеження та інші дані дозволяють швидко виявляти підозрілу активність, що дає можливість співробітникам служби безпеки вжити заходів щодо розслідування та пом’якшення потенційних загроз [11].

2.4 Програмні рішення

SIEM (Security Information and Event Management) – це рішення для забезпечення безпеки, яке допомагає організаціям розпізнавати потенційні загрози безпеці та вразливості до того, як вони встигнуть порушити роботу бізнесу. Воно виявляє аномалії у поведінці користувачів та використовує штучний інтелект для автоматизації багатьох ручних процесів, пов’язаних з виявленням загроз та реагуванням на інциденти, і стало основним елементом сучасних операційних центрів безпеки для управління безпекою та дотриманням нормативних вимог [15].

Більшість SIEM-систем мають наступні функції [15]:

– керування логами системи. SIEM збирає дані про події широкого спектру джерел по всій мережі організації. Журнали та дані потоків від користувачів, програм, активів, хмарних середовищ та мереж збираються, зберігаються та аналізуються в режимі реального часу, надаючи IT-відділам та службам безпеки можливість автоматично керувати журналами подій та даними мережевих потоків в одному централізованому місці;

– кореляція подій та аналітика. Використовуючи передову аналітику для виявлення та розуміння складних моделей даних, кореляція подій дозволяє швидко виявити та усунути потенційні загрози безпеці бізнесу. Рішення SIEM значно покращують середній час виявлення та середній час реагування для команд IT-безпеки, розвантажуючи ручні робочі процеси, пов’язані з поглибленим аналізом подій безпеки;

– моніторинг інцидентів та сповіщення безпеки. Рішення SIEM здатні ідентифікувати всі об’єкти IT-середовища, оскільки вони дозволяють централізовано керувати локальною та хмарною інфраструктурою. Це дозволяє

відслідковувати інциденти безпеки серед усіх підключених користувачів, пристроїв та програм, класифікуючи аномальну поведінку в міру її виявлення в мережі. Використовуючи налаштовані, заздалегідь визначені правила кореляції, адміністратори можуть негайно отримати попередження та вжити відповідних дій для пом’якшення наслідків, перш ніж вони матеріалізуються у більш серйозні проблеми безпеки.

IDPS (Intrusion Detecting and Preventing System) – це технологія, яка стежить за мережею щодо будь-яких шкідливих дій, які намагаються використовувати відому вразливість. Основна функція системи запобігання вторгненням полягає у виявленні будь-якої підозрілої активності і, або виявленні та дозволі (IDS), або запобіганні (IPS) загрози. Спроба реєструється та повідомляється мережним менеджерам або співробітникам Центру управління безпекою [17].

Технології IDPS можуть виявляти та запобігати атакам мережевої безпеки, такі як атаки грубої сили (Brute-force), атаки типу «відмова в обслуговуванні» (DoS) та використання вразливостей. Коли оголошується про експлойт, у зловмисників часто з’являється можливість використовувати вразливість до того, як буде застосовано оновлення безпеки. У таких випадках можна використовувати систему запобігання вторгненням, щоб швидко блокувати ці атаки [17].

Якщо говорити про окремі компоненти даної технології, а саме IDS (Intrusion Detecting System) IPS (Intrusion Preventing System), то перша з них відповідає за аналіз та відстеження мережевого трафіку у пошуках ознак, що вказують на те, що зловмисники використовують відому кіберзагрозу для проникнення або крадіжки даних із вашої мережі (системи IDS порівнюють поточну мережну активність із відомою базою даних загроз, щоб виявити кілька типів поведінки, таких як порушення політики безпеки, шкідливе програмне забезпечення та сканери портів), друга – проактивно забороняє мережевий трафік на основі профілю безпеки, якщо пакет представляє певну загрозу безпеці [21]. Оскільки технології IPS відстежують потоки пакетів, їх можна використовувати для примусового використання безпечних протоколів і заборони використання небезпечних протоколів, таких як ранні версії SSL або протоколи, що використовують слабкі шифри [17].

Обидва IDS/IPS зчитують мережні пакети та порівнюють їх вміст із базою даних відомих загроз. Основна різниця між ними у тому, що IDS – це інструменти виявлення та моніторингу, які самі по собі не роблять жодних дій, а IPS – це система управління, яка приймає або відхиляє пакет на основі набору правил [21].

IDS вимагає участі людини або іншої системи для перегляду результатів та визначення подальших дій, що може зайняти цілий робочий день залежно від обсягу мережного трафіку, що генерується щодня. IDS – це найкращий інструмент посмертної експертизи для CSIRT (Computer Security Incident Response Team – Команда комп'ютерної безпеки з реагування на інциденти), який можна використовувати у рамках розслідування інцидентів безпеки [21].

Мета IPS, з іншого боку, полягає в тому, щоб перехоплювати небезпечні пакети та відкидати їх до того, як вони досягнуть мети. Вона пасивніша, ніж IDS, і просто вимагає, щоб база даних регулярно оновлювалася новими даними про загрози [21].

DLP (Data Loss Prevention) – це набір інструментів і процесів, які використовуються для того, щоб конфіденційні дані не були втрачені, неправильно використані або доступні неавторизованим користувачам. Воно класифікує регульовані, конфіденційні та важливі для бізнесу дані та виявляє порушення політик, визначених організаціями або в рамках визначеного пакета політик, які зазвичай обумовлені відповідністю нормативним вимогам. Після виявлення таких порушень DLP забезпечує їх усунення за допомогою попереджень, шифрування та інших захисних дій, щоб кінцеві користувачі не могли випадково або зловмисно поділитися даними, які можуть зазнати організації ризику [22].

Програмне забезпечення та інструменти запобігання втраті даних відстежують та контролюють дії кінцевих точок, фільтрують потоки даних у корпоративних мережах та контролюють дані у хмарі для захисту даних у стані спокою, у русі та в процесі використання. DLP також надає звітність, щоб відповідати і вимогам відповідності аудиту, і виявленню слабких місць, і аномалій для криміналістики, і реагувань на інциденти [22].

Технології DLP загалом поділяються на дві категорії – Enterprise DLP та Integrated DLP.

Корпоративні DLP-рішення є комплексними та упаковані в програмне забезпечення агентів для комп'ютерів та серверів, фізичних та віртуальних пристроїв моніторингу мереж та поштового трафіку або програмних пристроїв для виявлення даних [23].

Інтегровані DLP обмежуються захищеними веб-шлюзами (SWG), захищеними шлюзами електронної пошти (SEG), продуктами шифрування електронної пошти, платформами управління корпоративним контентом (ECM), засобами класифікації даних, засобами виявлення даних та брокерами безпеки хмарного доступу (CASB) [23].

Організації зазвичай використовують DLP для [24]:

– захисту персонально ідентифікованої інформації (PII) та дотримання відповідних нормативних вимог;

– захисту інтелектуальної власності, критично важливої для організації;

– досягнення видимості даних у великих організаціях;

– захисту мобільних співробітників та забезпечення безпеки у середовищах Bring Your Own Device (BYOD);

– захисту даних у віддалених хмарних системах (див. рисунок 2.2).

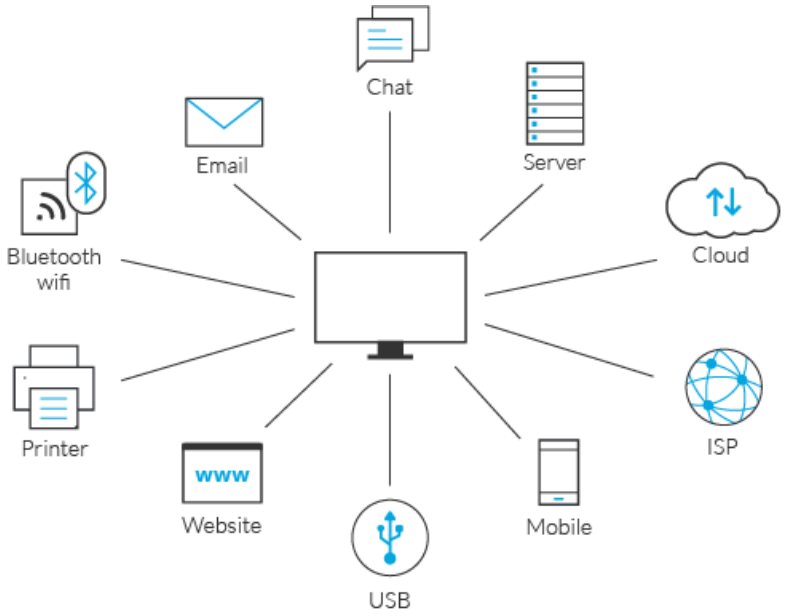

Рисунок 2.2 – Джерела, за якими спостерігає DLP-система

UEBA (User and Entity Behavior Analytics) – це рішення для кібербезпеки, яке використовує машинне навчання, алгоритми та статистичний аналіз для виявлення аномалій у поведінці не тільки користувачів корпоративної мережі, але й маршрутизаторів, серверів та кінцевих точок у цій мережі [25].

Дана технологія прагне розпізнати будь-яку незвичайну чи підозрілу поведінку – випадки, коли спостерігаються відхилення від звичайних повсякденних моделей або використання [25].

UEBA також може агрегувати дані, що містяться у звітах і журналах, а також аналізувати інформацію про файли, потоки та пакети [26].

В ній не відстежуються події безпеки або моніторингу пристроїв, свою роботу вона спрямовує на всіх користувачів та суб’єктів у вашій системі. Таким чином, ця технологія фокусується на внутрішніх загрозах, серверах, додатках та пристроях, які працюють у вашій системі. Наприклад, скомпрометовані співробітники, співробітники-вигнанці, і люди, які вже мають доступ до вашої системи, а потім здійснюють цільові атаки та спроби шахрайства [26].

Щоб рішення UEBA було ефективним, воно має бути встановлене на кожному пристрої, яке використовується кожним співробітником організації або

підключеним до нього. Сюди входять пристрої, що належать не лише компанії, а й співробітникам, оскільки навіть пристрої, що використовуються неповний робочий день, можуть стати ціллю кібератаки [25].

Після встановлення або підключення UEBA переходить у режим «мовчання» і починає збирати дані про використання пристроїв та мережі. У режимі «навчання» алгоритми цього рішення визначають, що вважається нормальним чи, навіть, оптимальним. IT-адміністратори можуть вирішити, як довго триватиме режим навчання, перш ніж система перейде до режиму тестування [25].

VA-система (Vulnerability Assessment) – це система огляду слабких місць у безпеці інформаційної системи. Вона оцінює, чи система схильна до будь-яких відомих вразливостей, привласнює рівень серйозності цих вразливостей і рекомендує виправлення або пом’якшення наслідків, якщо і коли це необхідно [29].

Існує кілька типів оцінки вразливості. До них відносяться [29]:

– оцінка хоста – оцінка критично важливих серверів, які можуть бути вразливі для атак, якщо вони не протестовані належним чином або створені з протестованого образу машини;

– оцінка мереж та бездротових мереж – оцінка політик та практик для запобігання несанкціонованому доступу до приватних або публічних мереж та ресурсів, доступних через мережу;

– оцінка баз даних – оцінка баз даних чи систем великих даних щодо уразливостей і неправильної конфігурації, виявлення неавторизованих баз даних чи небезпечних середовищ розробки/тестування, і навіть класифікація конфіденційних даних у інфраструктурі організації;

– сканування програм – виявлення вразливостей безпеки у веб-застосунках та їх вихідному коді шляхом автоматизованого сканування зовнішнього інтерфейсу або статичного/динамічного аналізу вихідного коду.

WAF (Web Application Firewall) – це інструмент безпеки для моніторингу, фільтрації та блокування вхідних та вихідних пакетів даних від веб-програми або веб-сайту. Вони можуть бути на базі хоста, мережі або хмари і зазвичай розгортаються через зворотний проксі-сервер і розміщуються перед програмою або

веб-сайтом (або декількома програмами та сайтами). WAF можуть працювати як мережні пристрої, серверні плагіни або хмарні служби, перевіряючи кожен пакет та аналізуючи логіку прикладного рівня моделі OSI відповідно до правил фільтрації підозрілого або небезпечного трафіку [30].

Зазвичай він захищає веб-програми від таких атак, як підробка міжсайтових даних, міжсайтовий скриптинг (XSS), включення файлів, впровадження SQL тощо від усіх типів атак. Цей метод захисту від атак зазвичай є частиною набору інструментів, які створюють цілісний захист від цілого ряду векторів атак [31].

При розгортанні WAF між веб-програмою та Інтернетом встановлюється щит. У той час як проксі-сервер захищає особистість клієнтської машини за допомогою посередника, він є типом зворотного проксі-сервера, захищаючи сервер від впливу, оскільки клієнти проходять через нього, перш ніж потрапити на сервер [31].

WAF працює на основі набору правил, які часто називають політиками. Ці політики спрямовані на захист від вразливостей у програмі шляхом фільтрації шкідливого трафіку. Цінність WAF частково полягає у швидкості та простоті модифікації політик, що дозволяє швидше реагувати на різні вектори атак [31].

Принцип роботи брандмауера веб-додатків зображено на рисунку 2.3.

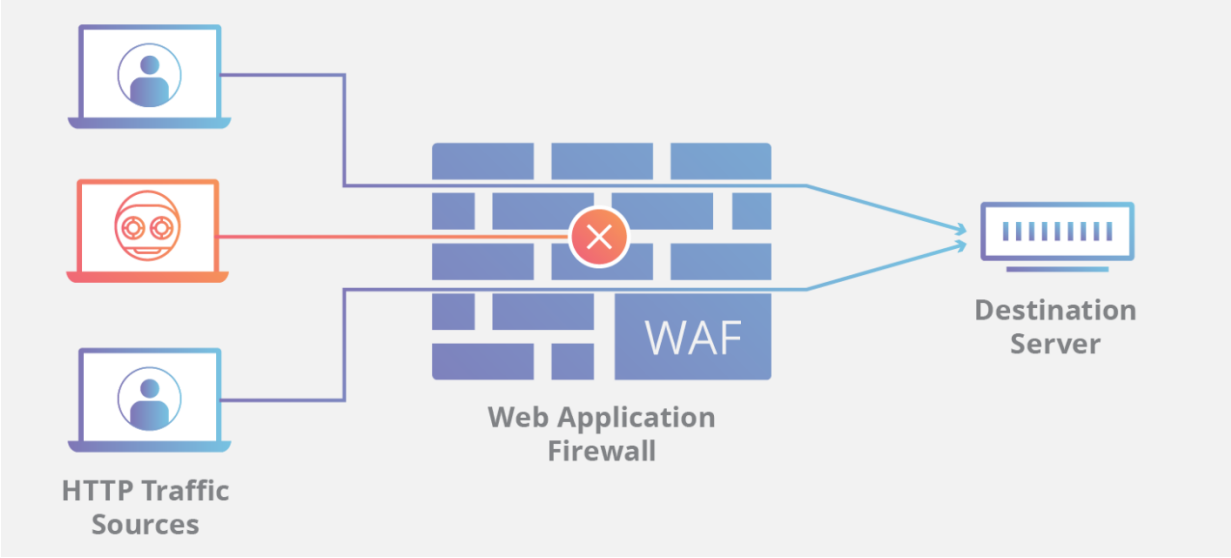

Рисунок 2.3 – Принцип роботи брандмауера при втручанні зловмисника

Висновки за розділом 2

У другому розділі досліджено вразливості та атаки на корпоративні мережі, методи захисту та уникнення загроз та програмні рішення, що дозволяють реалізовувати безпеку інформаційної діяльності організації.

З появою нових технологій, для розширення функціональних можливостей корпоративних мереж, з’являються й нові вразливості, якими згодом скористуються злочинці. Необхідно й не забувати про існуючі.

Великий відсоток загроз з’являється саме з боку людського фактору. Він впливає як на програмну інженерію, так і на соціальну, тобто, відсутність спостереження за оновленнями безпеки в спеціалізованих або сервісних додатках, створення простих, словникових паролей без підключення двофакторної автентифікації, відсутність професійних знань та навичок з налаштування мережевих пристроїв, а також найголовніше – «ображені» співробітники.

Допустивши прогалини в системі інформаційної діяльності підприємства, у злочинців з’являється привід нашкодити йому у вигляді кібератак. До основних програмно-технічних атак на не лише корпоративну, а й на інші типи мереж відносяться атаки «людина посередині», «відмова в обслуговуванні», міжсайтовий скриптинг, кодові та SQL-ін’єкції та фішинг.

Варто відзначити й про атаки за допомогою соціальної інженерії. Злочинець може влаштуватися у дружні стосунки з співробітником компанії та витягти з нього необхідні конфіденційні дані, налаштувати його на встановлення шкідливого програмного забезпечення у робочу систему, перейти за посиланням, яке йому відправили на електронну пошту, спровокувати фізичні пошкодження обладнанню тощо.

Задля запобігання вище зазначених загроз, використовується безліч організаційних та інженерно-технічних рішень. До основних можна віднести: оновлення безпеки в сервісних додатках та операційних системах, правильне налаштування мережевого обладнання, розмежування доступу, застосування політики безпеки на підприємстві, заохочення до кваліфікаційного зросту

співробітників та їх тестування, проведення аналізу вразливих точок в системах та додавання резервних механізмів, задля уникнення «єдиних точок відмови».

На сьогодні, існує вдосталь програмних рішень від передових розробників таких як: IBM, Imperva, FireEye, Digital Guardian, Palo Alto Networks, CloudFlare тощо. До таких рішення відносяться наступні системи: SIEM, DLP, UEBA, VA, WAF, IDS, IPS тощо.

РОЗДІЛ 3
КОНСТРУЮВАННЯ ПРОГРАМНОГО ЗАСОБУ МОНІТОРИНГУ ПОДІЙ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Задачі та функціональні можливості програмного засобу

Програмний засіб моніторингу подій в корпоративній мережі організації повинен:

– бути кросбраузерним, тобто працювати в будь-якому існуючому веб-браузері;

– встановлюватися на серверах компанії;

– мати розподіл ролей, задля розмежування доступу користувачів різних посад;

– слідкувати за подіями користувачів;

– мати базу даних, в якій зберігатимуться дані користувачів та ролі, що будуть присвоюватися стосовно кожного;

– шифрувати паролі криптостійкими алгоритмами з додаванням солі;

– мати зручне меню користувача;

– мати можливість налаштовувати панель приладів швидким та зрозумілим способом для користувача.

Оцінивши задачі, які повинен виконувати додаток, то він буде знаходитися на рівні між серверами та робочими станціями користувачів. Для повного представлення побудуємо його взаємодію в структурі інформаційної діяльності організації. Дана структура представлена на рисунку 3.1.

Додаток матиме назву «inVision» та буде встановлюватися на сервер додатків, який буде знаходитися в ЦОД компанії та взаємодіяти з робочими станціями підключеними до них.

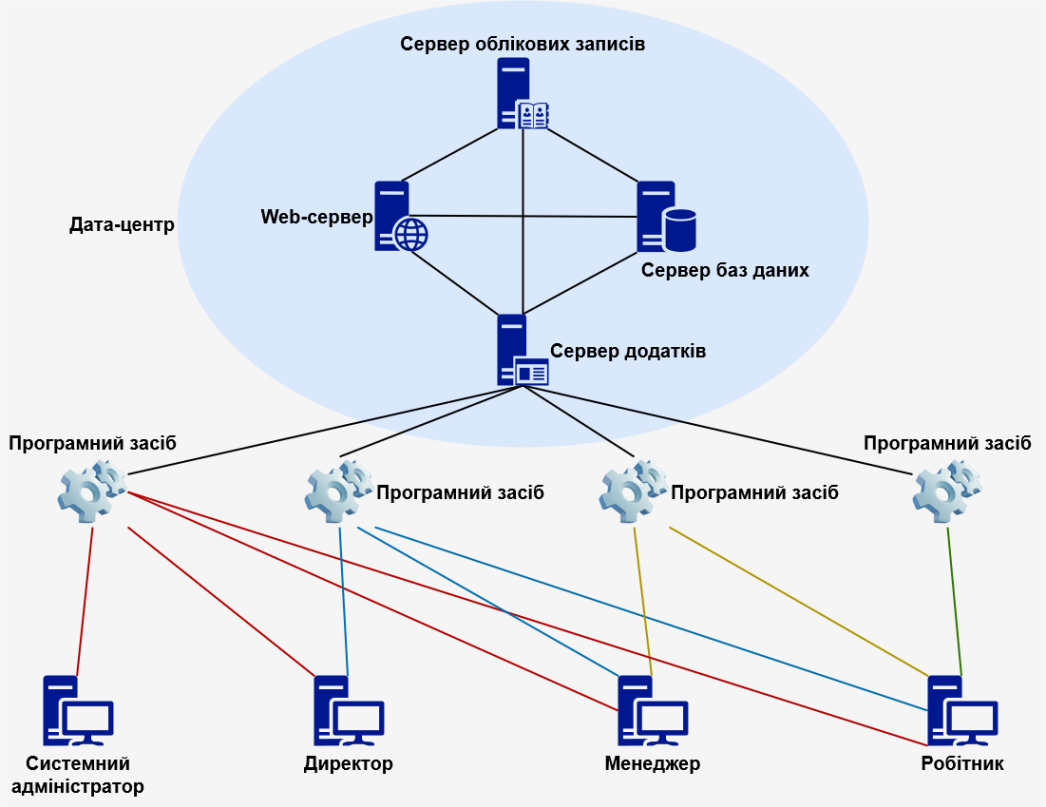

Рисунок 3.1 – Взаємодія додатку з серверами та робочими станціями компанії

Алгоритм роботи додатку полягає в наступному:

1. При переході за посиланням перед користувачем з’являється сторінка входу, де необхідно ввести логін та пароль.

2. Якщо користувача немає в системі, він повинен звернутися до відповідальної особи для реєстрації в ній.

3. Якщо користувач введе неправильний пароль, йому доведеться ввести його знову, в цей час в системі повинно з’явитися сповіщення про підозрілу поведінку.

4. При спробі входу в систему під не зареєстрованим логіном та паролем, система також повинна надати сповіщення про підозрілу активність.

5. При успішному вході користувача, перед ним з’явиться сторінка-дашборд з навігаційним меню, де, в залежності від його ролі, він зможе скористатися переглядом подій або створити власну, наприклад, відправити повідомлення.

6. При появі кожної події, будь-то вхід в систему, реєстрація користувача, відправлення повідомлення в чаті, відправлення електронного листа, зміна інформації профілю тощо, вона буде заноситися в базу даних організації.

7. Якщо подія, котра матиме загрозливий характер виникне, моніторингова система занесе подію в базу даних та сповістить про це відповідальним особам.

8. В залежності від наданої ролі користувачу системи, можна оперувати їх профілями, а саме: видаляти, оновлювати інформацію (паролі, логіни тощо), присвоювати іншу роль, посаду тощо.

9. Користувач має здатність виходити з свого профілю, тому при завершенні роботи він повинен вийти з системи, інакше автоматично відключиться у разі довгої неактивності сесії (принцип «Too long AFK»).

Посилаючись на алгоритм дії програмного засобу, уявимо ситуацію, коли користувач, що знаходиться на нижній ланці вертикальної ієрархії відсилає повідомлення з потенційною загрозою співробітнику позицією вище.

Він успішно зареєструвався, подія записалася в базу даних, як безпечна. Далі, в зв’язку з незадоволенням його заробітної плати та без бесіди з директором його відділу відносно цього, він намагається спровокувати менеджера задля змови, та спричинити атаку на мережу компанії, яка завдасть збитків. Програма фіксує подію, відправляє її в базу даних, по словнику помічає, що повідомлення несе загрозливий характер, заносить в таблицю вразливостей ідентифікатор події та визначає статус користувача як «небезпечний». У цей час, головам відділів, головному директору, офіцеру з безпеки (системному адміністратору) надходить сповіщення про негативну для компанії подію. При відкритті такого листа отримувачем, система помітить його статус як «підозрілий» і сповістить відповідальних осіб.

Візуальне представлення даної ситуації наведено на рисунку 3.2.

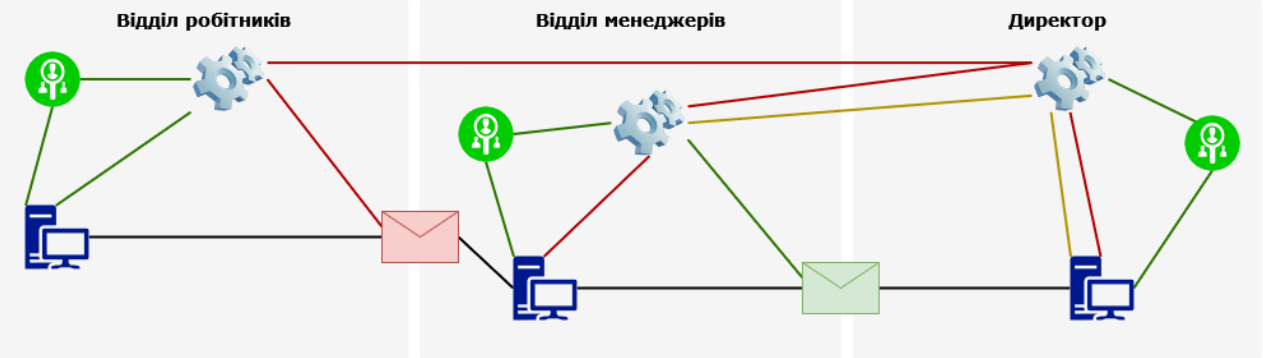

Рисунок 3.2 – Перехоплення повідомлення з потенційною загрозою

3.2 Проектування бази даних

Для адміністрування базами даних можна використовувати будь-які системи управління базами даних (СУБД). В даному випадку, буде використовуватися СУБД phpMyAdmin, що встановлена на хостинг сервісі.

Створимо базу даних з запропонованими таблицями: Roles, Positions, AuthorInfo, Users, Processes, Vulnerabilities.

Таблиця Roles відповідає за збереження визначених системним адміністратором ролей та має поля:

– RoleID – ідентифікатор ролі, первинний ключ;

– RoleName – назва ролі.

Таблиця Positions – за посади та в залежності від посади мати окремо визначену роль. Містить наступні поля:

– PosID – ідентифікатор посади, первинний ключ;

– PosName – назва посади;

– RoleID – ідентифікатор ролі, до якої присвоєна посада, зовнішній ключ.

AuthorInfo – містить логіни та паролі користувачів у зашифрованому вигляді. У цій таблиці знаходяться поля:

– AuthID – лічильник авторизаційних даних користувачів, первинний ключ;

– Login – логін користувача;

– Passwd – пароль користувача.

Таблиця Users містить відомості відносно співробітників компанії, їх посаду та ідентифікатор стосовно їх облікових записів. Це одна з головних таблиць та має поля:

– UserID – ідентифікатор користувача, первинний ключ;

– Name – ім’я користувача;

– Surname – прізвище користувача;

– Patronymic – по-батькові користувача;

– Birthday – дата народження користувача;

– Email – електронна пошта користувача;

– Phone – контактний телефон користувача;

– Registration – дата реєстрації користувача;

– PosID – ідентифікатор, за яким присвоєно посаду та роль користувача, зовнішній ключ;

– AuthID – ідентифікатор, за яким присвоєно авторизаційні дані користувача, такі як логін та пароль; зовнішній ключ.

Таблиці Processes та Vulnerabilities – останні з головних таблиць. Вони відповідають за процеси в самій системі, які події виникли, хто відповідає за процес в системі, який процес, його опис, причини вразливості тощо.

Processes містить у собі поля:

– ProcID – ідентифікатор процесу, первинний ключ;

– ProcessName – назва процесу;

– Description – опис процесу, тобто що в цьому процесі відбулося;

– ProcDate – дата виникнення процесу;

– UserID – ідентифікатор користувача, за яким створений процес закріплений, зовнішній ключ.

А Vulnerabilities наступні:

– VulnID – ідентифікатор вразливої події, первинний ключ;

– VulnDate – дата виникнення вразливої події;

– Statuss – статус вразливості («підозрілість», «небезпечність»);

– Reason – причина виникнення вразливості;

– Description – опис вразливості, що спровокувало її виникнення;

– ProcID – ідентифікатор процесу, за яким виникла дана вразливість; зовнішній ключ.

Для повного представлення зобразимо зв’язки між таблицями на рисунку 3.3.

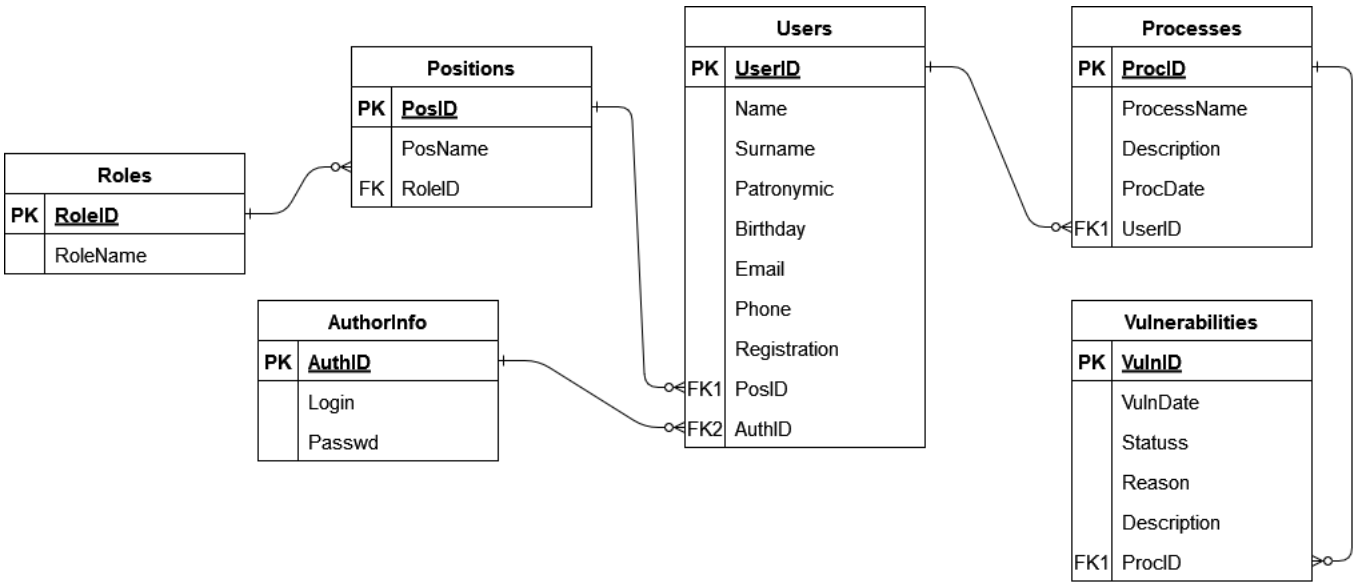

Рисунок 3.3 – Діаграма зв’язків пропонованої для організації бази даних

3.3 Програмна реалізація засобу моніторингу

Для візуальної реалізації додатку використовувалися мови HTML5, CSS3, JavaScript, а функціональної PHP та MySQL. Створення та редагування візуальної та функціональної складової виконувалося в редакторі коду Sublime Text 4. Оперування базами даних та запитами до них – через СУБД phpMyAdmin.

Для авторизації користувачів створено окрему сторінку з формою без можливості самостійної реєстрації, задля забезпечення інформаційної безпеки. Після заповнення користувачем полів з логіном та паролем і натискання клавіші авторизації спрацьовує шматок коду, що наведений на рисунку 3.4, який подає запит

до бази даних на наявність існуючих користувачів та співпадіння введеного та створеного раніше пароля.

Після успішної авторизації воно переведе користувача на головну сторінку програмного засобу.

Для перегляду будь-якого контенту, створення чи видалення, в кожному розділі буде використовуватися один і той самий шматок коду лише зі зміненими полями запитів до баз даних. Код, який зображено на рисунку 3.5, використовується для операцій з базами даних до перегляду відомостей про користувачів.

```php
<?php require_once("includes/initialize.php");
if(isset($_POST['btnlogin'])) {
  $name = $_POST['uname'];
  $pass = $_POST['upass'];
  $sql = mysql_query("SELECT * FROM accounts WHERE username='$name' and password=md5('$pass')");
  $rs = mysql_fetch_array($sql);
  $confirm = mysql_num_rows($sql);
  if($confirm == 1) {
    $_SESSION['acct_id'] = $name;
    $_SESSION['acct_id'] = $rs['acct_id'];
    $_SESSION['oic_id'] = $rs['oic_id'];
    $_SESSION['stud_id'] = $rs['stud_id'];
    $_SESSION['type'] = $rs['type'];
    header("location: index.php");//directing to main form index.php
    echo '<meta http-equiv="Refresh" content="0">';
  }
  else  {
    ?>
        <?php
  }
}
?>
```

Рисунок 3.4 – Код для авторизації користувачів

```php
<?php
                $dbhost = "localhost";
                $dbname = "invision";
                $dbusername = "root";
                $dbpassword = "";
                $conn = new PDO("mysql:host=$dbhost;dbname=$dbname",$dbusername,$dbpassword);

/*******************PDO QUERY***************************/
                $sql = "SELECT oic_id FROM accounts WHERE acct_id = '$_SESSION[acct_id]'";
                $gid = $conn->query($sql);
                $gid->execute();
                $row= $gid->fetch(PDO::FETCH_ASSOC);
                $oic_id = $row['oic_id'];
/*****************END*********************************************/
$query = $conn->prepare("SELECT o.oic_id, a.type, a.imagename, a.imagefile, CONCAT(O.oic_lname,' ',o.oic_fname,' ',o.
  oic_mname)as fullname, o.contact, a.username, a.password FROM oic o, accounts a WHERE o.oic_id = a.oic_id AND o.oic_id
  != '$oic_id'");
$query->execute();
$row = $query->fetchall();
```

Рисунок 3.5 – Код для перегляду наявних користувачів

Далі, на рисунку 3.6, наведено код, який виконує збір відомостей про користувача та показує наявність користувача в мережі для інших співробітників.

```php
<?php
                $dbhost = "localhost";
                $dbname = "invision";
                $dbusername = "root";
                $dbpassword = "";
                $conn = new PDO("mysql:host=$dbhost;dbname=$dbname",$dbusername,$dbpassword);
/*********************PDO QUERY*****************************/
                $sql = "SELECT oic_id FROM accounts WHERE acct_id = '$_SESSION[acct_id]'";
                $gid = $conn->query($sql);
                $gid->execute();
                $res= $gid->fetch(PDO::FETCH_ASSOC);
                $userid = $res['oic_id'];
$query = $conn->prepare("SELECT o.oic_id, a.type, a.imagename, a.imagefile, a.status, CONCAT(O.oic_lname,' ',o.oic_fname,'
    ',o.oic_mname)as fullname, o.contact, a.username, a.password FROM oic o, accounts a, contacts c WHERE o.oic_id = a.
  oic_id AND o.oic_id = c.oic_id AND c.owner = '$res[oic_id]'");
$query->execute();
$row = $query->fetchall();
```

Рисунок 3.6 – Код для перегляду статусу користувача

3.4 Тестовий приклад

В будь-якій компанії з розробки програмного забезпечення, після створення додатку, проект відправляється на тестування. Тому перевіримо працездатність створеного програмного засобу моніторингу подій в корпоративній мережі організації.

Для того, щоб перейти до створеної програми, необхідно відкрити будь-який веб-браузер та у URL-стрічці ввести доменне ім’я, за яким закріплений додаток на сервері. В даному випадку – це http://localhost/invision/login.php.

Після переходу по даному посиланню з’явиться форма авторизації, яка показана на рисунку 3.7.

Рисунок 3.7 – Форма авторизації користувача

Далі, при успішній авторизації користувача, незалежно від присвоєної йому ролі, з’явиться домашня сторінка, яка зображена на рисунку 3.8.

Рисунок 3.8 – Домашня сторінка додатку

В лівій частині домашньої сторінки знаходиться навігаційне меню, в якому можна переглядати список окремо визначених даних. Щоб обрати роботу з окремим

пунктом, необхідно на нього натиснути, після чого з’являться функції оперування, як вказано на рисунку 3.9.

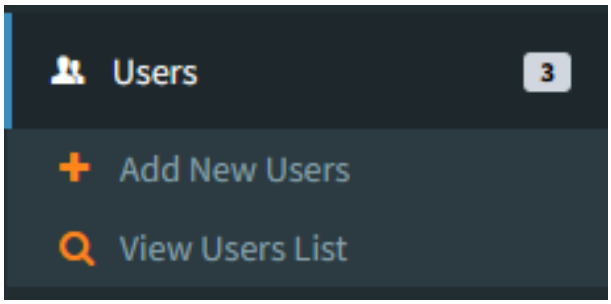

Рисунок 3.9 – Функціональні пункти розділу «Користувачі»

Для створення нового користувача в системі треба обрати пункт з додаванням користувача, після чого з’явиться форма додавання користувача, яка наведена на рисунку 3.10.

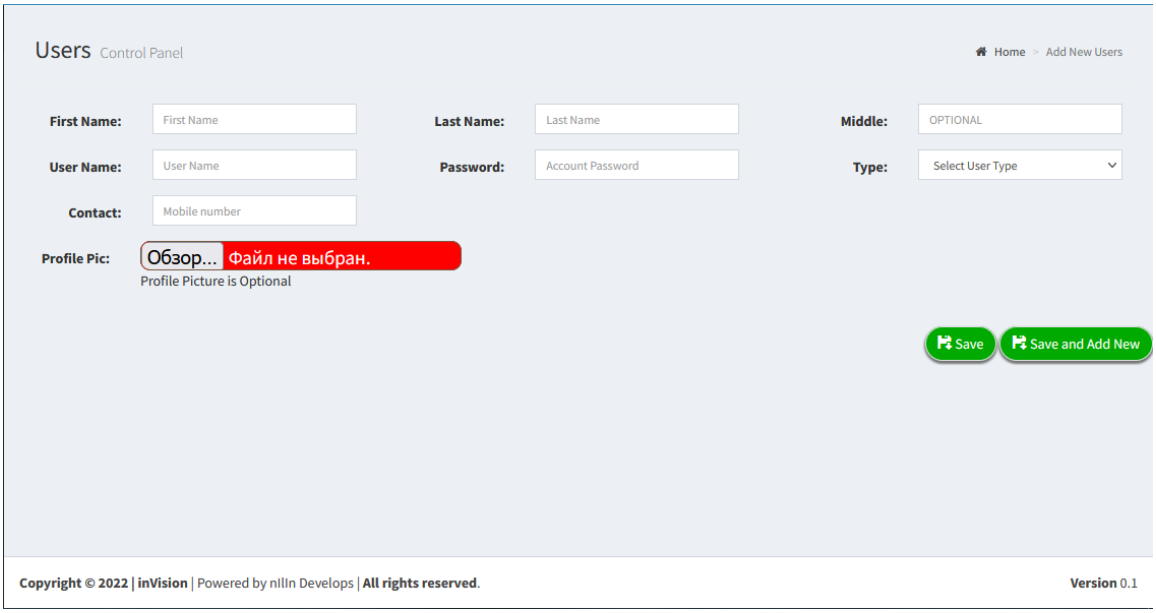

Рисунок 3.10 – Форма додавання користувача

За необхідності перегляду штату співробітників, потрібно натиснути на розділ, що відповідає за них та обрати пункт перегляду. Форма з переліком працівників компанії зображена на рисунку 3.11.

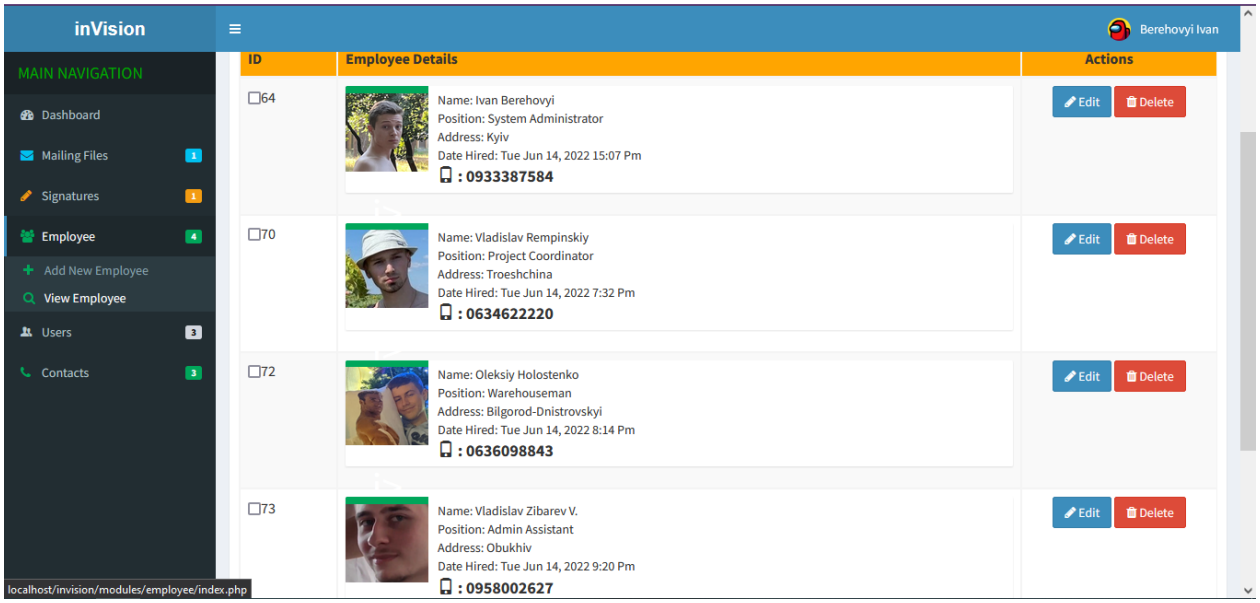

Рисунок 3.11 – Форма додавання користувача

Також, співробітники можуть відправляти повідомлення з прикріпленими файлами. Щоб переглянути, виконаємо аналогічні операції та побачимо форму з переліком повідомлень, що на рисунку 3.12.

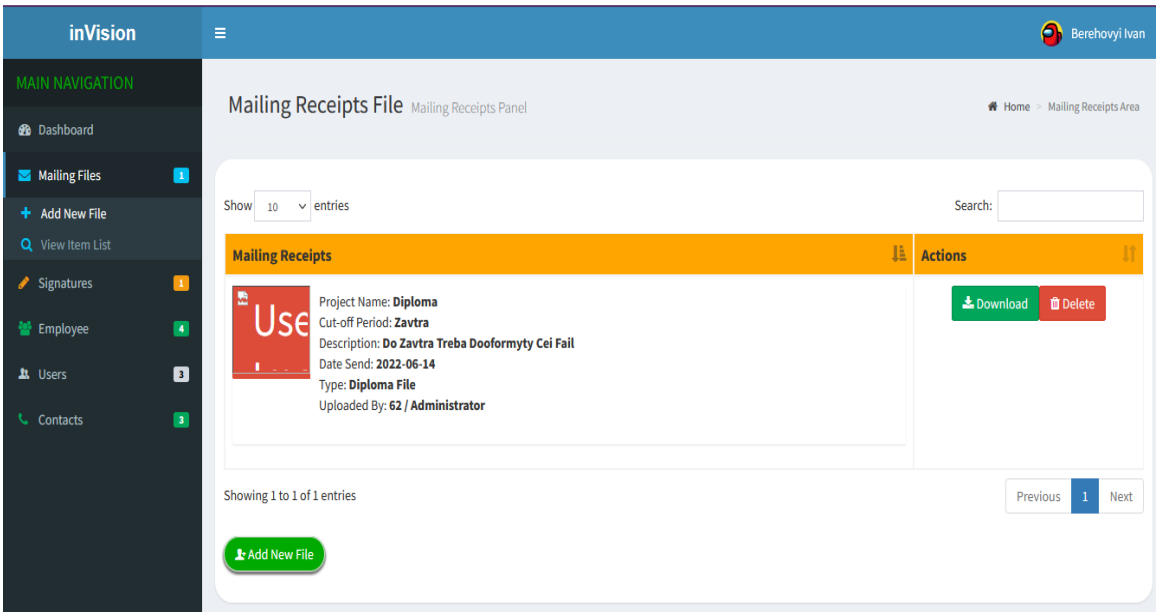

Рисунок 3.12 – Форма перегляду повідомлень

При додаванні нового користувача, інші можуть його додати в список контактів для подальшого спілкування або обговорень.

Перевіримо працездатність програмного засобу при роботі декількох користувачів, тобто як в реальних умовах, коли система встановлена на серверах компанії та працює в її корпоративній мережі, причому співробітники вже на робочих місцях та користуються ним. Для перевірки використаємо два різні браузери, та в кожному авторизуємося під різними користувачами. Результат перевірки зображено на рисунках 3.13-3.14.

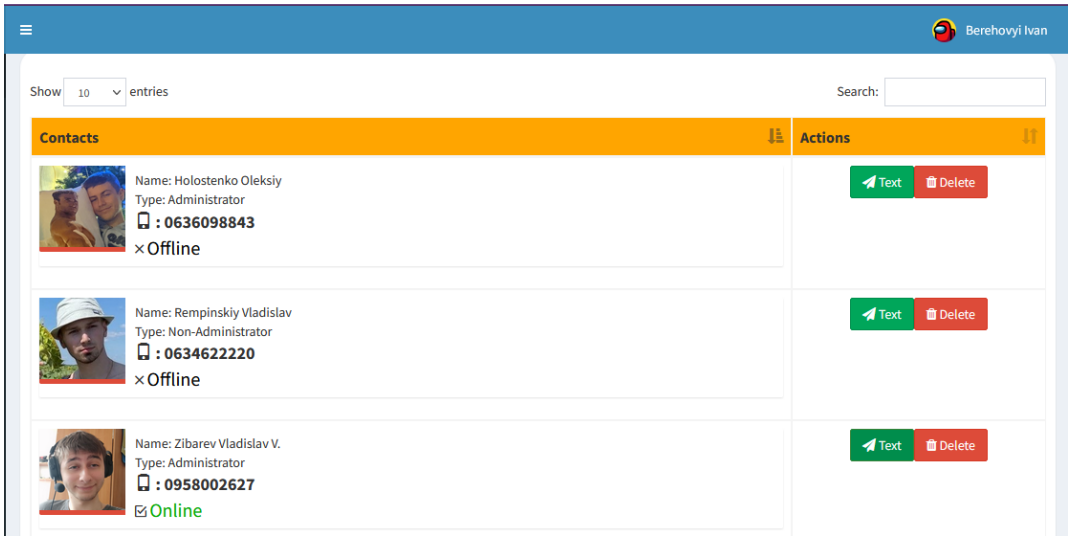

Рисунок 3.13 – Наявність співробітника в мережі

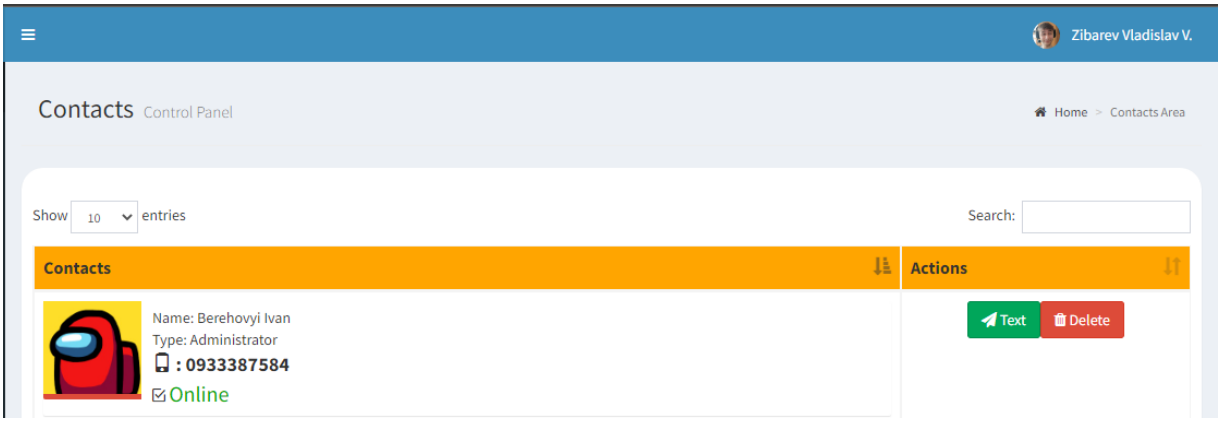

Рисунок 3.14 – Показ стану наявності робітника в мережі під іншим користувачем

Якщо, користувачам необхідно обговорити робочий процес, то вони можуть зв’язатися між собою натиснувши на кнопку листування. Форма, через яку буде вестися листування наведено на рисунку 3.15.

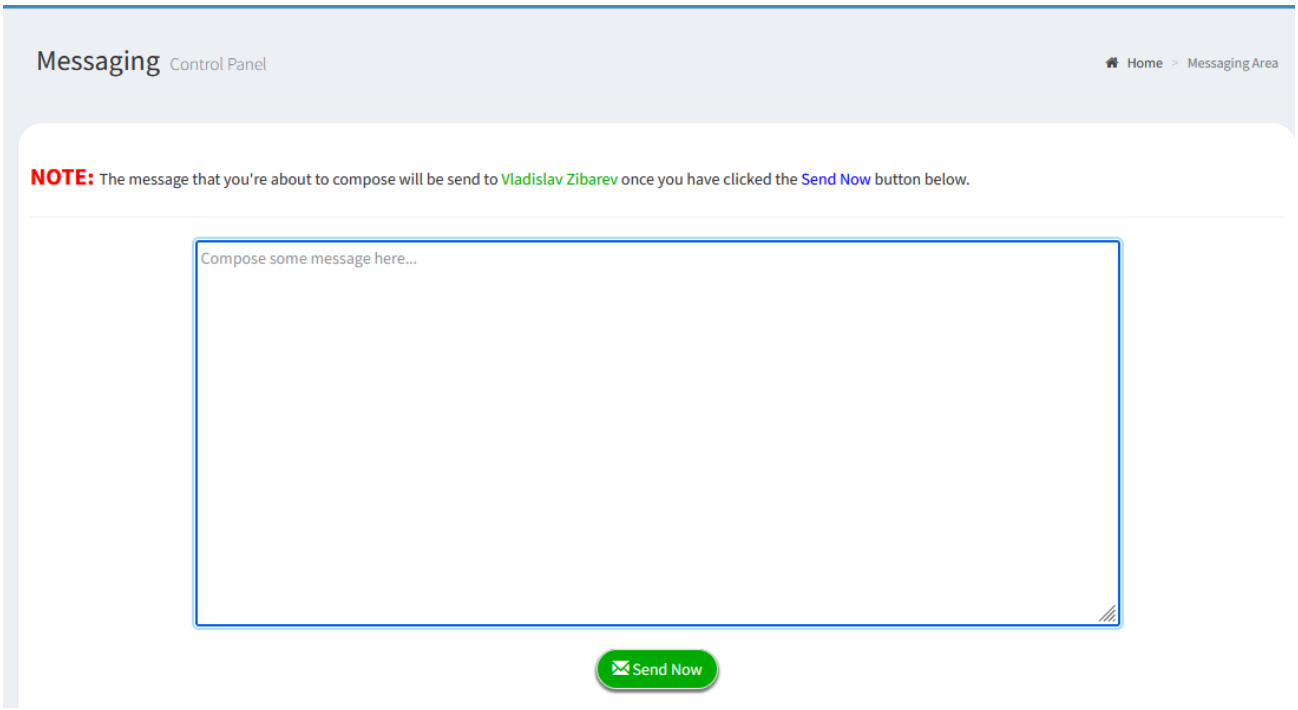

Рисунок 3.15 – Форма надсилання листа іншому користувачу

Висновки за розділом 3

У третьому розділі описано задачі та функціональні можливості, які програмний засіб повинен виконувати, як спроектовано базу даних та за що відповідає кожна таблиця й поля в кожній. Також показано програмну реалізацію додатку та його тестування.

Програмний засіб моніторингу подій розроблявся засобами веб-розробки, а саме мовами HTML, CSS, JavaScript, PHP та MySQL за допомогою редактора коду Sublime Text 4 та СУБД phpMyAdmin.

В програмній реалізації в основному застосовувалися операції з базами даних, а це означає, що в майбутньому для роботи з цим додатком необхідно забезпечити хороший захист баз даних.

Проведено тестування функціональних можливостей даного додатку, у результаті якого було виявлено декілька багів та неповну реалізацію поставлених задач.

ВИСНОВКИ

Досліджено компоненти корпоративні мережі. Вона є сучасним методом організації потоків інформаційних даних між різними офісами, але в межах однієї компанії. В неї є три види, що залежать від масштабів організації. Окрім зображення її структури, існує й багатошарове представлення. Для її створення необхідно знати основні етапи, серед яких: аналіз інформаційної діяльності, вибір архітектури та програмних засобів і визначення головних її компонентів після досліджень.

Розглянуто всі можливі вразливості корпоративних мереж. Корпоративна мережа є «братом по нещастю» інших. А це означає, що вразливості та способи атак на неї спільні з локальною, глобальною тощо мережами. Основний відсоток вразливостей в мережах спричиняється поганим відношенням до них людиною, а саме: погане налаштування апаратного обладнання, несвоєчасне оновлення безпеки в програмних продуктах, використання старих технологій зі зберігання даних (флеш-носії), потрапляння на наживку злодіїв, відсутність політик безпеки та нехтування кваліфікаційних тестувань співробітників.

Проаналізовано вплив атак на корпоративні мережі та надано рекомендації щодо їх уникнення. Вразливості надають змогу створювати атаки перебору паролей, «людини посередині», «відмови в обслуговувані», міжсайтовий скриптинг, ескалація привілеїв, ін’єкції шкідливого коду та фішингові атаки. Для запобігання або уникнення таких атак, більшість виробників програмних засобів з забезпечення безпеки інформаційної діяльності пропонують велику кількість продуктів, наприклад VPN, SIEM-, DLP-, VA-, UEBA-системи, IDPS тощо.

Створено програмний засіб моніторингу подій в корпоративній мережі організації. Виконано тестування його програмних модулів та визначено функціональні помилки програми.

Отже, метою даної дипломної роботи було створення програмного засобу моніторингу подій в корпоративних мережах організації.

Для досягнення поставленої мети були реалізовані й виконані наступні завдання:

– проведено аналіз структури та функціональних можливостей корпоративних мереж;

– досліджено вразливості та загрози корпоративних мереж;

– проаналізовано існуючі системи моніторингу, їх можливості, переваги та недоліки;

– побудовано програмний засіб моніторингу подій в корпоративних мережах.

Всі задачі були виконані в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум Э. Компьютерные сети / Эндрю Таненбаум. – С.-Петербург: Питер, 2019. – 960 с.

2. Корпоративна мережа [Електронний ресурс]. – Режим доступу: http://іт.словник.укр/index.php/Корпоративна_мережа

3. Поняття корпоративної системи та мережі. Корпоративні мережі. Як такі підсистеми можуть бути [Електронний ресурс]. – Режим доступу: https://androidas.ru/ponyatie-korporativnoi-sistemy-i-seti-referat-korporativnye/

4. Узагальнена структура корпоративної мережі. Загальні вимоги до адміністрування мережі [Електронний ресурс]. – Режим доступу: https://uchika.in.ua/koncepciya-informacijnoyi-bezpeki-zagaleni-polojennya-koncepci.html?page=2

5. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary.

6. Alina Georgiana Petcu. 10 Common Network Vulnerabilities and How to Prevent Them [Електронний ресурс]. – Режим доступу: https://heimdalsecurity.com/blog/common-network-vulnerabilities/

7. Top 10 Common Types of Cybersecurity Attacks [Електронний ресурс]. – Режим доступу: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

8. Top 10 Common Types of Network Security Attacks Explained [Електронний ресурс]. – Режим доступу: https://cisomag.eccouncil.org/top-10-common-types-of-network-security-attacks-explained/

9. Network Attacks and Network Security Threats [Електронний ресурс]. – Режим доступу: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

10. 1 найбільша загроза для корпоративних мереж пов’язана. Чому захист периметра корпоративної мережі більше не працює [Електронний ресурс]. – Режим

доступу: https://mkr-novo2.ru/uk/firmware/1-naibolshaya-ugroza-dlya-korporativnyh-setei-svyazana-pochemu-zashchita-perimetra.html

11. Five Ways to Defend Against Network Security Threats [Електронний ресурс]. – Режим доступу: https://www.eccouncil.org/cybersecurity-exchange/network-security/how-to-prevent-network-security-attacks/

12. Marco Piras. How to Prevent Network Security Threats [Електронний ресурс]. – Режим доступу: https://nira.com/preventing-network-security-threats/

13. David Jacobs. Common network vulnerabilities and how to prevent them [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/searchnetworking/tip/Common-network-vulnerabilities-and-how-to-prevent-them

14. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості [Електронний ресурс]. – Режим доступу: https://naurok.com.ua/tema-problemi-zabezpechennya-bezpeki-v-komp-yuternih-sistemah-i-merezhah-tipova-korporativna-merezha-rivni-informaciyno-infrastrukturi-korporativno-merezhi-merezhevi-zagrozi-vrazli-210577.html

15. What is Security Information and Event Management (SIEM)?[Електронний ресурс]. – Режим доступу: https://www.ibm.com/topics/siem

16. What is SIEM and how does it work? [Електронний ресурс]. – Режим доступу: https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

17. What is an Intrusion Prevention System (IPS)? [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/

18. What is an Intrusion Prevention System? [Електронний ресурс]. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

19. What is an intrusion prevention system? [Електронний ресурс]. – Режим доступу: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

20. What is an Intrusion Prevention System (IPS)? [Електронний ресурс]. – Режим доступу: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

21. Jeff Petters. IDS vs. IPS: What is the Difference? [Електронний ресурс]. – Режим доступу: https://www.varonis.com/blog/ids-vs-ips

22. Juliana De Groot. What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention [Електронний ресурс]. – Режим доступу: https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

23. What Is DLP and How Does It Work? [Електронний ресурс]. – Режим доступу: https://www.trellix.com/en-us/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works.html

24. What is Data Loss Prevention (DLP)? [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

25. What is User Entity and Behavior Analytics (UEBA)? [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/what-is-ueba

26. Chris Brook. What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More [Електронний ресурс]. – Режим доступу: https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

27. What is UEBA? Definition and use [Електронний ресурс]. – Режим доступу: https://www.fireeye.com/products/helix/what-is-ueba.html

28. What is UEBA? How UEBA Works & Best Practices [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/data-security/ueba-user-and-entity-behavior-analytics/

29. What is Vulnerability Assessment? VA Tools and Best Practices [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/application-security/vulnerability-assessment/

30. What Is WAF? Types, Security and Features Explained [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/application-security/what-is-web-application-firewall-waf/

31. What is a WAF? Web Application Firewall explained [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

32. Практикум з програмування на VBA: Навч. посібник / П.І. Каленюк, А.Ф. Обшта, Н.М.Гоблик, Н.Ф.Клочко, С.М.Ментинський. Львів: Видавництво Національного університету «Львівська політехніка», 2005. – 208 с.

ДОДАТКИ

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИПЛОМУ

Тези наукових доповідей:

1. S.Y. Dakov, A.P. Torchylo, I.G. Berehovyi. I2P – WHAT IS THE INVISIBLE INTERNET PROJECT & HOW DOES IT COMPARE VS. TOR BROWSER. 3rd International Scientific and Practical Conference on Problems of Cybersecurity of Information and Telecommunication Systems, PCSITS 2020., Kyiv – P. 368.
2. Дмитро Жебрак, Іван Береговий, Яніна Шестак. Методи, засоби та заходи менеджменту інформаційної безпеки. 4th International Scientific and Practical Conference on Problems of Cybersecurity of Information and Telecommunication Systems, PCSITS 2021., Kyiv – P. 191.