

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікації

(повне найменування інституту, назва факультету)

Кафедра захисту інформації

(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавр

(ступінь вищої освіти)

на тему РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ІТ-ОФІСІ
DEVELOPMENT OF AN INFORMATION SECURITY SYSTEM IN THE IT
OFFICE

Виконав: студент(ка) 4 курсу, групи РТ-819
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних
систем

ІВЛЄВ В.Ю.

(прізвище та ініціали)

Керівник ЛІЗУНОВ С.І.

(прізвище та ініціали)

Рецензент МАЛИЙ О.Ю.

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікацій
Кафедра захисту інформації
Ступінь вищої освіти бакалавр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і телекомунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, к.т.н, доц.
В.О. ВОСКОБОЙНИК
“01” “06” 2023 року

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

Івлєва Владислава Юрійовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка системи захисту інформації у IT-офісі
Development of an information security system in the IT office system

керівник проєкту (роботи) к.т.н., доцент ЛІЗУНОВ Сергій Іванович,
(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові.)

затверджені наказом закладу вищої освіти від “04” квітня 2023 року № 93

2. Строк подання студентом проєкту (роботи) 01 червня 2023 року

3. Вихідні дані до проєкту (роботи) розробити систему захисту інформації у IT-офісі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): навести теоретичні відомості про об'єкт та системи його захисту, провести аналіз можливих загроз та інструментів протидії, створити комплексну систему захисту інформації для IT - офісу

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): презентація

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Розділи 1-3	ЛІЗУНОВ С.І., к.т.н. доцент		
Нормоконтроль	КОРОЛЬКОВ Р. Ю., к.т.н. ст. викл.		

7. Дата видачі завдання « 01 » березня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Ознайомлення із завданням і підбір технічної літератури	1 тиждень	Завдання, ТЗ
2	Формування вимог до системи захисту об'єкта	1 тиждень	Розділ 1
3	Розрахунок параметрів системи безпеки об'єкту	2 тиждень	Розділ 2
4	Розробка охоронної системи захисту об'єкта	3-4 тижні	Розділ 2
5	Розробка системи контролю та управління доступом	5 тиждень	Розділ 3
6	Розробка системи захисту електронних даних	6-7 тиждень	Розділ 3
7	Аналіз запропонованої моделі захисту об'єкта та внесення корективів	8 тиждень	
8	Оформлення графічного матеріалу	9 тиждень	

Студент(ка)

(підпис) Владислав ІВЛЄВ
(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

(підпис) Сергій ЛІЗУНОВ
(Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:
86 с., 9 рис., 1 дод., 25 джерел.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІТ - ОФІС, МОДЕЛЬ OSI, ЗАГРОЗИ БЕЗПЕКИ, АНТИВІРУСИ

Об'єкт дослідження – офіс ІТ – компанії.

Предмет дослідження – комплексна система захисту інформації.

Мета роботи – створити комплексну систему захисту для ІТ – офісу, виявлення можливих загроз та способів запобігання загрозам.

Для реалізації було власноруч спроектовано схеми ІТ – офісу та різні системи в ньому.

В результаті було розроблено комплексну систему захисту інформації для об'єкту, проаналізовано можливі загрози та запропоновано способи протидії ним.

ABSTRACT

Explanatory note to the bachelor's diploma qualification work: 86 p., 9 fig., 1 app., 25 sources.

INFORMATION SECURITY SYSTEM, IT-OFFICE, OSI MODEL, SECURITY THREATS, ANTIVIRUSES

The object of study - IT office of a company.

The subject of research - comprehensive information security system.

The purpose of the work - create a comprehensive security system for an IT office, identify potential threats and ways to prevent them.

To implement this, diagrams of the IT office and various systems within it were designed by hand.

As a result, a comprehensive information security system was developed for the object, potential threats were analyzed and ways to counter them were proposed.

ЗМІСТ

Перелік скорочень	8
Вступ.....	9
1 Теоретичні відомості про об'єкт та системи його захисту	10
1.1 Визначення ІТ – офісу та визначення його типу	10
1.2 План будівлі.....	10
1.3 Різновид обладнання.....	16
1.4 Модель OSI	19
1.5 Комплексні системи цифрового захисту інформації.....	25
1.5.1 Система SIEM.....	25
1.5.2 Система виявлення вторгнень	27
1.5.3 Система протидії вторгнень.....	30
2 Аналіз можливих загроз та інструменти протидії	37
2.1 Аналіз загроз.....	37
2.2 Важливість аналізу та типи мережевих загроз.....	39
2.2.1 Типи вірусів	40
2.2.2 DDoS атаки	43
2.2.3 Фішинг.....	44
2.2.4 Витоки даних	44
2.2.5 Несанкціонований доступ	45
2.2.6 Викрадення особистої ідентичності.....	46
2.3 Аналіз загроз мережевої безпеки.....	46
2.4 Критичні ділянки та ризики	47
2.5 Заходи та інструменти щодо запобігання загроз мережевої безпеки в ІТ-офісі	48
2.5.2 Антивіруси та їх види	52
2.5.3 Антиспам-фільтри та їх види	67

3 Створення комплексної система захисту інформації для it - офісу	68
3.1 Запобігання загрозам кібератак	68
3.2 Запобігання загрозам соціального інжинірингу	69
3.3 Запобігання загрозам несанкціонованого фізичного доступу.....	69
3.4 Запобігання загрозам які утворюються через недбалість працівників .	73
3.5 Запобігання загрозам які утворились через помилки в програмному забезпеченні	74
3.6 Запобігання загрозам пов'язаних з мережею	74
3.7 Функціонування системи захисту офісу в неробочий час	75
Висновки	77
Перелік посилань.....	79
Додаток А Презинтація.....	81

ПЕРЕЛІК СКОРОЧЕНЬ

ПЗ – Програмне забезпечення

СЗІ – Система захисту інформації

AIPS – Application-based Intrusion Prevention System (Система запобігання вторгнень на основі програми)

DDoS – Distributed Denial of Service (Розподілена відмова в обслуговуванні)

FTP – File Transfer Protocol (протокол передачі файлів)

HIDS – Host-based Intrusion Detection System (Система виявлення вторгнень на основі хоста)

HIPS – Host-based Intrusion Prevention System (Система запобігання вторгнень на основі хоста)

HTTP – HyperText Transfer Protocol (протокол передачі гіпертекста)

IDS – Intrusion Detection System (Система виявлення вторгнень)

IPS – Intrusion Prevention System (Система запобігання вторгненням)

IPX – Internetwork Packet Exchange (Мережевий обмін пакетами)

IT – Information Technology (Інформаційні технології)

NIDS – Network-based Intrusion Detection System (Мережева система виявлення вторгнень)

NIPS – Network-based Intrusion Prevention System (Мережева система запобігання вторгненням)

OSI – Open Systems Interconnection (Відкрита система взаємозв'язку)

SIEM – Security Information and Event Management (Безпека інформації та управління подіями)

SMTP – Simple Mail Transfer Protocol (Простий протокол передачі пошти)

TCP – Transmission Control Protocol (Протокол керування передачею)

UDP – User Datagram Protocol (Протокол датаграм користувача)

VPN – Virtual private network (Віртуальна приватна мережа)

ВСТУП

У сучасному цифровому середовищі, де інформаційні системи відіграють ключову роль у діяльності більшості компаній, гарантування інформаційної безпеки стає пріоритетним завданням. IT-офіси, як осередки великої кількості даних, вимагають високого рівня уваги в плані захисту інформації. Існує численні потенційні загрози, що можуть призвести до втрати або витоку важливої інформації, що може спричинити суттєві фінансові втрати та негативно вплинути на репутацію компанії.

У цьому дипломі фокус був на розробці інтегрованої системи захисту інформації в IT-офісі. Дипломна робота містить теоретичний блок, в якому було розглянуто базові концепції, що стосуються IT-офісів та їх захисту, проаналізовано потенційні загрози та способи протидії, а також продемонстровано практичний аспект, пропонуючи рішення для створення надійної системи захисту інформації.

Було використано інформацію про основні ризики та можливі загрози, а також проаналізовано наявні методики та інструменти для їх нейтралізації, включаючи фаєрволи, антивірусні програми, антиспамфільтри, тощо. Мета - створити ефективну систему захисту, яка здатна впоратися з традиційними загрозами, а також з сучасними методами атак, і гарантувати стабільність інформаційної системи під час неробочого періоду.

У ході реалізації цієї дипломної роботи, глибоко вивчено потенційні зони ризику та виявлено вразливі місця в системі захисту. Дипломна робота ідентифікує слабкі точки в сучасних системах та розкриває специфічні рішення для їх виправлення. Більше того, було звернено увагу на питання попередження загроз, таких як кібератаки, соціальний інжиніринг, неавторизований фізичний доступ та помилки в програмному забезпеченні.

Заклучна частина дипломної роботи зосереджується на практичному виконанні розробленої інтегрованої системи захисту інформації для IT-офісу.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ОБ'ЄКТ ТА СИСТЕМИ ЙОГО ЗАХИСТУ

1.1 Визначення ІТ – офісу та визначення його типу

ІТ-офіс це простір, де активно працюють спеціалісти в галузі інформаційних технологій. Інформаційні технології охоплюють комплекс методів, процедур та підходів до використання комп'ютерної техніки та комунікаційних систем з метою генерації, збору, передачі, відшукування, обробки та дистрибуції інформації, що має на меті ефективне управління людською діяльністю.

ІТ-офіси мають різний характер залежно від виду ІТ-організації. Основні категорії ІТ-фірм охоплюють: компанії-виробники продуктів, аутсорсингові фірми, аутстаф компанії, консалтингові агенції та ІТ-відділи в нетехнологічних компаніях [1].

1.2 План будівлі

На рисунку 1.1 зображено план об'єкту ІТ-офісу, який має окрему одноповерхову будівлю та огорожену територію. Будівля має простий зовнішній вигляд та навколо неї простягається міцна металева огорожа. Для в'їзду на територію існує контрольно-пропускний пункт зі шлагбаумом.

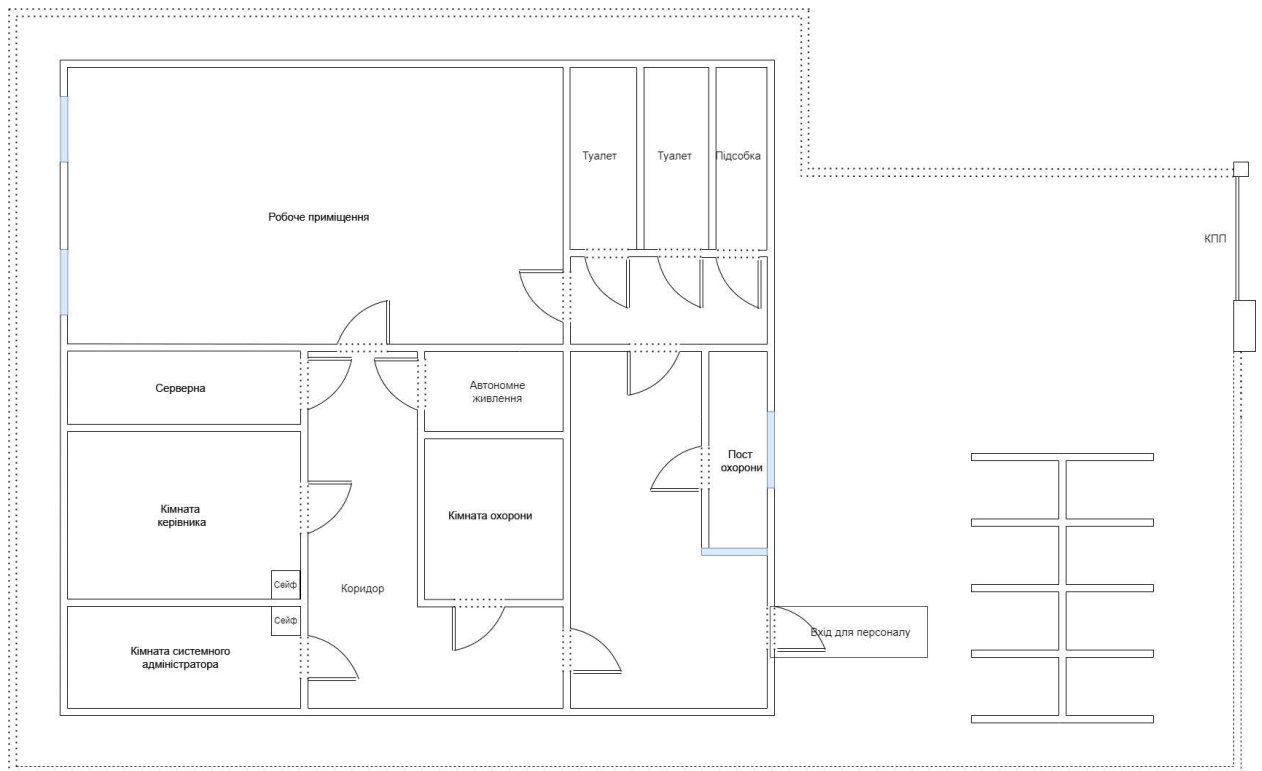


Рисунок 1.1 - Загальний план ІТ- офісу

В приміщенні присутні пост та кімната охорони яка забезпечує фізичну безпеку приміщення та співробітників. Охорона контролює доступ до будівлі, перевіряє посвідчення особи відвідувачів та співробітників, а також реагує на надзвичайні ситуації. Це допомагає запобігти несанкціонованому доступу до приміщення та конфіденційної інформації, а також забезпечує безпеку співробітників.

Крім того, кімната охорони містить системи безпеки, такі як відеоспостереження та контроль доступу. Ці системи забезпечують моніторинг та захист від несанкціонованого доступу до обмеженої інформації та активів компанії.

Охорона спостерігає за виконанням правил безпеки та допомагає у попередженні крадіжок або несанкціонованого доступу до конфіденційної інформації. Це допомагає забезпечити безпеку даних та інформації компанії.

Велику територію будівлі займає робоче приміщення в якому наявні комфортні умови для роботи. Воно обладнане сучасними технологіями які

забезпечують ефективну роботу співробітників. Робочі столи та стільці мають належну ергономіку, що забезпечує зручність та безпеку праці. Також встановлено кондиціонер який дає змогу працівникам відчувати себе зручно.

Окреме приміщення займає кімната начальника яка потрібна для наступного.

Збереження конфіденційної інформації: начальник може мати доступ до конфіденційної інформації, такої як розробка нових продуктів, стратегії маркетингу та ін. Тому для збереження цієї інформації він може мати окрему кімнату, де можна проводити конфіденційні наради та дискусії.

Місце для розробки стратегій та планування: начальник може використовувати свою кімнату для розробки стратегій та планування дій компанії. Він може використовувати цей простір для проведення зустрічей з керівництвом та іншими відділами, щоб обговорити проблеми та знайти способи їх вирішення.

Особистий простір для роботи: начальник може мати більше обов'язків та завдань, ніж інші співробітники, тому йому може знадобитися окремий простір для роботи. Він може використовувати свою кімнату для роботи над важливими проектами, підготовки презентацій та ін.

Символ статусу: кімната начальника може бути символом його статусу та позиції в компанії. Вона може мати ексклюзивний дизайн, комфортні меблі та високотехнологічні пристрої, що демонструє успіх та важливість начальника в компанії.

Також вона обладнана сейфом в якому начальник мусить зберігати носії важливої інформації.

Системний адміністратор контролює та моніторє комп'ютерні системи. Також він відповідає за забезпечення безпеки та надійності серверів, мереж та іншого обладнання, що підтримує роботу офісу. В нього є доступ до серверної кімнати, де розташоване серверне обладнання, а також до кімнати з автономним живленням. Кімната системного адміністратора має належне вентильовання та сейф в якому він зберігає резервні копії даних компанії.

В серверній кімнаті розташоване обладнання яке дає змогу працівникам використовувати обладнання задіяне при роботі. Кімната обладнана кондиціонером для запобігання перегріванню серверів. Також кондиціонери знаходяться у всіх кімнатах де довгий час перебуває персонал.

Перш ніж проводити аналіз будівлі, необхідно визначити, яка інформація перебуває в циркуляції в приміщенні (рисунок 1.2). IT-офіс може містити різноманітну інформацію з обмеженим доступом, таку як:

- коди програмного забезпечення та інтелектуальна власність компанії;
- корпоративні відомості про фінанси, бухгалтерську звітність та фінансові стратегії;
- персональну інформацію про працівників, зокрема зарплатню, контактні дані та відомості про здоров'я;
- інформацію про клієнтів, їх особисті дані, контактні дані та історію замовлень;
- конфіденційні документи та інформацію про проєкти, що знаходяться у розробці або плануються до випуску.

В компанії циркулює 3 види інформації: мовна, паперова та електронна. На рисунку 1.2 зображено, яка інформація може циркулювати в кожній кімнаті.

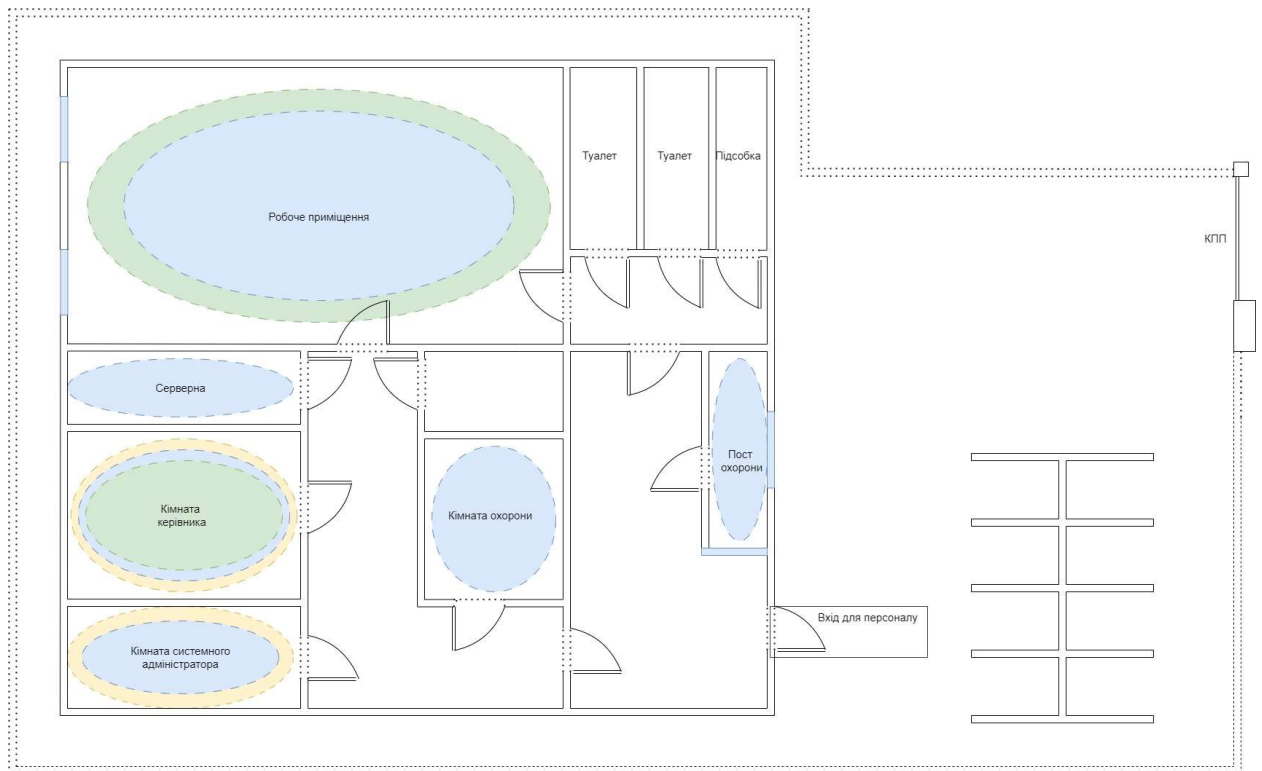


Рисунок 1.2 – Зони циркуляції інформації

Мовна інформація використовується між працівниками для кращого порозуміння в деталях спільного проєкту. Інформація такого роду може бути присутня під час розмови начальника з клієнтом з приводу заказу на розробку або уточнення деталей.

Паперова інформація може використовуватись в ІТ-офісі в різних контекстах.

Записки під час зустрічей та брейнштурмінгів. Незважаючи на те, що велика частина комунікації відбувається в електронному вигляді, під час зустрічей та брейнштурмінгів можуть виникати ідеї, які необхідно зафіксувати швидко та просто. У цьому випадку записи на папері можуть стати зручним інструментом для ідей наведених нижче.

Схеми архітектури та проєктні документи. Іноді складно зрозуміти взаємозв'язки між елементами архітектури чи проєктні рішення за допомогою електронної документації. У цьому випадку паперові документи можуть допомогти зробити проєкт більш доступним та зрозумілим.

Плани проєктів та схеми розкладу. У деяких випадках паперові графіки, діаграми та таблиці можуть допомогти краще відслідковувати прогрес проєкту та визначати, що має бути зроблено наступним кроком.

Схеми розвитку та стратегії компанії. Паперові документи також можуть бути корисними для зберігання стратегічної інформації, наприклад, планів розвитку компанії, що допоможуть зберегти головні ідеї та напрямки.

Ручні записи програмістів. У багатьох випадках програмісти ведуть ручні записи, де фіксують деталі проєктів, що вони розробляють. Ці записи можуть бути корисними, коли не доступний комп'ютер або випадає інтернет-з'єднання, або коли потрібно швидко щось зафіксувати без відволікання на комп'ютерну роботу.

Електронна інформація використовується на різних рівнях та в різних процесах. Наприклад.

Розробка програмного забезпечення: програмісти використовують електронну інформацію, щоб зберігати код, документацію, тестові дані та інші матеріали, необхідні для розробки продукту.

Управління проєктами: проєктний менеджмент та комунікації між різними командами відбуваються з використанням електронних інструментів, таких як електронна пошта, програми для спільної роботи над документами та проєктні системи управління.

Тестування продукту: тестери використовують електронні системи для зберігання тестових сценаріїв та результатів тестування.

Маркетинг та продажі: електронна інформація використовується для зберігання даних про клієнтів та їх поведінку, а також для створення та розсилки електронних рекламних кампаній.

Управління виробництвом: електронна інформація використовується для планування виробництва, зберігання даних про інвентар, стан виробництва та інші фактори, необхідні для ефективного управління виробництвом [2].

1.3 Різновид обладнання

На рисунку 1.3 можна побачити план будівлі з комп'ютерами та перегородками, щоб домогтись комфорту та конфіденційності між працівниками.

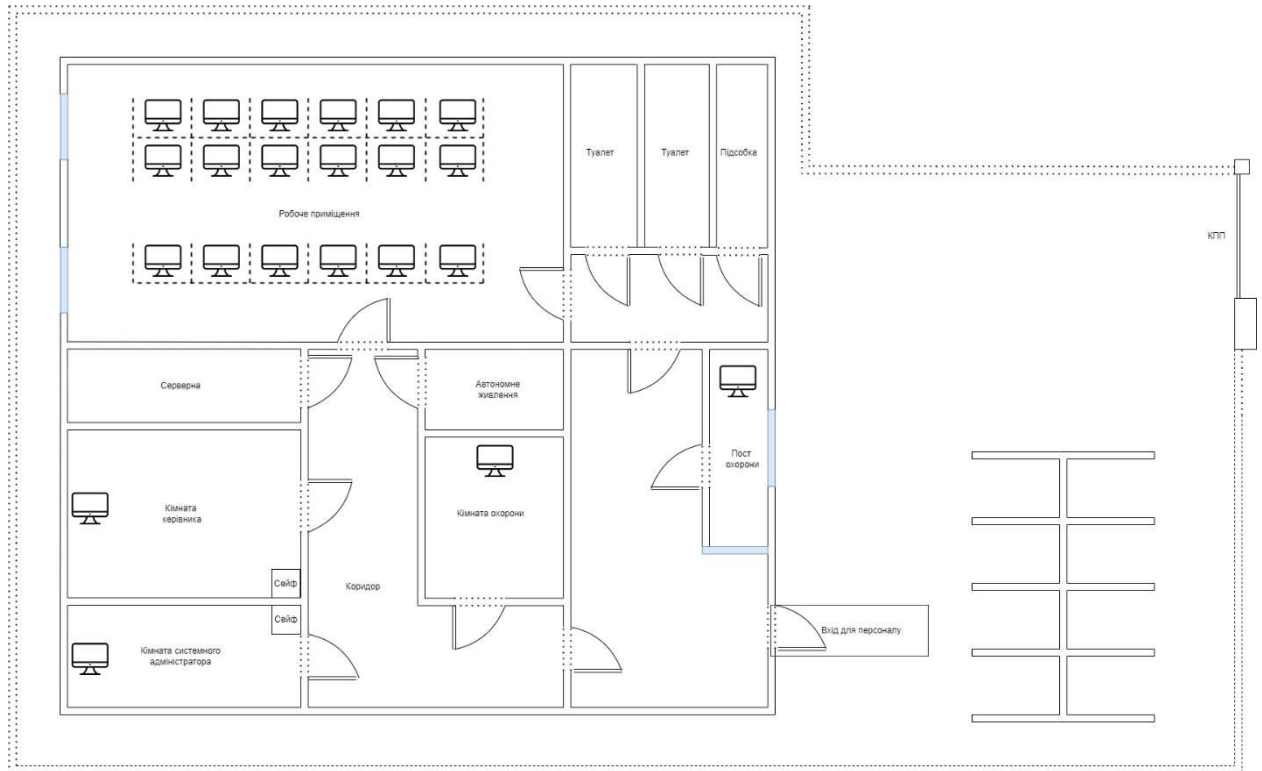


Рисунок 1.3 – Схематичне розташування комп'ютерів

Саме комп'ютери потребують найбільшого захисту. Вони знаходяться на посту та в кімнаті охорони, у кімнатах начальника та системного адміністратора й найбільша їх кількість сконцентрована в робочому приміщенні. Налаштована система фаєрволу яка є важливим інструментом захисту від хакерських атак та несанкціонованого доступу до мережі компанії. Вона дозволяє обмежити доступ до мережі тільки тим, хто має дозвіл, та блокувати небажаний трафік, що може містити шкідливі програми або віруси. Він також може допомогти у попередженні атак з використанням віддаленого

доступу, які можуть надавати злочинцям незаконний доступ до мережі і даних компанії [3].

Для забезпечення безперебійної роботи серверів встановлено пристрій безперебійного живлення, який забезпечує до 15 хвилин роботи після відключення електроенергії. Для довгострокової роботи також встановлено газовий генератор з належною вентиляцією, ізоляцією та заземленням. Датчики виявлення газу допомагають уникнути витoku газу в приміщенні.

В офісі створено дві електросистеми для додаткового захисту, на виході з контрольованої зони обидві системи обладнані фільтрами. Також в будівлі присутнє заземлення для зменшення радіоелектронного випромінювання від працюючих приладів (рисунок 1.4). На вікнах встановлені датчики розбиття скла, а при вході та в кімнаті начальника розташовані датчики руху. Ці пристрої зв'язані з кімнатою охорони для швидкого реагування.

На вентиляційних отворах в робочому приміщенні та в кімнаті начальника встановлено звукоізоляційний матеріал для забезпечення захисту від витoku акустичної інформації (рисунок 1.5).

Серверна кімната та кімната автономного живлення обладнані для захисту від несанкціонованого доступу, пожеж та перегріву. Система кондиціонування забезпечує оптимальну температуру, а система виявлення проникнення допомагає запобігти несанкціонованому доступу.

Умови середовища контролюються для підтримки стабільної температури та вологості. Меблі для зберігання даних виготовлені з вогнетривких матеріалів та мають підвищену стійкість до пожеж [4].

На рисунку 1.6 можна побачити місця розташування датчиків диму. Для тушіння пожеж використовується піна яка не завдає шкоди апаратурі, а в серверній та в кімнаті автономного живлення використовується газова система тушіння.

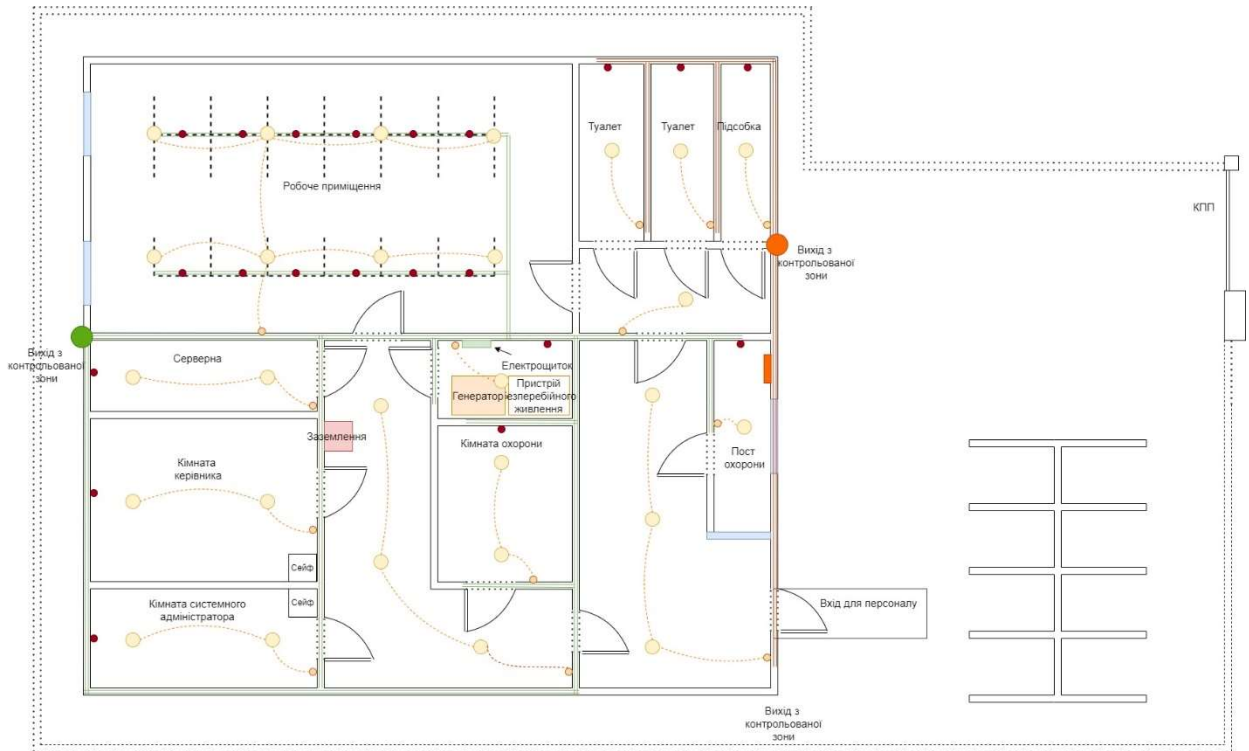


Рисунок 1.4 - Схема живлення, розташування розеток та освітлення

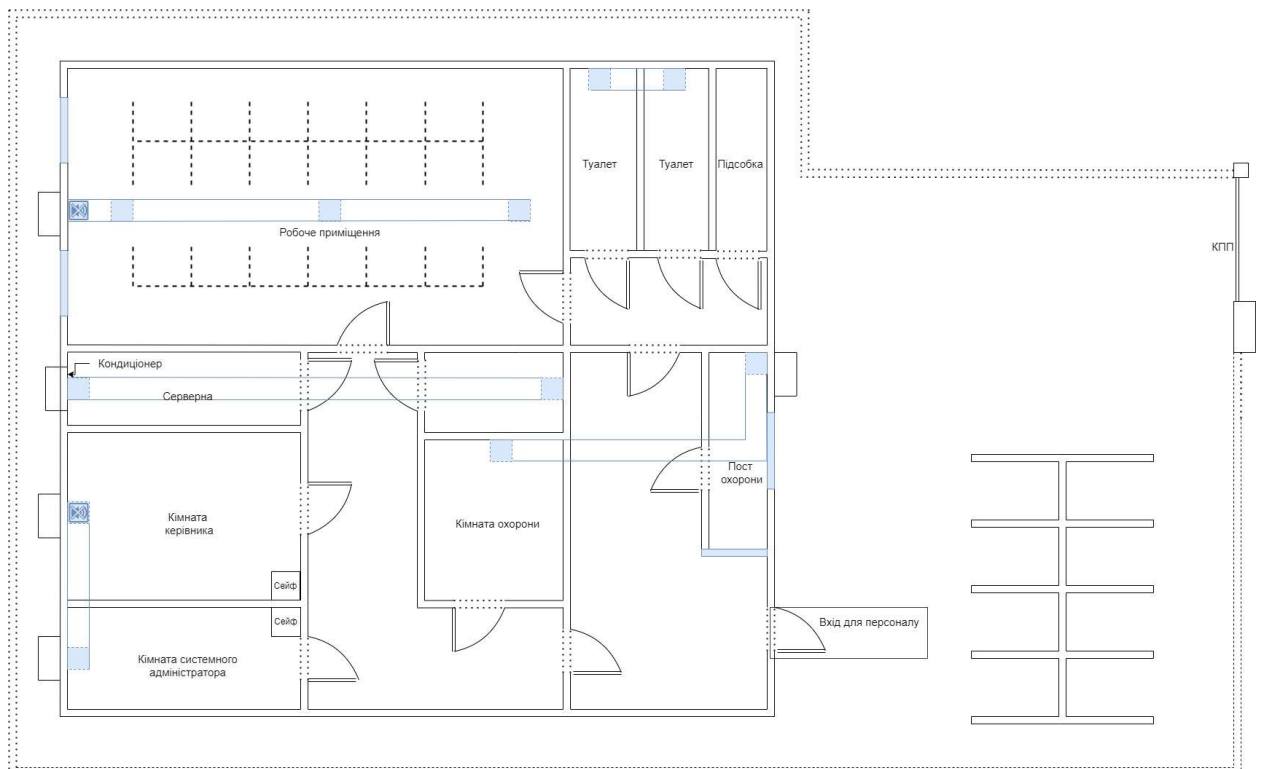


Рисунок 1.5 – Схема розташування вентиляції

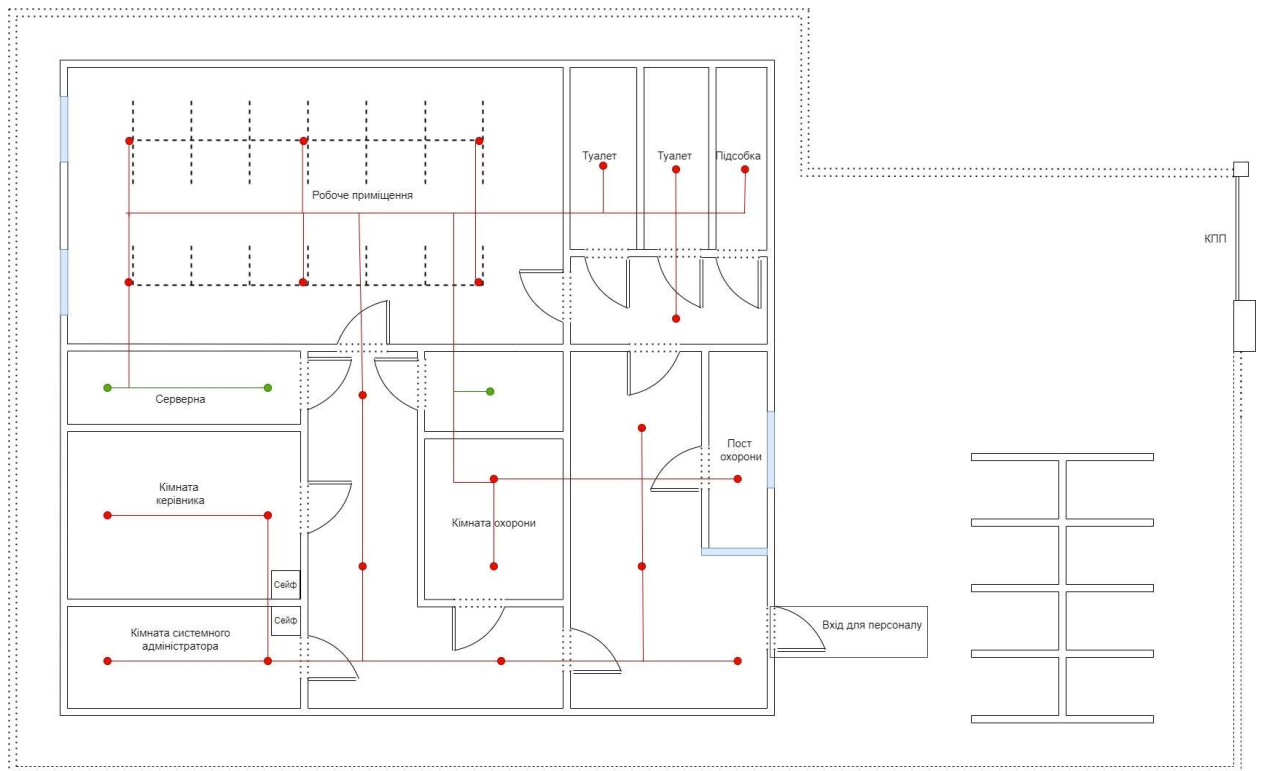


Рисунок 1.6 – Схема розташування протипожежних датчиків

1.4 Модель OSI

Модель Open Systems Interconnection (OSI), створена Міжнародною організацією зі стандартизації (ISO) у 80-х роках минулого століття, служить теоретичною схемою для розуміння та опису взаємодії мережевих протоколів. Вона була створена з метою полегшення процесу проектування мережевих протоколів та асистування у розв'язанні проблем мережевої взаємодії.

Модель OSI включає сім шарів або рівнів, кожен з яких має специфічні обов'язки. Вони від першого до останнього наведено нижче.

1. У моделі відкритих систем взаємодії, фізичний шар, відомий як перший шар, знаходиться на найнижчому рівні. Його головна задача - це передача потоку бітів по мережі з одного пристрою до іншого. Цей шар не здійснює обробку даних, але регулює методи передачі сирих бітів.

Нижче наведено основні функції фізичного шару.

Трансмісія даних: фізичний шар забезпечує пряму передачу сирих бітів між пристроями в мережі. Це може включати двонаправлену трансмісію даних.

Особливості медіа: фізичний шар встановлює характеристики медіа, такі як тип кабелю, роз'єми, сигнали, напруга, швидкість передачі даних тощо.

Фізичне кодування: фізичний шар визначає процес кодування та передачі бітів через мережу. Це включає методи кодування, які перетворюють біти в сигнали для передачі.

Синхронізація бітів: фізичний шар також відповідає за синхронізацію бітів, створюючи "тактові" сигнали для координування передачі бітів між двома пристроями.

Електромагнітний інтерфейс та фізичне з'єднання: фізичний шар регулює параметри електромагнітного інтерфейсу для передачі сигналів, а також ставить вимоги до фізичного з'єднання між пристроями.

Незважаючи на те, що фізичний шар є базовим шаром в моделі OSI, він відіграє вирішальну роль у процесі передачі даних через мережу.

2. Другий шар моделі OSI, відомий як шар передачі даних, виконує ключову роль у забезпеченні надійності обміну інформацією між мережевими пристроями.

Основні задачі цього шару перераховані нижче.

Створення рамок: шар передачі даних відповідає за перетворення потоку бітів, який приходить від фізичного шару, у впорядковані дані, що формують рамки. Кожна рамка включає поле з даними, адресну інформацію та контрольні біти.

Управління доступом до мережі: шар передачі даних контролює доступ до мережеских ресурсів, що є особливо важливим в ситуаціях, коли декілька пристроїв намагаються виконати передачу даних одночасно.

Виявлення та виправлення помилок: на цьому шару можливе виявлення та в деяких випадках корекція помилок, що виникають під час передачі даних.

Для цього використовуються різні методи перевірки на помилки, такі як контрольна сума або циклічний код для перевірки на помилки.

Адресація: шар передачі даних використовує фізичні (або МАН) адреси для ідентифікації відправника та одержувача кожної рамки, що дозволяє чітко встановити напрямок доставки даних.

Контроль потоку: шар передачі даних може застосовувати техніки контролю потоку, щоб переконатися, що відправник не перевантажує одержувача, надсилаючи дані занадто швидко.

Відповідальність шару передачі даних за надійну, організовану та контрольовану передачу даних між пристроями в мережі має критичне значення.

3. Третій шар моделі OSI, відомий як мережевий шар, відіграє вирішальну роль в процесі мережевого обміну. Він забезпечує розподіл даних між різними мережами і контролює розподіл та направлення пакетів даних. Основні обов'язки мережевого шару перераховано нижче.

Визначення адрес: шар три використовує систему логічної адресації для встановлення відправника та отримувача кожного пакета даних. В контексті Інтернету, це зазвичай здійснюється за допомогою IP-адрес.

Розподіл маршрутів: мережевий шар забезпечує маршрутизацію пакетів між різними мережами. Маршрутизатори, що працюють на цьому рівні, визначають оптимальний шлях для кожного пакета.

Керування мережею: шар 3 також може мати вбудовані механізми для керування мережею, включаючи контроль над засобами зв'язку та регулювання пропускної здатності.

Фрагментація: у випадку, коли пакет даних занадто великий для передачі в певній мережі, мережевий шар може розділити його на більш менші пакети, які потім можуть бути зібрані назад при отриманні.

Захист: мережевий шар може включати інструменти безпеки, такі як фільтрація пакетів і захист від несанкціонованого доступу.

Головним протоколом на мережевому шарі є Internet Protocol (IP), хоча також використовуються і інші протоколи, такі як IPX (Internetwork Packet Exchangд) і AppleTalk.

4. Шар чотири моделі OSI, відомий як транспортний шар, відповідає за забезпечення надійного обміну даними між системами. Цей шар забезпечує з'єднання від кінця до кінця.

Нижче описано деякі ключові ролі транспортного шару.

Регулювання потоку: шар використовує механізми для керування потоком даних, щоб запобігти перевантаженню одержувача від відправника, який передає дані занадто швидко.

Створення з'єднання: транспортний шар також має на собі завдання встановлення, контролю та розриву сесій з'єднання між відправником і одержувачем.

Сегментація даних: дані, отримані від верхніх шарів, розбиваються на менші блоки, відомі як сегменти, перед їхньою передачею до нижчих шарів.

Забезпечення доставки: транспортний шар забезпечує достовірну доставку, використовуючи підтвердження та повторні передачі.

Мультикастинг: цей шар може також допомогти у реалізації мультикастингу за допомогою таких протоколів, як UDP.

Два основних протоколи, що використовуються на транспортному шарі, це TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP забезпечує надійність та впорядкованість передачі даних, тоді як UDP фокусується на швидкості без гарантії доставки.

5. Сеансовий шар, він же 5-й шар в моделі OSI, бере на себе функції управління комунікаційними сеансами між програмами. Цей шар дозволяє програмам, що розташовані на різних комп'ютерах, встановлювати, контролювати та завершувати з'єднання.

Далі описано відмінні властивості сеансового шару.

Створення сеансів: сеансовий шар регулює процес створення сеансів між двома процесами, які збираються обмінятися інформацією.

Нагляд за сеансами: цей шар також контролює обмін даними під час сеансу, регулюючи потік даних між двома процесами.

Закінчення сеансів: сеансовий шар займається завершенням сеансів, що включає в себе відпуск всіх ресурсів, використаних під час сеансу.

Обробка виключних ситуацій: цей шар також може впоратися з деякими виключеннями, що виникають під час сеансу. Наприклад, у випадку перервання з'єднання через неполадки в мережі, сеансовий шар може намагатися відновити з'єднання.

Синхронізація інформації: для великих об'ємів переданої інформації сеансовий шар може створювати контрольні точки або "точки синхронізації" в даних. Якщо передача перебивається, системи можуть продовжити передачу від останньої контрольної точки, замість повторення передачі з самого початку.

Мультикаст та дуплексні передачі: сеансовий шар здатний організовувати мультикаст-трансляції, коли дані розсилаються одночасно до багатьох вузлів, а також дуплексні передачі, де дані можуть обмінюватися в два боки одночасно.

Контроль діалогу: сеансовий шар визначає, хто з учасників комунікації має право передавати дані в конкретний момент часу.

Варто зазначити, що деякі інтернет-протоколи, такі як TCP/IP, не мають вираженого сеансового шару. В таких моделях функції, які зазвичай виконує сеансовий шар, зазвичай переносяться на транспортний шар.

6. Шар подання в моделі OSI, який знаходиться на шостій позиції, відіграє важливу роль у форматуванні та кодуванні даних перед їхнім пересиланням по мережі.

Основні ролі шару розписані нижче.

Модифікація даних: шар подання перетворює дані з вихідного формату, який використовує програма, в такий формат, який можна передати по мережі. Цей процес також здійснюється у зворотному порядку при отриманні даних.

Кодування і декодування: шар подання відповідає за кодування даних для ефективного пересилання та їхнє декодування при отриманні.

Серіалізація важких структур даних: шар подання здатний серіалізувати складні структури даних у потік байтів для пересилання та виконувати зворотній процес при отриманні.

Шифрування і дешифрування: шар подання може зашифровувати дані для забезпечення їхньої приватності та дешифрувати їх при отриманні.

Стиснення даних: для підвищення ефективності передачі, шар подання може стискати дані перед відправкою та розпаковувати їх при прийманні.

В цілому, шар подання створює зв'язок між форматами даних, які використовуються додатками, і форматами, що використовуються для передачі даних по мережі. Він забезпечує коректне розуміння даних обома сторонами в процесі комунікації.

7. Сьомий шар моделі OSI, або аплікаційний шар, служить мостом між програмами користувача та мережевими службами, з якими вони взаємодіють. Він забезпечує взаємодію між програмами, розташованими на користувацькому обладнанні, та мережею.

Основними функціями аплікаційного шару будуть наступні пункти.

Взаємодія з програмами: аплікаційний шар безпосередньо зв'язується з програмами, що використовують мережеві служби, такі як веб-браузери, електронна пошта та інші мережеві програми.

Послуги мережевих служб: аплікаційний шар забезпечує широкий спектр мережевих служб для програм. Це може включати підтримку HTTP для веб-браузерів, SMTP для служб електронної пошти, FTP для передачі файлів і т.д.

Визначення та авторизація: аплікаційний шар може надавати сервіси розпізнавання та авторизації для контролю доступу до мережевих ресурсів.

Координація сеансів: аплікаційний шар також може узгоджувати сеанси спілкування між різними додатками.

Хоча аплікаційний шар має таку назву, він не включає в себе власні програми користувача; натомість він надає послуги, які допомагають цим додаткам ефективно використовувати мережеві ресурси [5].

Однією з ключових особливостей моделі OSI є вимога, що кожен шар може спілкуватися тільки з шаром, який знаходиться безпосередньо над ним або під ним. Дані переміщуються від шару до шару, проходячи всі шари, починаючи від аплікаційного шару на відправнику та завершуючи фізичним шаром. На стороні отримувача цей процес повторюється в оберненому порядку.

Ця модель слугує інструментом для розуміння роботи мереж та полегшення процесу розробки та налагодження мережевих протоколів. Однак варто пам'ятати, що багато сучасних мережевих протоколів не притримуються строгої послідовності моделі OSI, але використовують її як основний орієнтир.

1.5 Комплексні системи цифрового захисту інформації

Системи цифрової захисту інформації включають в себе асортимент технологій, методик та політик, які задіяні в охороні даних, що знаходяться в електронному вигляді. Основна ціль цих систем полягає в забезпеченні інформації від неправомірного доступу, експлуатації, витоку, порушення, альтерації, перегляду, запису чи вилучення.

1.5.1 Система SIEM

Системи управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) відіграють критичну роль в сфері кібербезпеки. Їх основна мета полягає в об'єднанні, інтерпретації та реагуванні на різноманітні події безпеки, що відбуваються в мережевому середовищі організації.

Далі наведені основні елементи SIEM.

Інтеграція та об'єднання інформації: SIEM-системи керують логами та іншими даними про безпеку, що надходять з різних джерел у мережі, зокрема від серверів, мережевих пристроїв, систем протидії вторгненням, антивірусних програм та інших.

Співставлення та обробка даних: зібрані дані проходять через процес кореляції та аналізу в системі SIEM. Це означає, що SIEM аналізує різні події, шукаючи збіги або зв'язки, які можуть вказувати на можливу небезпеку або вторгнення. Наприклад, несподівано висока кількість запитів до певного сервера може свідчити про можливу DDoS-атаку.

Автоматичний відгук: якщо SIEM виявляє потенційну загрозу, він може автоматично вжити заходів для її усунення. Це може означати ізоляцію потенційно вразливого ресурсу, блокування IP-адреси або навіть активацію процедур відновлення.

Сповіщення та звітність: SIEM також здатний інформувати адміністраторів про виявлені загрози, а також створювати докладні звіти про події безпеки для подальшого аналізу та відповідності регулятивним вимогам.

Системи управління інформацією та подіями безпеки (SIEM) відіграють значущу роль у сфері кібербезпеки, надаючи організаціям можливість відстежувати свої мережі та системи в режимі реального часу, ефективно виявляючи та реагуючи на небезпеки. Інтеграція з різними системами безпеки: SIEM-системи можуть співпрацювати з різними інструментами та системами безпеки, такими як системи протидії вторгненням, антивірусні захисти, фаєрволи та інше. Така співпраця дозволяє SIEM обробляти більший обсяг даних і краще розуміти контекст можливих загроз.

Дотримання нормативних вимог: велика кількість організацій мають відповідати вимогам, які стосуються зберігання та аналізу логів безпеки. SIEM допомагає задовольнити ці вимоги, надаючи централізоване збереження логів та інструменти для обробки цієї інформації.

Покращення роботи команди безпеки: автоматизація та централізація, які надає SIEM, можуть значно покращити роботу команди безпеки,

дозволяючи їм оперативно виявляти, досліджувати та реагувати на події безпеки [6].

Підсумовуючи, SIEM є важливим інструментом, який допомагає організаціям виявляти, досліджувати та реагувати на різні загрози безпеки в їх мережах та системах.

1.5.2 Система виявлення вторгнень

Система виявлення вторгнень (Intrusion Detection System, IDS) - це інструмент безпеки, розроблений для автоматичного виявлення спроб проникнення або шкідливої діяльності в мережі чи комп'ютерній системі. Ці системи спостерігають за трафіком, діями користувачів та системними подіями, аналізують їх на наявність порушень безпеки та повідомляють про можливі загрози. IDS поділяються на дві основні категорії описані нижче.

1. Мережеві системи виявлення вторгнень (Network-based Intrusion Detection System, NIDS): належать до видів систем виявлення вторгнень (IDS) та спеціалізуються на аналізі мережевих потоків. NIDS контролюють та досліджують увесь мережевий трафік, який проходить крізь визначені мережеві точки, де вони розташовані. Ці системи можуть виявляти різні атаки чи шкідливі дії, такі як перевірка портів, DoS-атаки, віруси та інші загрози безпеки.

Основні особливості NIDS розписано далі.

Спостереження за мережевим трафіком: NIDS досліджують весь мережевий трафік, що проходить крізь певні мережеві вузли, такі як роутери, комутатори або фаєрволи. Це дозволяє виявляти загрози, які можуть впливати на кілька систем або проникати в мережу із зовнішніх джерел.

Аналіз атак за сигнатурами: NIDS використовують аналіз сигнатур для порівняння поточного мережевого трафіку з відомими шаблонами атак. Якщо виявлено збіг, система позначає відповідний трафік як підозрілий та повідомляє адміністратора безпеки.

Аналіз аномалій: NIDS також можуть застосовувати аналіз відхилень для виявлення незвичайних або аномальних моделей поведінки в мережевому трафіку. Це допомагає виявляти нерозпізнані атаки або нові варіанти відомих загроз.

Активні та пасивні методи реагування: NIDS можуть бути налаштовані для відповіді на виявлені загрози, застосовуючи активні чи пасивні підходи. У активному режимі NIDS здатні здійснювати заходи, спрямовані на блокування або припинення шкідливої діяльності, такі як розірвання з'єднання, налаштування фаєрвола або надсилання сповіщення адміністратору. У пасивному режимі NIDS контролюють трафік та виявляють неправильні дії, але не вживають прямих заходів, а сповіщають адміністратора безпеки, який потім може вирішити, як відреагувати на загрозу.

Взаємодія з іншими безпековими системами: З метою забезпечення більшої ефективності NIDS можуть інтегруватися з іншими безпековими системами, такими як фаєрволи, системи контролю доступу, антивіруси та системи виявлення вторгнень з орієнтацією на хости. Це дає можливість створити єдину систему оборони, яка забезпечує кращий захист організації від загроз.

Масштабування: NIDS можуть масштабуватися від дрібних офісних мереж до великих корпоративних мереж з тисячами користувачів. Це робить їх адаптивними та гнучкими до різних розмірів та вимог організацій.

Протоколювання та формування звітів: NIDS збирають дані про виявлені атаки та неправильні дії та можуть створювати докладні звіти про стан безпеки мережі.

Реакція на виявлені загрози: хоча NIDS здатні виявляти шкідливу діяльність, зазвичай вони не мають можливостей для вирішення питань безпеки. Адміністраторам та безпековим експертам необхідно відповідати на отримані сповіщення та вживати заходів для усунення безпекових проблем. Це може включати відновлення пошкоджених систем, зміну конфігурації фаєрволів, виявлення та вилучення вірусів або інших шкідливих програм.

Пристосування до нових загроз: зловмисники неперервно розробляють нові методи атак та виявляють способи оминають системи безпеки, включаючи NIDS. Компаніям необхідно систематично оновлювати свої системи виявлення вторгнень, щоб вони могли виявляти та реагувати на нові загрози та уразливості.

Незважаючи на ці виклики та обмеження, мережеві системи виявлення вторгнень продовжують бути цінним та важливим засобом забезпечення мережевої безпеки. Вони допомагають організаціям виявляти загрози, інформувати про можливі вторгнення та вживати необхідних заходів для захисту своїх мереж та інформації.

2. Системи виявлення вторгнень на основі хостів (Host-based Intrusion Detection System, HIDS): є системами виявлення вторгнень, які фокусуються на спостереженні за активністю на конкретному комп'ютері або сервері. Вони встановлюються безпосередньо на цільових системах, забезпечуючи захист на рівні окремих пристроїв, таких як робочі станції, сервери або мобільні пристрої.

HIDS використовують такі методи для спостереження та виявлення потенційних загроз які наведено нижче.

Аналіз системних логів: HIDS стежать за системними журналами для виявлення неавторизованої активності, як-от спроби доступу до файлів, невдалі спроби входу та зміни в системній конфігурації.

Перевірка цілісності файлів: HIDS контролюють цілісність системних файлів, виявляючи несанкціоновані зміни, які можуть свідчити про вторгнення чи наявність шкідливого ПЗ.

Спостереження за процесами: HIDS відстежують активні процеси в системі, виявляючи можливі зловмисні програми або незвичайну активність, що може свідчити про атаку.

Перевірка конфігурації системи: HIDS здатні аналізувати системні налаштування щодо наявності потенційних вразливостей або ризикованих конфігурацій.

Контроль доступу: HIDS можуть відстежувати спроби доступу до системи, виявляючи неавторизовані спроби доступу та спроби отримання вищих привілеїв.

Розпізнавання атак за сигнатурами: HIDS можуть застосовувати бази даних з відомими атаками для виявлення шкідливої діяльності, такої як віруси, троянські коні або інші зловмисні програми. Вони порівнюють поточну активність системи з раніше відомими шаблонами атак для прискореного виявлення.

Виявлення відхилень: HIDS можуть використовувати алгоритми машинного навчання чи статистичні моделі для виявлення незвичайної поведінки або активності, яка відступає від типових поведінкових моделей.

Аналіз поведінки: HIDS можуть досліджувати поведінку користувачів та застосунків для виявлення підозрілої активності або відхилень від звичайних дій, які можуть свідчити про атаку.

Відповідь на інциденти: окрім виявлення, HIDS також можуть автоматично вживати заходів щодо виявлених загроз, блокуючи доступ, змінюючи паролі, відключаючи мережеве з'єднання або вживаючи інші дії для забезпечення безпеки.

Системи виявлення вторгнень на рівні хоста доповнюють мережеві системи виявлення вторгнень та інші засоби безпеки для створення комплексної та ефективної системи захисту. Вони можуть надавати більш детальний огляд активності на рівні хоста та допомагати фахівцям з безпеки краще розуміти та реагувати на загрози, які можуть впливати на окремі системи та користувачів [7].

1.5.3 Система протидії вторгнень

Система протидії вторгнень (Intrusion Prevention System, IPS) є розвитком та вдосконаленням системи виявлення вторгнень IDS. Відмінність IPS полягає в тому, що вона активно блокує та запобігає проникненню та

шкідливим діям в мережі або комп'ютерній системі, а не лише виявляє можливі атаки.

Далі наведено основні функції IPS.

Спостереження: IPS безперервно відстежує мережевий трафік, дії користувачів та системні події, перевіряючи їх на порушення безпеки та потенційні загрози.

Виявлення: IPS застосовує різноманітні методи виявлення, такі як ідентифікація атак за сигнатурами, виявлення непередбачуваної поведінки та аналіз поведінки, для виявлення шкідливої активності.

Протидія: на відміну від IDS, який лише виявляє та сповіщає про можливі атаки, IPS активно запобігає проникненню та шкідливим діям. Це може передбачати блокування атаки в реальному часі, модифікацію налаштувань безпеки, оновлення правил фаєрволу та інші захисні дії.

Реагування на інциденти: IPS може також відповідати на виявлені загрози, наприклад, надсилати сповіщення адміністратору безпеки, від'єднуючи можливо уразливий пристрій від мережі або запускаючи процес відновлення системи.

Мережеві системи протидії вторгненням - є розвитком та вдосконаленням мережевих систем виявлення вторгнень. Заснована на відстеженні мережевого трафіку, NIPS не тільки ідентифікує можливі атаки, але й активно зупиняє та відвертає вторгнення та шкідливу діяльність у мережі.

Основні функції NIPS описані нижче.

Спостереження: NIPS безперервно вивчає мережевий трафік, перевіряючи його на предмет зловмисних атак або порушень безпеки.

Виявлення: NIPS застосовує різні методи виявлення, такі як аналіз сигнатур, виявлення неправильностей та поведінковий аналіз, для виявлення шкідливої діяльності та спроби проникнення.

Протидія: NIPS активно зупиняє та відвертає вторгнення, блокуючи атаки, змінюючи налаштування безпеки, оновлюючи правила фаєрволів та вживаючи інші заходи безпеки в реальному часі.

Реагування на інциденти: NIPS може автоматично відгукнутися на виявлені загрози, такі як інформування адміністраторів безпеки, відключення скомпрометованих пристроїв від мережі або навіть ініціювання відновлення системи.

NIPS може працювати разом з HIDS та іншими системами безпеки для створення більш комплексної та ефективної системи захисту. Така взаємодія дозволяє адміністраторам безпеки краще розуміти та відповідати на загрози, виявляти атаки в реальному часі та попереджати можливі порушення безпеки.

Системи протидії вторгненням зосереджені на хостах (Host-based Intrusion Prevention System, HIPS): системи протидії вторгненням, орієнтовані на хости представляють собою вдосконалені та розвинені системи виявлення вторгнень орієнтовані на хости HIDS. HIPS зосереджується на спостереженні та нейтралізації загроз на рівні індивідуальних комп'ютерів чи серверів, слідкуючи за діями операційних систем, застосунків та файлів.

Далі описано основні можливості HIPS.

Спостереження: HIPS неперервно відслідковує активність на ПК або серверах, досліджуючи дії користувачів, операційних систем, програм та файлів щодо порушень безпеки або потенційних загроз.

Виявлення: HIPS застосовує різні методи розпізнавання, такі як аналіз сигнатур, виявлення неправильностей та аналіз поведінки, для розкриття зловмисної активності та спроб проникнення на рівні хости.

Превентивні заходи: на відміну від HIDS, який виявляє та інформує про можливі атаки, HIPS активно перешкоджає проникненню та негативній діяльності. Це може включати блокування атак у реальному часі, модифікацію налаштувань безпеки, оновлення правил мережевого екрану та інші хост-орієнтовані заходи захисту.

Реагування на інциденти: HIPS також може відгукатися на виявлені загрози, наприклад, надсилаючи сповіщення адміністратору безпеки, від'єднуючи потенційно скомпрометований пристрій від мережі або ініціюючи процес відновлення системи.

HIPS може співпрацювати з NIPS та іншими захисними системами для створення більш узагальненої та ефективної системи оборони. Інтеграція HIPS з NIPS та іншими засобами безпеки, такими як мережеві екрани та системи управління подіями безпеки (SIEM), забезпечує розширений та глибший захист інформації та мережі.

Взаємодія між HIPS та іншими захисними системами дозволяє фахівцям з безпеки краще розуміти та відгукуватися на загрози, виявляти атаки в режимі реального часу та попереджати можливі порушення безпеки. Використання HIPS дозволяє контролювати віддалені пристрої та захищати їх від загроз, сприяючи поліпшенню загальної безпеки мережі та даних.

Проте варто відзначити, що HIPS може спричинити додаткове навантаження на ресурси хоста, оскільки вони безперервно стежать і аналізують активність на індивідуальних комп'ютерах або серверах. Важливо знайти рівновагу між потребами у ресурсах та безпеці, а також налаштувати правила та параметри HIPS для мінімізації можливого впливу на ефективність системи.

Загалом, HIPS є важливим засобом у комплекті мережевої безпеки, який доповнює NIPS та інші захисні системи для забезпечення більш глибокого захисту від проникнень та зловмисної діяльності.

Бездротові системи протидії вторгненням (Wireless Intrusion Prevention System, WIPS): бездротові системи запобігання вторгненням - це спеціалізовані системи захисту, розроблені для виявлення, недопущення та відповіді на різні загрози, пов'язані з бездротовими мережами. Вони відстежують радіочастотний діапазон та аналізують бездротовий мережевий трафік з метою виявлення аномальної активності, неавторизованого доступу та інших форм шкідливої дії.

Основні характеристики WIPS наведено далі.

Спостереження: WIPS неперервно контролює радіочастотний діапазон та бездротовий мережевий трафік, виявляючи зміни у сигналі, неперервні спроби з'єднання та інші аномалії, які можуть свідчити про зловмисну дію.

Виявлення: WIPS застосовує різні методи для виявлення можливих атак, несанкціонованих пристроїв та різних видів шкідливої активності у бездротовій мережі, такі як аналіз сигнатур, виявлення аномалій та аналіз поведінки.

Профілактика: WIPS активно блокує та запобігає вторгненням та зловмисним діям, зокрема забороняє зловмисникам підключатися до мережі, автоматично змінює параметри безпеки або відключає скомпрометовані точки доступу.

Відповідь на інциденти: WIPS може автоматично відповідати на виявлені загрози, інформуючи адміністраторів безпеки, ізолюючи пошкоджені пристрої або навіть ініціюючи процедури відновлення системи.

Документування: WIPS надає звіти про виявлені загрози, інциденти та вжиті заходи для їх усунення. Це дозволяє керівникам безпеки аналізувати тенденції, виявляти вразливі місця в мережі та підвищувати рівень безпеки бездротових мереж.

Управління безпековими політиками: WIPS надає можливість керівникам безпеки встановлювати та керувати безпековими політиками для бездротових мереж, забезпечуючи відповідність корпоративним нормам та регулятивним вимогам.

WIPS може співпрацювати з HIPS, NIPS та іншими системами захисту для розробки більш інтегрованої та ефективної системи безпеки. Інтеграція WIPS з іншими безпековими інструментами гарантує широкий та всебічний захист даних та мережі, а також допомагає керівникам безпеки краще розуміти та реагувати на загрози, виявляти атаки в реальному часі та уникати можливих порушень безпеки.

Загалом, WIPS є значущим засобом у комплекті мережевої безпеки, який доповнює HIPS, NIPS та інші системи захисту для забезпечення більш ретельного захисту від вторгнень та зловмисної діяльності у бездротових мережах.

Системи протидії вторгненням на рівні додатків (Application-based Intrusion Prevention System, AIPS): представляють собою спеціалізовані системи безпеки, які зосереджуються на захисті від атак, орієнтованих на програми та служби, що працюють на серверах та комп'ютерах. Вони аналізують додатковий трафік, щоб виявити незвичайні шаблони, неправильний доступ та різні види шкідливих дій, які можуть створювати ризик для додатків та даних користувачів.

Ключові можливості AIPS являють собою наведені нижче.

Виявлення: AIPS застосовує різноманітні методи виявлення, такі як аналіз відбитків, виявлення відхилень та аналіз поведінки, для розпізнавання потенційних атак, націлених на програми та служби. Вони також можуть виявляти уразливості та проблеми в налаштуваннях додатків.

Профілактика: AIPS активно відсікає та усуває вторгнення та небезпечні дії на рівні додатків, автоматично приймаючи заходи для захисту від атак, такі як блокування зловмисників, зміна параметрів безпеки або відключення пошкоджених програм.

Реагування на інциденти: AIPS може автоматично відгукнутися на виявлені небезпеки, інформуючи адміністраторів безпеки, ізолюючи зіпсовані програми або вводячи процедури відновлення.

Управління політиками безпеки: AIPS надає можливість адміністраторам безпеки визначати та керувати політиками безпеки для програм, забезпечуючи відповідність корпоративним нормам та законодавчим вимогам. Відзначення результатів: AIPS надає інформацію про виявлені загрози, інциденти та дії, прийняті для їх ліквідації на рівні програм. Це дозволяє адміністраторам безпеки вивчати тенденції, виявляти вразливі місця в програмах та покращувати загальний рівень захисту програм та даних.

AIPS може співпрацювати з HIPS, NIPS, WIPS та іншими системами безпеки для створення універсальної та ефективної системи захисту. Інтегруючи AIPS з іншими інструментами безпеки, можна досягти більш широкого та глибокого захисту інформації та мережі, а також допомогти адміністраторам безпеки краще розуміти та відповідати на загрози, виявляти атаки в режимі реального часу та уникати можливих порушень безпеки.

Загалом, AIPS є значним інструментом в арсеналі мережевої безпеки, що доповнює HIPS, NIPS, WIPS та інші системи безпеки для надання більш глибокого захисту від небезпечних дій та вторгнень на рівні програм [8].

Інтеграція системи протидії вторгненням (IPS) з системою виявлення вторгненням та іншими засобами безпеки, такими як фаєрволи та системи управління безпековими подіями (SIEM), може забезпечити більш всеосяжний та детальний захист інформації та мережі. Вони допомагають адміністраторам безпеки краще розуміти та відповідати на загрози, виявляти атаки в реальному часі та попереджати можливі порушення безпеки.

2 АНАЛІЗ МОЖЛИВИХ ЗАГРОЗ ТА ІНСТРУМЕНТИ ПРОТИДІЇ

2.1 Аналіз загроз

Існують різні типи загроз викрадення інформації в ІТ-офісі. Наприклад:

- кібератаки;
- соціальний інжиніринг;
- фізичний доступ;
- недбалість співробітників;
- помилки в програмному забезпеченні.

Кібератака - це будь-яка спроба несанкціонованого доступу до комп'ютерних систем, мережі, баз даних або іншої інформації, яка зберігається на комп'ютерах або інших пристроях в офісі з метою отримання конфіденційної інформації, шкоди компанії або витоку даних.

Кібератаки можуть бути різних типів, таких як віруси, черви, троянські програми, фішинг, DDoS-атаки та інші. Хакери можуть використовувати ці методи, щоб зламати системи безпеки та отримати доступ до конфіденційної інформації, такої як фінансові дані, інтелектуальна власність, персональні дані користувачів та інші.

Кібератаки можуть призвести до серйозних наслідків для компанії, таких як витрати на відновлення систем, втрата даних та інформації, порушення довіри клієнтів та інших зацікавлених сторін, а також можуть призвести до великих фінансових втрат. Тому важливо забезпечити належний рівень безпеки та захисту в ІТ-офісі та бути готовими до можливих кібератак[9].

Соціальний інжиніринг - це метод атак, який полягає в маніпулюванні людською поведінкою з метою отримання доступу до конфіденційної інформації. Це може бути використано хакерами та зловмисниками, які хочуть отримати доступ до важливих даних або системи компанії.

Цей метод може включати в себе використання соціальних мереж, електронної пошти, телефонних дзвінків, фізичного доступу та інших способів, щоб переконати людей розкрити конфіденційну інформацію або виконати дії, які дозволяють зловмисникам отримати доступ до системи.

Наприклад, зловмисники можуть надіслати спам-листи або фішингові повідомлення, що містять лінки на підроблені сторінки, які виглядають так само, як сторінки компанії, і спонукають користувачів ввести свої логіни та паролі. Зловмисники також можуть використовувати соціальні мережі для переслідування співробітників та збирання даних про них, які можуть бути використані для атак на компанію [10].

Несанкціонований фізичний доступ - це ситуація, коли неповноважені особи отримують доступ до фізичної інфраструктури компанії, такої як комп'ютери, сервери, мережеве обладнання, документи та інше обладнання або матеріали, які містять конфіденційну інформацію [11].

Це може включати в себе використання фізичної сили, відкритих дверей, крадіжки пропусків, використання підроблених документів або інших методів для отримання доступу до областей, які повинні бути захищені.

Несанкціонований фізичний доступ може стати відкриттям дверей для кіберзлочинців та інших злочинців, які шукають шляхи отримати доступ до конфіденційної інформації компанії, або ж невірною поведінкою самого співробітника, який може привести до скомпрометування безпеки.

Причиною несанкційного доступу можуть бути не тільки особи які намагаються викрасти або нанести шкоду компанії ззовні, а й працівники цієї ж компанії.

Є декілька типів працівників, які можуть спричинити загрозу:

- зловмисники: це особи, які навмисно завдають шкоди організації з метою отримання вигоди або з інших мотивів;
- випадкові зловмисники: це особи, які ненавмисно завдають шкоди через помилки або необережність;

- скомпрометований персонал: це особи, які стали жертвами зовнішніх загроз і використовувались для отримання доступу [12].

Недбалість співробітників - це ситуація, коли працівники компанії не дотримуються правил безпеки та не беруть належних заходів для захисту конфіденційної інформації, що може призвести до порушення безпеки компанії та уразити її репутацію.

Це може бути пов'язано зі слабкими паролями, неадекватними заходами безпеки при роботі з електронною поштою, зберіганні паролів та інших конфіденційних даних на ненадійних пристроях, використанні небезпечних програм або програмного забезпечення з піратських джерел, а також іншими формами несанкціонованого використання даних.

Недбалість співробітників може бути наслідком недостатньої освіти та підготовки з питань безпеки в мережі Інтернет, відсутності в компанії чітких правил та процедур щодо захисту конфіденційної інформації, а також відсутності контролю за діяльністю працівників [13].

Помилки в програмному забезпеченні - це непередбачувані помилки, викликані дефектами в програмному коді. Помилки можуть виникати з різних причин, таких як неправильне введення даних, відсутність валідації введених даних, використання застарілих бібліотек, невірна логіка програми та інші. Помилки в програмному забезпеченні можуть призвести до некоректної роботи програми, втрати даних, вразливості програми до кібератак та інших проблем.

Недостатньо якісне програмне забезпечення може також призвести до великої кількості помилок, що збільшує ризик виникнення проблем та порушення безпеки інформації в ІТ-офісі [14].

2.2 Важливість аналізу та типи мережесих загроз

Аналіз загроз мережевої безпеки є важливим етапом в розробці і впровадженні заходів забезпечення безпеки в ІТ-офісі. Недостатній рівень

захисту може стати причиною витоку, викривленню або пошкодженню конфіденційної інформації, а також вірусних атак, витоку персональних даних користувачів та фінансових втрат. Аналіз загроз мережевої безпеки допомагає виявити потенційні проблеми та відповідні заходи безпеки, необхідні для забезпечення належного рівня безпеки в ІТ-офісі. Одержана інформація допоможе вжити заходів, щоб запобігти втратам, пов'язаним з несправністю обладнання, кіберзлочинністю, вірусними атаками або несанкціонованим доступом.

Існує декілька основних типів мережових загроз, які можуть виникнути в ІТ-офісі, такі як:

- віруси;
- відмова в обслуговуванні;
- фішинг;
- витоки даних;
- несанкціонований доступ;
- викрадення ідентичності.

2.2.1 Типи вірусів

Вірус - це програма, яка може реплікувати свою копію та розповсюджуватися між комп'ютерами, що підключені до мережі. Шкода, завдана вірусами, полягає у пошкодженні файлів, оперативної пам'яті або навіть самого операційного середовища комп'ютера.

Віруси можуть мати різноманітні форми та виконувати різні сценарії. Наприклад, деякі віруси можуть ховатися в системі, щоб уникнути виявлення антивірусним програмним забезпеченням. Інші можуть блокувати доступ до важливих файлів або програм, або вимагати викупу, щоб повернути доступ до них.

Існує декілька типів вірусів, кожен з яких може завдати різної шкоди в ІТ-офісі. Деякі з них включають:

- програмні віруси;
- бомби-віруси;
- макровіруси;
- черв'яки.

Програмні віруси представляють собою шкідливе програмне забезпечення, яке може завдати значної шкоди системі та її даним. Цей тип вірусів має різноманітні форми та методи поширення. Наприклад, віруси, що приховуються, вбудовуються в інші файли та програми, що робить їх важко виявити. Троянські програми, з іншого боку, маскуються під корисні програми та виконують зловмисні дії без відома користувача.

Ці програми можуть поширюватися різними способами, включаючи мережу Інтернет, електронну пошту та порти підключення. Вони можуть бути передані на інші комп'ютери через копіювання програм або підключення заражених USB-носіїв.

Поява програмного вірусу може призвести до різних наслідків, включаючи збір конфіденційної інформації, підміну або видалення файлів, а також зараження інших систем. Тому важливо мати антивірусне програмне забезпечення, яке допоможе запобігти зараженню комп'ютера програмними вірусами та іншими видами шкідливих програм.

Бомби-віруси, що також відомі як "логічні бомби", є видом зловмисного програмного забезпечення, яке створюється з метою виконання шкідливих дій у певний момент часу або після відповідного виклику. Ці віруси можуть мати різноманітні цілі, такі як видалення файлів, виконання злочинних дій або спричинення збоїв у роботі системи. Для створення бомб-вірусів можуть використовуватися програми-скрипти, мови програмування та інші інструменти для розробки програмного забезпечення.

Існує кілька способів зараження систем бомбами-вірусами, які часто вбудовуються в програми або файлові системи. Це може зробити виявлення цих вірусів досить складним до моменту їх активації. Крім того, віруси можуть

поширюватися через заражені веб-сторінки, електронну пошту або порти зв'язку.

Макровіруси - це віруси, що поширюються через документи з макросами, такими як Microsoft Word, Excel, PowerPoint тощо. Макрос - це набір команд, що автоматично виконуються при відкриванні документу або за певних умов.

Макровіруси можуть виконувати шкідливі дії без дозволу користувача, наприклад, вставляти шкідливий код, змінювати налаштування системи, крадіжку особистих даних, відправку шкідливих файлів іншим користувачам тощо.

Електронна пошта є одним з найпоширеніших способів поширення макровірусів. Зловмисники можуть надіслати електронне повідомлення з документом, що містить макрос, і намагатися переконати отримувача відкрити документ та дозволити виконання макросів. Також шкідливі документи можуть бути розміщені на веб-сайті з описом здавалося б безпечного вмісту, що змушує відвідувачів завантажувати його на свої комп'ютери.

Черв'яки - можуть поширюватися через комп'ютерні мережі з використанням різноманітних комунікаційних засобів, таких як електронна пошта, мережеві протоколи та флеш-накопичувачі. Зазвичай, ці віруси вбудовуються в програмне забезпечення або операційні системи, використовуючи вразливості в програмному забезпеченні, що дозволяє їм проникати у систему та поширюватися на інші комп'ютери у мережі. Також черві можуть використовувати соціальну інженерію, щоб надати користувачам інформацію, яку ті потім можуть використати для поширення вірусу.

Особливістю черв'яків є їх здатність самостійно розмножуватися та поширюватися на інші системи, що робить їх особливо небезпечними. Ці віруси можуть завдати шкоди комп'ютерній системі, знизити її продуктивність, видалити або модифікувати файли та програми, а також порушити системну безпеку [15].

Крім того, віруси можуть завдавати іншу шкоду, таку як злам користувацьких облікових записів, витік конфіденційної інформації або шифрування даних на жорсткому диску, що може призвести до втрати даних.

2.2.2 DDoS атаки

DDoS атака - це вид кібератаки, який має на меті перевантажити мережу, сервер або веб-сайт надмірною кількістю запитів. Зловмисники використовують ботнети - мережі комп'ютерів, що були заражені вірусами, щоб здійснювати атаку. Надсилання великої кількості запитів до цільового сервера під час DDoS атаки може призвести до відмови в обслуговуванні, тобто неможливості користувачів отримати доступ до веб-сайту або сервісу. Крім того, зловмисники можуть використовувати DDoS атаки як спосіб відволікти увагу від інших кібератак або для вимагання викупу. Ці атаки можуть призвести до значних втрат доходів та негативного впливу на репутацію бренду, тому вони є серйозною загрозою для бізнесу та інших організацій, які залежать від доступності своїх веб-сайтів та сервісів для користувачів.

DDoS атаки можуть бути здійснені з різних причин, наприклад, для отримання вимог викупу, з політичними мотивами або для демонстрації хакерських навичок. Ці атаки можуть бути досить складними для виявлення та запобігання, оскільки зловмисники використовують різні методи та техніки для приховування своїх слідів. Щоб захиститися від таких атак, компанії та організації вкладають значні зусилля використовуючи різноманітні технології та сервіси для виявлення та запобігання цим атакам [16].

Також варто зазначити, що не тільки великі компанії та організації можуть бути атаковані DDoS. Малий бізнес, веб-сайти та індивідуальні користувачі також можуть бути піддастися цим атакам, особливо якщо вони не мають достатнього захисту.

2.2.3 Фішинг

Фішинг - один із видів кібератак, який має на меті зламати безпеку користувача та отримати доступ до його конфіденційної інформації, такої як паролі, номери кредитних карток, особисті дані та інші. Зазвичай такі атаки проводяться через електронну пошту, соціальні мережі, месенджери, веб-сайти та інші канали комунікації. Фішинг може набувати різних форм, але зазвичай маскується під повідомлення від довіреної компанії або особи, що відома користувачеві. Зловмисники можуть надіслати лист, який виглядає, як повідомлення від банку з проханням підтвердити особисті дані, або з посиланням на вигадану проблему, що потребує негайної уваги. При відкритті листа або посилання користувач може бути перенаправлений на сайт, який маскується під довірену компанію, але насправді належить зловмисникам. На цьому сайті користувач може бути попрошений ввести свої логін та пароль, або здійснити іншу дію, що дозволить зловмисникам отримати доступ до його конфіденційної інформації. Фішинг-атаки можуть також включати в собі використання шкідливого програмного забезпечення, яке автоматично встановлюється на комп'ютері користувача при відкритті посилання або документу [17].

2.2.4 Витоки даних

Витоки даних виникають, коли чутлива інформація, яка зберігається в комп'ютерних системах або передається через Інтернет, стає доступною через невірний або неповний захист даних. Це може мати серйозні наслідки для індивідів, організацій та держав, так як витоки даних можуть бути викликані злочинністю, технічними несправностями, недбалістю або вразливостями в системах безпеки. Наприклад, злочинці можуть використовувати витоки даних для крадіжки особистої інформації, фінансових даних та інших чутливих даних. Компанії можуть зазнати шкоди внаслідок витоків

конфіденційної інформації про свої продукти, технології, бізнес-плани тощо, що може призвести до втрати довіри клієнтів та інвесторів, позовів і негативної реклами. Особисті користувачі також можуть стати жертвами витоків даних, наприклад, їх фінансові дані можуть бути викрадені та використані для крадіжки грошей, або їх особиста інформація може бути використана для злочинних цілей, таких як відкриття фальшивих банківських рахунків.

2.2.5 Несанкціонований доступ

Випадки, коли особа або програма, що не має відповідних прав, намагається отримати доступ до інформації, ресурсів або служб, є прикладом несанкціонованого доступу до системи або мережі. Це є одним із найбільших загроз, які виникають у сфері інформаційної безпеки.

Несанкціонований доступ може виявлятися в різних формах та включати наведені нижче дії.

Проникнення в мережу: нападник може використовувати різні техніки для отримання доступу до мережі, включаючи використання вразливостей у ПЗ, слабкості мережевих протоколів або використання фішингу для здобуття даних для входу.

Недозволений доступ до фізичних ресурсів: Це може включати незаконне проникнення до серверних кімнат, робочих місць або до іншого обладнання, яке містить або обробляє конфіденційні дані.

Несанкціонований доступ до інформації: Зловмисник може намагатися отримати доступ до збережених або даних, що передаються використовуючи методи, такі як перехоплення мережевого трафіку, експлуатацію вразливостей в ПЗ або крадіжку облікових даних.

Незаконне використання системи: Це відбувається, коли особа або програма використовують систему або мережу без належного дозволу,

наприклад, для проведення атак на інші системи, для розповсюдження шкідливого ПЗ або для здійснення незаконних дій.

Системи цифрового захисту даних розроблені з метою запобігання несанкціонованому доступу, використовуючи широкий спектр методів та технологій.

2.2.6 Викрадення особистої ідентичності

Викрадення особистої ідентичності означає, що зловмисники отримують доступ до особистої інформації, такої як ім'я, адреса, номер соціального страхування та інші дані, щоб вдалися за іншу людину. Це може бути здійснене шляхом крадіжки документів, використання шпигунського програмного забезпечення на комп'ютері або через фішинг.

Зловмисники можуть використати отриману інформацію для крадіжки грошей, відкриття кредитних карток, взяття під кредит на ім'я потерпілого, замовлення товарів та послуг або навіть для здійснення злочинів. Такі дії можуть призвести до значних матеріальних втрат та порушення кредитної історії потерпілого.

2.3 Аналіз загроз мережевої безпеки

У мережевій безпеці будь-яка можлива небезпека для інформації, яка передається через мережу, наприклад, віруси, хакерські атаки, крадіжка даних, фішинг тощо. У сфері ІТ-офісу має місце неперервна передача даних, тому важливо бути усвідомленим щодо можливих загроз та дізнатися, як їх попередити.

Всі перераховані у розділі 3.1 типи загроз можуть являти собою потенційну загрозу для ІТ-компанії.

Залежно від вірогідності та наслідків для мережі та інфраструктури ІТ-офісу, можливо оцінити рівень небезпеки кожної з цих загроз. Наприклад,

небезпечність загроз, таких як атаки на паролі та несанкціонований доступ до системи, може бути високою, оскільки вони можуть призвести до доступу до конфіденційної інформації, втрати даних та матеріальних збитків. У той же час, нестабільність мережевої інфраструктури може бути менш ризикованою загрозою, але вона може призвести до значних перерв у роботі та втрати продуктивності [18].

Окрім перерахованих загроз мережеві пристрої, такі як маршрутизатори, комутатори та фаєрволи, можуть бути піддані атакам з боку зловмисників, які можуть намагатися зламати їх для перехоплення мережевого трафіку, внесення змін у налаштування мережі або відправки шкідливих пакетів даних. Ризик таких загроз може бути значним, оскільки від атак на мережеві пристрої може залежати працездатність мережі, що може спричинити серйозні проблеми в роботі IT-офісу.

2.4 Критичні ділянки та ризики

Критичні ділянки представляють собою складові системи, які відзначаються особливою вразливістю до можливих загроз мережевої безпеки. Вони є важливими для забезпечення функціонування системи та бізнес-процесів компанії і можуть мати значний вплив на них. Критичні ділянки можуть включати такі компоненти системи, як сервери, мережевий периметр, мережеві пристрої, а також інші складові, на яких зберігаються та обробляються конфіденційні дані. Захист критичних ділянок від можливих загроз та відновлення їх у разі компрометації вимагає вживання додаткових заходів безпеки та моніторингу.

Однією з ділянок, яка може бути критичною, є зовнішня мережа IT-офісу, яка може бути піддається хакерським атакам та іншим загрозам. Якщо цей периметр не буде захищений відповідними заходами безпеки, це може призвести до порушення конфіденційності, цілісності та доступності даних.

Ще однією критичною ділянкою є сервери, на яких зберігається конфіденційна інформація. Якщо сервери не будуть захищені відповідними заходами безпеки, можливість несанкціонованого доступу до них може призвести до витоку конфіденційної інформації та втрати даних.

Також критичною може стати мережева інфраструктура, зокрема маршрутизатори, комутатори та фаєрволи. Якщо зловмисники отримають несанкціонований доступ до цих пристроїв, вони можуть внести зміни в налаштування мережі, відправляти шкідливі пакети даних або перехоплювати мережевий трафік. Це може призвести до повного зупину мережі та серйозно нашкодити роботі IT-офісу.

Ризики мережевої безпеки включають потенційні наслідки, які можуть виникнути у разі виявлення загроз для безпеки мережі. Такі наслідки можуть бути різного характеру, включаючи фінансові втрати, збитки від відновлення системи, втрату важливих даних або негативний вплив на репутацію компанії.

2.5 Заходи та інструменти щодо запобігання загроз мережевої безпеки в IT-офісі

Щоб запобігти загрозам мережевої безпеки в IT-офісі, необхідно приймати ряд заходів. Один з найважливіших заходів - це захист мережі та інфраструктури. Для цього можна використовувати багато різних інструментів та технологій.

Фаєрвол. Програмне або апаратне забезпечення, яке контролює трафік в мережі, фільтрує його та забезпечує безпеку мережі від можливих загроз - так можна описати фаєрвол. В залежності від призначення та місця встановлення, фаєрволи можуть бути різних типів, видів і способів встановлення.

Апаратні фаєрволи, які є конкретними пристроями, діють як вартів безпеки між внутрішньою мережею (наприклад, мережею організації) та зовнішнім світом (наприклад, Інтернет). Їх розміщують у мережевому

коридорі для аналізу вхідного та вихідного трафіку на основі визначених правил безпеки.

Нижче наведено декілька основних обов'язків, які виконують апаратні фаєрволи.

Фільтрування пакетів: вони перевіряють кожен пакет даних, що пройшов через них, щоб визначити, чи відповідає він встановленим критеріям. Якщо пакет даних відповідає критеріям, його можна пропустити. В іншому випадку його блокують.

Відслідковування стану з'єднань: апаратні фаєрволи можуть слідкувати за активними мережевими з'єднаннями і переконатися, що вхідний трафік є відповідним для відомих з'єднань. Це допомагає відсіяти непередбачуваний або небезпечний трафік.

Підтримка VPN: деякі апаратні фаєрволи мають інтегровану підтримку віртуальних приватних мереж, що дозволяє забезпечити безпечне з'єднання між віддаленими користувачами або мережами.

Забезпечення розподілу навантаження та відмовостійкості: у більш передових системах апаратні фаєрволи можуть також надавати функції розподілу навантаження та відмовостійкості для обробки великого обсягу трафіку та забезпечення неперервної роботи.

Апаратні фаєрволи зазвичай використовуються в комерційних умовах, де вимагається високий ступінь захисту та здатність обслуговувати великі потоки мережевого трафіку. Зазвичай вони потребують професійного налаштування та керування, але можуть забезпечити значно більший рівень безпеки порівняно з програмними фаєрволами.

Однією з важливих переваг апаратних фаєрволів є їхня висока продуктивність. Вони можуть обробляти значно більші потоки трафіку в порівнянні з програмними фаєрволами, з мінімальним впливом на продуктивність системи.

До того ж, апаратні фаєрволи можуть включати додаткові функції безпеки (такі як системи виявлення вторгнень, системи запобігання вторгненням (IPS), антивірусні сканувачі та фільтрацію веб-вмісту).

Варто відзначити, що вибір між апаратним та програмним фаєрволом часто визначається конкретними вимогами та обставинами. Наприклад, для домашнього користувача або малого підприємства програмний фаєрвол може бути більш економічно ефективним рішенням, тоді як велика корпорація з великим обсягом мережевого трафіку може отримати більше вигоди від використання апаратного фаєрвола.

Програмні фаєрволи - це додатки, що встановлюються на комп'ютер або інший пристрій і слідкують за мережевим трафіком, регулюючи його. Вони виконують функції, схожі на апаратні фаєрволи, але на рівні програмного забезпечення. Вони широко використовуються в приватних будинках та малому бізнесі через свою простоту налаштування і менші витрати порівняно з апаратними фаєрволами.

Основні аспекти програмних фаєрволів включають наведені нижче параметри.

Фільтрація пакетів: програмні фаєрволи вивчають пакети даних, які проходять через мережевий інтерфейс, перевіряючи, чи вони відповідають встановленим критеріям безпеки. Якщо пакет відповідає правилам, його допускають; в протилежному випадку, він блокується.

Слідкування за з'єднаннями: програмні фаєрволи мають можливість відслідковувати активні мережеві з'єднання та переконатися, що вхідний трафік відповідає відомим сесіям з'єднання. Це допомагає відсікти непотрібний або шкідливий трафік.

Контроль на рівні застосунків: програмні фаєрволи, як правило, дають користувачам можливість встановлювати правила, які спеціалізуються на конкретних програмах, регулюючи їх доступ до мережі на рівні конкретного додатка.

Легкість в налаштуванні та керуванні: програмні фаєрволи, як правило, мають дружній до користувача інтерфейс, що дозволяє користувачам легко налаштовувати та управляти правилами безпеки.

Незважаючи на певні переваги, програмні фаєрволи також мають свої обмеження. Вони можуть погіршити продуктивність системи, використовуючи системні ресурси (ЦП, пам'ять тощо) для аналізу та обробки мережевого трафіку. Більш того, вони можуть стати уразливими до атак, якщо сама система постраждає, оскільки вони працюють на тому ж рівні, що й інші програми.

Ще однією суттєвою відмінністю є те, що програмні фаєрволи переважно контролюють вхідний трафік, а не вихідний. Це означає, що вони можуть бути менш ефективними у блокуванні шкідливого вихідного трафіку, наприклад, коли шпигунський застосунок намагається надіслати зібрані дані на віддалений сервер.

Враховуючи всі вищезгадані аспекти, програмні фаєрволи є важливим засобом захисту для багатьох користувачів і середовищ, але найкраще використовувати їх разом з іншими заходами безпеки, такими як антивірусні програми, додатки для виявлення вторгнень та освіта користувачів.

Фаєрволи використовуються в різних операційних системах для контролю та захисту мережевого трафіку. Як апаратні, так і програмні фаєрволи можуть бути використані з різними операційними системами, але програмні фаєрволи часто вбудовані безпосередньо в операційну систему.

Windows має вбудований фаєрвол, який називається Windows Firewall. Він дозволяє контролювати вхідний та вихідний трафік, створювати правила для окремих програм та служб, а також блокувати весь вхідний трафік. З появою Windows 10, Windows Firewall було перейменовано в Windows Defender Firewall.

macOS також має вбудований фаєрвол, який можна налаштувати через системні налаштування. Він дозволяє користувачам встановлювати правила для вхідного трафіку, включаючи дозволи та заборони для окремих служб та

програм. За замовчуванням, фаєрвол macOS вимкнено, але користувачі можуть включити його самостійно.

Linux, на відміну від Windows та macOS, не має вбудованого графічного інтерфейсу для фаєрволу. Замість цього, більшість дистрибутивів Linux використовують систему названу iptables для управління мережевими правилами. Iptables є дуже потужним і гнучким інструментом, але він може бути складним для нових користувачів. В деяких дистрибутивах Linux, таких як Ubuntu, є додаткові інструменти, такі як ufw (Uncomplicated Firewall), які надають більш простий інтерфейс для управління правилами фаєрволу.

Android також має вбудовані можливості фаєрволу на рівні операційної системи, хоча вони можуть бути менш видимими для кінцевих користувачів. Вони дозволяють контролювати мережевий доступ на рівні окремих додатків. Додатково, є багато сторонніх додатків фаєрволу для Android, які надають більш глибокий контроль над мережевим трафіком.

iOS має вбудовані заходи безпеки, включаючи можливості фаєрволу, але вони зазвичай є прозорими для користувачів. Apple контролює доступ до мережі на рівні окремих додатків і служб. У кінцевому результаті, хоча iOS не дає користувачам прямого контролю над фаєрволом, він все ще забезпечує важливі заходи захисту мережі [19].

У розробці безпеки, важливо розглянути, як фаєрволи можуть бути використані в різних операційних системах. Однак, як і з усіма інструментами безпеки, фаєрволи найкраще використовуються в комбінації з іншими заходами безпеки, включаючи антивірусні програми, системи виявлення вторгнень та навчання користувачів щодо кращих практик в галузі безпеки.

2.5.2 Антивіруси та їх види

Антивірусні програми призначені для оборони комп'ютерних систем від зловмисного програмного забезпечення, як-от віруси, черви, троянці,

браундмауери та інші форми шкідливих програм. Вони відіграють відповідальну роль у забезпеченні безпеки інформації та приватності даних.

Різні критерії дозволяють класифікувати антивіруси.

Нижче наведено антивіруси за видом сканування.

1. Запитні сканери (On-demand scanners): представляють собою вид антивірусних програм, що перевіряють систему на шкідливе програмне забезпечення за бажанням користувача. Вони не функціонують у режимі реального часу, а замість цього запускаються за необхідності, що може мати переваги у деяких випадках.

Далі описано характеристики запитних сканерів.

Запуск вручну: такі антивірусні програми активуються за бажанням користувача, наприклад, коли є підозра на інфекцію або перед відкриттям незнайомого файлу.

Сканування за вибором: сканери за запитом дозволяють перевірити окремі файли, теки або весь комп'ютер. Користувач може налаштовувати параметри сканування залежно від своїх потреб.

Відсутність постійного спостереження: оскільки сканери за запитом не працюють у режимі реального часу, вони не використовують системні ресурси, коли не активовані. Це може знизити навантаження на комп'ютер та поліпшити продуктивність.

Додатковий рівень захисту: сканери за запитом можуть служити додатковим захистом разом з антивірусами, що працюють в режимі реального часу. Вони можуть виявляти загрози, які основний антивірус не виявив.

Немає автоматичного захисту: однією з недоліків сканерів за запитом є відсутність автоматичного захисту від шкідливих програм. Користувачу слід періодично проводити сканування, аби гарантувати безпеку своєї системи.

Сканери за запитом можуть стати ефективним засобом у боротьбі зі шкідливим програмним забезпеченням, особливо як доповнення до головного антивірусу. Однак варто зрозуміти, що використання їх окремо може не надавати комплексного захисту від усіх можливих загроз.

Для забезпечення оптимального захисту варто поєднувати сканери запитом з антивірусними програмами, які функціонують у режимі реального часу. Такий підхід дозволяє гарантувати захист від широкого діапазону шкідливих програм та врахувати різні атакуючі стратегії [20].

2. Сканери доступу (On-access scanners): працюють у режимі реального часу і забезпечують постійний захист від шкідливого програмного забезпечення. Під час виконання операцій, таких як відкриття, збереження або завантаження, вони автоматично перевіряють файли та програми на наявність вірусів.

Серед особливостей сканерів доступу можна виділити автоматичний захист, моніторинг у реальному часі, застосування антивірусних баз, невеликий вплив на продуктивність та автоматичні оновлення. Сканери доступу відстежують шкідливі дії та блокують віруси автоматично, щоб запобігти їх поширенню та інфікуванню системи. Вони використовують алгоритми для аналізу файлів та програм на предмет шкідливих характеристик у реальному часі, що забезпечує своєчасне виявлення та нейтралізацію загроз. Сканери доступу постійно використовують останні версії вірусних сигнатур та інших ознак шкідливого програмного забезпечення для ефективного виявлення та блокування. Хоча сканери доступу працюють у реальному часі, більшість сучасних антивірусів оптимізовані для мінімізації впливу на ресурси комп'ютера та забезпечення підвищеної продуктивності. Крім того, сканери доступу зазвичай мають вбудовані механізми для автоматичного оновлення антивірусних баз, що дозволяє забезпечувати надійний захист проти нових загроз.

Також антивіруси розподіляються за призначенням.

Базові антивіруси: основний рівень захисту від шкідливого програмного забезпечення, такого як віруси, черв'яки, троянські коні та інші загрози. Ці антивіруси можуть бути безкоштовними або є стандартним компонентом операційної системи.

Основні характеристики базових антивірусів описані нижче.

Основний рівень захисту: базові антивіруси зазвичай зосереджуються на виявленні та видаленні найбільш поширених типів шкідливого програмного забезпечення, що дозволяє захистити комп'ютери від найбільш очевидних загроз.

Обмежені функції: порівняно з платними антивірусами, базові антивіруси мають менше функцій та можливостей. Наприклад, вони можуть не мати розширених інструментів безпеки, таких як брандмауери, захист від вимагачів або захист банківських операцій.

Безкоштовність: багато базових антивірусів є безкоштовними, що дозволяє їм бути доступними для широкого кола користувачів. Проте варто зазначити, що безкоштовні антивіруси можуть мати обмеження у підтримці та оновленнях.

Автоматичні оновлення: базові антивіруси зазвичай мають автоматичні оновлення вірусних баз, хоча частота оновлень може бути меншою, ніж у платних альтернатив.

Невеликий вплив на систему: Базові антивіруси зазвичай мають менший вплив на продуктивність системи, оскільки вони не включають додаткових функцій та інструментів, які можуть споживати ресурси комп'ютера.

Важливо знати, що базові антивіруси, хоч і забезпечують деякий рівень захисту, можуть бути недостатніми для повного захисту від усіх можливих загроз, особливо в світі де програмне забезпечення та атаки постійно змінюються [21].

Отже, для забезпечення найкращого рівня захисту рекомендується розглянути можливість встановлення розширеного антивірусного рішення, яке надає додаткові функції та інструменти безпеки.

3. Комплексні рішення Інтернет-безпеки (Internet Security Suites): призначені для захисту вашого комп'ютера та даних від різних видів загроз, зокрема під час використання Інтернету. Ці пакети зазвичай містять кілька різних інструментів та функцій безпеки, що допомагають забезпечити більш широкий спектр захисту, ніж прості антивірусні програми.

Основні компоненти Інтернет-захисту можуть включати наступні характеристики:

- Антивірусний захист, що забезпечує базовий захист від вірусів, троянців, черв'яків та іншого шкідливого програмного забезпечення;
- Брандмауер, що контролює вхідний та вихідний мережевий трафік, блокуючи небажані сполучення та атаки ззовні;
- Антишпигунський захист, що виявляє та блокує шпигунське програмне забезпечення та інші програми, які можуть відстежувати вашу діяльність та збирати особисті дані;
- Захист від спаму, що фільтрує небажані електронні листи та спам, забезпечуючи захист від фішингу та інших шахрайських спроб;
- Батьківський контроль, що дозволяє обмежувати та контролювати доступ дітей до певних сайтів, програм та інтернет-ресурсів;
- Захист від вимагачів (ransomward), що виявляє та блокує вимагацьке програмне забезпечення, яке шифрує дані на вашому комп'ютері та вимагає викупу за їх розблокування;
- Оцінка та блокування небезпечних сайтів, що можуть містити шкідливе програмне забезпечення або сприяти іншим онлайн-загрозам, забезпечують безпечніше переглядання веб-сторінок.

Інтернет-захист (Internet Security Suites) надає комплексний захист для вашого комп'ютера та даних від різних видів загроз під час користування Інтернетом. За допомогою декількох інструментів та функцій безпеки, інтернет-захист забезпечує більш широкий спектр захисту, ніж просто антивірусні програми.

Крім захисту від вірусів, троянців, черв'яків та іншого шкідливого програмного забезпечення, інтернет-захист включає інші компоненти, такі як брандмауер, антишпигунський захист, захист від спаму, батьківський контроль, захист від вимагачів, захист від експлойтів та захист від мережесих атак. Інтернет-захист також може включати віртуальну приватну мережу, яка забезпечує безпечне та анонімне підключення до Інтернету.

Інтернет-захист рекомендується для тих, хто активно використовує Інтернет, зокрема для онлайн-покупок, банкінгу та соціальних мереж, а також для батьків, які хочуть контролювати інтернет-доступ своїх дітей. Незважаючи на те, що інтернет-захист надає більш глибокий рівень захисту, порівняно з базовими антивірусами, він може вимагати платну передплату та використовувати більше системних ресурсів [22].

За методом виявлення зловмисного програмного забезпечення розподіляються на наведені нижче.

4. Антивіруси на основі сигнатур: це тип антивірусного програмного забезпечення, який використовує унікальні відбитки вірусів, троянських коней, черв'яків та іншого шкідливого програмного забезпечення для їх виявлення та блокування. Сигнатурний антивірус проводить сканування файлів та процесів на вашому комп'ютері, щоб визначити, чи містять вони шкідливий код, використовуючи відомі шаблони шкідливого коду.

Основні особливості антивірусів на основі сигнатур є описані нижче.

Базу даних сигнатур: антивіруси на основі сигнатур містять велику базу даних сигнатур, яка оновлюється регулярно, щоб захистити від найновіших загроз.

Сканування файлів та процесів: сигнатурні антивіруси проводять аналіз файлів та процесів на вашому комп'ютері, порівнюючи їх з відомими сигнатурами шкідливого коду.

Блокування відомих загроз: якщо антивірус на основі сигнатур виявляє шкідливий код, він блокує його виконання.

Оновлення бази даних: щоб виявляти нові загрози, важливо регулярно оновлювати базу даних сигнатур, оскільки шкідливе програмне забезпечення постійно розвивається.

Недоліки антивірусів на основі сигнатур полягають у тому, що вони не можуть виявити нові або невідомі загрози, для яких ще не було створено сигнатур. Крім того, вони можуть мати складнощі з виявленням поліморфних вірусів, які змінюють свій код, щоб уникнути виявлення. Антивіруси на основі

сигнатур є одним з методів виявлення та блокування шкідливого програмного забезпечення, який зазвичай використовується в поєднанні з іншими методами, такими як антивіруси на основі поведінки та репутації файлів, для забезпечення більш комплексного захисту від широкого спектра загроз.

Незважаючи на те, що антивіруси на основі сигнатур мають свої недоліки, вони залишаються важливим компонентом у багатьох антивірусних рішеннях, завдяки своїй здатності швидко та точно виявляти та блокувати відомі шкідливі програми. Однак для досягнення найкращого рівня захисту від широкого спектра загроз рекомендується використовувати багаторівневий підхід, який поєднує різні методи виявлення та блокування шкідливого програмного забезпечення [21].

5. Евристичні антивіруси - це певний тип програмного забезпечення, який застосовує евристичний аналіз, щоб виявити віруси та інші шкідливі програми. Цей метод аналізу базується на припущеннях та висновках, які зроблені на основі обмеженої кількості інформації. У випадку евристичних антивірусів, код програми аналізується для виявлення незвичних характеристик або дій, які можуть свідчити про наявність шкідливого коду.

За використання евристичних антивірусів є деякі переваги в порівнянні з антивірусами, які використовують лише сигнатурний наприклад наведені нижче.

Здатність виявляти нові та невідомі загрози: евристичні антивіруси можуть виявляти шкідливий код, навіть якщо його сигнатура не відома. Це дозволяє захиститись від нових та невідомих загроз.

Проактивний захист. Евристичні антивіруси намагаються запобігти інфікуванню системи, виявляючи підозрілі дії або характеристики коду перед тим, як вони можуть завдати шкоди.

Також є описані нижче недоліки.

Ймовірність помилкових спрацювань (false positives): через свою природу евристичного аналізу, програма може помилково віднести безпечний

файл або програму до шкідливих, що може призвести до незручностей з блокуванням безпечних файлів або проблемами зі стабільністю системи.

Евристичний аналіз може бути важким процесом, оскільки потребує аналізу програмного коду на наявність підозрілих характеристик. Це може призвести до погіршення продуктивності комп'ютера, що знижує продуктивність користувача.

Крім того, евристичні антивіруси можуть бути менш ефективними проти деяких видів шкідливих програм, які використовують складні методи обфускації або поліморфізму, щоб уникнути виявлення.

З урахуванням переваг та недоліків, евристичні антивіруси часто використовуються в поєднанні з іншими методами виявлення шкідливих програм, наприклад, сигнатурним аналізом та поведінковим аналізом. Такий підхід забезпечує кращий рівень захисту від широкого спектру загроз та дозволяє адаптуватися до кіберландшафту, що змінюється.

6. (Behavior-based): Антивіруси на основі поведінки програм (Behavior-based) - це захисне програмне забезпечення, яке визначає шкідливі програми та загрози, спираючись на їхню поведінку, а не на традиційні методи сигнатур. Вони аналізують дії програм і процесів, що відбуваються на комп'ютері, та приймають рішення про блокування або дозвіл на виконання дій, враховуючи допустимі та шкідливі шаблони поведінки [23].

Далі описано особливості антивірусів на основі поведінки програм.

Виявлення нових та невідомих загроз: такі антивіруси можуть виявити шкідливий код, навіть якщо він не має відомої сигнатури, оскільки вони фокусуються на аналізі поведінки програм, а не на відповідності сигнатурі.

Проактивний захист: антивіруси на основі поведінки програм надають проактивний захист, оскільки вони можуть блокувати потенційно шкідливі дії перед тим, як вони завдають шкоди системі.

Зменшення ризику помилкових сигналів: ці антивіруси спираються на аналіз поведінки, що може знизити кількість помилкових сигналів, порівняно з методами на основі сигнатур.

Адаптивність до змінюваних загроз: антивіруси на основі поведінки програм можуть адаптуватися до постійно змінюваних шкідливих програм та кібератак, що збільшує їхню ефективність з часом.

Однак, антивіруси на основі поведінки програм також мають деякі недоліки:

Можливі помилкові виявлення: хоча антивіруси, що засновані на поведінці, мають менші шанси на помилкові спрацювання порівняно з сигнатурними антивірусами, іноді вони можуть помилково виявляти безпечні програми як шкідливі, коли їхні дії відповідають шаблонам шкідливої поведінки.

Ресурсоемкість: антивіруси, засновані на поведінці, можуть вимагати більше системних ресурсів, оскільки вони здійснюють неперервний аналіз дій програм та процесів у реальному часі.

Можливість обходу: кіберзлочинці все частіше створюють шкідливе програмне забезпечення, яке здатне маскувати свою поведінку або використовувати техніки самозахисту, щоб уникнути виявлення поведінковими антивірусами.

Потреба в комбінації з іншими методами захисту: хоча антивіруси, засновані на поведінці, можуть виявити багато нових та невідомих загроз, вони краще працюють в комбінації з іншими методами захисту, такими як сигнатурні антивіруси, для досягнення всебічного захисту [21].

В цілому, антивіруси, що засновані на поведінці, можуть стати ефективним доповненням до вашої системи захисту від шкідливого програмного забезпечення. Вони допоможуть виявляти та блокувати нові та невідомі загрози, але слід використовувати їх у поєднанні з іншими антивірусними програмами для досягнення найкращого захисту.

7. Хмарні антивіруси (Cloud-baser): це тип антивірусних програм, які використовують хмарні технології та опираються на віддалені сервери для обробки та вивчення даних, на відміну від їхнього виконання на

користувацькому комп'ютері. Вони пропонують кілька переваг у порівнянні з класичними антивірусами:

Менше навантаження на ресурси: так як хмарні антивіруси використовують сервери для аналізу та переробки даних, вони вимагають менше ресурсів від користувацької системи. Це означає, що хмарні антивіруси можуть ефективно працювати навіть на застарілих або менш потужних пристроях.

Більш швидкі оновлення: хмарні антивіруси забезпечують оперативні оновлення, оскільки їх бази даних знаходяться на віддалених та централізованих серверах. Це дозволяє антивірусній програмі швидко отримувати актуальні сигнатури шкідливого програмного забезпечення та ефективно протистояти новим загрозам.

Віддалений доступ та управління: деякі хмарні антивіруси надають користувачам можливість віддаленого доступу до своїх комп'ютерів та управління налаштуваннями антивірусу через веб-інтерфейс. Це може бути корисним для адміністраторів або користувачів, які бажають керувати захистом декількох пристроїв одночасно.

Швидка відповідь на нові загрози: використовуючи хмарні технології, хмарні антивіруси можуть оперативно реагувати на свіжі загрози, оскільки вони безперервно підключені до централізованих серверів. Це забезпечує більш актуальний та ефективний захист проти нових вірусів та атак. Спільна розумна система: Хмарні антивіруси стають сильнішими завдяки спільному навчанню від користувачів у всьому світі. Якщо одному користувачеві доводиться стикатися з новою загрозою, хмарний антивірус оперативно оновлює базу даних і забезпечує захист від цієї загрози для всіх інших користувачів.

Легка інтеграція з іншими системами безпеки: хмарні антивіруси можуть бути просто інтегровані з іншими засобами безпеки, такими як фаєрволи, антишпигунські програми або фільтри контенту. Це дозволяє користувачам розробляти більш складні та ефективні захисні системи.

Проте слід відзначити, що хмарні антивіруси мають також деякі недоліки. Зокрема, їхня робота залежить від стабільного інтернет-з'єднання, оскільки вони мають постійно зберігати зв'язок з віддаленими серверами. Більше того, через обробку даних на віддалених серверах, можуть виникнути питання щодо конфіденційності та захисту даних.

Загалом, хмарні антивіруси можуть стати ефективним та новаторським варіантом для захисту від шкідливого ПЗ. Вони пропонують ряд переваг у порівнянні з класичними антивірусами, але користуватись ним потрібно прорахувавши його недоліки.

За способом поширення та застосування бувають описані далі антивіруси.

Безоплатні антивіруси: безоплатні антивірусні програми надають користувачам основний рівень захисту без витрат. Вони можуть стати корисним варіантом для тих, хто шукає просте і доступне антивірусне рішення для своїх ПК. Ось декілька ключових характеристик безоплатних антивірусів:

Обмеження функціональності: безоплатні антивіруси зазвичай мають менш розширені можливості в порівнянні з платними антивірусними програмами. Вони забезпечують лише базовий захист від вірусів, троянів та іншого шкідливого ПЗ. Відсутність додаткових функцій, таких як фаєрвол, антиспам та блокування шкідливих сайтів, може дещо обмежувати рівень захисту [20].

Реклама та пропозиції оновлень: безоплатні антивірусні програми часто включають рекламу або спливаючі вікна, які заохочують користувачів купити платну версію або оновитися до преміум-пакету. Це може виявитися некомфортним для деяких користувачів.

Зрідка оновлюється: безоплатні антивіруси можуть оновлюватися менш часто з порівнянні з платними аналогами. Це може знижувати ефективність захисту від нових загроз.

Обмежена підтримка: безоплатні антивіруси зазвичай пропонують обмежену технічну підтримку користувачам. Це може ускладнити процес вирішення проблем або знаходження відповідей на питання.

Безоплатні антивіруси, хоча й мають деякі обмеження, все ж надають основний рівень захисту для користувачів, які не бажають витратити кошти на комерційні антивірусні продукти. Деякі безоплатні антивіруси славляться своєю ефективністю та можуть виявляти та ліквідувати багато видів шкідливого ПЗ.

Чудовий початковий вибір: безоплатні антивіруси можуть бути хорошим вступом для користувачів, які тільки знайомляться з антивірусним захистом. Вони дозволяють користувачам дослідити різноманітні функції та налаштування без витрат.

Випробування різних варіантів: оскільки на ринку є безліч безоплатних антивірусів, користувачі можуть спробувати кілька з них, щоб визначити найбільш підходящий для своїх потреб та вимог щодо захисту.

Поєднання з іншими засобами захисту: безоплатні антивіруси можна використовувати разом з іншими інструментами захисту, такими як фаєрволи, анти-малварний захист та спеціалізовані сканери на вимогу, для забезпечення більш глибокого та всебічного захисту.

Варто пам'ятати, що хоча безоплатні антивіруси забезпечують базовий захист, вони не можуть замінити комерційні антивірусні програми. Найефективніший захист досягається шляхом комбінування безоплатних антивірусів з іншими інструментами та методами безпеки.

Комерційні антивіруси: це антивірусні програми, які створюються та продаються компаніями, що фокусуються на продуктах та послугах зі сфери комп'ютерної безпеки. Зазвичай такі програми забезпечують ширший та потужніший захист від шкідливого програмного забезпечення та інших загроз у порівнянні з безкоштовними антивірусами. Ось декілька особливостей платних антивірусів:

Покращені можливості захисту: платні антивіруси зазвичай мають додаткові функції, такі як захист від шпигунського ПЗ, антифішингові заходи та захист від руткітів, які допомагають покращити базовий антивірусний захист.

Заздалегідь попереджувальний захист: більшість платних антивірусів застосовують передбачувальні техніки, такі як евристичний та поведінковий аналіз, для виявлення невідомих загроз і забезпечення кращого захисту від свіжих вірусів.

Часті оновлення: платні антивіруси, як правило, отримують оновлення частіше, що дозволяє їм бути в курсі і ефективно протистояти найсвіжішим загрозам.

Підтримка користувачів: оскільки ви оплачуєте платний антивірус, ви маєте право на високоякісну технічну підтримку від розробника програми. Це може включати підтримку через онлайн-чат, телефонну підтримку та електронну пошту.

Налаштування за потребами користувача: платні антивіруси дозволяють користувачам змінювати параметри захисту та функціонал продукту відповідно до власних вимог. Це може охоплювати налаштування опцій сканування, управління списками дозволених та заборонених програм, переналаштування сповіщень та багато іншого.

Покращена якість продукту: здебільшого платні антивіруси пройшли більш суворий контроль якості, що гарантує відмінні результати у виявленні та ефективності програми. Вони також забезпечують менше можливості для помилок або проблем, пов'язаних з продуктом.

Ліцензійні пропозиції: платні антивіруси нерідко пропонують ліцензійні пакети для домашніх користувачів або організацій. Це дозволяє користувачам легко охопити кілька комп'ютерів та пристроїв за одну ціну ліцензії.

Додаткові інструменти: чимало платних антивірусів містять екстра інструменти для покращення безпеки, такі як менеджери паролів, фаєрволи, програми захисту від крадіжки даних та оптимізації системи.

Однак варто відзначити, що платні антивіруси мають деякі недоліки. Наприклад, вони можуть коштувати більше, ніж безкоштовні антивіруси, і часто потребують підписки з періодичними платежами. Крім того, деякі користувачі можуть відчувати погіршення продуктивності своїх пристроїв через використання ресурсів комп'ютера [20].

Корпоративні антивіруси: програми представляють собою спеціалізовані захисні рішення, розроблені з метою оборони організацій від шкідливих програм та різноманітних загроз. У порівнянні з антивірусами для домашнього використання, вони мають більш високий рівень функціональності та управління, оскільки враховують особливості роботи великих компаній, для яких безпека є важливим пріоритетом. Ось декілька ключових особливостей корпоративних антивірусів:

Уніфіковане управління: корпоративні антивірусні програми здебільшого надають централізовані системи управління, які дозволяють адміністраторам контролювати та забезпечувати безпеку усіх комп'ютерів та пристроїв мережі організації. Такий підхід допомагає оперативно відгукнутися на потенційні загрози та виконувати оновлення політик безпеки.

Гнучкість масштабування: корпоративні антивірусні рішення розроблені таким чином, щоб легко інтегруватися та масштабуватися в мережах різних розмірів, що дозволяє компаніям без зусиль захищати численні пристрої.

Забезпечення мережевої безпеки: такі програми також можуть мати функції для мережевого захисту, наприклад, системи виявлення вторгнень, контроль витоку інформації та безпечний віддалений доступ. Це сприяє створенню комплексного підходу до захисту корпоративної інфраструктури.

Підтримка різних платформ: зазвичай корпоративні антивірусні програми сумісні з багатьма операційними системами та платформами, такими як Windows, macOS, Linux, а також мобільними пристроями на основі Android та iOS. Це допомагає організаціям захищати велику кількість пристроїв та працювати з різним програмним забезпеченням. Висока швидкість виявлення

та реагування на загрози: Корпоративні антивіруси характеризуються високою швидкістю виявлення нових загроз та можливістю швидко реагувати на них за допомогою різних захисних технологій, таких як хмарні бази даних, аналіз поведінки та інші прогностичні методи.

Оцінка безпеки та звіти: корпоративні антивіруси забезпечують змогу проводити оцінку безпеки та створювати детальні звіти про стан захисту організації. Це дозволяє адміністраторам та керівництву краще контролювати захист комп'ютерів та мережі, виявляти проблеми та планувати відповідні заходи.

Технічна допомога та консультації: Організації, які використовують корпоративні антивірусні рішення, зазвичай мають доступ до висококваліфікованої технічної підтримки та консультацій від виробника. Це може бути корисним для вирішення технічних питань, навчання та отримання порад щодо найкращих практик у сфері інформаційної безпеки.

Втім, корпоративні антивірусні рішення також мають деякі недоліки, такі як високі витрати на ліцензування, складність управління та обслуговування, а також можливе зниження продуктивності через споживання системних ресурсів. Проте, для більшості організацій переваги корпоративних антивірусів зазвичай переважають недоліки, що робить їх важливим засобом для забезпечення безпеки та стабільності корпоративних мереж. Вони допомагають знижувати ризик від потенційних загроз, таких як віруси, троянські коні та інші види зловмисного ПЗ, які можуть призвести до втрати інформації, простоїв роботи чи інших витрат для організації [23].

Для підтримки оптимального рівня безпеки корпоративні антивіруси слід поєднувати з іншими засобами захисту, такими як брандмауери, системи контролю доступу, регулярне створення резервних копій даних та розробка планів відновлення після аварій. Такий інтегрований підхід допоможе забезпечити найвищий рівень захисту для організації та її ресурсів.

2.5.3 Антиспам-фільтри та їх види

Антиспам-фільтри - це програмне забезпечення, яке застосовується для виявлення та блокування небажаних електронних листів (спаму), що надходять на поштові скриньки користувачів.

Існує кілька видів антиспам-фільтрів, включаючи:

Фільтри на основі правил: ці фільтри використовують встановлені правила та налаштування, щоб визначити, які електронні повідомлення будуть вважатися спамом. Вони можуть блокувати повідомлення, що містять певні ключові слова або фрази, або повідомлення з певних IP-адрес.

Фільтри на основі списків: ці фільтри використовуються для блокування повідомлень, що містять IP-адреси, які відомі як джерела спаму. Вони працюють на основі списків, які містять інформацію про IP-адреси, які відомі як джерела спаму, та блокують будь-які повідомлення, що надходять з цих адрес.

Фільтри на основі статистичного аналізу: ці фільтри аналізують структуру повідомлень, щоб визначити, чи є вони спамом. Вони аналізують заголовки, текст повідомлення, адреси відправника та інші параметри, щоб визначити, чи є повідомлення спамом.

Антиспам-фільтри можуть бути встановлені на серверах електронної пошти, які обробляють вхідну пошту, або на комп'ютері користувача для обробки вхідної пошти. Деякі антиспам-фільтри працюють в хмарних сервісах та обробляють пошту на віддалених серверах [24].

3 СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ІТ - ОФІСУ

3.1 Запобігання загрозам кібератак

Щоб захиститись від кібератак була забезпечена надійність паролів. Вимагалось від співробітників використання складних паролів, які містять комбінацію цифр, літер та символів. Також використовувалась двофакторна аутентифікація [9].

Регулярно оновлюються всі програми та операційні системи до останньої версії, щоб запобігти використанню вразливостей.

Встановлено та оновлено антивірусне програмне забезпечення, щоб захиститись від вірусів, троянів та інших шкідливих програм.

Проводяться регулярні тренінги для співробітників з превенції фішинг-атак та попередив їх про небезпеку відкривати невідомі листи або додатки.

Робляться регулярні резервні копії даних, щоб в разі атаки на інформацію мати можливість відновити її.

Використовуються віртуальні приватні мережі, щоб захистити свою інформацію від зловмисників, які можуть перехоплювати мережевий трафік.

Проводиться регулярний аудит безпеки даних для виявлення потенційних загроз та вразливостей у системі безпеки.

Обмежено доступ до конфіденційної інформації тільки тим співробітникам, які потребують її для своєї роботи.

Треба проаналізувати дані та моніторити мережевий трафік, щоб вчасно виявляти потенційні загрози та діяти на їхній виявлення.

Захистити серверні приміщень та комп'ютери, де зберігається конфіденційна інформація.

Перевірити рівень безпеки у своїх постачальників та здійснюється контроль їхнього доступу до вашої інформації.

Встановити систему моніторингу, яка відстежує активність на мережі та допомагає виявляти потенційні загрози [12].

3.2 Запобігання загрозам соціального інжинірингу

Щоб захиститися від соціального інжинірингу, треба ознайомити співробітників з методами соціального інжинірингу та навчити їх виявляти та уникати таких атак.

Встановити сильні паролі для облікових записів, а також змінити їх з часом.

Регулярно проводити аудити безпеки системи та виявляються вразливості, які можуть бути використані зловмисниками.

Заборонити доступ до важливої інформації та ресурсів з пристроїв, які не належать компанії.

Довести не виконувати невідомі запити на виконання дій з комп'ютера або інших пристроїв, навіть якщо вони здаються легітимними.

Встановити програмне забезпечення для виявлення та блокування спроб соціального інжинірингу.

Регулярно створювати копії важливої інформації та зберігати на зовнішніх носіях або у хмарних сервісах.

Забезпечити фізичну безпеку серверних кімнат та інших приміщень, в яких зберігається важлива інформація та обладнання.

Проводити інформаційну кампанію серед співробітників про методи захисту від соціального інжинірингу та розробляються процедури відповідно до стандартів безпеки [10].

3.3 Запобігання загрозам несанкціонованого фізичного доступу

Щоб забезпечити захист від несанкціонованого фізичного доступу треба встановити систему контролю доступу до офісу, щоб управляти фізичним

доступом до приміщень та комп'ютерів. Це може включати в себе використання карток доступу, біометричних технологій (відбитків пальців, розпізнавання обличчя тощо) або кодів доступу.

Встановити камери в приміщеннях офісу та на входах, щоб відстежувати активність та виявляти потенційні загрози, а також датчиків руху в деяких кімнатах будівлі та встановлення ємкісного датчику руху ззовні, який використовують паркан та стіни будівлі як пластини конденсатора.

Проводити навчання співробітників з питань безпеки, щоб вони могли вчасно виявляти потенційні загрози та повідомляти про них відповідні служби.

Регулярно перевіряти системи безпеки, щоб переконатися, що вони працюють належним чином. Це включає в себе сканування мережі, тестування зламу та інші процедури.

Захищати конфіденційну інформацію та документи, що містять конфіденційну інформацію. Встановити шафи або сейфи для зберігання документів з замком.

Захищати бездротову мережу Wi-Fi від несанкціонованого доступу, встановити складний пароль і шифрування даних. Використовуються такі методи аутентифікації, як WPA2 або WPA3.

Перевіряти аккаунти компанії в соціальних мережах та забезпечте, щоб вони були захищені від зламу. Переконатись, що паролі до цих аккаунтів також є складними та регулярно змінюються [11].

На рисунку 3.1 можна побачити як реалізовано схему розділення доступу в ІТ-компанії.



червона – високий рівень доступу, жовта – середній рівень доступу,
зелена – низький рівень доступу

Рисунок 3.1 - Схема зон доступу

На рисунку 3.2 можна побачити як реалізовано зв'язок в комп'ютерній мережі, розташування та підключення камер відеоспостереження, розташування датчиків руху, датчиків розбиття скла та дверей в які можна ввійти тільки за допомогою ключ-карти, яка є персональною для кожного працівника.

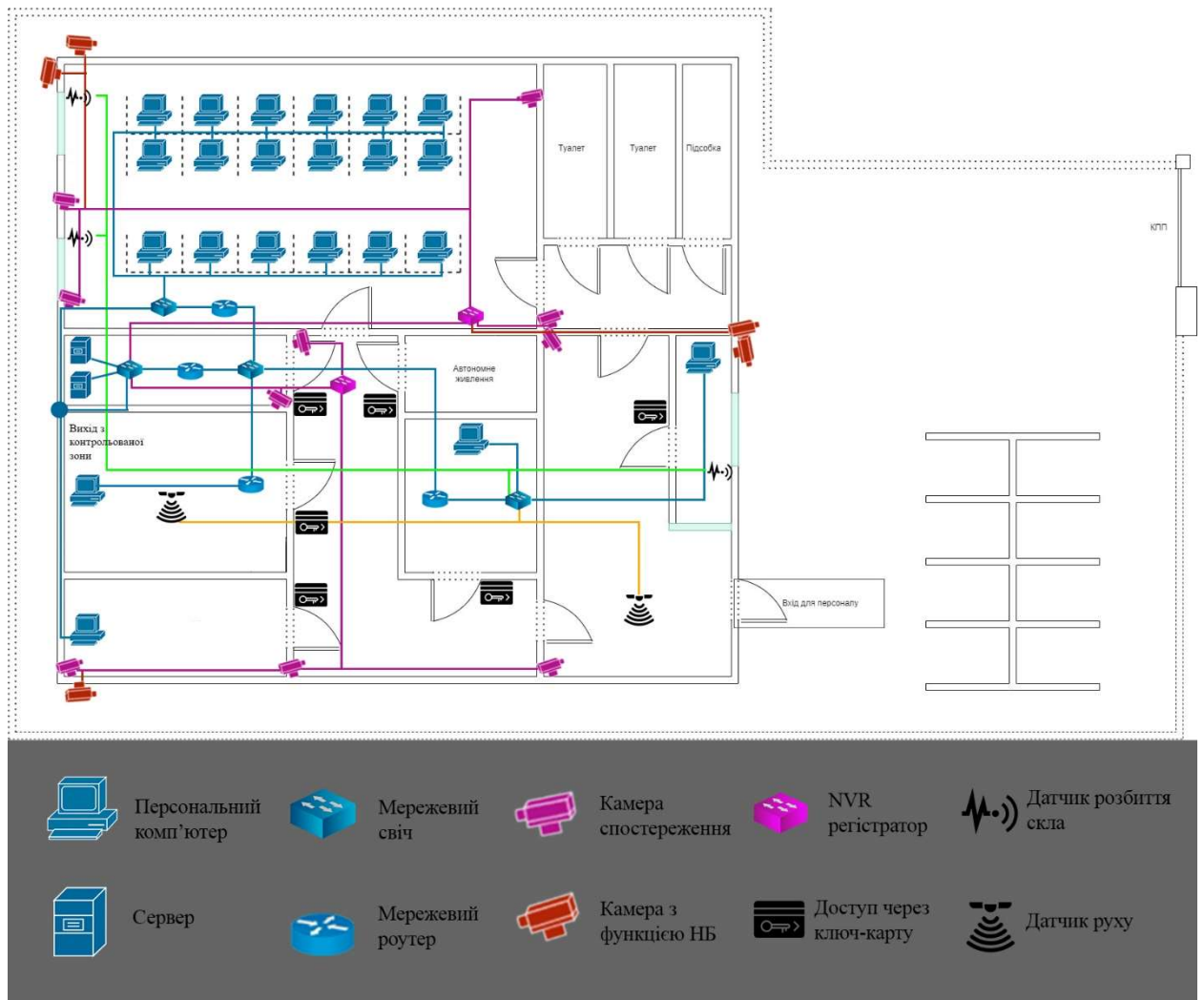


Рисунок 3.2 - Схема комп'ютерної мережі та обладнання системи безпеки

На рисунку 3.3 наведено кут огляду камер відеоспостереження. Слід зазначити, що камери розташовані під кутом, щоб на них не фіксувалось зображення з робочих моніторів персоналу.

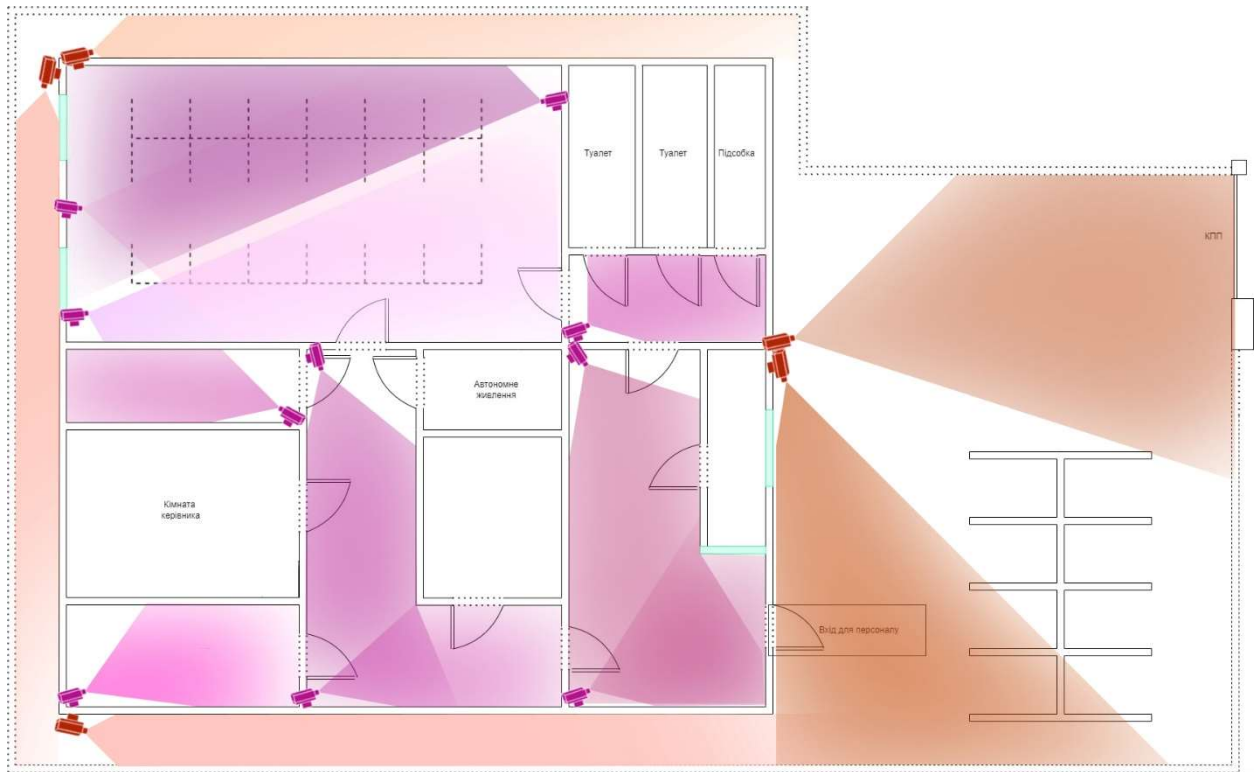


Рисунок 3.3 – Зони огляду камер відеоспостереження

3.4 Запобігання загрозам які утворюються через недбалість працівників

Щоб зменшити ризик загрози через недбалість працівників потрібно надавати достатню підготовку співробітникам. Треба організувати регулярні тренінги з безпеки, де буде навчено співробітників як захищати свої пристрої та дані.

Установлені процедури, які забезпечують, щоб відповідні керівники були на чолі з управлінням конфіденційними даними.

Забезпечити безпеку зовнішніх пристроїв: вимагати від співробітників використовувати тільки довірені USB-пристрої. Не дозволяти підключати невідомі зовнішні пристрої до комп'ютерів, такі як флешки, зовнішні жорсткі диски або мобільні пристрої, якщо вони не пройшли перевірку на віруси та шкідливі програми. Для підвищення безпеки треба встановити на комп'ютери спеціальні програмні засоби для контролю підключення зовнішніх пристроїв та блокування небезпечних. Крім того, ознайомити співробітників з ризиками від підключення невідомих зовнішніх пристроїв та правильні процедури

роботи з ними, такі як сканування на віруси та шкідливі програми перед використанням [13].

3.5 Запобігання загрозам які утворились через помилки в програмному забезпеченні

Щоб захиститись від помилок в програмному забезпеченні треба регулярно оновлювати програмне забезпечення та встановлено всі важливі патчі і оновлення.

Використано антивірусне програмне забезпечення та забезпечення регулярного оновлення вірусних баз.

Використовувати кодування і шифрування для захисту важливих даних.

Використовувати методи тестування програмного забезпечення перед випуском.

Використовувати контроль версій програмного забезпечення.

Навчити та підвищити кваліфікації розробників та тестувальників.

Відстежувати та проаналізувати помилки програмного забезпечення, які вже були виявлені, для того, щоб уникнути їх повторення у майбутньому.

Застосовувати принципи безпеки при розробці та тестуванні програмного забезпечення, таких як перевірка на вразливості та забезпечення коректної обробки вхідних даних [14].

3.6 Запобігання загрозам пов'язаних з мережею

На периферії мережі для сортування та регулювання вхідного та вихідного трафіку треба розгорнути апаратний та програмний брандмауери. Вибір брандмауера був здійснений з огляду на його здатність конфігурувати правила для окремих додатків та служб, що дозволяє забезпечити більш вдосконалений контроль над мережевим трафіком.

На кожній комп'ютерній та серверній системі треба встановити антивірусне програмне забезпечення для захисту від шкідливого ПЗ. Встановити систему постійних оновлень та циклічного сканування системи.

На мережевому обладнанні треба впровадити системи IDS та IPS для допомоги в виявленні та блокуванні потенційних атак у режимі реального часу.

Треба реалізувати систему SIEM для збирання, обробки та реагування на логи та іншу інформацію з різних джерел у IT-середовищі. SIEM дозволяє ідентифікувати аномалії та можливі загрози, а також спрощує процес управління інцидентами безпеки.

Регулярне резервування важливих даних та систем забезпечує можливість відновлення в разі атаки або апаратного збою.

Існує постійний моніторинг оновлень та нових патчів, та в разі виходу оновлень для системи, вони негайно встановлюються.

3.7 Функціонування системи захисту офісу в неробочий час

Треба організувати постійний присутній персонал охорони: в позаробочий час в офісі обов'язково має бути присутній охоронний персонал. Вони мають проходити періодичні інструктажі щодо процедур безпеки та користування обладнанням безпеки.

Регулювання доступу: всі входи та вікна мають бути надійно закриті. Необхідно активувати систему обмеження доступу, яка включає в себе пропускні картки, біометричну ідентифікацію та інше.

Слідкування за відео наглядом: Відео системи, розташовані по периметру, повинні функціонувати безперебійно. Обов'язок охорони - систематично переглядати записи відео для контролю ситуації.

Активні системи безпеки: системи IDS/IPS і SIEM мають бути увімкнені та налаштовані на автоматичне виявлення та реагування на потенційні загрози.

Резервне електропостачання: у випадку відключення основного електропостачання, системи безпеки та важливі ІТ-системи мають автоматично переходити на резервне джерело живлення.

Реагування на інциденти: при виявленні будь-яких проблем з безпекою, охоронці повинні негайно сповістити про це відповідних ІТ-фахівців або керівництво компанії.

Періодичні обходи: охоронці повинні регулярно проводити інспекцію приміщень, щоб контролювати стан офісу і забезпечити безпеку.

Система тривоги: у випадку спроби незаконного проникнення система безпеки повинна негайно повідомити про це охорону і відповідальних співробітників.

Створення резервних копій: незалежно від робочого графіка, важливо проводити постійне резервне копіювання інформації, аби гарантувати своєчасність даних та змогу відновлення в разі необхідності.

Протидія надзвичайним ситуаціям: в разі виникнення аварійних обставин, персонал охорони повинен бути ознайомлений про порядок повідомлення службам екстреної реакції та відповідальним співробітникам організації.

Оновлення та виправлення: можливо налаштувати ІТ-системи на автоматичне оновлення в неробочий період, що дозволить зменшити час простою під час робочого дня.

Аудит системи: на початку робочого дня, ІТ-спеціалісти повинні провести огляд статусу ІТ-інфраструктури, включаючи перегляд журналів системи безпеки, для виявлення можливих проблем, які могли виникнути в неробочий час.

Зміна охорони: при зміні охорони, особа, яка завершує свою зміну, має повідомити нового охоронця про всі події, які стались протягом її дії.

ВИСНОВКИ

У процесі виконання цієї дипломної роботи було проведено дослідження та запропоновано систему захисту інформації для ІТ-офісу. Це включало вивчення теоретичних основ, аналіз потенційних ризиків і розробку відповідних заходів протидії, а також реалізацію вибраної стратегії безпеки.

У першій частині було розглянуто поняття ІТ-офісу, його різновиди, вивчено креслення будівлі, а також різноманітність приладів і модель OSI. Було виконано огляд основних комплексних систем захисту інформації, включаючи такі як SIEM, IDS та IPS.

У другій частині було здійснено аналіз можливих загроз і наголошено на важливості такого розгляду. Було розглянуто основні види вірусів, DDoS атак, способи фішингу, потенційні джерела витоку даних, несанкціонований доступ та викрадення особистої інформації. Було вивчено критичні області та ризики, а також методи та інструменти для протидії загрозам мережевої безпеки в ІТ-офісі, включаючи фаєрволи, антивіруси та антиспам-фільтри.

У третій частині було проаналізовано комплексну систему захисту інформації для ІТ-офісу, яка містить заходи протидії широкому спектру загроз, включаючи кібератаки, соціальний інжиніринг, несанкціонований фізичний доступ, недбалість працівників, помилки програмного забезпечення та мережеві загрози. Було також розглянуто режим роботи системи захисту в неробочий час.

Значна увага була приділена не лише виявленню потенційних ризиків, але й розробці специфічних стратегій та інструментів для їх протидії.

Реалізація створеної системи дозволить зменшити ризики, що виникають внаслідок кібератак, соціального інжинірингу, несанкціонованого фізичного доступу, недбалості працівників, помилок в програмному забезпеченні та мережевих загроз.

Варто підкреслити, що система захисту повинна бути адаптивною, здатною пристосовуватися до змінних умов і протистояти новим загрозам.

Механізми, розроблені в рамках цієї роботи, враховують ці вимоги, що робить їх відповідними для будь-якого ІТ-офісу.

Нарешті, робота показує важливість безперервного спостереження та оцінки системи захисту, з метою своєчасного виявлення і усунення потенційних слабких пунктів.

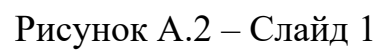
Таким чином, результати дипломної роботи можна включити в розробку та впровадження систем захисту інформації в ІТ-офісах, орієнтованих на безпеку корпоративних даних і стабільності операцій компаній.

Основні результати цієї роботи доповідались та обговорювались на «Тиждень науки 2023: щорічна наук.-практ. конф. викладачів, науковців, молодих учених, аспірантів та здобувачів вищої освіти НУ «Запорізька політехніка», 24-28 квітня 2023 р.» [25].

ПЕРЕЛІК ПОСИЛАНЬ

1. Kim G., Behr K., Spafford G. The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win - IT Revolution – 2018p. – 432с.
2. Lars Mönch, John W. Fowler, Scott Mason, Production Planning and Control for Semiconductor Wafer Fabrication Facilities: Modeling, Analysis, and Systems - Springer Science & Business Media – 2012p. - 288с.
3. Brian Komar, Firewalls For Dummies - John Wiley & Sons – 2003p. – 432с.
4. Автоматична система пожежогасіння – надійний захист життя і майна ЕЛЕКОН (Науково-технічна спілка) – Електронний ресурс – Режим доступу: <https://elekon.ub.ua/analITic/30761-avtomatichna-sistema-pojejogasinnya--nadiyniy-zahist-jITtya-i-mayna.html> (дата звернення 8.04.2023)
5. William Stallings, Data Communications and Networking - Pearson Education. – 2020p. – 912с.
6. Griff James, SIEM for Dummies – Wiley – 2020p. – 400с.
7. Richard Bejtlich, Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response - No Starch Press – 2021p. – 544с.
8. Michael Rash, Intrusion Prevention and Active Response: Deploying Network and Host IPS - O'Reilly Media – 2013p. – 360с.
9. Ю.П. Лісовська, Кібербезпека: ризики та заходи – Кондор – 2019р. – 272с.
10. Christopher Hadnagy, Social engineering the science of human hacking – Wiley – 2018p. – 362с.
11. Kim L. Robertson, Physical SecurITy for IT – Syngress – 2004p. – 512с.
12. В. Л. Бурячок, В. Б. Толубко, Інформаційна та кібербезпека: соціотехнічний аспект - Київ ДУТ – 2015р. – 288с.
13. Gregory J. Touhill and C. Joseph Touhill, CybersecurITy for Executives: A Practical Guide – Wiley – 2019p. – 214с.

- 14 Gary McGraw, Software SecurITy: Building SecurITy In - Addison-Wesley - 2018p. – 848c.
15. Jonathan Wright and Engin Kirda, Computer Viruses and Malware – Springer – 2017p. – 370c.
16. Simon SmITh, Denial of Service Attacks: Detection, Analysis and Defense – Springer – 2015p. – 368c.
17. Markus Jakobsson, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic IdentITy Theft - Wiley Publishing – 2015p. – 568c.
18. William Stallings, Network SecurITy Essentials: Applications and Standards - Pearson Education – 2021p. – 560c.
19. Mark Newcomb, Firewalls: A Complete Guide - CRC Press – 2018p. – 492c.
20. John Aycock, Computer Viruses and Malware – Springer – 2019p. – 331c.
21. Antivirus software for Windows: the good, the bad and the ugly, Virus Bulletin, Електронний ресурс – Режим доступу: <https://www.virusbulletin.com/virusbulletin/> (дата звернення 15.04.2023).
22. Joxean Koret та Elias Bachaalany, Antivirus Hacker's Handbook – Wiley – 2015p. – 480c.
23. Guide to Antivirus and Malware Protection Software SafeWise – Електронний ресурс – Режим доступу: <https://www.safewise.com/guide-to-antivirus-and-malware-protection-software/> (дата звернення 17.04.2023).
24. Martin Brown, Antispam: Managing Spam Messages, Malware, and Other Junk – Apress – 2013p. – 448c.
25. Івлєв В.Ю. Система захисту інформації в ІТ – офісі / В.Ю. Івлєв, С.І. Лізунов // Тиждень науки 2023: щорічна наук.-практ. конф. викладачів, науковців, молодих учених, аспірантів та здобувачів вищої освіти НУ «Запорізька політехніка», 24-28 квітня 2023 р.: тези доповідей. – Запоріжжя, 2023.



Зони циркуляції інформації

3/11

Мовна інформація циркулює в робочому приміщенні, кімнаті керівника.

Паперова циркулює в кімнаті керівника та системного адміністратора.

Електронна циркулює в робочому приміщенні, кімнаті керівника, кімнаті системного адміністратора, серверній кімнаті, а також на посту та в кімнаті охорони.

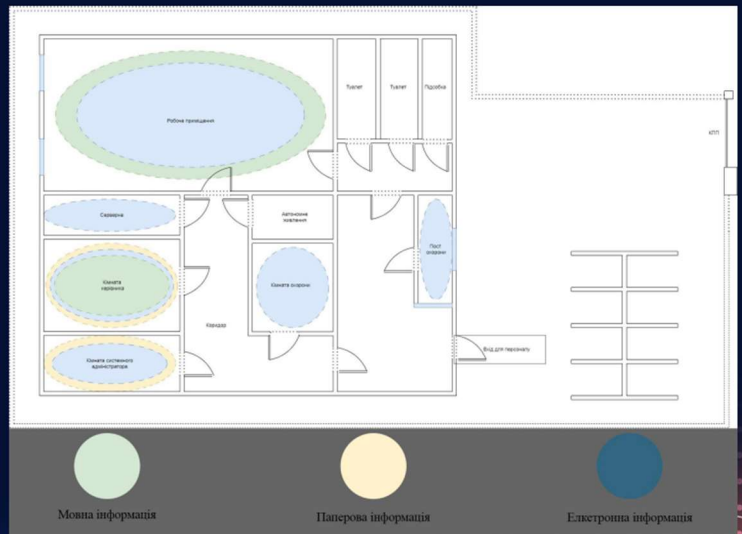


Рисунок А.3 – Слайд 2

Меблювання офісу

4/12

Більшість комп'ютерів розташована в робочому приміщенні. По одному комп'ютеру встановлено в кімнаті керівника, системного адміністратора, а також в кімнаті та на посту охорони.

В кімнаті керівника та системного адміністратора встановлено сейфи.

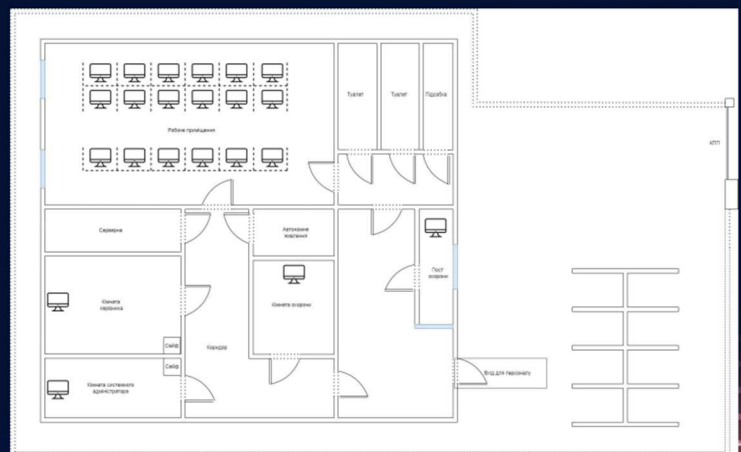


Рисунок А.4 – Слайд 3

Схема живлення, розташування розеток та освітлення

5/12

Для захисту від витоку інформації в офісі знаходиться дві системи живлення.

На виходах з контрольованої зони встановлені фільтри.

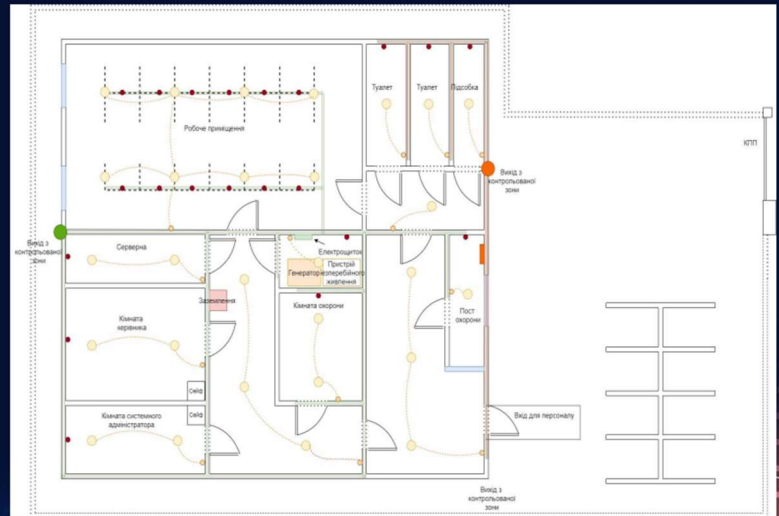


Рисунок А.5 – Слайд 4

Схема вентиляції

6/12

Вентиляцією забезпечене кожне приміщення де довгий час перебуває людина.

Для захисту від витоку мовної інформації у вентиляції встановлено звукоізоляційний матеріал.

В кімнатах розташовані кондиціонери для забезпечення оптимальної температури в офісі, а також для охолодження обладнання.

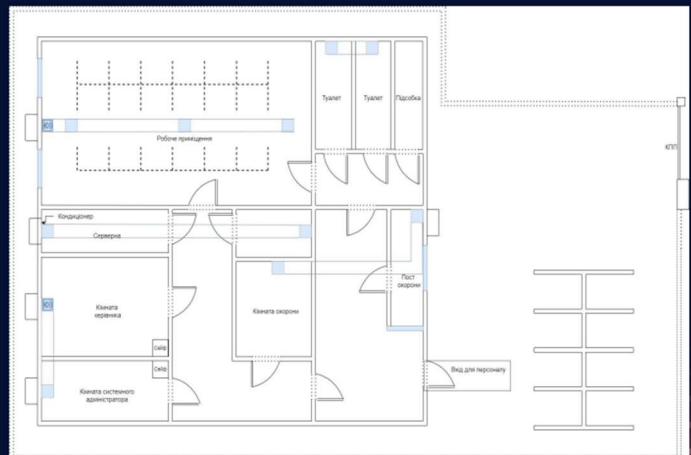


Рисунок А.6 – Слайд 5

Схема розташування протипожежних датчиків

7/12

На території всієї будівлі знаходяться датчики диму та датчиків витоків газу для забезпечення протипожежної безпеки та запобігання отруєнню газом, а також прилади для тушіння пожеж.

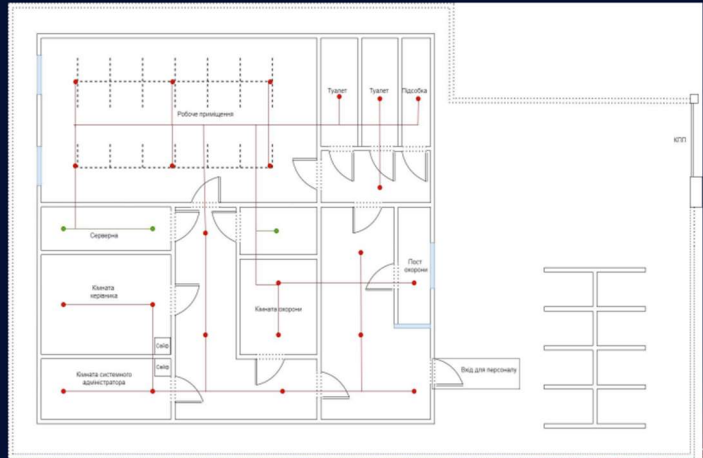


Рисунок А.7 – Слайд 6

Розділення доступу

8/12

Для підвищення захисту була запроваджена система розділення зон доступу.

- червона – високий рівень доступу;
- жовта – середній рівень доступу;
- зелена – низький рівень доступу.



Рисунок А.8 – Слайд 7

Зони огляду камер відеоспостереження

9/12

Камери відеоспостереження знаходяться по всій території приміщення та забезпечують такі кути огляду, які охоплюють важливі місця будівлі при цьому не захоплюють монітори працівників.

Зовні встановлено дві інфрачервоні камери для контролю входу на територію та в будівлю.

Всі камери з'єднанні з NVR регістраторами.

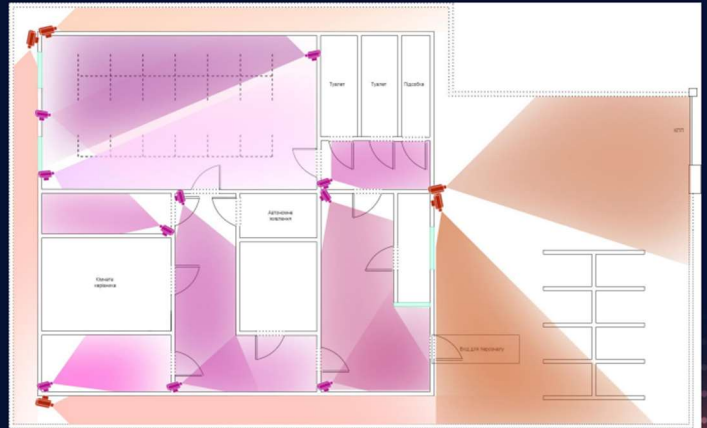


Рисунок А.9 – Слайд 8

Мережева безпека

10/12

Для забезпечення мережевої безпеки та для контролю трафіку треба розгорнути апаратний та програмний брандмауери.

Кожен комп'ютер треба обладнати антивірусними програмами.

На мережевому обладнанні треба впровадити системи IDS та IPS.

Слід регулярно проводити оновлення програмного забезпечення на комп'ютерах та сервері.

Велике значення має регулярне створення резервних копій.



Рисунок А.10 – Слайд 9

Комп'ютерні мережі та обладнання

11/12

Майже все обладнання, крім датчиків руху та розбиття скла, з'єднано з сервером.

Всі комп'ютери захищені паролями та мають обмежений доступ тільки до потрібної інформації.

Доступ до важливих приміщень таких, таких як кімната охорони, системного адміністратора, керівника, серверної та кімнати автономного живлення контролюється за допомогою ключ-карти.

Роутери мають змінені паролі та знаходяться в захищеному місці.

Датчики розбиття скла встановлені на всіх вікнах які мають вихід зовні.

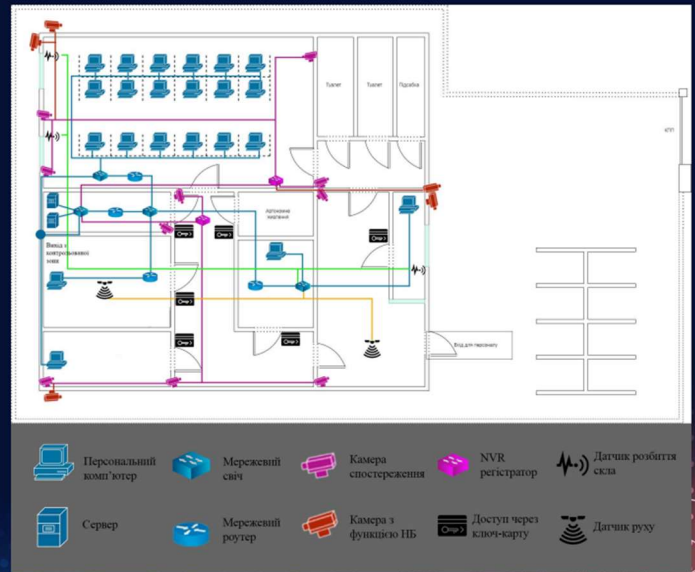


Рисунок А.10 – Слайд 11

12/12

Дякую за увагу!

Рисунок А.14 – Фінальний слайд