

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

(повне найменування інституту, назва факультету)

Кафедра інформаційної безпеки та наноелектроніки

(повна назва кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

бакалавр

(ступінь вищої освіти)

на тему Захист інформації у відділенні комерційного банку

(назва теми)

Protection of information in a commercial bank branch

Виконав: студент(ка) 4 курсу, групи БК-810

Спеціальності 125 Кібербезпека

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних систем

БУДЬОННИЙ А.В.

(ПРІЗВИЩЕ та ініціали)

Керівник ЛІЗУНОВ С.І.

(ПРІЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.

(ПРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
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 ІБтаН, к.ф.-м.н., доц.
Андрій КОРОТУН
“___” _____ 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

БУДЬОННОГО Андрія Віталійовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Захист інформації у відділенні комерційного банку
Protection of information in a commercial bank branch
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 «03» травня 2024 року № 192
2. Строк подання студентом проєкту (роботи) 01 червня 2024 року
3. Вихідні дані до проєкту (роботи) побудова системи захисту інформації у відділенні комерційного банку
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): проведення аналізу об'єкта на захист ІОД та обладнання від витоку інформації, проведення аналізу загроз витоку інформації на об'єкті, реалізація захисту інформації у відділенні комерційного банку
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): презентація у Microsoft power point (14 слайдів)

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	24.03.24	23.05.24
Нормоконтроль	КОРОЛЬКОВ Р.Ю., к.т.н. доцент	03.06.24	05.06.24

7. Дата видачі завдання « 24 » березня 2024 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	Виконано
2	Планування та розробка об'єкта дослідження	1 тиждень	Виконано
3	Збір та аналіз теоретичних відомостей	2 тиждень	Виконано
4	Аналіз обладнання та його захист	3-4 тижні	Виконано
5	Аналіз загроз інформаційної безпеки	5 тиждень	Виконано
6	Аналіз атак на безпеку мережі	6 тиждень	Виконано
7	Розробка системи захисту інформації	7-8 тижні	Виконано
8	Оформлення ПЗ та графічного матеріалу	9 тиждень	

Студент(ка)

_____ Андрій БУДЬОННИЙ
(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

_____ Сергій ЛІЗУНОВ
(підпис) (Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:
53 с., 9 рис., 1 таб., 20 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ РИЗИКИ,
ІНФОРМАЦІЙНІ СИСТЕМИ, КІБЕРАТАКИ, КІБЕРБЕЗПЕКА, КІБЕРБЕЗПЕКА
В БАНКІВСЬКІЙ СФЕРІ, КІБЕРЗАХИСТ, КОМЕРЦІЙНИЙ БАНК

Об'єкт дослідження – відділення комерційного банку.

Предмет дослідження – комплексна система захисту інформації.

Мета роботи – розробка системи захисту інформації у відділенні комерційного банку.

Для досягнення чинного рівня захисту об'єкта було проаналізовано рівень захисту інформації у відділенні комерційного банку.

В результаті було розроблено комплексну систему захисту інформації для об'єкту та запропоновано способи протидії потенційним загрозам.

ABSTRACT

Explanatory note to the diploma qualification work of the bachelor: 53 p., 9 fig., 1 tab., 20 sources.

INFORMATION SECURITY, CYBER PROTECTION, COMMERCIAL BANK, CYBER SECURITY, CYBER ATTACKS, INFORMATION SYSTEMS, CYBER SECURITY IN BANKING, INFORMATION RISKS

The object of the study - branch of a commercial bank.

The subject of the research - complex information protection system.

The purpose of the work - develop an information protection system in a branch of a commercial bank.

In order to achieve the current level of object protection, the level of information protection in the branch of a commercial bank was analyzed.

As a result, a complex information protection system was developed for the object and methods of countering potential threats were proposed.

ЗМІСТ

Перелік скорочень	7
Вступ	8
1 Теоретичні відомості про об'єкт та системи його захисту.....	9
1.1 Опис відділення банку та його класифікація	9
1.2 План будівлі	9
1.3 Види ІОД у комерційному банку	11
1.4 Обладнання на об'єкті	14
2 Аналіз загроз витоку інформації на об'єкті	21
2.1 Загрози безпеці і вразливі місця	21
2.2 Атаки на безпеку мережі.....	25
3 Розробка системи захисту інформації банку	31
Висновки	51
Перелік джерел посилання.....	52

ПЕРЕЛІК СКОРОЧЕНЬ

- ІОД- Інформація з обмеженим доступом
- ПЗ – Програмне забезпечення
- ЦПП - Центральна пожежна панель
- LAN – Local Network (локальна мережа)
- VLAN - Virtual Local Area Network (Віртуальна локальна комп'ютерна мережа)
- UPS - Uninterruptible Power Supply (джерело безперебійного живлення)
- DOS - Denial of Service (Відмова в обслуговуванні)
- DDOS - Distributed Denial of Service (Розподілена відмова в обслуговуванні)
- Spoofing- підробка
- DNS - Domain Name System (Система доменних імен)
- ARP - Address Resolution Protocol (Протокол вирішення адрес)
- VPN – Virtual Private Network (Віртуальна приватна мережа)
- IPS - Intrusion Prevention System (Система запобігання вторгненням)
- IDS - Intrusion Detection System (Система виявлення вторгнень)
- AC - Access Control (система контролю доступу)
- WAF - Web Application Firewall (Брандмауер веб-додатків)
- EDR - Endpoint Detection and Response (Виявлення кінцевої точки та відповідь)
- SIEM - Security Information and Event Management (Інформація про безпеку та управління подіями)
- DLP - Data Loss Prevention (Запобігання втраті даних)
- EMM – Enterprise Mobility Management (Управління мобільністю підприємства)

ВСТУП

Прийняття рішень у всіх сферах ділового чи організаційного життя все більше базується на інформаційних процесах. Аналіз цих процесів і подальша розробка управлінських рішень здійснюється на основі інформаційних моделей, що базуються на сучасних інформаційно-телекомунікаційних технологіях. Тому захист інформації є самостійною складовою загальної безпеки підприємства, і її значення з кожним роком зростає.

У даній дипломній роботі основний акцент ставився на розробці та впровадженні інтегрованої системи захисту інформації для відділення комерційного банку. Дана робота включає теоретичний аспект, що охоплює аналіз потенційних загроз та розробку ефективних стратегій протидії. Крім того, було виконано практичну частину, де розглядалися конкретні рішення для забезпечення безпеки інформаційних потоків у банківському середовищі.

Робота також містить аналіз основних ризиків, які можуть вплинути на безпеку інформації, та розгляд наявних методів та інструментів для їх запобігання. Важливою метою було створення надійної системи захисту, яка забезпечувала б стабільність та захищеність інформаційних ресурсів, у тому числі під час робочого та неробочого часу.

У заключній частині дипломної роботи продемонстровано практичне втілення розробленої системи захисту інформації для відділення комерційного банку.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ОБ'ЄКТ ТА СИСТЕМИ ЙОГО ЗАХИСТУ

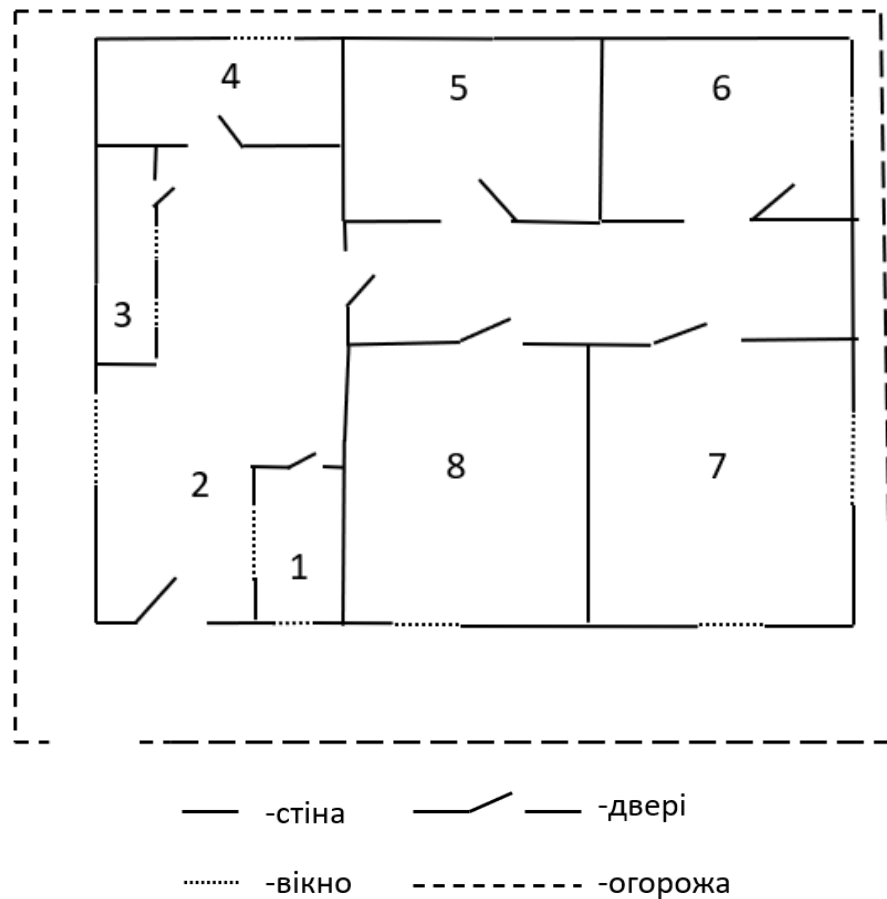
1.1 Опис відділення банку та його класифікація

Відділення комерційного банку - це приміщення, де активно працюють фахівці в галузі фінансів та банківських послуг. Діяльність в цьому приміщенні орієнтована на забезпечення фінансових операцій, обслуговування клієнтів і забезпечення безпеки фінансових транзакцій.

Робота відділення комерційного банку базується на комплексі методів і підходів до фінансових операцій, управління ризиками та забезпечення якості обслуговування клієнтів. Важливою складовою діяльності є забезпечення безпеки фінансових даних та інформаційних потоків, що вимагає використання сучасних технологій та методів захисту.

1.2 План будівлі

На рисунку 1.1 зображено план об'єкту комерційного банку, який розташований на 1 поверсі 5 поверхневого будинку. Під відділенням комерційного банку знаходиться підвал, над відділенням - житлові квартири. Навколо будівлі є огорожувальний паркан, проте вхід на територію вільний.



1 - кабінет охорони 2 - касовий зал 3 - операційні каси 4 - туалет
5 - серверна кімната 7 – бухгалтерія 8 - відділення інвестицій та кредитів

Рисунок 1.1 – План комерційного банку

Вхід до приміщення комерційного банку реалізується через охоронний пункт. Перед входом до відділення охоронець, який відповідає за контроль доступу до приміщення, перевіряє документи, ідентифікаційні картки. Охоронець також відповідальний за збереження матеріально-технічних цінностей і техніки, яка знаходиться на території банку [1].

Касовий зал та операційні каси у комерційному банку використовуються для здійснення готівкових операцій та обслуговування клієнтів.

Службовий простір обладнаний дверима з ключем доступу. Тільки авторизовані співробітники, які мають відповідний ключ, мають доступ до цього приміщення. Такий захід було проведено через то, що в даній частині об'єкта знаходяться сервери, апаратне забезпечення та інші важливі ресурси, необхідні для обробки даних та підтримки безпеки інформації. Цей простір захищений від

несанкціонованого доступу, що допомагає додатково запобігти від витоку конфіденційних даних та забезпечити їх збереження.

У серверній кімнаті комерційного банку розміщені сервери та інфраструктура для зберігання та обробки фінансової інформації. Роль серверів для банку полягає у забезпеченні функціонування банківської мережі, зберігання даних клієнтів, обробці транзакцій та забезпечення безпеки інформації.

Кабінет керівника призначений для прийняття стратегічних рішень та формування політики банку. Це приміщення використовується керівником для проведення зустрічей з ключовими клієнтами, управлінських нарад, а також для роботи над стратегічними планами банку.

Відділ бухгалтерії комерційного банку відповідає за облік фінансових операцій, складання звітності та аналіз фінансових даних. У цьому відділі працюють бухгалтери, які ведуть облік операцій з грошима, створюють фінансові звіти та забезпечують ведення обліку фінансових потоків банку.

Кредитно-інвестиційний відділ комерційного банку надає клієнтам комплексне фінансове обслуговування. Співробітники цього відділу консультують з усіх аспектів фінансів: від отримання кредитів до ведення інвестиційного портфеля [2].

1.3 Види ІОД у комерційному банку

В комерційному банку циркулюють наступні види інформації: паперова, мовна, електронна. Для початку, слід визначити, яка інформація перебуває з обмеженим доступом.

Банк зберігає конфіденційну та режимну інформацію, що включає власні коди програмного забезпечення й інтелектуальну власність, що використовуються для безпечного оброблення фінансових даних і потребують захисту від несанкціонованого доступу. На об'єкті такий вид інформації зазвичай циркулює в

серверному приміщенні у вигляді бази даних, кабінеті керівника у вигляді стратегічних планів, документації та фінансових звітів, а також відділенні інвестицій та кредитів, яка зберігає інформацію про інвестиційні портфелі, кредитні договори, клієнтські дані та фінансові плани.

Особиста інформація клієнтів, включаючи їхні фінансові стани та історії транзакцій, "біометрична інформація", така як унікальні біометричні дані про клієнтів або співробітників, наприклад, відбитки пальців, розпізнавання обличчя, голосові зразки, також знаходиться під суворим контролем охорони на об'єкті для забезпечення конфіденційності та відповідності законодавству про захист персональних даних. Охорона в свою чергу здійснює перевірку автентифікації кожного суб'єкта, який бажає отримати доступ до конфіденційної інформації.

Також, банк займається розробкою нових продуктів або послуг, а отже інформація про ці проекти, їх розробку та плани також є обмеженою і доступною лише обмеженому колу осіб у банку.

Детальний розподіл видів ІОД по відділенням наведено в табл. 1.1

Таблиця 1.1 – Циркулювання ІОД в приміщенні

Відділення	Види інформації
Кабінет охорони	цифровий, паперовий, розмовний
Касовий зал (зона клієнтів)	цифровий, паперовий
Операційні каси	цифровий, паперовий
Серверна кімната	цифровий
Кабінет керівника	цифровий, паперовий, розмовний
Бухгалтерія	цифровий, паперовий, розмовний
Відділення інвестицій та кредитів	цифровий, паперовий, розмовний

Мовна інформація відіграє важливу роль у всіх відділеннях банку, забезпечуючи комунікацію між клієнтами та персоналом. Задля загальної уяви варто зазначити види поширення мовної інформації в відділах.

У касовому залі та операційних касах співробітники здійснюють усні пояснення та консультації з клієнтами стосовно фінансових операцій та послуг.

В кабінеті охорони усна комунікація використовується для передачі інструкцій та внутрішньої комунікації між співробітниками охорони.

Відділення інвестицій та кредитів надає усні консультації щодо умов кредитування та інвестиційних можливостей.

У кабінеті керівника усна комунікація використовується для обговорення стратегій управління та планування діяльності банку.

Бухгалтерія використовує усну комунікацію для обговорення фінансових звітів та узгодження облікових документів.

Паперова та цифрова інформація може використовуватись в комерційному банку в різних контекстах.

Кабінет охорони використовує паперову інформацію, таку як журнали відвідувань та списки співробітників охорони, для обліку відвідувань та перевірки присутності персоналу. Тут також застосовуються цифрові системи відеоспостереження та контролю доступу для забезпечення безпеки [1].

Касовий зал та операційні каси зберігають денні звіти касира, які реєструють готівкові операції протягом робочого дня, а також документацію щодо виплат, вкладів, обміну валют і платіжних операцій. Також тут можуть зберігатися форми операційних документів, необхідні для здійснення різних фінансових транзакцій та підтримки обліку операцій банку.

Серверна кімната використовується для зберігання та обробки цифрової інформації, що зберігається на серверах.

Кабінет керівника використовує як цифрові системи управління та звітності, так і паперові документи для контролю та аналізу фінансових даних. Також, керівник може проводити наради або зустрічі у своєму кабінеті. В кабінеті знаходяться різноманітні документи, такі як фінансові звіти банку, протоколи нарад, аналітичні звіти, бізнес-плани, контракти з ключовими клієнтами, а також внутрішні положення і стратегічні документи, пов'язані з управлінням банком.

Бухгалтерія використовує паперові бухгалтерські документи для ведення обліку та цифрові системи для аналізу фінансових даних. В даному кабінеті існують документи, які використовуються для бухгалтерського обліку та звітності

й інші робочі матеріали, необхідні для ведення бухгалтерської діяльності.

У відділенні інвестицій та кредитів використовуються паперові документи для укладання угод та цифрові системи для управління фінансовими активами, а також, обробляються кредитні заявки та аналізуються фінансові документи клієнтів для надання кредитів. Тут обмінюються звітами, розрахунками, приймають рішення щодо інвестиційних портфелів та проводять аналіз ринків [2, 6].

1.4 Обладнання на об'єкті.

На рисунку 1.2 зображено план об'єкта з цифровим обладнанням, яке використовується в роботі.

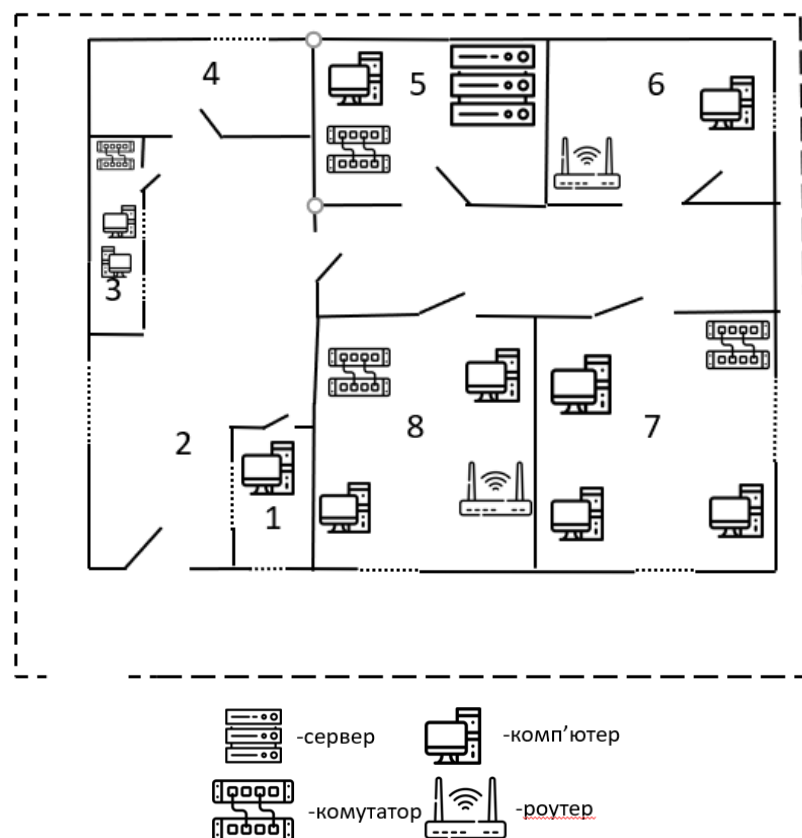


Рисунок 1.2 – Схематичне розташування обладнання

Комутатори виконують критично важливу роль у мережевій інфраструктурі, дозволяючи ефективно розподіляти трафік і забезпечувати високошвидкісне з'єднання між різними пристроями.

Комутатори дозволяють створювати мережеві сегменти, що підвищує продуктивність мережі шляхом зменшення кількості колізій і підвищення швидкості обміну даними. Вони з'єднують робочі станції співробітників банку з серверами, що зберігають фінансові дані, облікову інформацію та інші важливі ресурси [2].

Комутатори створюють VLAN (віртуальні локальні мережі), що дозволяє ізолювати різні частини мережі для підвищення продуктивності та організації роботи. Вони забезпечують з'єднання мережевих принтерів, сканерів і телефонних систем з основною мережею. Крім того, комутатори дозволяють підключати внутрішню мережу банку до зовнішніх мереж через маршрутизатори.

Маршрутизатори в банку використовуються для швидкого та надійного підключення до мережі Інтернет, забезпечуючи доступ клієнтів до онлайн-банківських послуг. Вони відіграють ключову роль у забезпеченні стабільного з'єднання між різними відділеннями банку, обробляючи великий обсяг мережевого трафіку з мінімальними затримками. Завдяки високій пропускній здатності маршрутизатори здатні підтримувати одночасне виконання численних транзакцій та операцій, що є критично важливим для безперебійної роботи банківських систем.

Вони також дозволяють інтегрувати різні мережеві сервіси, такі як VoIP для внутрішнього телефонного зв'язку, і оптимізувати маршрути передачі даних для підвищення ефективності роботи мережі. Маршрутизатори забезпечують з'єднання між внутрішньою мережею банку і зовнішніми партнерами, дозволяючи здійснювати безпечний обмін даними та інтеграцію з іншими фінансовими установами [3,5].

Роль сервера полягає в обробці запитів працівників банку, забезпечуючи їм доступ до необхідної інформації. Основні технології, які використовуються в цих серверах, включають віртуалізацію, що дозволяє ефективно використовувати

апаратні ресурси, такі як пам'ять та обчислювальну потужність, шляхом створення віртуальних екземплярів операційних систем на одному фізичному сервері. Також використовуються технології забезпечення високої доступності, такі як кластеризація серверів і механізми резервного копіювання даних, для запобігання відмовам і втраті інформації [3].

Комп'ютери у банку використовуються для обробки фінансових транзакцій, управління клієнтськими рахунками, аналізу фінансових даних та забезпечення доступу до банківських послуг, видачу кредитів, ведення бухгалтерського обліку та інші банківські послуги з використанням сучасних технологій. У банківській діяльності застосовуються різні протоколи для забезпечення ефективного обміну даними між комп'ютерами та іншими пристроями. Наприклад, для забезпечення безпечного з'єднання можуть використовуватися протоколи HTTPS або SSH. Для внутрішньої мережі банку можуть використовуватися протоколи Ethernet або Wi-Fi для швидкого та надійного обміну даними [3].

Для серверів та комп'ютерів існують джерела аварійного електроживлення, що гарантують безперервну роботу та захист даних у разі перебоїв з основним живленням. При відмові основного живлення, джерела аварійного електроживлення автоматично включаються, надаючи короткий час для продовження роботи сервера та комп'ютерів. Це дає користувачеві можливість зберегти роботу та вимкнути комп'ютер без втрати даних або можливих пошкоджень обладнання.

Електроживлення у приміщенні розміщено у вигляді централізованої електромережі. Так як серверна кімната більш контрольована з боку охорони, там знаходяться прилади аварійного електроживлення, такі як:

- стабілізатори напруги, які допомагають підтримувати стабільну напругу для обладнання в разі коливань напруги в електричній мережі;

- UPS пристрій, який використовуються для тимчасового забезпечення енергією у випадку відключення основного джерела живлення;

-автоматична система переключення живлення, яка перемикає живлення на резервні джерела (UPS пристрій) у разі відключення основного електропостачання [5].

Також, в кімнаті знаходиться електрощиток.

Інформаційні кабелі в комерційному банку включають у себе мережеві кабелі (Ethernet, волоконно-оптичні кабелі тощо), що забезпечують зв'язок між комп'ютерами, серверами, принтерами, телефонних систем та систем захисту, такими як, відеоспостереження та датчики руху [6].

На рисунку 1.3 зображено схему електроживлення та інформаційної мережі на об'єкті.

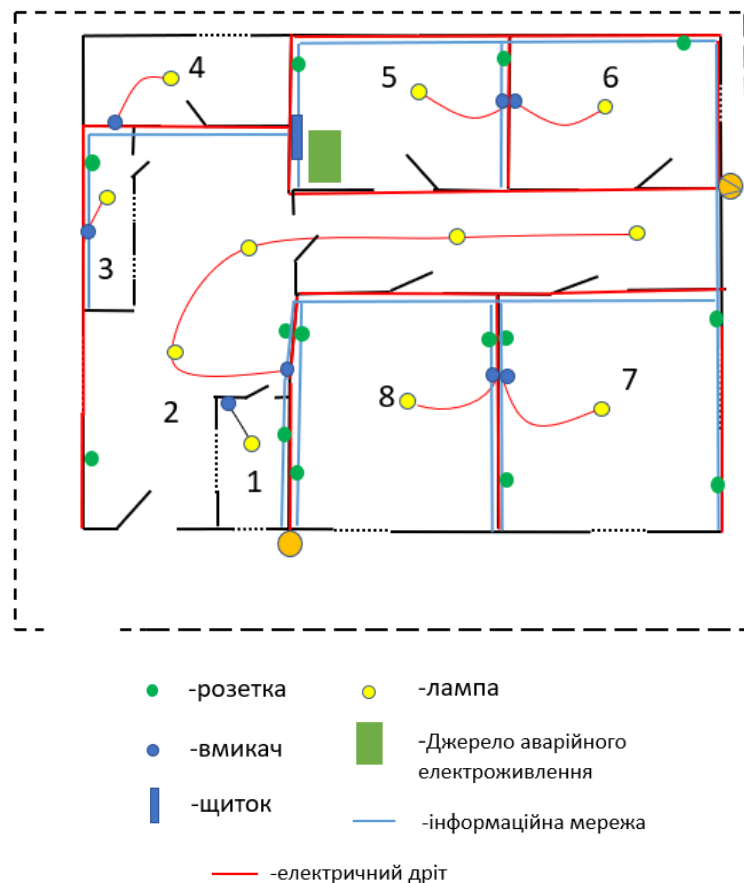


Рисунок 1.3 – Схематичне розташування електромережі та інформаційної мережі

Протипожежні датчики виявляють можливі загрози пожежі на ранніх стадіях. Коли пожежний датчик спрацює, він надсилає сигнал на ЦПП

(центральну пожежну панель), яка знаходиться в кабінеті охорони що активує пожежну сигналізацію та інші системи безпеки. Це дозволяє персоналу банку, а також службам пожежної охорони, оперативно реагувати на ситуацію та приймати необхідні заходи. Реагуючи на пожежу вчасно, банк може запобігти серйозним пошкодженням майна, включаючи фінансові документи, обладнання та інші цінності. Сигнали з протипожежних датчиків надходять до охоронного приміщення в центральну пожежну панель.

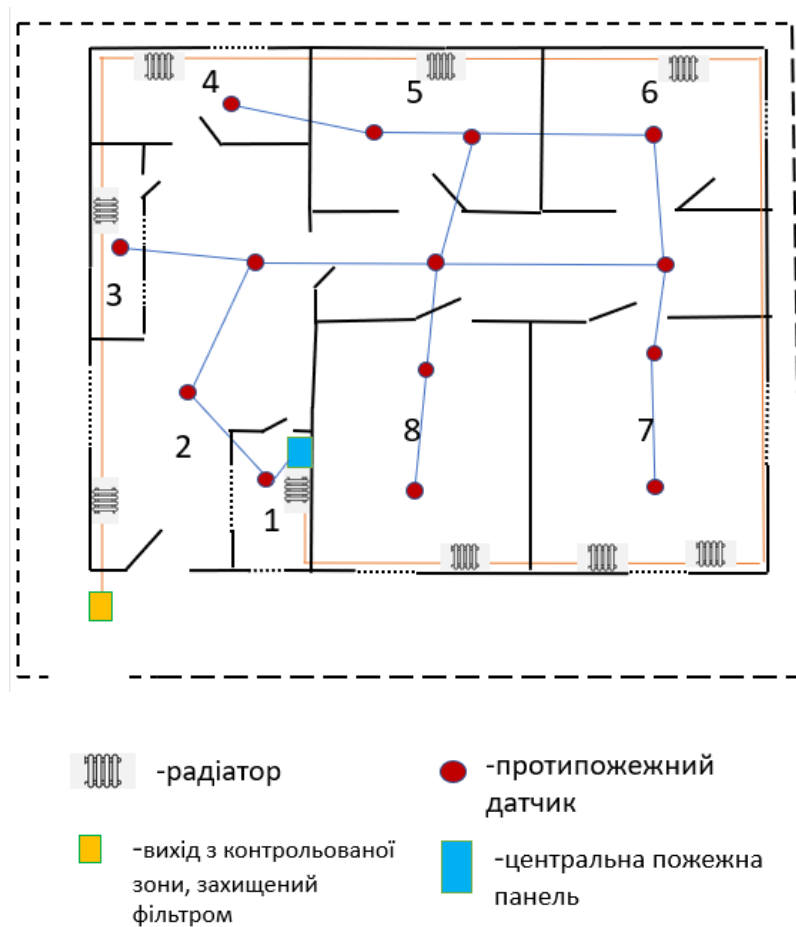


Рисунок 1.4 – Схематичне розташування протипожежних датчиків та опалення

Вентиляція регулює температуру та вологість, відводить тепло, яке генерує обладнання, що допомагає у запобіганні їх перегріву та збереженні їх працездатності, а також, сприяє тривалому терміну служби. Крім того, вентиляційна система виконує важливу функцію у видаленні пилу та інших частинок з повітря, що допомагає підтримувати чистоту обладнання та зменшує

можливості засмічення внутрішніх компонентів, що може вплинути на його роботу [3].

Система водопостачання та водовідведення в банку проходить через спеціально обладнані технічні шахти та канали, які забезпечують оптимальне розташування інженерних комунікацій. Це дозволяє мінімізувати зайвий простір та забезпечити легкий доступ для технічного обслуговування та ремонту. Шахти та канали, через які проходять труби, розташовані таким чином, щоб не заважати роботі співробітників та обслуговуванню клієнтів.

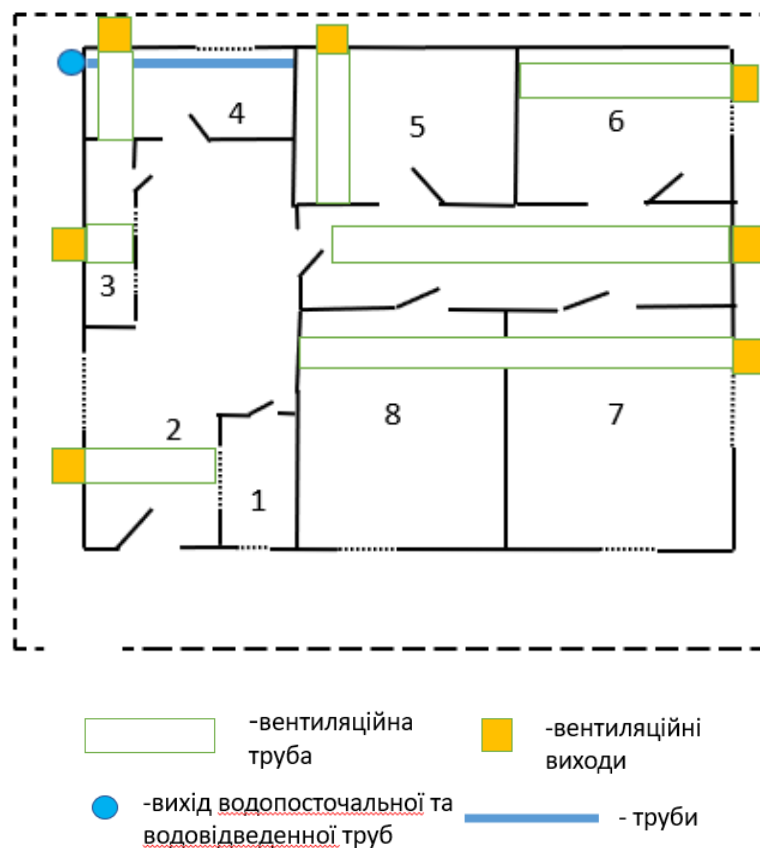


Рисунок 1.5 – Схематичне розташування вентиляції та труб

Система датчиків руху в приміщенні комерційного банку є важливою складовою системи безпеки. Ці датчики можуть виявляти будь-який рух або неправильну активність, спрацьовуючи при спробах незаконного доступу чи вторгнень у приміщення. Вони активують спеціальні системи сигналізації та

одразу сповіщають охорону про потенційну загрозу або події.

Камери відеоспостереження також відіграють важливу роль у забезпеченні безпеки. Вони розміщені в стратегічних місцях, які включають входи, коридори, зони обслуговування клієнтів та інші критичні ділянки приміщення. Ці камери реєструють відео зображення, які можуть бути використані для відслідковування подій, виявлення порушників та надання доказів у випадку інцидентів чи потенційних правопорушень [1].

Інформація з камер та датчиків руху зберігається на комп'ютері, розташованому в кабінеті охорони. Цей комп'ютер обладнаний спеціальним програмним забезпеченням для моніторингу та збереження відео- та аудіозаписів, отриманих від камер та датчиків руху. Доступ до цього комп'ютера обмежено та захищено паролем і відбувається лише за необхідності перегляду або аналізу інформації. Це забезпечує конфіденційність та безпеку зібраної інформації [5].

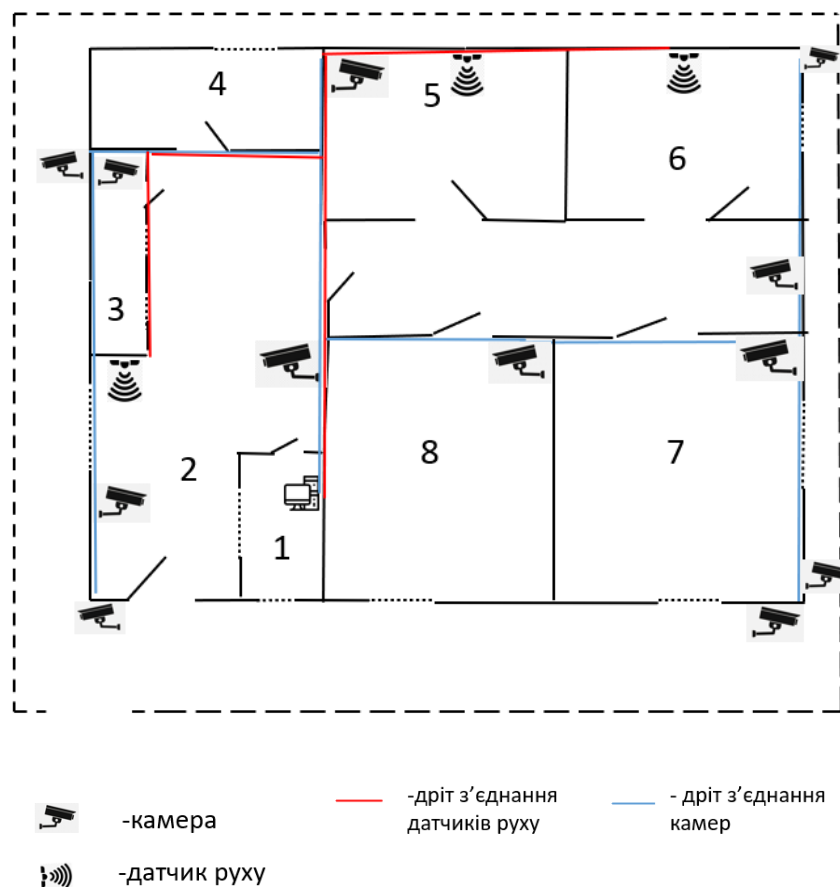


Рисунок 1.6 – Схематичне розташування систем датчиків руху та відеоспостереження

2 АНАЛІЗ ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ

2.1 Загрози безпеці і вразливі місця

Кібербезпека в банківській справі – це набір технологій і методів, призначених для забезпечення безпеки даних і активів клієнтів і підтримки репутації банку. Добре продумана стратегія кібербезпеки може допомогти фінансовій установі ефективно захистити своїх клієнтів від пов'язаних загроз, таких як кібератаки, крадіжка даних, зловмисне програмне забезпечення, хакерство тощо. Комп'ютери в банку можуть стати мішенню для кібератак. Недостатня оновлення програмного забезпечення, відсутність антивірусів чи захисту від зловмисних програм можуть призвести до несанкціонованого доступу до інформації.

Сервери, де зберігаються великі обсяги конфіденційних даних, можуть стати об'єктом спроб кібератак. Недостатня захищеність серверів, слабкі паролі адміністраторів або вразливості в програмному забезпеченні можуть призвести до витоку цінної інформації. У серверній кімнаті копії конфіденційних даних зберігаються на зовнішніх носіях, таких як жорсткі диски, флеш-накопичувачі.

Зовнішні загрози включають побічні електромагнітні випромінювання і наведення, які можуть становити потенційну загрозу для безпеки інформації, оскільки їх можна використовувати для несанкціонованого збору конфіденційної інформації [11].

Електромагнітні хвилі, що випромінюються обладнанням банку, таким як комп'ютери, мережеві пристрої, можуть бути перехоплені зовнішніми приладами і використані для збору інформації [10,11].

Електромагнітні поля можуть наводити електрорушійну силу в проводах, які не мають фізичного з'єднання з обладнанням, але перебувають у його безпосередній близькості. Це може призвести до витоку інформації через наведення на кабелі та дроти [10].

Захист конфіденційної інформації від витоку через акустичні (вентиляція)

та віброакустичні канали, такі як вентиляційні, опалювальні системи, системи водопостачання та водовідведення, двері та вікна, які можуть стати серйозною загрозою для безпеки інформації. Такі канали можуть передавати звукові коливання, які виникають від роботи комп'ютерів, обладнання, розмов та інших джерел, і в цей спосіб конфіденційна інформація може стати доступною стороннім особам.

Однією з основних переваг будь-якої мережі є спільне використання ресурсів, таких як файли та принтери. Проте, це також створює потенційну загрозу безпеці, оскільки будь-хто може спробувати отримати несанкціонований доступ до мережі через спільні ресурси. Поділ пароля, методи вгадування та захоплення - це три поширені методи отримання несанкціонованого доступу. Використання спільного пароля та вгадування - це вже відомі способи незаконного доступу, тому важливо вживати ефективні заходи захисту для запобігання подібним загрозам [7].

В банківському середовищі неналежний доступ до ресурсів може стати серйозною проблемою безпеки. Внутрішні загрози можуть виходити від персоналу, у вигляді доступу до ІОД. Недбале обговорення чи передача паролів, копіювання конфіденційних даних на зовнішні носії або пошкодження (модифікація) ІОД можуть призвести до загроз витоку або знищення інформації.

Неавторизований доступ виникає, коли користувач намагається отримати доступ до ресурсів, до яких він не має права доступу. Це може відбутися через помилки в призначенні прав доступу адміністраторами або недостатність привілеїв для користувача [7,11].

У банківських установах, де працюють різні відділи та категорії користувачів, такі як фінансові аналітики, клієнтські менеджери та технічний персонал, необхідно ретельно керувати доступом до ресурсів. Наприклад, доступ до фінансових даних бухгалтерії повинен бути обмежений лише для відповідних фахівців з фінансів, а не доступним для інших відділів або осіб, які не мають відношення до фінансової діяльності.

Адміністратори систем безпеки в банку повинні встановлювати і строго

контролювати права доступу до різних мережесих ресурсів, забезпечуючи, що лише авторизовані користувачі отримують доступ до конфіденційної інформації та фінансових ресурсів. Це допомагає уникнути можливих порушень безпеки та зберегти конфіденційність інформації клієнтів та банківських операцій [11].

У банківській сфері несанкціонована модифікація даних є серйозною загрозою для цілісності та безпеки інформації. Якщо дані або програмне забезпечення були модифіковані без дозволу, це може призвести до серйозних проблем, включаючи пошкодження баз даних, електронних таблиць та інших важливих програм. Навіть невеликі зміни в програмах можуть спричинити недоречні наслідки, такі як несправність операційних систем або взаємодіючих програм, що вимагають повторної установки [14].

Цю атаку можуть здійснити як несанкціоновані користувачі, так і авторизовані особи. Будь-які зміни в даних або програмах можуть призвести до перенаправлення інформації в непередбачені місця призначення. Ця модифікована інформація може бути використана зловмисниками для власних цілей, наприклад, для внесення подальших змін та перенаправлення до інших систем або користувачів.

Причини несанкціонованої модифікації даних можуть бути різноманітними, включаючи відсутність шифрування даних, помилкове надання дозволів на читання та запис, недостатність механізмів контролю доступу та відсутність ефективних засобів захисту. Важливо вживати заходів захисту даних та механізмів контролю доступу для запобігання подібним інцидентам та збереження безпеки інформації в банківській системі [12].

Розголошення мережевого трафіку також може стати серйозною загрозою для безпеки та конфіденційності даних клієнтів та фінансових транзакцій. Коли ми говоримо про безпеку даних, ми бачимо, що є два різних типи даних: перший тип - дані, які знаходяться в системі або комп'ютерах, і другий - дані, які передаються від комп'ютерної системи до системи або поділяються між користувачами мережі. Ці два типи даних підпадають під два типи безпеки: комп'ютерна безпека та мережева безпека. Засоби, які призначені для захисту

перших типів даних, у комп'ютерній безпеці, а захист даних під час їх передачі називається безпека мережі. Однак ми не можемо розрізнити чітку різницю між цими двома типами безпеки. Користувачі знають, які типи даних є конфіденційними, і це також важливо підтримувати конфіденційність цих даних під час їх передачі. Дані, які можуть бути скомпрометовані, містять паролі, повідомлення електронної пошти, імена користувачів або будь-яку іншу корисну інформацію, яка може бути використана в майбутньому з негативною метою. Навіть електронні листи та паролі, які зберігаються у зашифрованому форматі в системі, можуть бути захоплені під час передачі як відкритий текст [13].

Часом природа демонструє свою силу, і втрата через стихійні лиха може бути навіть небезпечнішою, ніж віруси. Повінь, пожежа, страйки, гроза, землетруси, виверження вулканів, вибухи під водою, втрата зв'язку – це лише кілька прикладів того, які небезпеки може нести природа, завдаючи шкоди як фізичній, так і мережевій інфраструктурі. Іноді ці катастрофи настають несподівано, наприклад, у зимову бурю, коли комп'ютерні мережі можуть працювати на повну потужність, але люди не можуть потрапити до офісу через втрату інфраструктури [8].

Будь-який хто намагається отримати незаконний доступ до комп'ютерних систем з метою крадіжки або пошкодження даних називається хакером. Хакери є реальною та найнебезпечнішою загрозою для організацій з великою комп'ютерною системною мережею. Вони можуть бути зсередини організації, поза нею або навіть на іншому континенті. Хакери порушують безпеку систем, компрометують систему та викрадають дані до виявлення незаконного доступу. Злом може бути двох типів: етичне та неетичне хакерство. Неетичні хакери завдають шкоди будь-якій організації. Щоб відбити хакерську атаку, спочатку потрібно знати, як вони думають. Сучасні організації наймають хакерів, щоб знайти вразливі місця в механізмі безпеки мережі. Такий вид злomu називається етичним хакерством, і таких хакерів називають етичними хакерами [8].

2.2 Атаки на безпеку мережі

Атака на систему – це будь-яка спроба отримати несанкціонований доступ до інформаційних ресурсів системи, порушити їх конфіденційність, цілісність або доступність. Система, яка забезпечує точне надання послуг, необхідних користувачеві, і запобігає незаконному використанню системних ресурсів, називається безпечною системою. Атаки можна розділити на такі основні категорії: переривання, перехоплення, модифікація та вигадка.

Для використання даних або ресурсів необхідно, щоб вони були доступні 24/7 уповноваженим сторонам, коли і де їм це потрібно. Атака на доступність даних називається перериванням. На доступність можуть впливати навмисні чи ненавмисні дії. Прикладами ненавмисних дій є випадковий збій системи, видалення та перезапис даних і деякий час через нелюдські фактори, такі як повені, пожежі та землетруси. Тоді як руйнування інфраструктури через війни, страйки та окремі атаки хакерів, які призводять до збою системи, як-от відмова в обслуговуванні (DOS) і розподілена відмова в обслуговуванні (DDOS) атаки, є прикладами навмисних дій. Захист від доступності атак включає резервне копіювання та відновлення [8].

Основна концепція перехоплення полягає в тому, що дані повинні бути приховані від неавторизованих користувачів. Якщо хтось, хто не має права переглядати особисті дані, може переглядати або копіювати дані, які можуть далі використовуватися в інтенсивній активній атаці. Така атака відома як атака на конфіденційність. Цілісність даних може бути досягнута за допомогою сильної та суворої автентифікації та контролю доступу, тому що певний час авторизовані користувачі також можуть становити загрозу для конфіденційності даних. Вони можуть отримати облікові дані іншої особи [3,15].

Цілісність даних стосується запобігання навмисній чи ненавмисній модифікації даних. Атака на цілісність даних називається модифікацією. Різні алгоритми використовуються для перевірки даних, які можуть протистояти зміні

даних. Захист даних від модифікації є першочерговою проблемою, ніж виявлення. Цілісність даних може підтримуватися на багатьох рівнях моделі системи OSI.

Напад на автентичність називається вигадкою. Автентичність означає, що повідомлення походить від видимого джерела. Це гарантує, що ви той, за кого себе видаєте. Ім'я користувача та пароль є найпоширенішим способом досягнення автентифікації. Деякі інші методи включають смарт-картки та цифрові сертифікати.

Зловмисне програмне забезпечення та програми-вимагачі залишаються головним болем, який не зникає. З кожним роком ці атаки стають дедалі прогресивнішими та створюють численні проблеми для банківської галузі. Вони працюють таким чином: кіберзлочинці заражають комп'ютери шкідливим програмним забезпеченням, як правило, за допомогою фішингових електронних листів, і обмежують доступ до деяких даних за допомогою шифрування. Тоді шахраї стверджують, що банківські організації повинні заплатити суму грошей, щоб отримати доступ до даних [11].

Атаки зловмисного програмного забезпечення мають жахливі потенційні наслідки, такі як зрив бізнесу та операцій, фінансові втрати та репутаційні збитки. Крім того, кіберзлочинці можуть використовувати вразливі веб-сервіси для доставки програм-вимагачів багатьом користувачам.

Фішинг є одним із улюблених інструментів, які використовують кіберзлочинці для поширення шкідливого програмного забезпечення. Потім вони використовують різні хитрощі, щоб змусити людей встановити його на своїх пристроях під фальшивим приводом. Деякі зловмисники також можуть вимагати, щоб клієнти поділилися своїми особистими даними, щоб використовувати їх у шахрайських цілях [9].

Таким чином, клієнти можуть отримувати фішингові електронні листи, замасковані під офіційне банківське листування. Таким чином вони зможуть отримати доступ до фінансової інформації та викрасти гроші з рахунків клієнтів. Також такі напади можуть бути спрямовані на співробітників. Кіберзлочинці можуть захотіти заволодіти обліковими даними для входу, які надають доступ до

внутрішньої інформації, зокрема даних клієнтів.

Після карантину на тлі пандемії COVID-19 дистанційна робота стала звичайною практикою і доступна в багатьох сферах діяльності, включаючи банківський сектор. А у випадку, коли віддалений працівник має доступ до важливої або конфіденційної інформації, дуже важливо серйозно ставитися до кібербезпеки.

Люди, які працюють віддалено, часто працюють у кафе, вдома чи в коворкінгу зі своїх персональних пристроїв. Таким чином, виникають додаткові ризики, пов'язані з витоком даних. Більше того, банківські ІТ-фахівці не можуть забезпечити безпеку програмного забезпечення співробітників або будь-яким чином контролювати його. Таким чином, віддалена робота пов'язана з більшою потенційною вразливістю кібербезпеки. Саме тому банківським організаціям необхідно особливо старанно інформувати віддалених співробітників про потенційні загрози. Співробітники повинні знати, як розпізнавати їх і залишатися в безпеці у віддаленому робочому середовищі.

Дані, які зберігаються на пристрої банку, але залишаються незашифрованими, створюють багато потенційних загроз. Якщо дані незашифровані, хакери можуть легко отримати доступ до всієї конфіденційної інформації. Тому вся інформація, що зберігається, повинна бути зашифрованою. Таким чином, шахраї не зможуть ним скористатися, навіть якщо вони вкрадуть його з вашого комп'ютера [8,13].

Перехоплення пароля – це техніка, за якої хакер несвідомо викрадає ідентифікатор користувача та пароль. Надійні, довгі та зашифровані паролі не означають, що вони незламні; це лише питання часу. Кілька років тому час для злому пароля міг становити 100 днів, але зараз це лише питання двох-трьох тижнів. Різні типи атак злому паролів.

Словникова атака - це метод злому пароля, в якому зловмисник використовує словник або список часто вживаних паролів або можливих комбінацій для спроби відгадати пароль. Програма для виконання такої атаки перебирає словник, шукаючи збіги зі списком паролів.

Атака грубою силою - це метод злому пароля, в якому зловмисник випробовує всі можливі комбінації символів один за одним, починаючи з найкоротших і закінчуючи найдовшими паролями. Цей метод дуже ресурсомісткий і зазвичай вимагає значної кількості часу для успішного злому складного пароля [8,14].

Гібридна атака - це комбінований підхід, який поєднує методи словникової атаки та атаки грубою силою. Зазвичай гібридна атака спочатку використовує словниковий список для швидшого перебору можливих варіантів, а потім переходить до атаки грубою силою для більш складних паролів, які не вдалося взламатися за допомогою словника.

Хмарні атаки стають популярними, оскільки багато фінансових служб зберігають свою конфіденційну інформацію в хмарі. Тому кіберзлочинці починають організовувати масові атаки, щоб отримати необхідні дані з хмарних сховищ. Тому фінансовим установам слід бути обережними. Рекомендується забезпечити безпечну конфігурацію хмарної інфраструктури, щоб уникнути витоку даних [12].

Кібератаки, які здійснюються через ланцюг постачання програмного забезпечення. Цей метод розповсюдження зловмисного програмного забезпечення використовує ланцюжок постачання банку для доставки шкідливого програмного забезпечення. Для кіберзловмисників це чудова можливість скомпрометувати системи розподілу та залишатися в них протягом тривалого часу. Такі атаки зазвичай мають форму законних оновлень, які містять шкідливий код. Щоб протистояти кібератаці, фінансові організації повинні інформувати своїх клієнтів про те, як кіберзлочинці можуть отримати їхні особисті дані через оновлення [13].

Штучний інтелект приносить багато переваг у сфері кібербезпеки. З його допомогою ІТ-фахівці створюють новітні автоматизовані системи безпеки, які допомагають фінансовим установам покращувати протоколи безпеки та запобігати кіберзагрозам. Однак кіберзловмисники також можуть використовувати інструменти на основі штучного інтелекту для розробки розумних інструментів зловмисного програмного забезпечення та доставки

шкідливого коду в обхід інноваційних систем безпеки [8].

Соціальна інженерія близька до фішингу. Однак ці загрози кібербезпеці можуть переслідувати різні цілі. Соціальна інженерія також може проявлятися у формі китобійних атак або надсилання фальшивих рахунків. Простіше кажучи, це форма загрози, яка використовує тактику поведінки, щоб змусити людей розкрити конфіденційну чи конфіденційну інформацію або віддати свої гроші кіберзлочинцям [13].

Методи, якими зазвичай користуються зловмисники, базуються на зміцненні довіри та ввічливості. Наприклад, шахраї можуть зламати обліковий запис вашого друга та попросити вас позичити їм гроші від їхнього імені. Важливо пам'ятати, що люди є найбільш вразливою ланкою цього ланцюга. Тому вкрай важливо інформувати клієнтів і співробітників про методи, які використовують шахраї для запобігання кіберзлочинам [13].

Шахрайство та крадіжка особистих даних не є новими для фінансового сектора, але все ще досить успішні для зловмисників. Це пояснюється тим, що вони приймають різні форми та використовують інші канали та ланцюги для обробки персональних даних. Тому важливо впроваджувати сучасні стратегії кібербезпеки, щоб захистити клієнтів і співробітників від цих кіберзагроз. Це включає інструменти, які можуть виявляти підозрілу активність облікового запису та блокувати його, щоб запобігти подальшим злочинним діям [14].

Спуфінг (Spoofing) трохи схожий на фішинг, але більш складний і заплутаний. Він може бути у формі підробленого домену, який дуже схожий на існуючий законний домен. Таким чином, не дуже уважні клієнти можуть прийняти це за справжню банківську послугу та поділитися своїми даними зловмисникам. Деякі шахраї також можуть написати або зателефонувати клієнту банку від його імені, використовуючи сфабрикований номер телефону, який неможливо відрізнити від законного номера [12].

DDoS-атаки працюють, спрямовуючи зловмисний трафік до цілі через кілька комп'ютерів або машин. Часто ці машини утворюють ботнет: групу пристроїв, які були скомпрометовані зловмисним програмним забезпеченням і

можуть контролюватися одним зловмисником. Інші DDoS-атаки можуть залучати кількох зловмисників або інструменти DDoS-атаки, такі як програми для стрес-тестування (наприклад, LOIC) або програми з низьким і повільним доступом (наприклад, Slowloris). Зачастую ці машини утворюють ботнет: групу пристроїв, заражених шкідливим ПО і які можуть керувати одним зловмисником. В інших DDoS-атаках можуть брати участь кілька зловмисників або інструменти DDoS-атаки, такі як програми для стрес-тестування (наприклад, LOIC) або низько- і повільні програми (наприклад, Slowloris).

Отруєння DNS — це поширена техніка злому, яка маніпулює відомими вразливими місцями в системі доменних імен (DNS) мережі. Після завершення загрози мають можливість перенаправляти трафік з одного сайту на підроблену версію цього сайту [17].

З іншого боку, отруєння ARP (також відоме як ARP-спуфінг) є іншим типом поширеної кібератаки, яка натомість здійснюється через локальну мережу (LAN). Він передбачає надсилення зловмисних ARP-пакетів до шлюзу за замовчуванням у локальній мережі, щоб змінити пари в його таблиці IP-адрес до MAC-адрес [15].

Обидва ініціюють перехоплення часто конфіденційних даних і можуть призвести до фінансової та репутаційної шкоди.

Атака нульового дня (також відома як Day Zero) — це атака, яка використовує потенційно серйозну слабкість безпеки програмного забезпечення, про яку постачальник або розробник може не знати. Зазвичай він містить рекламне або шпигунське програмне забезпечення [12].

Команди безпеки повинні негайно усунути використану вразливість, як тільки вона буде виявлена, щоб обмежити загрозу для користувачів програмного забезпечення. Через те, наскільки підступними є багато атак нульового дня, на їх виявлення можуть знадобитися тижні або навіть місяця [13].

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ БАНКУ

Для захисту від прослуховування вентиляційні системи оснащені спеціальними акустичними фільтрами. Ці фільтри призначені для поглинання звукових хвиль і запобігання їх проникненню через вентиляційні отвори. Їхнє використання дозволяє зменшити можливість перехоплення чутливої інформації за допомогою акустичних методів. Акустичні методи прослуховування включають аналіз звуків у приміщенні або вібрацій, що походять з будівлі. Ці методи можуть використовувати спеціальне обладнання для запису або аналізу звукових сигналів з метою збору чутливої інформації.

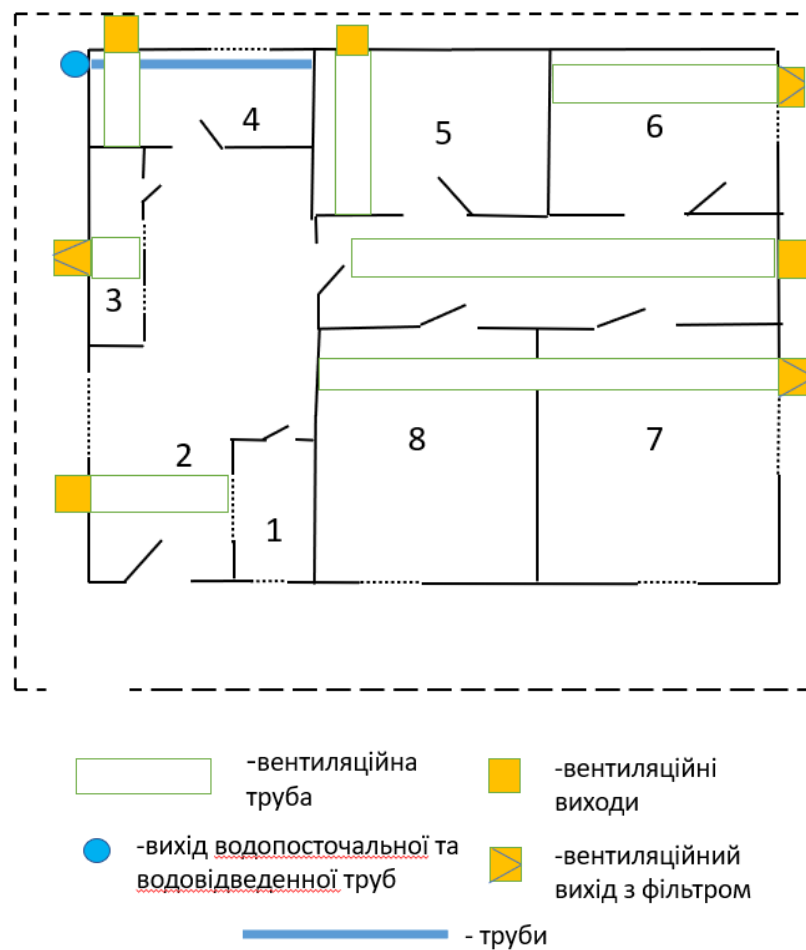


Рисунок 3.1 – Розташування фільтрів вентиляції

Для захисту інформації від витоку акустичними та віброакустичними каналами по водопостачанню та водовідведення виконується за допомогою спеціальних матеріалів для ізоляції труб. Застосування акустичних ізоляторів, таких як гумові або пластикові прокладки, може значно зменшити передачу звукових коливань через труби. Це допомагає запобігти несанкціонованому прослуховуванню, яке може використовувати акустичні сигнали, що передаються через водопровідні системи.

Захист виходу з контрольованої зони системи опалення здійснений за допомогою віброакустичного фільтра. Ці фільтри призначені для приглушення або блокування звукових коливань, які можуть передаватися через опалювальну систему. Вони ефективно запобігають можливості прослуховування або запису конфіденційної інформації, що обговорюється в приміщеннях з опалювальною системою.

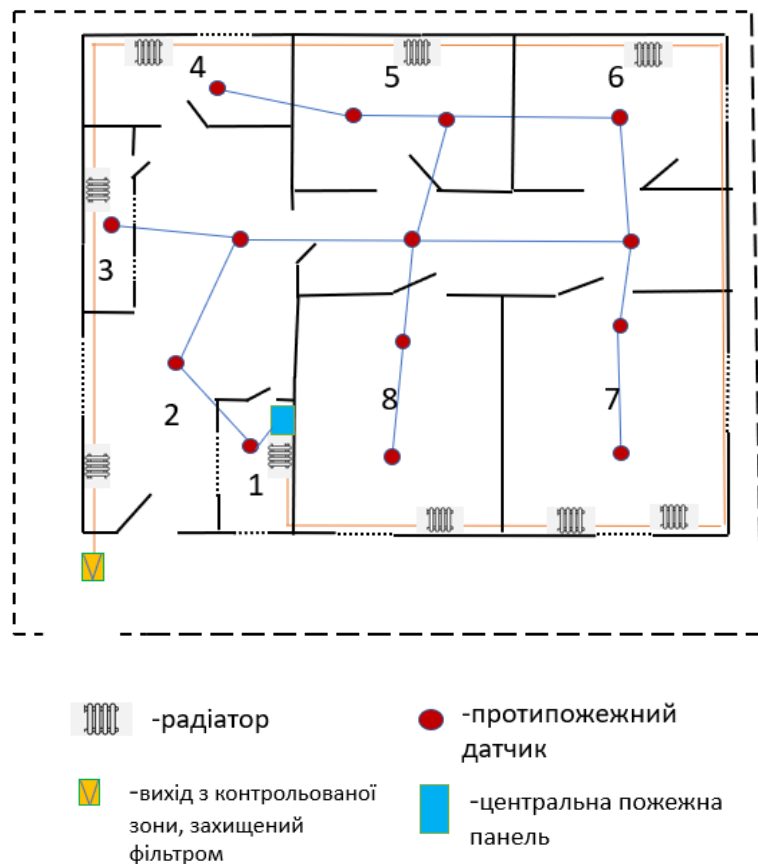


Рисунок 3.2 – Розташування фільтра на виході з контрольованої зони опалення.

Для зниження ризику витоку інформації через віброакустичний канал поділяються на наступні заходи.

Архітектурно-конструкторські рішення реалізовані з метою максимального послаблення акустичного сигналу від джерела звуку, що передається по комунікаціям. Звукова хвиля спочатку проходить через матеріали з високим згасанням, щоб досягти максимальної звукоізоляції. Для цього використовуються наповнення звукопоглинаючим матеріалом, пориста штукатурка на стінах, порт'єри та жалюзі для захисту вікон, а також двері з подвійними коробками та тамбурами. Для скляних перегородок використовуються спеціальні панелі або плити, що мають акустичні властивості, які допомагають поглинати або розсіювати звукові хвилі. Вони виготовлені з пористих матеріалів, таких як пористий фільтрований поліуретан.

Регулярна перевірка та обслуговування систем. Проводиться регулярна перевірка стану вентиляційних, трубопровідних та опалювальних систем, а також здійснюється їхнє обслуговування.

Встановлення систем виявлення витоку інформації, які виявляють незвичайні або підозрілі звукові сигнали у вентиляційних та опалювальних каналах, допомагають вчасно виявити потенційні загрози та вжити відповідних заходів безпеки.

Встановлені електричні фільтри на кабелі і обладнання допомагають зменшити рівень електромагнітних перешкод. ЕМІ (Electromagnetic Interference) виникають внаслідок природних явищ або техногенних джерел і можуть суттєво впливати на роботу електронних пристроїв, а також створювати ризики безпеки через можливість перехоплення даних. Фільтри знижують рівень шуму, що проникає через силові та сигнальні кабелі. Вони діють як бар'єр, відсікаючи високочастотні перешкоди і дозволяючи лише корисному сигналу проходити через систему, що зменшує можливість впливу ЕМІ на електронне обладнання. Крім того, фільтри забезпечують додаткове екранування кабелів та пристроїв від зовнішніх електромагнітних полів, запобігаючи проникненню небажаних сигналів і зменшуючи ймовірність перехоплення даних зловмисниками.

Фільтри також використовуються для зменшення радіочастотних перешкод (РЧП), які можуть виникати під час роботи різних пристроїв. Вони забезпечують стабільну роботу електронних систем, мінімізуючи вплив зовнішніх електромагнітних полів і запобігаючи виникненню помилок у передачі даних.

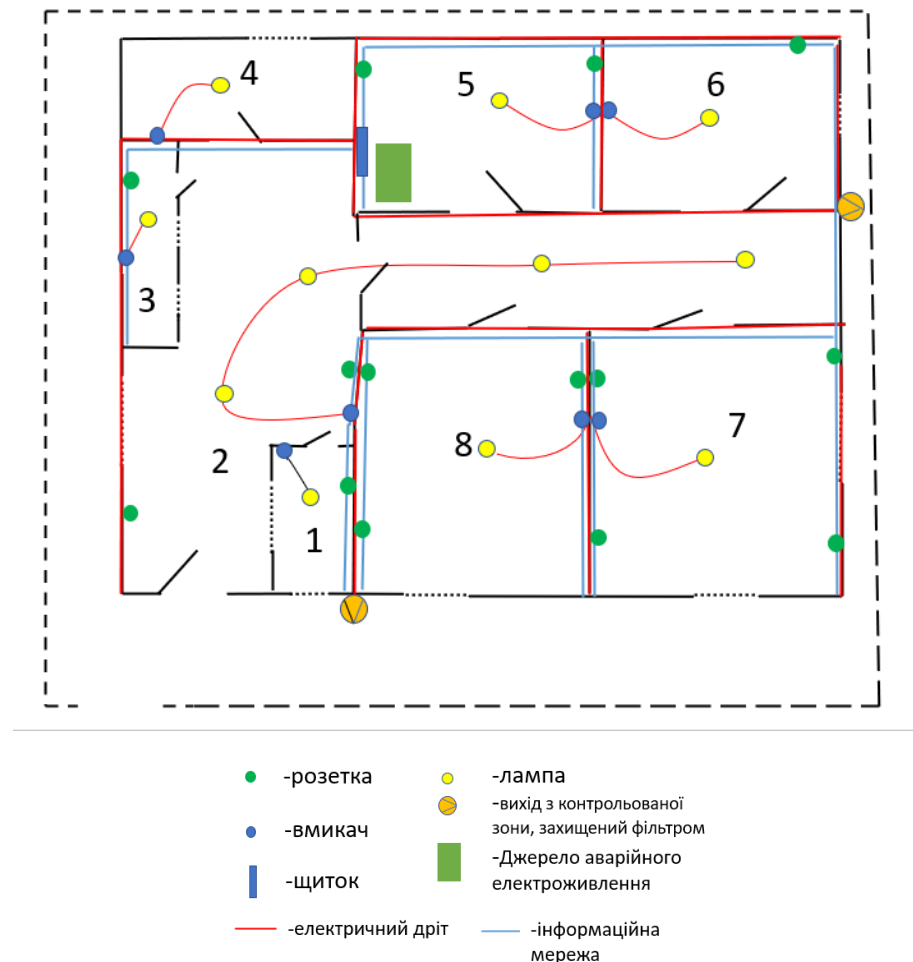


Рисунок 3.3 – Розташування фільтру на виході з контрольованої зони електромережі та інформаційної мережі.

В банку використовуються наступні методи захисту від ПЕМВтаН.

Екранування застосовується для обмеження рівнів електромагнітних сигналів і зменшення ризику їх перехоплення ззовні. Для серверів і корпусів комп'ютерів використовуються спеціальні металеві або вуглецеві матеріали, що екранують, які поглинають або відображають електромагнітні хвилі, зменшуючи їх інтенсивність. Такі матеріали встановлені у вигляді екрануючих кришок або плівок усередині корпусу комп'ютера та на стінах серверної кімнати. Це

допомагає запобігти несанкціонованому доступу до електромагнітних сигналів, які можуть містити конфіденційну інформацію.

Використання криптографічних методів шифрування даних також допомагає у захисті конфіденційної інформації в разі її несанкціонованого збору через електромагнітні канали.

Симетричне шифрування застосовується для захисту даних всередині банківської мережі, забезпечуючи швидке та ефективне шифрування великих обсягів даних, таких як фінансові транзакції та клієнтські дані. Алгоритми AES і 3DES часто використовуються для захисту баз даних і внутрішньої комунікації. Симетричне шифрування є важливим компонентом для забезпечення безпеки інформації в банківській системі завдяки своїй високій швидкості та ефективності [6].

Асиметричне шифрування є ключовим для захисту даних під час передачі через зовнішні канали, наприклад, при обміні даними між банками або між банком і клієнтом через Інтернет. Використання RSA забезпечує безпечну передачу даних, а електронні цифрові підписи гарантують автентичність і цілісність документів та транзакцій. Асиметричне шифрування дозволяє використовувати різні ключі для шифрування та дешифрування, що підвищує безпеку передачі даних [6,10].

Хешування є ще одним важливим типом криптографії, який використовується для перетворення відкритого тексту в унікальний і необоротний зашифрований текст. Хеш-функції, такі як SHA-256, SHA-512 і MD5, створюють унікальний відбиток даних, який може бути використаний для перевірки цілісності інформації, що зберігається або передається [14].

Цифрові підписи також відіграють важливу роль у банківських операціях, дозволяючи відправнику підписати повідомлення своїм особистим ключем, а одержувачу – перевірити підпис відкритим ключем відправника. Це забезпечує автентичність і цілісність переданої інформації. Приклади алгоритмів цифрових підписів включають RSA та DSA. Цифрові підписи використовуються для підтвердження особи відправника та забезпечення того, що повідомлення не було

змінено під час передачі.

Криптографія також використовується для наступних цілей.

Електронна комерція. Криптографія є важливим інструментом для захисту даних в електронній комерції, запобігаючи крадіжці та зловживанню інформацією. В електронній комерції використовуються цифрові підписи для підтвердження автентичності транзакцій та учасників. Протоколи шифрування, такі як SSL/TLS, забезпечують захищене з'єднання між веб-браузером користувача та сервером магазину, шифруючи дані, які передаються, щоб зловмисники не змогли їх перехопити або змінити. Автентифікація користувачів за допомогою багатфакторної автентифікації (MFA) додає додатковий рівень безпеки, гарантуючи, що доступ до облікових записів мають лише авторизовані користувачі.

Безпечне зберігання. Шифрування забезпечує безпеку даних, що зберігаються на різних пристроях, таких як зовнішні жорсткі диски, USB-накопичувачі та карти пам'яті. Використання алгоритмів шифрування, таких як AES (Advanced Encryption Standard), гарантує, що дані залишаються конфіденційними та недоступними для несанкціонованих осіб навіть у випадку крадіжки чи втрати пристрою. Крім того, шифрування може бути інтегроване в хмарні сервіси для захисту даних, що зберігаються на віддалених серверах [17].

Безпека бездротової мережі. Криптографія захищає бездротові мережі від атак, таких як перехоплення даних (sniffing) та атаки типу "людина посередині" (MITM). Використання протоколів безпеки, таких як WPA3 (Wi-Fi Protected Access 3), забезпечує шифрування даних, які передаються через бездротові мережі, та захист від несанкціонованого доступу. Криптографія також використовується для автентифікації пристроїв і користувачів у мережі, що запобігає підключенню зловмисників [14,17].

Інтернет-банкінг. Криптографія є критично важливою для забезпечення безпеки онлайн-банкінгових операцій. Вона використовується для автентифікації користувачів за допомогою методів, таких як OTP (одноразові паролі) і цифрові сертифікати. Дані транзакцій шифруються, щоб запобігти їх перехопленню та

зміні під час передачі. Крім того, криптографічні методи використовуються для безпечного зберігання чутливих даних, таких як номери рахунків та персональні дані, на серверах банку.

Захищена електронна пошта. Криптографія забезпечує безпечне надсилання та отримання електронних листів, використовуючи методи шифрування та автентифікації. Протоколи, такі як S/MIME (Secure/Multipurpose Internet Mail Extensions) та PGP (Pretty Good Privacy), дозволяють шифрувати вміст електронних листів та вкладень, забезпечуючи конфіденційність інформації. Цифрові підписи використовуються для автентифікації відправника та забезпечення цілісності повідомлення, запобігаючи його зміні під час передачі.

Система управління ключами (KMS) використовується для безпечного зберігання та управління криптографічними ключами, що забезпечує додатковий рівень захисту і запобігає несанкціонованому доступу до ключів. KMS забезпечує генерацію криптографічних ключів з високим рівнем ентропії, що гарантує їхню унікальність та складність для зломів. Ці ключі можуть бути симетричними (один ключ для шифрування та дешифрування) або асиметричними (пара відкритого та закритого ключів). Один з найважливіших аспектів, система використовує апаратні модулі безпеки (Hardware Security Modules, HSM) для захисту ключів від несанкціонованого доступу та фізичного вилучення. HSM забезпечують захищене середовище для зберігання та використання ключів [6].

Ще одним аспектом KMS є те, що вона відповідає за безпечний розподіл ключів між учасниками системи. Це включає передачу ключів між серверами, базами даних та іншими пристроями з використанням захищених каналів зв'язку. У банківській сфері, де безпека транзакцій критично важлива, забезпечення безпечного розподілу ключів є першочерговим завданням. Для підтримання високого рівня безпеки KMS забезпечує регулярну ротацію криптографічних ключів. Це означає, що ключі змінюються через визначені інтервали часу або після використання визначеної кількості разів. Ротація ключів допомагає мінімізувати ризик компрометації ключів.

Також, KMS забезпечує можливості аудиту та моніторингу використання

криптографічних ключів. Це включає збирання та аналіз логів доступу до ключів, виявлення аномальних дій та генерацію звітів для відповідності вимогам безпеки та регуляторних стандартів. KMS також забезпечує безпечне знищення ключів, які більше не потрібні. Це критично важливо для запобігання можливості відновлення ключів та використання їх зловмисниками. Процедури знищення ключів забезпечують повне та безповоротне видалення ключів з усіх систем зберігання.

KMS може інтегруватися з іншими системами безпеки, такими як системи виявлення та запобігання вторгнень (IDS/IPS), системи управління інформацією та подіями безпеки (SIEM) та системи захисту даних (DLP). Зокрема, у банківській системі KMS допомагає забезпечити надійний захист транзакцій, зберігання та обробку конфіденційної інформації, що є критично важливим для довіри клієнтів та дотримання регуляторних вимог [2,4].

На об'єкті використовуються комплексні підходи до запобігання витоку інформації, охоплюючи організаційні, технічні та фізичні заходи.

Організаційні заходи включають проведення регулярних навчань та інструктажів щодо правил обробки і зберігання конфіденційної інформації. Також розробляється та впроваджується політика безпеки, що визначає вимоги до захисту інформації та відповідальність за її дотримання. Використовуються процедури контролю доступу, яка виконується охороною об'єкта, до приміщень та інформаційних ресурсів, включаючи розподіл прав доступу з метою доступу до обмеженого обсягу інформації мінімальної кількості працівників. Розробляються чіткі інструкції для кожного співробітника банку [16].

Технічні заходи включають встановлення та регулярне оновлення антивірусного програмного забезпечення для захисту від загроз з інтернету, а також використання шифрування для захисту конфіденційної інформації під час її обробки та зберігання. Також встановлені системи контролю доступу, такі як картки доступу та біометричні сканери відбитків пальців, для обмеження фізичного доступу до об'єктів та інформаційних ресурсів [14].

Фізичні заходи включають розміщення обладнання та робочих місць таким

чином, щоб запобігти візуальному доступу до екранів моніторів ззовні, встановлення фізичних бар'єрів для обмеження видимості екранів моніторів та забезпечення належного контролю освітлення та спеціальних плівок, що звужують кут огляду зображення на моніторах, щоб зменшити ризик витоку інформації через вікна або інші візуальні канали [5].

Також, в операційних касах мають бути встановлені куленепробивні перегородки для захисту касирів та цінностей. У касовому залі (зоні клієнтів), відділенні інвестицій та кредитів, бухгалтерії та операційних касах слід встановити щільні штори для захисту від сторонніх поглядів з вулиці, що забезпечує конфіденційність операцій. В кабінеті охорони та касових залах, а саме на моніторах повинні бути встановлені світловідбиваючі покриття, що звужують кут огляду, операційних касах світловідбиваючі покриття на скляній перегородці, у кабінеті керівника звукопоглинаючі матеріали на стінах та світловідбиваючі покриття на вікнах, серверних кімнатах, бухгалтерії. Ці матеріали допомагають зменшити шум та відбиття світла, що забезпечує приватність, знижує можливість прослуховування та візуального спостереження за конфіденційною інформацією.

Також використовується моніторинг і аудит електронних систем для виявлення незвичайних дій та витоків інформації через електронні канали. Ця інформація зазвичай зберігається в захищених облікових записах на комп'ютерних серверах, що знаходяться у серверному приміщенні.

Системи захисту інформації на об'єкті мають різні режими роботи залежно від часу доби та робочих годин. Основні режими роботи СЗІ можуть включати:

1. Робочий час (вдень):

У робочий час СЗІ активно функціонує та забезпечує захист інформації в режимі реального часу. Виконується моніторинг, виявлення та відстеження потенційних загроз інформаційній безпеці. Застосовуються заходи забезпечення безпеки, такі як автентифікація, шифрування даних, контроль доступу тощо. Всі співробітники, що працюють з інформацією, повинні дотримуватися встановлених правил та процедур безпеки.

2. Неробочий час (вночі та вихідні дні):

У неробочий час деякі функції СЗІ можуть бути активовані, оскільки обсяг активності користувачів падає однак ризики безпеки можуть бути більшими. У повному обсязі працює система відеоспостереження, а також активуються майже усі датчики руху, задля миттєвого виявлення проникнення до об'єкту сторонніх осіб. Також, продовжуються базові заходи безпеки, такі як моніторинг заходів безпеки, резервне копіювання даних.

3. Робочий та неробочий час (весь час):

Деякі аспекти СЗІ, такі як моніторинг системних журналів та реагування на надзвичайні ситуації функціонують безперервно, незалежно від часу доби.[5]

Серед програмних методів захисту інформації на об'єкті застосовуються: активні (превентивні) / пасивні (детективні), мережеві / хостові, аналітичні / користувально-центрична / датацентричні.

Превентивний засіб захисту інформації спрямований на недопущення порушення стану інформаційної безпеки активу, наприклад, блокування запуску шкідливого файлу антивірусом або заборона на несанкціоноване підключення міжмережевим екраном. Таким чином, загрози інформаційній безпеці припиняються в зародку - все спрямоване на збереження інформації за допомогою превентивних (запобіжних) засобів. Превентивний спосіб захисту інформації включає в себе антивірусне програмне забезпечення, брандмауери (фаєрволи), системи запобігання вторгнень (IPS), засоби шифрування даних, багатофакторну аутентифікацію (MFA), засоби управління доступом (Access Control), засоби захисту веб-додатків (WAF), системи управління патчами (Patch Management), антивірусні сканери електронної пошти та засоби антиспам-фільтрації [8,16].

Детективний засіб захисту інформації спрямований на збір якомога більшої інформації про певну подію чи дію, за умови, що ми точно не знаємо, чи ці події чи дії є легітимними чи ні. Далі зібрана інформація надсилається фахівцю з інформаційної безпеки для того, щоб він проаналізував її та ухвалив рішення. Детективний спосіб захисту інформації включає системи виявлення вторгнень (IDS), системи моніторингу безпеки (SIEM), засоби аналізу поведінки користувачів і об'єктів (UEBA), рішення для виявлення і реагування на кінцевих

точках (EDR), мережеві аналізатори трафіку, журнали аудиту, засоби контролю доступу та аналізу активності (IAM) [8,16].

Мережеві та хостові системи захисту інформації в банку використовуються для забезпечення безпеки мережевої інфраструктури та серверів банку. Вони захищають мережевий трафік і дані від несанкціонованого доступу та кіберзагроз, забезпечують конфіденційність і цілісність даних під час їх передачі, контролюють доступ до мережевих ресурсів та серверів, запобігають атакам на банківські системи, виявляють і блокують підозрілу активність, а також забезпечують безпечний віддалений доступ для співробітників і клієнтів. Ці системи також допомагають виявляти та реагувати на інциденти безпеки, забезпечують моніторинг і аналіз мережевого трафіку та активності на хостах, і підтримують відповідність нормативним вимогам щодо захисту даних [11,16].

Аналітичний захист інформації включає в себе використання технологій і методів для моніторингу, аналізу та виявлення аномалій і загроз у мережевому трафіку та даних. Це дозволяє ідентифікувати підозрілу активність і реагувати на потенційні інциденти безпеки. В банку аналітичний захист необхідний для забезпечення безперервного моніторингу мереж і систем, що дозволяє своєчасно виявляти та запобігати кіберзагрозам, таким як фішинг, DDoS-атаки, шкідливе ПЗ та несанкціонований доступ [8,16].

Користувачецентричний захист інформації орієнтований на безпеку кінцевих користувачів і їхніх дій. Він включає в себе заходи для контролю доступу, автентифікації, навчання користувачів щодо безпеки, а також виявлення та запобігання загрозам, пов'язаним із людським фактором, таким як соціальна інженерія та фішинг. В банку користувачецентричний захист потрібен для забезпечення безпеки облікових записів і даних користувачів, а також для запобігання внутрішнім загрозам і помилкам, які можуть призвести до витоку конфіденційної інформації [8,11].

Датацентричний захист інформації зосереджений на захисті даних, незалежно від їх розташування або способу передачі. Це включає шифрування даних, управління доступом до даних, моніторинг і контроль дій, пов'язаних з

обробкою даних, та забезпечення їх цілісності і конфіденційності. В банку датацентричний захист є критично важливим для забезпечення безпеки фінансових транзакцій, персональних даних клієнтів, конфіденційної інформації та відповідності нормативним вимогам.

Підсумовуючи всі ці методи програмного захисту слід виділити основні засоби захисту ПЗ.

1. Засоби антивірусного захисту запобігають виконання шкідливого коду та діяльності шкідливого програмного забезпечення на кінцевих точках у локальному та веб-трафіку, в електронній пошті. У банківському середовищі засоби антивірусного захисту використовуються для захисту робочих станцій, серверів та мережевого трафіку від потенційно шкідливих програм та коду. Вони перевіряють як локальний, так і веб-трафік, а також електронну пошту на наявність загроз.

На робочих станціях та серверах банку антивірусні програми виявляють та блокують шкідливі програми та код за допомогою сигнатурного аналізу, що базується на відомих підписах вірусів, евристичного аналізу для виявлення невідомих загроз шляхом аналізу їхньої поведінки, репутаційного аналізу для оцінки надійності джерел файлів та аналізу на основі індикаторів компрометації, який виявляє ознаки можливої кібератаки або порушення безпеки.

Нижче наведено функціональну архітектуру антивірусної технології у послідовності операцій.

Виявлення. Перший крок антивірусної програми полягає у виявленні появи вірусу або іншої шкідливої програми в системній програмі або файлі даних.

Ідентифікація. Після функції виявлення наступним кроком антивірусу є ідентифікація типу вірусу та його шкідливих цілей.

Видалення. Видалення вірусу є останнім етапом антивірусної програми, спрямованим на повне усунення вірусу з інфікованої системи.

Цифрова імунна система або цифровий імунний антивірус - це техніка захисту від вірусів, які поширюються через мережу, таких як хробаки. Вона

використовує елементи сканування на кожній клієнтській машині в мережі. Спочатку ці сканери виявляють віруси на локальних машинах, а потім надсилають цю інформацію на головний сервер адміністратора в мережі. Адміністраторська машина збирає ці дані для подальшого аналізу. Машина для аналізу вірусів може бути в тій же мережі або в глобальній мережі та має кілька робочих блоків у своїй архітектурі.

Перший блок ізольований від інших та використовується для виявлення вірусів та визначення їх структури або типу.

Другий блок виявляє сигнатури вірусів.

Третій блок видаляє віруси з заражених файлів.

Після видалення вірусів машина аналізу вірусів надсилає цю інформацію всім мережевим клієнтам, які оновлюють дані про сигнатури вірусів у своїх базах даних. Цифрова імунна система є ефективною для виявлення та видалення вірусів, що поширюються через мережу.

Програмне забезпечення для блокування поведінки інтегрується з операційною системою хоста та відстежує поведінку програми в реальному часі. Воно працює як на сервері, так і на клієнтській стороні, проте основний захист забезпечується на сервері. Система блокування поведінки контролює системні файли та виявляє будь-які їх зміни, надсилаючи звіт адміністратору та очікуючи дії від нього. Оновлення головного сервера є відповідальністю адміністратора [3, 8].

2. Засоби антиексплойт захисту використовуються для виявлення та запобігання шкідливому впливу експлойтів на систему банку. Вони спрямовані на захист від використання вразливостей у встановленому програмному забезпеченні, що можуть бути використані для зловживання та зламу безпеки.

Засоби антиексплойт захисту в банку можуть контролювати звернення до певних ділянок оперативної пам'яті, виявляти спроби заміни адреси повернення під час виконання програмної функції, а також перевіряти спроби перевизначення типу об'єктів, що використовуються в пам'яті, які можуть бути використані для

зловживання. Крім того, вони можуть виявляти спроби заповнення певних ділянок оперативної пам'яті своїм кодом, що може свідчити про спробу виконання шкідливого програмного коду [4].

3. У банківському середовищі засоби детектування, реагування та захисту на кінцевих точках використовуються для захисту банківської інфраструктури та конфіденційної інформації від кіберзагроз.

Ці засоби аналізують роботу кінцевих точок в мережі банку та пошукають відповідності їхній поведінці відомим індикаторам компрометації, таким як хеш-суми запущених файлів або IP-адреси. Вони також проводять репутаційний аналіз та кореляцію даних від усіх оснащених цією системою кінцевих точок, щоб виявити підозрілу активність або атаки.

По виявленню загрози ці засоби можуть вживати заходів реагування, таких як ізоляція заражених вузлів в мережі або блокування підозрілих процесів. Крім того, вони збирають форензичні дані, які можуть бути використані для подальшого комп'ютерного криміналістичного дослідження, щоб з'ясувати джерело та механізм атаки та приймати відповідні заходи з попередження подібних інцидентів у майбутньому [10].

4. Засоби створення захищеного програмного середовища та контролю цілісності забезпечують захист та моніторинг використовуваного системного та прикладного програмного забезпечення для виключення запуску шкідливого або небажаного ПЗ, а також здійснюють контроль цілісності та справжності використовуваних санкціонованих програм. Цей функціонал досягається шляхом інвентаризації та побудови списків дозволеного та забороненого до використання системного та прикладного ПЗ; контролю версій, цифрового підпису видавця, контрольних сум, імен компонент системного та прикладного ПЗ; контролю запуску програм, включаючи моніторинг файлової та мережевої активності, а також запитів на підвищення привілеїв та взаємодію з даними користувача [16].

5. Засоби контролю та управління обліковими записами (АС) здійснюють централізоване управління обліковими записами користувачів та адміністраторів інформаційних систем протягом повного життєвого циклу від створення до

видалення, включаючи контроль членства у групах, повноважень, делегування, успадкування привілеїв, а також здійснюють управління сервісними (технологічними) обліковими записами та управління авторизацією користувачів, адміністраторів, інших сутностей в інформаційних системах. Такі системи, як правило, підтримують інтеграцію з системами кадрового діловодства, документообігу, планування та адміністрування, системами контролю та обліку доступу та з системами мультифакторної автентифікації з використанням одноразових паролів або біометричних даних. Однією з опцій функціоналу даного класу систем є журнал дій облікових записів систем, адміністраторів та користувачів[11].

6. Засоби запобігання витоку даних (DLP) призначені для контролю обробки інформації в інформаційних системах, включаючи передачу по різних каналах, обробку (зберігання, зміну, видалення) на кінцевих точках та віддалених мережесих ресурсах, виведення на друк, копіювання на знімні носії інформації та інше. Крім того, функціонал даних систем дозволяє проводити класифікацію даних з маркуванням конфіденційної інформації, пошук такої інформації на кінцевих точках, мережесих ресурсах, потоках мережного трафіку [6].

7. Засоби міжмережевого екранування здійснюють моніторинг та контроль вхідного та вихідного мережного локального та інтернет-трафіку на кінцевих точках та мережному обладнанні.

Міжмережеві екрани відповідають наведеним нижче параметрам.

Контроль служби: міжмережевий екран контролює служби, які намагаються пройти через нього, а також контролює комунікаційні служби з додатковими параметрами, такими як IP-адреси джерела/одержувача з визначеними портами та типами протоколів.

Контроль напрямку: брандмауер контролює комунікаційні служби, які мають право на зв'язок. Це означає, що він може обмежити вхідний трафік всередині мережі і обмежити вихідний трафік за її межами, або дозволити обидва типи трафіку.

Контроль користувача: брандмауер може визначати, які користувачі мають

доступ до певних служб. Ці користувачі можуть бути з локальної мережі або зовнішнього світу.

Контроль поведінки: за допомогою брандмауера адміністратори можуть контролювати робочу поведінку служби та користувача. Вони можуть надавати повний або обмежений доступ до служби чи системи для конкретного користувача, а також обмежувати доступ до певних частин цих служб або систем для того самого користувача.

Міжмережні екрани нового покоління (NGFW – Next Generation Firewalls) відрізняються інтеграцією додаткових засобів моніторингу та аналізу мережного трафіку, таких як системи глибокого аналізу трафіку, мережеві антивірусні системи та системи запобігання вторгнень, системи глибокого аналізу додатків та їх контексту, механізми URL- веб-ресурсів залежно від категорії розміщеної ними інформації, механізми розкриття зашифрованого трафіку (SSL/TLS-інспекція)[9].

Міжмережеві екрани веб-додатків (англ. WAF – Web Application Firewall) є на даний момент найсучаснішими засобами міжмережевого екранування, які призначені для глибокого аналізу даних, що передаються з Інтернету всередину мережі, наприклад, веб-додатків і включають функціонал поведінкового аналізу роботи клієнтів з веб-додатком та блокування підозрілих дій на основі евристики, системи репутації клієнтів, що підключаються за IP-адресами та географічним розташуванням, системи захисту користувачів від найбільш поширених атак на веб-додатки, системи встановлення віртуальних патчів (т.зв. «латок»), які не дозволяють експлуатувати відомі вразливості у веб-застосунку до моменту їх усунення [9,14].

8. Засоби виявлення/запобігання вторгненням(IDS,IPS) призначені для аналізу мережевого трафіку та поведінки системи з метою виявлення шкідливої активності, такої як використання експлойтів, несанкціонований доступ до ресурсів, що захищаються, функціонування шкідливого або небажаного ПЗ. Цей клас засобів захисту функціонує або на мережному рівні, або на рівні кінцевих точок. Є відмінності у функціоналі систем виявлення і запобігання вторгнень: системи виявлення вторгнень детектують шкідливий код або експлойти і видають

попередження про це адміністратору системи для здійснення подальших дій, а системи запобігання вторгнень не дозволяють виявленому шкідливому коду або експлойтам запускатися, своєчасно пристрої або у мережному трафіку [15].

Цей клас систем відрізняється також за способом виявлення загроз:

- сигнатурні системи базуються на заздалегідь заданих шаблонах (сигнатурах), що характеризують специфічну поведінку шкідливого коду чи особливі ділянки коду чи команд експлойтів;

- системи на основі аналізу стану та виявлення аномалій оцінюють кінцеві точки або мережеві вузли за наявністю відхилень у їхній нормальній поведінці, наприклад, за кількістю та типом трафіку, операціями з файлами, зверненням до пам'яті та гілки реєстру тощо;

- системи на основі правил отримують дані про поведінку мережевих вузлів з журналів трафіку або логів функціонування систем, а потім роблять їх порівняння із заданими умовами для реагування відповідно до налаштованих правил (тобто набором логічних виразів виду «якщо»);

- системи на основі правил додатків використовуються в тому випадку, якщо програма функціонує за пропрієтарними протоколами, для яких потрібні особливі правила детектування вторгнень, що враховують усі нюанси роботи конкретного програмного забезпечення.

9. Засоби ізолюваного виконання програм (т.зв. «пісочниці») дозволяють запускати програмний код, що перевіряється, в деякому ізолюваному віртуальному середовищі, яке спеціально призначене для виявлення аномалій або потенційно шкідливого впливу. Пісочниці можуть бути встановлені локально в ЦОД компанії, так і в хмарній інфраструктурі постачальника цього рішення. За методом детектування та способом включення до мережі пісочниці поділяються на:

- активні пісочниці, встановлені в розрив з'єднань та одержують дані на перевірку безпосередньо від мережевих пристроїв чи серверів;

- пасивні пісочниці, які отримують дані від користувача за його командою

та за його безпосередньою участю, а також отримують лише копію веб- або поштового трафіку без можливості перервати передачу підозрілих файлів;

- пісочниці, що використовують техніку придушення технік їх обману, наприклад, при пересиланні електронною поштою запароленого архіву з підозрілим файлом та при повідомленні пароля до архіву в тексті, темі або окремим листом;

- пісочниці, які використовують техніки штучного інтелекту для розпізнавання технік їх обходу, а також емулюючі дії реальної людини для аналізу потенційно шкідливих файлів, наприклад, при пересиланні електронною поштою посилання на скачування файлу, яке веде на сторінку, що вимагає Captcha[8].

10. Засоби сканування на наявність уразливостей призначені для аналізу вразливостей різних систем шляхом отримання даних про використовувані версії прикладного і системного ПЗ і порівнянням даної інформації з каталогами відомих уразливостей, застосовних до даних версій. Сканування можуть проводитися як в аутентифікованому режимі, коли сканер має можливість аутентифікуватися в системі та отримати широкий доступ до поточних налаштувань, так і в неаутентифікованому режимі, коли сканер буде вивчати систему тільки зовні [8].

11. Системи ресурсів-приманок для зловмисників (англ. honeypots і honeynets) є заздалегідь створені «муляжі» інформаційної системи, призначені для аналізу поведінки атакуючого в середовищі, схожій на реальне середовище організації, але не містить жодних цінних даних. Розрізняють як окремі системи (honeypots), наприклад, підроблені сервери для заманювання атакуючих, і цілі мережі (honeynets), службовці тієї ж мети і відтворюють зменшену картину інфраструктури організації. Атакуючі, потрапивши в таку пастку, спробують застосувати свій інструментарій для проведення атаки, а в цей момент їхні дії будуть ретельно журналуватися і потім вивчатимуться підрозділами кіберрозвідки для виявлення тактик, технік та процедур атак.

12. Засоби управління портативними пристроями (англ. MDM – Mobile

Device Management або EMM – Enterprise Mobility Management) є рішеннями для контролю портативних пристроїв співробітників банку (смартфонів, планшетів, портативних комп'ютерів) і дозволяють:

- контролювати відповідність моделі, версії операційної системи, встановлених програм заздалегідь заданому стандарту;
- контролювати відсутність внесених змін у прошивку пристроїв (відсутність прав root, відсутність jailbreak);
- дистанційно керувати пристроями для встановлення корпоративного ПЗ, відключення непотрібних або потенційно небезпечних функцій, віддаленого стирання даних з апарата у разі втрати чи крадіжки;
- надавати захищений доступ до корпоративних ресурсів, як правило, через VPN-з'єднання;
- забезпечувати роботу з корпоративними даними на виділеній зашифрованій ділянці внутрішнього сховища;
- виключати обмін даними між корпоративними та особистими програмами.

13. Засоби моніторингу та кореляції подій ІБ здійснюють збирання, агрегацію, запис, зберігання, пошук, таксономію, збагачення, кореляцію подій безпеки. Крім цього, важливою складовою безпеки є системи контролю дій користувачів, які виявляють аномальні дії або підозрілу активність користувачів у мережі, а також системи аналізу та пошуку актуальних загроз, які забезпечують постійний моніторинг та аналіз потенційних загроз для вчасного реагування на них [8].

Дані системи поділяються на системи управління подіями ІБ (Log Management), в яких немає повноцінної кореляції подій з різних джерел на підставі правил, що задаються, і на повноцінні системи SIEM (Security Information and Event Management), які, крім кореляції подій і створення інцидентів, можуть також оснащуватися додатковими функціями, такими як управління ризиками та вразливістю, інвентаризація активів, автоматизоване реагування на інцидент,

інтеграція з джерелами Threat Intelligence (TI Feeds), побудова звітів та діаграм тощо [17].

Дані системи необхідні у разі роботи з великим потоком різноманітних подій інформаційної безпеки від різних джерел з метою виявлення потенційних інцидентів та своєчасного реагування на них.

14. Засоби захисту інформації в банку, такі як системи захисту від DDoS-атак, які спрямовані на захист онлайн-сервісів від великомасштабних атак. DDoS (Distributed Denial of Service) атака полягає в переповненні мережі або серверів великою кількістю запитів, що робить їх недоступними для легітимних користувачів. Це може призвести до перерви у наданні послуг онлайн-систем, включаючи банківські сервіси. Важливо мати системи захисту від DDoS-атак, які здатні виявляти та фільтрувати шкідливий трафік перед тим, як він дістанеться до серверів банку [8,19].

Одним з методів боротьби з DDoS-атаками є використання спеціалізованих апаратних та програмних рішень, що моніторять трафік і виявляють аномальність, які можуть вказувати на атаку. Крім того, важливо мати гнучкі мережеві структури, що дозволяють реагувати на зміни обсягу та характеру трафіку.

Кешування і CDN (Content Delivery Network) дозволяють розподілити трафік між різними серверами та зберегти копії ресурсів на різних вузлах, що допомагає зменшити навантаження на сервери.

Великопропускні канали дозволяють адекватно обробляти великий обсяг трафіку, що є необхідним для забезпечення доступності банківських сервісів під час DDoS-атак [18].

15. Також використовуються системи захисту хмарних сервісів, що забезпечують безпеку використання хмарних технологій, та системи аналізу дій користувачів та сутностей, які виявляють ненормальні дії чи зловживання доступом до ресурсів. Хмарні сервіси можуть бути фізично та логічно відокремлені для забезпечення високого рівня ізоляції між клієнтами та їхніми даними, що допомагає запобігти несанкціонованому доступу та розповсюдженню загроз [20].

ВИСНОВКИ

В даній дипломній роботі було проведено аналіз об'єкта комерційного банку щодо інформаційної безпеки та розроблено захист інформації. Задля досягнення результату було розглянуто теоретичні відомості про об'єкт та системи його захисту, далі проаналізовано загрози витоку інформації з об'єкту та розроблено систему захисту інформації.

У першій частині роботи було розроблено план об'єкта та наведено короткий опис діяльності відділів банку. Також, було визначено види циркулюючої інформації, а саме ІОД для кожного відділу. При дослідженні обладнання на об'єкті, було приділено увагу захисту комунікаціям та пристроям обробки інформації.

У другій частині роботи було проаналізовано основні загрози витоку інформації в банку. Серед них є перехоплення електромагнітних хвиль та поля, перехоплення паролей, вразливість доступу до ресурсів, несанкціонована модифікація даних, розголошення мережевого трафіку, вірусні технології, програми-вимагачі, фішинг, атаки на хмарні дата-центри, соціальна інженерія, спуфінг та ін.

У третій частині роботи було розроблено систему захисту інформації для ПЗ. Серед методів захисту віднесено активні (превентивні) / пасивні (детективні), мережеві / хостові, аналітичні / користувачецентричні / датацентричні. Від цих методів були взяті найефективніші засоби захисту інформації на об'єкті, такі як антивірусного захисту, антиексплойт захисту засоби детектування, реагування IDS та захисту на кінцевих точках EDR та ін. Також, проведено розподілення режимів роботи системи захисту інформації на об'єкті залежно від часу доби та робочих годин, в робочий час, неробочий, та весь час.

Таким чином, дипломна робота спрямована на забезпечення високого рівня захисту інформації у комерційному банку, щоб запобігти можливим загрозам та забезпечити безпеку та конфіденційність даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Магауєнов Р.А. Системи охоронної сигналізації: основи теорії та принципи побудови: Навчальний посібник. - М.: Гаряча лінія - Телеком, 2004. - 367 с.
2. Ситник Н.С., Стасишин А.В., Банківська система: Навчальний посібник. - м, 2020 - 291с.
3. Петраков А.В. Основи практичного захисту інформації. 2-ге вид. Навчальний посібник .- м.: Радіо та зв'язок, 2000. - 368с.
4. Хорошко В.А., Чекатков А.А.Методи та засоби захисту інформації / За ред. Ю.С.Ковтанюка.- К.: Видавництво „Юніор”, 2003. - 504с.
5. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
6. Розробка правил інформаційної безпеки: Пров. з англ.-М.: Видавничий дім "Вільямс", Бармен Скотт, 2002. - 208 с.
7. Ю.П. Лісовська, Кібербезпека: ризики та заходи – Кондор, 2019. – 272с.
8. Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution – Nadeem Ahmad, M. Kashif Habib 2010. – 93с.
9. Загальні критерії безпеки інформаційних технологій. ISO/IEC 15408:1999. Information Technology. Security techniques. Evaluation criteria for IT security.
10. Захист інформації в автоматизованих системах управління: навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
11. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К.: ДУТ-КНУ, 2016. – 178 с.
12. Соколов В.Ю. Інформаційні системи і технології: Навч. посіб. /

Соколов В.Ю. – К.: ДУІКТ, 2010. – 138 с.

13. Юринець В. Є. Інформаційні системи управління персоналом, діловодства і документообігу: навч. посіб. / Юринець В. Є., Юринець Р. В. – Л. : Тріада плюс, 2008. – 628 с.

14. Інформаційні системи і технології в банківській сфері: навч. посіб. для студ. спец. 6.050105 "Банківські справи". / Аніловська Г. Я., Чуй І. Р., Вус М. Л., Стоколоса Т. М. – Л. : ЛКА, 2008. – 332 с.

15. Інформаційні системи в сучасному бізнесі : навчальний посібник / В. С. Пономаренко, І. О. Золотарьова, Р. К. Бутова та ін. – Х. : Вид. ХНЕУ, 2011. – 484 с.

16. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.

17. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. - 78 с.

18. Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. - 222 p.

19. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. - 482 p.

20. Long Fred. Java coding guidelines : 75 recommendations for reliable and secure programs / Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda. - New York: Pearson Education Inc., 2014. - 277 p