

**звукоізоляція НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра інформаційної безпеки**

«На правах рукопису»

УДК 004.056

«До захисту допущено»

В.о. завідувача кафедри

\_\_\_\_\_ М.В.Грайворонський

“ \_\_\_\_ ” \_\_\_\_\_ 2019 р.

## Магістерська дисертація на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Методи підвищення захищеності систем обробки критичної  
інформації \_\_\_\_\_

Виконав (-ла): студент (-ка) \_\_\_\_\_ курсу, групи ФБ-81мп  
(шифр групи)

Іванченкіо Олексій Вячеславович \_\_\_\_\_  
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник Барановський Олексій Миколайович \_\_\_\_\_  
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент \_\_\_\_\_  
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації  
немає запозичень з праць інших авторів без  
відповідних посилань.

Студент \_\_\_\_\_  
(підпис)

Київ – 2019 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра інформаційної безпеки**

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою  
Спеціальність (освітньо-професійна програма) – 125 Кібербезпека («Системи, технології та математичні методи кібербезпеки»)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

\_\_\_\_\_ М.В.Грайворонський  
(підпис)

« \_\_\_\_ » \_\_\_\_\_ 2019 р.

**ЗАВДАННЯ  
на магістерську дисертацію студенту  
Іванченку Олексію Вячеславовичу**

1. Тема дисертації «Методи підвищення захищеності систем обробки критичної інформації»,  
науковий керівник дисертації Барановський Олексій Миколайович, к.т.н., доцент,  
затверджені наказом по університету від «15» листопада 2019 р. № 3927-с
2. Термін подання студентом дисертації 10.12.2019 р.
3. Об'єкт дослідження: Системи обробки критичної інформації.
4. Вихідні дані: Модель захищеної системи обробки критичної інформації.
5. Перелік завдань, які потрібно розробити: Дослідити системи обробки критичної інформації: склад, методи захисту, вразливості притаманні даним системам; Дослідити методи захисту систем обробки критичної інформації: способи виявлення вторгнень, вразливості, переваги та недоліки їхнього використання; Спроекувати модель системи обробки критичної інформації, що забезпечить надійний захист критичної інформації .
6. Орієнтовний перелік ілюстративного матеріалу: 1)Тема та мета дипломної роботи; 2) Склад систем обробки критичної інформації 3)Недоліки сучасних засобів захисту 4) Спроекована модель системи обробки критичної інформації 5)Методи захисту спроекованої моделі системи обробки критичної інформації 6)Переваги спроекованої моделі системи обробки критичної інформації 7)Висновки.

## 7. Орієнтовний перелік публікацій

---



---

## 8. Дата видачі завдання 2 жовтня 2018 року.

## Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Аналіз отриманого завдання	13.10.2018	
2.	Постановка мети магістерської дисертації та розробка попереднього змісту	12.11.2018	
3.	Формування вступної частини пояснювальної записки	02.12.2018	
4.	Формування першого розділу пояснювальної записки	15.02.2019	
5.	Формування другого розділу пояснювальної записки	05.05.2019	
6.	Формування третього розділу пояснювальної записки	03.09.2019	
7.	Формування четвертого розділу пояснювальної записки	31.10.2019	
8.	Оформлення магістерської дисертації	14.11.2019	

Студент

\_\_\_\_\_  
(підпис)

Іванченко О. В.

Науковий керівник дисертації

\_\_\_\_\_  
(підпис)

Барановський О. М.

## РЕФЕРАТ

Обсяг роботи 118 сторінки, 25 ілюстрацій, 3 додаток, 27 таблиць, 17 джерел літератури.

Метою та завданням даної роботи є аналіз типових методів захисту, що використовуються в системах обробки критичної інформації, аналіз їх вразливостей та рекомендації щодо покращення методів захисту враховуючи їх недоліки та вразливості.

Об'єктом дослідження є системи обробки критичної інформації, предметом дослідження є методи захисту систем обробки критичної інформації та їх недоліки при впровадженні безпосередньо в систему.

Метою дослідження було проведення аналізу вразливостей складових частин систем захисту систем обробки критичної інформації, часткова практична реалізація.

Новизною одержаних результатів являється удосконалення та спонукання до подальших досліджень розвідку методів захисту, що використовуються для захисту систем обробки критичної інформації.

Практичним значенням одержаних результатів являється побудова моделі захищеної системи обробки критичної інформації, з використанням удосконалених методів захисту а також порівняння результатів та одержання підтвердження покращення надійності системи.

На підставі отриманих висновків необхідне подальше дослідження проблеми вразливості систем обробки критичної інформації.

Подальші дослідження слід направити на розробку прискореної криптосистеми шифрованої передачі критичних даних без втрат захищеності. У вдосконаленні методів та засобів захисту критичної інформації. Також слід реалізувати модернізацію технічних засобів захисту, для приміщення в якому буде знаходитися системи обробки критичної інформації та її складові, це обумовлено їх високою вартістю, що впливає у свою чергу на безпеку системи. Критична інформація, порівняльний аналіз, системи захисту, протидія.

## ABSTRACT

118 pages of work, 25 illustrations, 3 appendixs, 27 tables, 17 literature sources.

The purpose and purpose of this paper is to analyze the typical security methods used in critical information processing systems, to analyze their vulnerabilities and to recommend improvements to security methods, taking into account their shortcomings and vulnerabilities.

The object of the research is the systems of processing of critical information, the subject of research is the methods of protection of the systems of processing of critical information and their disadvantages when implemented directly into the system.

The purpose of the study was to analyze the vulnerabilities of the components of the systems of protection of systems of critical information processing, partial practical implementation.

The novelty of the obtained results is the improvement and encouragement to further research of the security methods used to protect the systems of critical information processing.

The practical value of the results obtained is to build a model of a secure system for processing critical information, using advanced methods of protection, as well as to compare the results and to confirm the improvement of system reliability.

Based on the findings, further investigation of the vulnerability of critical information processing systems is needed.

Further research should be directed towards the development of an accelerated crypto-system of encrypted transmission of critical data without wiping security. In improving the methods and means of protection of critical information. It is also necessary to implement modernization of technical means of protection, for the premises in which the systems of processing of critical information and its components will be found, this is due to their high cost, which in turn affects the security of the system.

Critical information, benchmarking, security systems, counteraction.

## ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів .....	8
Вступ.....	9
1. Методи та засоби захисту систем обробки критичної інформації.....	11
1.1 Системи обробки критичної інформації.....	11
1.2 Загрози системам обробки критичної інформації. ....	12
1.3 Методи та засоби захисту, їх недоліки .....	18
Висновок до розділу 1.....	29
2 Моделювання захищеної системи обробки критичної інформації.....	30
2.1 Вимоги захисту систем обробки критичної інформації.....	30
2.2 Вибір засобів захисту на основі аналізу вимог .....	35
2.3 Запропоновані заходи для забезпечення захисту системи обробки критичної інформації.....	41
Висновки до розділу 2 .....	47
3 Створення моделі захищеної системи обробки критичної інформації .....	49
3.1 Модель системи.....	49
3.2 Засоби захисту, їх опис .....	56
3.3 Характеристика приміщення .....	67
3.4 Захищеність системи від атак .....	73
3.5 Аналіз результатів дослідження .....	78
Висновки до розділу 3 .....	82
4 Аналіз виходу на ринок стартап проекту.....	83
4.1 Опис ідеї стартап проекту .....	83
4.2 Технологічний аудит ідеї проекту.....	86
4.3 Аналіз ринкових можливостей запуску стартап проекту .....	87

4.4 Розроблення маркетингової програми .....	88
4.5 Розроблення ринкової стратегії проекту .....	98
4.6 Розроблення маркетингової програми стартап-проекту .....	101
Висновки до розділу 4 .....	104
Висновки .....	105
Перелік джерел посилань .....	107
Додаток А .....	110
Додаток Б.....	110
Додаток В .....	115

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

СОКІ - системи обробки критичної інформації;

ТЗІ – технічні засоби захисту;

DPI - Deep packet inspection;

ІБ – інформаційна безпека;

ОС – операційна система;

ЗЗ – засоби захисту;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

ТЗІ – технічний захист інформації;

НД – нормативний документ;



## ВСТУП

Системи захисту для систем обробки критичної інформації розвивалися та удосконалювалися протягом досить великого періоду однак з інтенсивним розвитком технологій з кожним роком з'являється все більша кількість вразливостей та знаходяться недоліки складових частин систем захисту, які дають зловмисника можливості викрадення чи перехоплення критичної інформації.

Системи обробки критичної інформації досить суттєво поширилися на комерційну сферу діяльності, що сприяла росту попиту на даний продукт та послугу. Очевидно, що важливо використовувати методи захисту та профілактики для вже існуючих систем обробки критичної інформації, співставлення їх із сучасними технологіями та методами взлому, адже прогрес не стоїть на місці тому існує необхідність контролю та профілактичних перевірок якості встановленої апаратури.

Нажаль існує велика кількість недоліків та вразливостей методів захисту систем обробки критичної інформації.

Метою та завданням даної роботи є аналіз типових методів захисту, що використовуються при проектуванні систем обробки критичної інформації та аналіз їх вразливостей, розроблення рекомендацій, щодо покращення методів захисту враховуючи їх вразливість.

Об'єктом досліджень є системи обробки критичної інформації, предметом дослідження є засоби та методи захисту систем обробки критичної інформації та їх недоліки при впровадженні безпосередньо в систему.

Метою дослідження було проведення аналізу вразливостей засобів захисту систем обробки критичної інформації, часткова практична реалізація деяких з них.

Новизною одержаних результатів являється удосконалення та спонукання до подальших досліджень розвитку методів та засобів захисту систем обробки критичної інформації.

Практичним значенням одержаних результатів являється побудова моделі захищеної системи обробки критичної інформації, з використанням удосконалених методів захисту складових частин системи а також порівняння результатів й одержання підтвердження покращення надійності системи.

## **1. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ СИСТЕМ ОБРОБКИ КРИТИЧНОЇ ІНФОРМАЦІЇ.**

Збереження критичної інформації під час її обробки в мережі актуальна тема на сьогоднішній день, оскільки під час роботи в мережі існує велика кількість загроз як із зовнішнього так і з внутрішнього середовища. Критична інформація при потраплянні в руки зловмисників може суттєво нашкодити її власнику чи організації.

На даний момент існують методи та засоби що можуть забезпечити безпечну роботу систем обробки критичної інформації. Проте, більшість з них мають програмні та технічні недоліки, складність у використанні та встановленні. Вони містять велику кількість недоліків, що згодом можуть перерости у досить суттєві проблеми.

У данному розділі буде розглянуто методи та засоби що використовуються для забезпечення захисту систем обробки критичної інформації, їх переваги та недоліки, поширеність на ринку та простоту використання, приклади використання методів та засобів захисту систем обробки критичної інформації.

### **1.1 Системи обробки критичної інформації.**

Системою обробки критичної інформації називається система в якій реалізована робота та обробка критичної інформації. [15]

Критична інформація — це будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.[15]

Кожне приватне підприємство само може регулювати методи та засоби захисту системи обробки критичної інформації, однак якщо це державна установа або установа яка працює з критичними даними держави чи населення країни система має відповідати певним вимогам, що вказані в законах.

Таким чином перед проектування та створенням систем обробки критичної інформації варто проаналізувати та вирішити яку саме інформацію буде вона обробляти, чи варто дотримуватися стандартів встановлених державою, чи буде достатньо самостійного аналізу та створення системи обробки конфіденційної інформації з використанням необхідних засобів захисту.

## **1.2 Загрози системам обробки критичної інформації.**

Через стрімке зростання технологій відбувається зростання варіативності загроз у всіх сферах життя, що негативно впливає на безпеку всіх суб'єктів, які користуються мережею в тому числі й системи обробки критичної інформації. В зв'язку з цим необхідно забезпечувати системам обробки критичної інформації від зовнішніх та внутрішніх загроз. Тому необхідно виявляти та опрацьовувати всі види та типи загроз, аби забезпечити надійний захист систем обробки критичної інформації та протидію різноманітним атакам.

### **1.2.1 Загроза DPI при передачі даних в мережі.**

Для покращення швидкості передачі інформації було створено CDN, а для безпеки передачі інформації DPI. Дані технології були створені для безпечного прискорення передачі даних. За допомогою цих технологій можливо значно пришвидшити передачу в той же час не втрачаючи фактор безпечної передачі через можливість прослуховувати та блокувати трафік. DPI реалізує перевіряє та фільтрує пакети за змістом, тобто аналізує весь вміст пакета. DPI здатен виявляти віруси та фільтрувати інформацію.

Дана технологія може збирати детальну статистику з'єднання кожного користувача. За допомогою DPI інтернет-провайдери контролюють прохідний трафік будь-якого клієнта. Програми DPI іноді використовують для виявлення і блокування трафіку, що містить незаконні матеріали або порушує авторські права.

За допомогою DPI можливо реалізовувати аналіз трафіку, виявлення та використання чужої критичної інформації, що може значно нашкодити безпеці та економічному стану корпорації чи окремому споживачу.

### **1.2.2 Загрози ідентифікації користувачів у мережі.**

При роботі користувача з критичними даними будь – якої організації варто розуміти, що не лише на робочому місці можливі спроби її викрадення. При скануванні мереж корпорацій зловмисники можуть ідентифікувати, користувача та реалізувати за ним нагляд, для виявлення його слабких сторін та використання їх для отримання інформації, наприклад, даних про особисте життя жертви, ім'я її дітей чи батьків, їх дати народження.

Зловмисники викрадають бази даних із інформацією про користувачів після чого їх можна купити в інтернеті чи на звичайному ринку в центрі міста. Дані бази можуть містити як дані з поштою, мобільним телефоном, днем народження так і адреси проживання. Уся ця інформація може стати в пригоді зловмисникам наприклад для генерування паролів до робочого місця чи робочої пошти.

Зловмисники користуючись конфіденційною інформацією можуть дізнатися реальні адреси та місцезнаходження цілі. Особливо багато уваги слід приділити керівництву великих організацій та державних установ. Це обумовлено тим, що вони мають у своєму розпорядженні критичну інформацію про організацію в якій працюють чи державні таємниці, заволодіння якими може зруйнувати організацію чи навіть країну.

За допомогою сканування мережі можливо дізнатися внутрішню модель системи та засобів захисту. Це досить важлива інформація, що може дати можливість зловмисникам реалізувати атаки. Укупі зібрана і оброблена інформація формує образ особистості, її звички, місце роботи, місцезнаходження та можливість дізнатися наскільки корисною інформацією або даними може володіти об'єкт аналізу та скільки вона може коштувати.

### 1.2.3 Загроза атак соціальної інженерії

Атаки соціальної інженерії досить поширені та зберігають свою актуальність на сьогоднішній день, адже де не можуть впоратися інші засоби отримання інформації атаки соціальної інженерії можуть впоратися досить просто не потребуючи на це значних витрат.

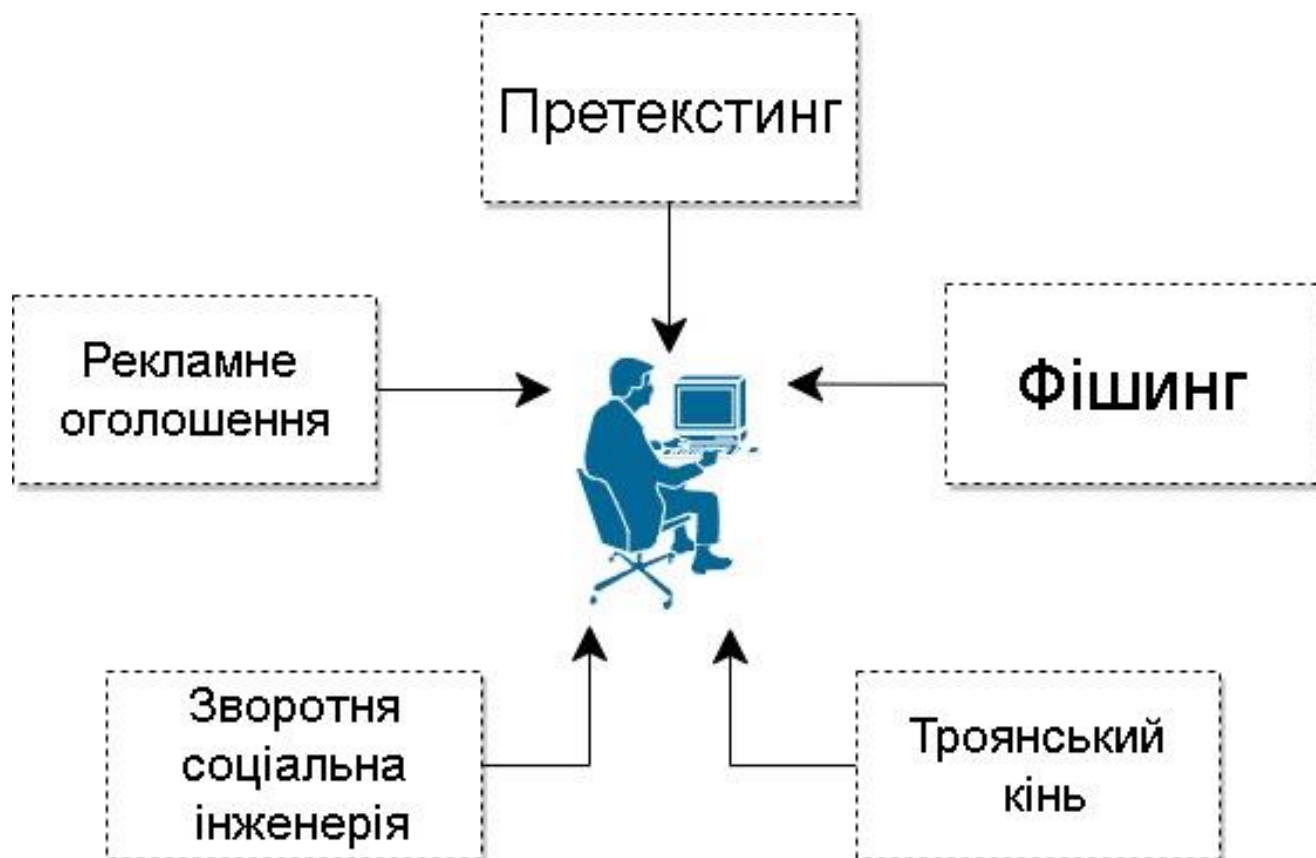


Рисунок 1.1 - Атаки соціальної інженерії

Ці атаки досить прості у реалізації та не потребують великої кількості спеціальних знань та навичок, можуть продовжуватися протягом тривалого терміну та досить складно відслідковуються. Усе це реалізовується через користувача а не систему обробки критичної інформації.

Суть атаки полягає у пошуку інформації про жертву, встановлення довірливих відносин, експлуатація цілі або використання отриманих даних для отримання необхідної інформації, знищення слідів своїх дій.

Приклад: фішинг, троянський кінь (збереження небезпечного ПО під виглядом відео, архіву, застосунка), атаки по телефону, зловмисники можуть обіцяти винагороду в обмін на інформацію тощо.

#### **1.2.4 Загрози потенційно небажаних програм**

Потенційно небажані програми - це програмні застосунки, що розмножуються вірусним шляхом та можуть викликати зміну системних налаштувань та програмах. Дане зловмисне програмне забезпечення може перехоплювати особисті дані користувачів через що може відбуватися викрадення критичної інформації користувача навіть без його відома. Їх можна скачати при завантаженні файлів з торрент - сайтів, відео на сайтах, завантаження даних з пошти тощо.

Суть атаки полягає у встановленні потенційно небезпечних програм, що можуть отримувати контроль над комп'ютером та передавати конфіденційні дані зловмиснику.

Приклад: встановлення програми для аналізу температури процесора з додатковою функцією по аналізу та передачі даних.

Небезпека даної загрози полягає в тому, що дані програми можуть встановлюватися без відома користувача маскуючись під якусь корисну програму.

#### **1.2.5 Атаки на відмову в обслуговуванні**

Атаки направлені на відмову в обслуговуванні небезпечні можливістю перевантаження та виходу з ладу каналу зв'язку чи повністю всієї системи. Без належного засобу захисту подібні атаки стають дуже небезпечними.

Дані види атак деколи поєднують з іншими різновидами, так атака на відмову в обслуговуванні може бути лише приманкою, а сама атака реалізовуватиметься в інший спосіб.

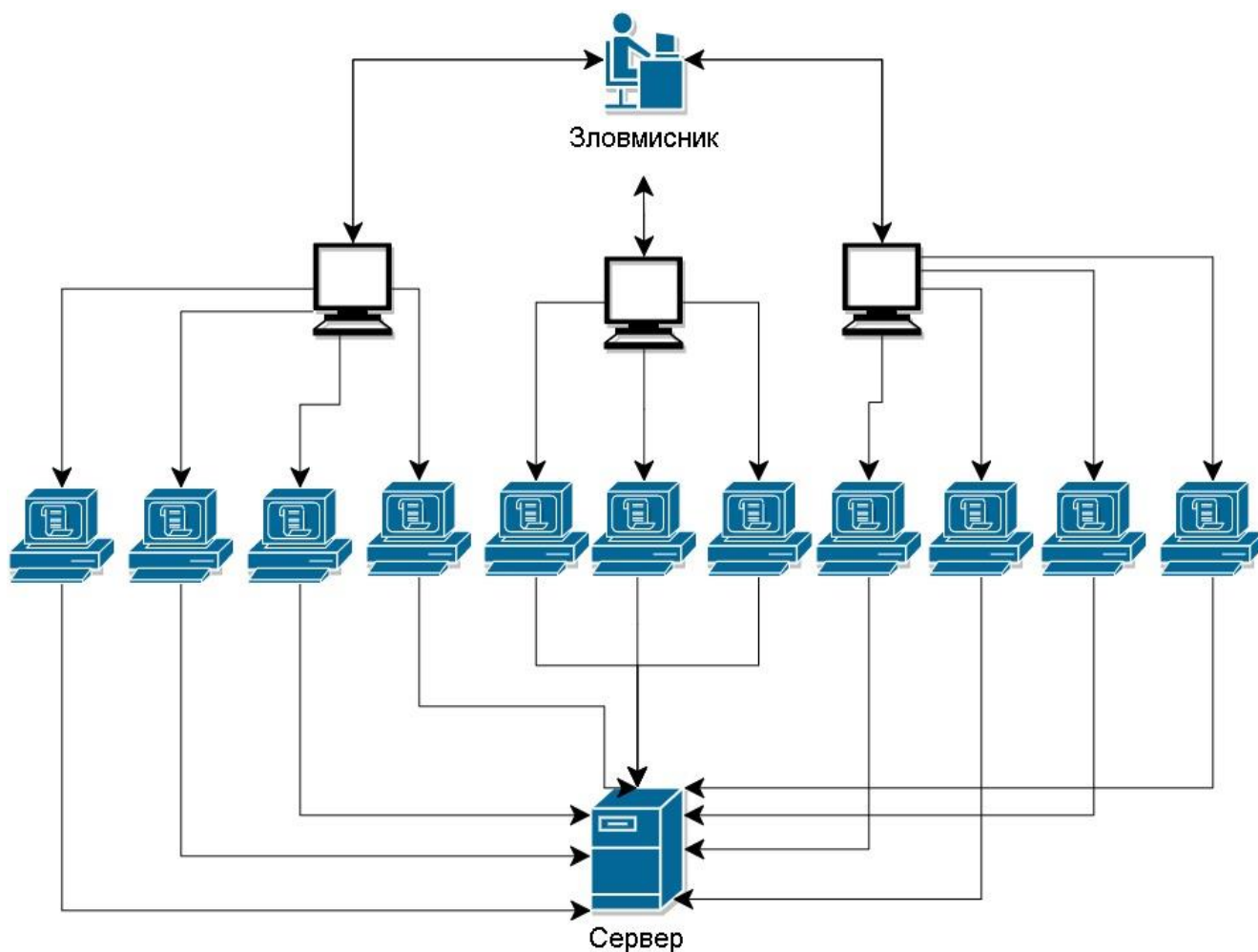


Рисунок 1.2 - Графічна ілюстрація атаки на відмову в обслуговуванні

### 1.2.6 Загроза прослуховуванню трафіка

Прослуховування трафіку може реалізовуватися майже будь де й жертва ніяк не зможе в більшості випадків дізнатися про це. Через прослуховування трафіку зловмисники можуть дізнатися: паролі або логіни до пошти, сайти та сервіси, що були відвідані, навіть перехоплювати та читати повідомлення, що були відправлені чи отримані.

Прослуховування трафіку може відбуватися безпосередньо на робочому місці. Наприклад в системах обробки критичної інформації можуть внутрішні агенти реалізувати перехоплення чи прослуховування вхідного трафіку, а якщо буде використовуватися бездротовий зв'язок для передачі та отримання даних то



навіть із сусідніх кімнат чи будівель в залежності від потужності та радіусу дії бездротового зв'язку.



Рисунок 1.3 - Графічна ілюстрація прослуховування трафіку

Суть атаки: отримання інформації через прослуховування трафіку. На цьому етапі інформація або вже несе в собі шукані дані або буде використовуватися для подальших дій.

### 1.2.7 Загрози внутрішніх атак

Внутрішні атаки неможливо повністю прорахувати та бути до них готовими. Дана вразливість може бути створена як користувачем системи шляхом комерційного шпигунства так і через шантаж користувачів. Також можливе викрадення чи копіювання даних системи як користувачем так і зловмисником, що проник на територію.

Суть атаки: реалізація атаки виконується шляхом комерційного шпигунства, шантажу користувачів системи, корисливих дій користувачів тощо.

Приклад: співробітник заради своїх інтересів бажає продати конфіденційну інформацію про фірму чи інших користувачів шляхом збереження даних на зовнішній носій.

### 1.2.8 Загрози SQL –ін'єкцій

SQL-ін'єкцією називають виконання зловмисником запиту до бази даних, з метою отримання інформацію про ціль атаки. Запит може містити команди на читання модифікацію або видалення даних, що зберігаються в базі.

Також через дані запити можливо отримати доступ до локальних записів чи навіть до виконання коду зловмисника все залежить від цілей та можливостей. Дані атаки можливо виконувати віддалено та всередині системи.

Суть атаки: виконання зловмисником запиту до бази даних з метою отримання інформацію про ціль атаки чи виконання коду зловмисника.

Приклад: модифікований запит вводиться у поле логін та пароль та видає перелік зареєстрованих користувачів та їх паролі.

### 1.3 Методи та засоби захисту, їх недоліки

До основних засобів захисту відносяться: технічні, програмні, апаратно – програмні, організаційні. Вони реалізують захист інформації які поодиноці так і в поєднанні один з одним. Оптимального захисту можна досягти поєднуючи ці методи та засоби, однак перед тим як використовувати будь який метод слід ретельно проаналізувати та прорахувати вигідність його використання.

Технічні засоби – це електричні, електромеханічні, електронні засоби по забезпеченню захисту інформації. Технічні засоби захисту поділяються на апаратні та фізичні: апаратні вбудовуються або сполучаються в апаратуру, а фізичні працюють автономно.

Переваги технічних засобів:

- надійність
- незалежністю від суб'єктивних факторів
- високу стійкість до модифікації

До слабких сторін відносяться:

- недостатня гнучкість

- відносно великі обсяг і маса
- висока вартість

Переваги програмних засобів: універсальність, гнучкість, надійність, простота в установці, модифікування. Недоліки: обмежена функціональність, використання ресурсів сервера, залежність апаратних засобів. Спеціалізовані програмні засоби захисту інформації мають кращі характеристики, ніж вбудовані засоби мережесих ОС.

### **1.3.1 Шифрування даних**

Шифрування даних вимагає значних ресурсів для стабільної та швидкої роботи з даними та користувачами. Адже досить складно реалізовувати швидкісну роботу системи при шифруванні великої кількості даних та користувачів, що будуть звертатися до цих даних, тому треба правильно реалізувати правила по яким будуть взаємодіяти користувачі з системою.

За допомогою описання правил та правильного підходу до реалізації шифрування можливо реалізувати досить надійну та швидку систему. Нажаль на сьогоднішній день більшість алгоритмів шифрування та протоколів передачі даних мають перелік вразливостей в залежності від різновиду та виду.

#### **1.3.1.1 Недоліки шифрування даних**

Алгоритми симетричного шифрування набагато швидші та вимагають менше обчислювальної потужності, але їх основним недоліком є розподіл ключів. Оскільки один і той же ключ використовується для шифрування і дешифрування інформації, цей ключ повинен бути переданий всім, кому потрібно доступ, що природно створює певні ризики.

Асиметричне шифрування вирішує проблему розподілу ключів, використовуючи відкриті ключі для шифрування, а приватні для дешифрування.

Компроміс полягає в тому, що асиметричні системи дуже повільні в порівнянні з симетричними і вимагають набагато більшої обчислювальної потужності через довжини ключа.

Ще одна проблема що може ускладнити використання шифрування – потужності системи та її можливість обробляти велику кількість операцій. Через це необхідно використовувати потужні обчислювальні машини та приладі, що коштують досить великі суми й не завжди є необхідність їх використання. Тому доводиться обирати слабший алгоритм та більш швидкий при роботі або жертвувати швидкістю роботи системи.

### **1.3.2 Засоби ідентифікації та аутентифікації користувачів**

Аутентифікація забезпечує захист від отримання доступу злоумисником до критичної інформації корпорації. При аутентифікації використовують персональні ідентифікатори. Методи аутентифікації та ідентифікації користувачів: біометричні, через обліковий запит, через пошту.

Нажаль дані засоби захисту не завжди можуть забезпечити достатню безпеку через можливість викрадання паролів користувачів та їх облікових записів, що використовуються ними для входу на робоче місце. Для повноцінного захисту їх необхідно комбінуватися з іншими засобами захисту наприклад шифрування.

#### **1.3.2.1 Аутентифікація за допомогою СМС, її недоліки**

Аутентифікація за допомогою СМС-повідомлень досить популярна та актуальна на сьогоднішній день.

Процедура даної аутентифікації складається з наступних кроків:

- Користувач вводить логін та пароль

- Надсилається одноразовий пароль у вигляді текстового SMS-повідомлення.
- Пароль використовується для аутентифікації

Даний метод полягає в отриманні ключа не з каналу, по якому проводиться аутентифікація, такий метод використовується в банківських.

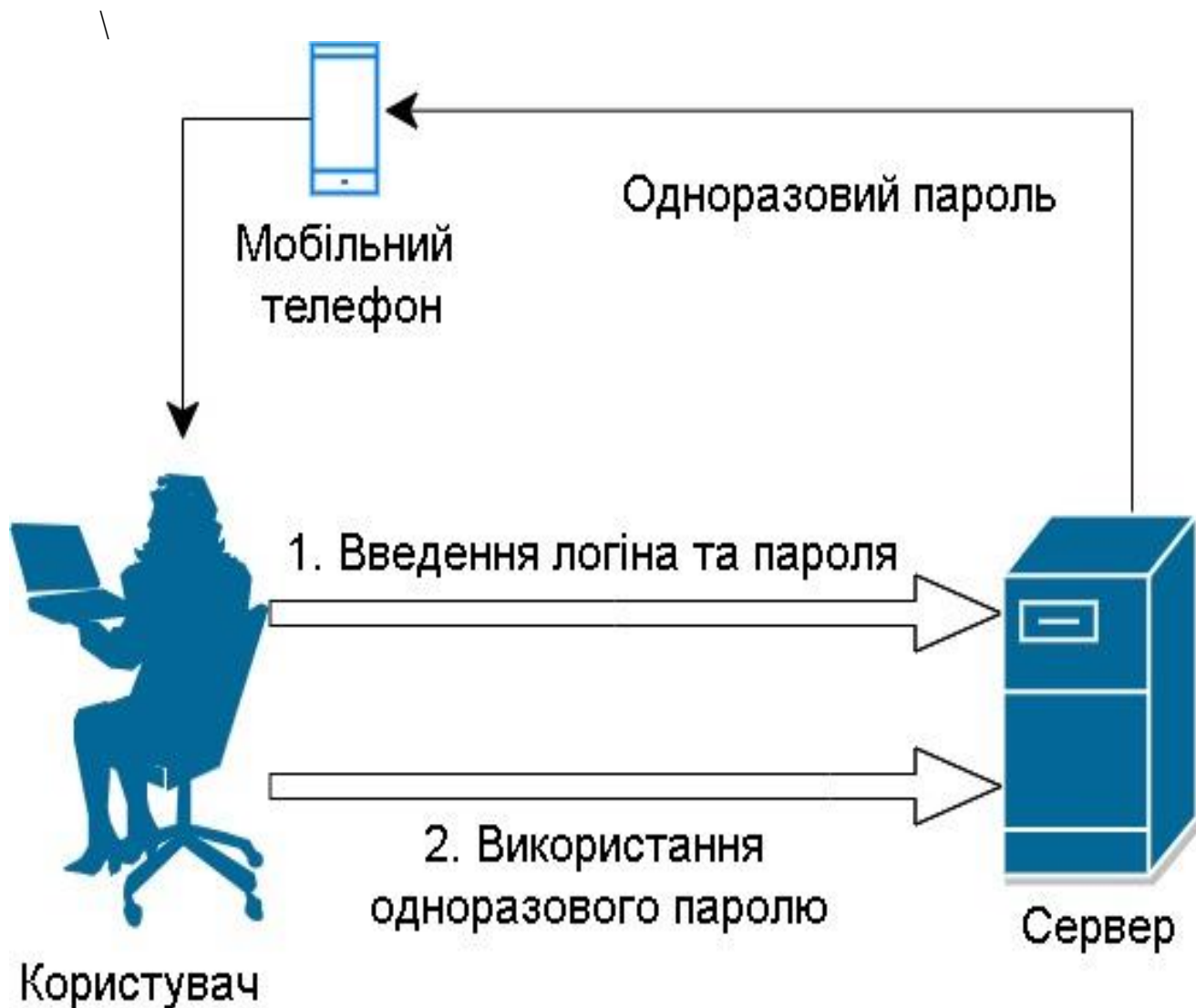


Рисунок 1.4 - Графічна ілюстрація аутентифікації за допомогою SMS

Недоліки:

- Можлива відсутність зв'язку.
- Можлива підміна номера.
- Можливе викрадення телефону та його використання.

### 1.3.2.2 Біометрична аутентифікація, її недоліки

Біометрична аутентифікація досить дорога та не завжди може себе окупити при використанні. Її можна обійти різноманітними методами та засобами:

- Програмно:
- біометрично
- сторонніми засобами.

Біометричні системи можуть розпізнавати людей на основі: відбитків пальців, райдужної оболонки, голоси, малюнка ліній долоні, підпису, ходи.

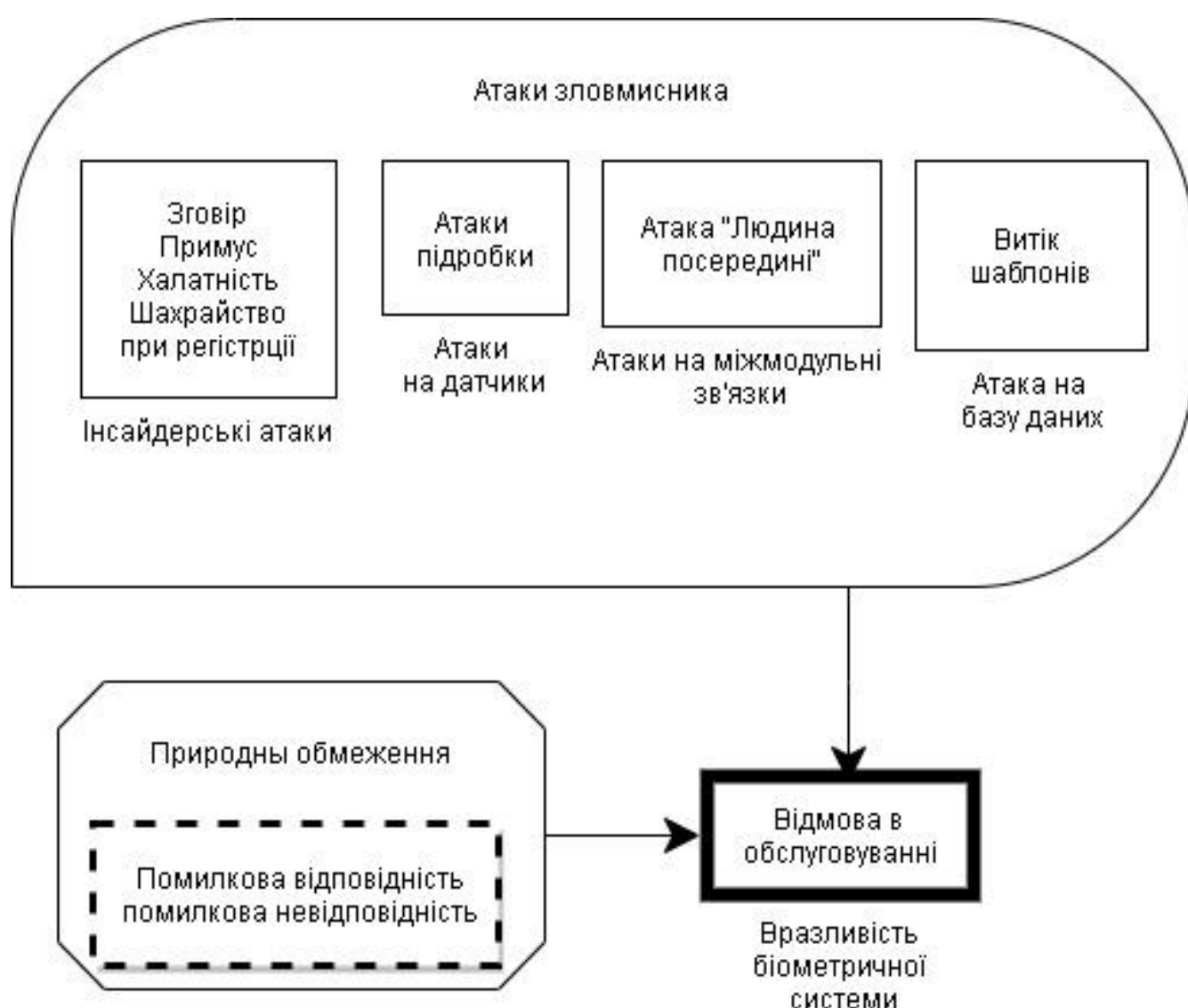


Рисунок 1.5 - Атаки зломисника на біометричну систему аутентифікації

Біометрична система вразлива для двох видів помилок.

- Коли система не розпізнає легітимного користувача, відбувається відмова в обслуговуванні.
- Коли самозванець невірно ідентифікується як авторизований користувач.

Наприклад при використанні відбитку пальця або сітчатки ока можливо підробити або використовувати дані органи без їх власника. Біометрична аутентифікація покладається на ступінь схожості двох біометричних зразків. Хибне невідповідність відбувається, коли два зразка від одного і того ж індивідуума мають низьку схожість і система не може їх зіставити. Хибне відповідність відбувається, коли два зразка від різних індивідуумів мають високу подібність і система некоректно оголошує їх збігаються. Біометрична система також може дати збій в результаті злочинних маніпуляцій, які можуть проводитися через інсайдерів або шляхом прямої атаки на інфраструктуру.

Дві серйозні вразливості:

- атаки підробки на призначений для користувача інтерфейс
- витік з бази шаблонів

Ці дві атаки мають серйозний негативний вплив на захищеність біометричної системи. Атака підробки полягає в наданні підробленої біометричної риси: пластиліновий палець, знімок або маска особи, реальний відрізаний палець легітимного користувача.

### **1.3.2.3 Аутентифікація за допомогою пароля, її недоліки**

Найпопулярніший спосіб аутентифікації – використання логіна та паролю. Алгоритм простої аутентифікації:

- Суб'єкт вводить логін і пароль.
- Введені дані порівнюються з еталоном.
- При збігу аутентифікація успішна, при розбіжності – аутентифікація не успішна.

Недоліки парольної аутентифікації:

- Багато користувачів використовують однаковий пароль для різних систем.
- Близько 60% користувачів записують паролі на папірцях.
- Можливість передачі пароля іншій особі, що відбувається досить часто.

Отже процес аутентифікації не завжди може забезпечити надійний захист через велику кількість вразливостей.

### **1.3.3 Засоби управління доступом**

Система контролю управління доступом дозволяє: контролювати вхід/вихід на об'єкт, що охороняється, призначати співробітникам графік роботи, зберігати інформацію про події за день.

У даних засобах є істотний недолік – вартість реалізації та найм працівників для реалізації контролю доступу. Це досить затратно та не вигідно у більшості випадків. Дані системи забезпечують захист від внутрішніх атак на систему, проте не реалізують захисту проти зовнішніх, тому необхідно використовувати додаткові засоби захисту.

### **1.3.4 Протоколювання і аудит**

Протоколювання забезпечує накопичення та збереження інформації про події, що відбуваються в інформаційній системі. У кожної системи існує набір можливих подій: зовнішні, що викликані діями інших сервісів, внутрішні, що викликані діями самого сервісу, та клієнтські, що викликані діями користувачів і адміністраторів.



Аудит - це процес аналізу накопиченої інформації. Він проводиться або з незначною затримкою, майже в реальному часі, або періодично в залежності від налаштувань системи.

Причини впровадження протоколювання і аудиту:

- забезпечення підзвітності користувачів і адміністраторів;
- забезпечення можливості реконструкції тайм лайнів;
- виявлення спроб вторгнень у систему;
- надання інформації для виявлення і аналізу проблем.

#### **1.3.4.1 Недоліки протоколювання та аудиту**

Проблеми при впровадженні протоколювання та аудиту:

- не всі компоненти системи можуть забезпечувати протоколювання
- необхідно пов'язувати між собою події в різних сервісах.
- залежність від інших засобів безпеки.

В вищезазначеного витікає висновок, що процес протоколювання та аудиту потребує додаткових компонентів системи та засобів захисту інакше він буде вразливим та малоефективним.

#### **1.3.5 Антивірусні програми**

Всі антивірусні програми діляться на три види: полифаги, ревізори, блокувальники. Робота полифагов полягає в пошуку вірусних файлів в оперативній системі і завантажувальних дисків.

Ревізори підраховують контрольну суму всіх файлів, і при знахідці зайвого видають повідомлення про помилку.

Недоліки ревізорів: якщо в комп'ютерному антивірусі не забиті дані про нову інформацію ревізор може прийняти її, як заражений файл.

Блокувальники перехоплюють вірусні посилання і файли.

### **1.3.5.1 Недоліки антивірусних програм**

Основним недоліком є залежність від своєчасного оновлення бази даних вірусів. Бо через не своєчасне оновлення або не виявлення загроз антивірус не зможе забезпечити повну безпеку системи.

Враховуючи швидкість створення зловмисного програного забезпечення то даний недолік досить суттєвий.

Антивірусна програма забирає обчислювальні ресурси системи, навантажуючи центральний процесор і жорсткий диск.

Антивірусні програми можуть помилково спрацьовувати на незаражені та безпечні файли.

За допомогою шифрування та упаковок вірусів можна приховати загрозу, й антивірус її не зможе ідентифікувати.

### **1.3.6 Системи шифрування дискових даних, їх недоліки**

Щоб зробити інформацію безкорисною для зловмисників, застосовують системи шифрування.

Вони можуть здійснювати криптографічні перетворення даних. За способом функціонування системи шифрування дискових даних поділяють на два класи:

- В системах прозорого шифрування криптографічні перетворення здійснюються в режимі реального часу.
- системи, яку являють собою утиліти, що необхідно запускати для здійснення шифрування.

Даний метод потребує значної кількості дискового простору та швидкодії системи. Це обумовлено тим, що шифрування дискових даних відбувається повільно, а розшифрування ще повільніше.

### 1.3.7 Недоліки мережевих екранів

Фаєрволи - це система або комбінація систем, що дозволяють розділити мережу на дві або більше частин і реалізувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Даний захист дозволяє сильно зменшити загрозу несанкціонованого доступу ззовні в системі, але не усуває цю небезпеку повністю. Апаратний брандмауер представляє собою пристрій, що фізично підключається до мережі. Програмний брандмауер виконує ті ж функції, використовуючи не зовнішній пристрій, а встановлену на комп'ютері програму

Кожен з видів фаєрвола: мережного рівня, прикладного рівня і рівня з'єднання, має свої переваги й недоліки тому даний хасіб захисту не може повноцінно забезпечити захищеність системи.

До основних недоліків відносяться:

- апаратний фаєрвол дуже дорогий.
- програмний фаєрвол використовує велику кількість системних ресурси
- програмні фаєрволи необхідно встановлювати на всіх робочих станціях і серверах мережі.
- висока ймовірність того, що він може заблокувати деякі необхідні для користувача служби.
- якщо на об'єкт, захист якого здійснює фаєрволи, дозволяється необмежений модемний доступ, зловмисники можуть обійти фаєрволи.
- не може забезпечити захист від внутрішніх загроз.
- не захищає від завантаження користувачами заражених вірусів, програм та перевіряє зміст пошти на загрози.
- у більшості приладів, відсутні механізми аудиту та подачі сигналу тривоги.
- фаєрволи прикладного рівня знижують ККД мережі.

- фаєрволи прикладного рівня вимагають програмного забезпечення для кожної мережевої служби.
- Відсутній захист проти атак соціальної інженерії.

### 1.3.8 Proxy-servers, недоліки

Суть захисту полягає в тому, що весь трафік мережевого / транспортного рівнів між локальної та глобальної мережами забороняється.

Звернення з локальної мережі в глобальну відбуваються через сервери-посередники, при цьому звернення з глобальної мережі в локальну стають неможливими.

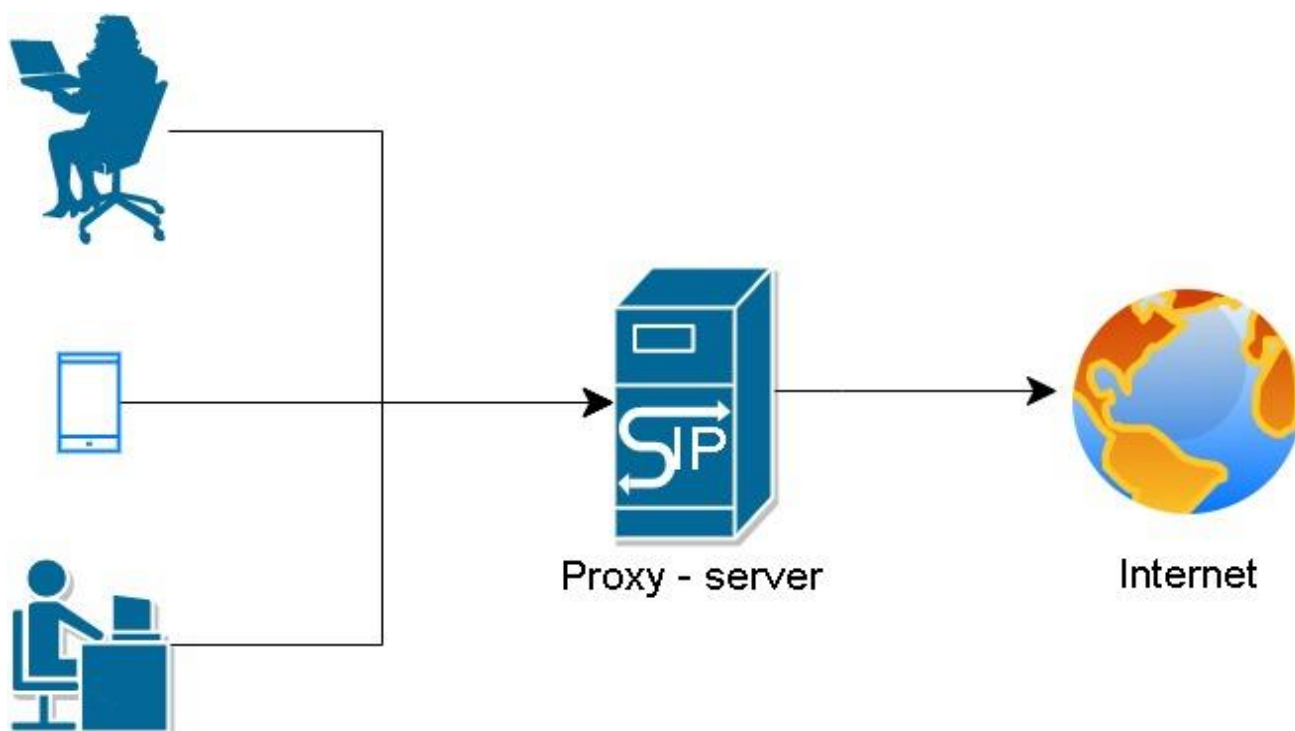


Рисунок 1.6 - Приклад зв'язку через проксі - сервер

Недоліки:

- не дає достатнього захисту проти атак на рівні додатку.
- не відбувається шифрування даних
- можливе значне сповільнення роботи.

## **Висновок до розділу 1**

Системи обробки критичної інформації мають забезпечувати надійний захист та варіативність використання методів захисту. Необхідна можливість віддаленого використання при збереженні надійності та безпеки критичної інформації.

На сьогоднішній день існує велика різноманітність методів та засобів забезпечення безпеки подібних систем. Нажаль, вони мають свої недоліки, тому незважаючи на їх переваги необхідні дієві рішення що зможуть забезпечити не лише надійність але й варіативність.

Через це для мінімізації можливих вторгнень у системи обробки критичної інформації варто створити таку модель системи, що зможе забезпечити безпеку на кожному етапі роботи з критичною інформацією та отриманням доступу до неї.

## **2 МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ СИСТЕМИ ОБРОБКИ КРИТИЧНОЇ ІНФОРМАЦІЇ.**

На сьогоднішній день основними проблемами захисту інформації у мережі є велика кількість зловмисного програмного забезпечення, що генерується щодня, фактор соціальної інженерії, велика масштабованість програмних продуктів як для роботи в мережі так і для забезпечення захисту.

Проблема масштабованості обумовлена тим, що при виявленні вразливості у продукті велика кількість споживачів потраплять у пастку та ризикують своєю критичною інформацією.

У даному розділі будуть проаналізовані існуючі засоби захисту критичної інформації, аналіз вимог щодо захисту систем обробки критичної інформації, моделі використання засобів захисту інформації та запропоновано створення системи, що зможе забезпечити високий рівень захисту систем обробки критичної інформації.

### **2.1 Вимоги захисту систем обробки критичної інформації.**

Існують закони та загальні вимоги до систем обробки критично інформації, які можна використовувати при проектуванні та створенні системи обробки критичної інформації. Дані вимоги були затверджені постановою Кабінету Міністрів України від 19 червня 2019 р.

Організаційні та технічні заходи повинні забезпечувати[1]:

- формування політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів;
- ідентифікацію та автентифікацію користувачів та адміністраторів;
- реєстрацію подій об'єктами системи та їх періодичний аудит;
- мережевий захист;
- доступність та відмовостійкість;

- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації;
- визначення умов використання програмного та апаратного забезпечення;
- визначення умов розміщення компонентів системи.

Не всі вимоги з даного переліку буде необхідно використовувати у даній роботі, однак більшість з них все ж таки будуть проаналізовані та використані задля забезпечення високо рівня захисту системи обробки критичної інформації.

### **2.1.1 Ідентифікація та автентифікація користувачів.**

Ідентифікація та автентифікація користувачів та адміністраторів необхідна в системах обробки критичної інформації. Даний засіб захисту суттєво підвищить захищеність всієї системи як проти зовнішніх так й проти внутрішніх атак та спроб отримання критичної інформації.

Для доступу до служб та інформації повинна використовуватися багатфакторна автентифікація користувачів та адміністраторів. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні.[1]

Повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів. Під час звільнення з посади працівника його обліковий запис повинен бути негайно заблокований або видалений.[1]

Обладнання, яке підключається до системи управління технологічними процесами об'єкта критичної інфраструктури, повинно бути ідентифіковане, а також повинні бути вжиті заходи, які унеможливають роботу обладнання в мережі без відповідної ідентифікації.[1]

Таким чином буде даний засіб захисту значно підвищує усю захищеність системи та дає можливість реалізовувати контроль дій користувачів та

адміністраторів задля запобігання зовнішніх та внутрішніх атак на систему обробки критичної інформації.

### **2.1.2 Реєстрація подій у системі**

Необхідна реалізувати реєстрацію, та захист від модифікації інформації про наступні події:

- доступ до інформації
- дії з інформацією
- вхід/вихід користувачів та адміністраторів
- невдалі спроби входу користувачів та адміністраторів
- реєстрація та видалення облікових записів користувачів та адміністраторів
- зміна пароля користувачів системи
- реєстрація подій, пов'язаних із зміною конфігурації
- спроби здійснення несанкціонованого доступу
- всі дії адміністратора з журналами реєстрації подій

Повинні вестися журнали реєстрації подій та забезпечення їх надійного захисту та цілісності. Журнали подій мають реалізовувати повну фіксацію всіх дій користувачів та подій у системі. Зберігатися у шифрованому вигляді та бути стійкими до спроб їх модернізації.

### **2.1.3 Мережевий захист компонентів та інформаційних ресурсів**

Даний захист повинен ключати в себе фільтрацію трафіку та розмежування доступу між внутрішньою мережею та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. Блокування трафіку та з'єднань, які не відповідають визначеним критеріям;



Фільтрацію та аналіз трафіку, моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення, моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення.

Також необхідно реалізувати захист від:

- захист від атак “відмова в обслуговуванні”;
- захист від несанкціонованого доступу через Інтернет;
- балансування навантаження;
- маскуванню структури і мережевих адрес мережі;
- завершення з’єднання з вузлом у разі атаки;
- здійснення реєстрації подій, що мають відношення до безпеки.

Вимоги:[1]

- Сервери та обладнання, повинні бути розміщені в зовнішній зоні системи обробки критичної інформації. [1]
- З’єднання серверів та обладнання, в зовнішній зоні, із серверами та обладнанням внутрішньої мережі повинні захищатися міжмережним екраном. [1]
- Повинні бути визначені та відключені програмні порти, які є небезпечними для забезпечення кібербезпеки.
- Передача даних бездротовими мережами повинна здійснюватися виключно захищеними з’єднаннями.
- Для захисту даних, які передаються через незахищене середовище необхідно використовувати захищені з’єднання.
- Систему дозволяється підключати до глобальних мереж тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту.[1]
- До глобальних мереж передачі даних, необхідно підключатися через провайдерів, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними КСЗІ з підтвердженою відповідністю.[1]

### **2.1.4 Відмовостійкість компонентів системи**

Для забезпечення відмовостійкості повинно здійснюватися:

- періодичне створення резервних копій інформаційних ресурсів.
- Резервування критичних програмних та апаратних компонентів.
- Зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами). [1]
- Під час розроблення, модернізації або оновлення компонентів системи необхідно використовувати тестову програмно-апаратну платформу, для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення, перед тим як впровадити їх в промислову експлуатацію.

### **2.1.5 Умови використання зовнішніх пристроїв**

Повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. [1]

Повинна здійснюватися ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора. [1]

Повинно бути унеможливлено використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані. [1]

Повинно бути відключено автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації. [1]

Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами. [1]

### **2.1.6 Умови використання програмного та апаратного забезпечення**

Повинна проводитися перевірка на цілісність та автентичність оновлень компонентів об'єкта. [1]

Повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів. [1]

Повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій. [1]

Повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор. [1]

Повинно забезпечуватися неприйняття файла/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файла/повідомлення, що надійшов/надійшло. Ця подія повинна відображатися в журналі реєстрації подій. [1]

## **2.2 Вибір засобів захисту на основі аналізу вимог**

Для створення захищеної системи обробки критичної інформації необхідно виконати вимоги до кіберзахисту об'єктів критичної інфраструктури та підібрати відповідне, що забезпечить надійний захист системи. Для цього варто проаналізувати вартість, властивості та характеристики існуючих засобів захисту, створити модель системи, проаналізувати її захищеність, технічні характеристики та вартість засобів, що будуть використовуватися.

### **2.2.1 Аналіз необхідних засобів захисту**

Для розробки захищеної системи обробки критичної інформації необхідно створити плану реалізації та створення системи. Для цього необхідно

скористатися нормативним документом системи технічного захисту інформації про критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99[3].

Проаналізувавши вимоги захисту систем обробки критичної інформації можна зробити висновок, що найголовнішим фактором при проектуванні даної системи буде врахування конфіденційності та цілісності критичної інформації, що буде циркулювати в системі.

Для побудови системи засобів захисту та плану моделі необхідно буде проаналізувати чотири групи критеріїв: конфіденційність, цілісність, доступність та спостережність.

За допомогою такого підходу можна спроектувати комплекс засобів захисту для системи обробки критичної інформації, що буде враховувати захист критичних об'єктів системи та задовольняти вимогам до системи.

Таблиця 2.1 - Перелік критеріїв

Конфіденційність	КА-2	КВ-3	КО-1				
Цілісність	ЦО-2	ЦВ-3					
Доступність	ДЗ-1	ДВ-1					
Спостережність	НР-2	НИ-1	КН-1	НО-1	НВ-1	НА-1	НЦ-1

Через обробку критичної інформації в нашому випадку система буде з підвищеними вимогами до забезпечення конфіденційності та цілісності оброблюваної інформації.

Проектована системи буде розподіленою багатомашинною та багатокористувачевою системою в якій оброблятиметься критична інформація, частина якої буде передаватися через незахищене середовище, наприклад мережа інтернет.

З вищезазначеного можна виявити клас системи – «3».

Таким чином наша система матиме наступний функціональний профіль:

3.КЦ.3 = { КА-2, КВ-3, КО-1,  
ЦО-2, ЦВ-3,  
ДЗ-1, ДВ-1,  
НР-2, НИ-1, НК-1, НО-1, НВ-1, НА-1, НЦ-1 }

Даний функціональний профіль забезпечить надійний захист системі обробки критичної інформації.

Необхідні заходи в системі обробки критичної інформації у відповідності до функціонального профілю:

Таблиця 2.2 - Критерії проектованої системи

КА-2	Базова адміністративна конфіденційність	Дозволяє адміністратору керувати потоками інформації від захищених об'єктів до користувачів.
КВ-3	Повна конфіденційність при обміні	Забезпечує захист об'єктів від несанкціонованого ознайомлення, під час їх передачі через незахищене середовище.
КО-1	Повторне використання об'єктів	Коректність повторного використання об'єкта гарантуючи що він не міститиме інформації, попереднього користувача.
ЦО-2	Повний відкат	Можливість відмінити операцію та повернути об'єкт до попереднього стану.
ЦВ-3	Повна цілісність при обміні	Забезпечує захист від несанкціонованої модифікації інформації її передачі через незахищене середовище.

Кінець таблиці 2.2

ДЗ-1	Модернізація	Гарантувати доступність КС в процесі заміни окремих компонентів.
ДВ-1	Ручне відновлення	Забезпечує повернення системи у захищений стан після переривання обслуговування.
НР-2	Захищений журнал	Реєстрація дозволяє контролювати небезпечні для КС дії.
НИ-1	Зовнішня ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють визначити та перевірити особистість користувача.
НК-1	Однонаправлений достовірний канал	Дозволяє користувачу можливість взаємодії з КЗЗ.
НО-1	Виділення адміністратора	Зменшує збитки від навмисних або помилкових дій користувача.
НВ-1	Автентифікація вузла	Дозволяє одному КЗЗ ідентифікувати інший КЗЗ і забезпечити іншому КЗЗ можливість ідентифікувати перший, перед взаємодією.
НА-1	Базова автентифікація відправника	Забезпечує захист від відмови від авторства.
НЦ-1	Контроль цілісності	Визначає здатність системи захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

### 2.2.2 Вибір апаратури для проектування системи

Для забезпечення захисту проектувальної системи необхідно дотримуватися наступних властивостей: розмежування доступу, шифрування даних при передачі, використання цифрового підпису, автентифікація складових системи,

адміністрування системи, захищений журнал, можливість відновити систему, можливість повернути дані до необхідного стану.

Дана система буде забезпечувати захист критичній інформації. Засоби та методи що будуть використовуватися для забезпечення захисту системи:

- на машині користувачів:
  - a. Аудит та протоколювання дій користувачів
  - b. Ідентифікація та аутентифікація перед використання машини
  - c. Антивірус
- на машині адміністратора:
  - a. Аудит та протоколювання дій адміністратора
  - b. Контроль дій користувачів
  - c. Ідентифікація та аутентифікація перед використання машини
  - d. Антивірус
  - e. Шифрування даних стандартними засобами БД
- на сервері:
  - a. Виконання функції проксі сервера
  - b. Фаєрволл
  - c. Антивірус
  - d. Захист від ддос - атак
- додаткові засоби захисту та правила:
  - a. Дротове з'єднання всіх елементів системи
  - b. Підключення лише по MAC – адресу
  - c. Заборона використання зовнішніх тимчасових приладів
  - d. Розмежування прав доступу
  - e. Заборона використання бездротового зв'язку
  - f. Резервування критичних складових системи (наприклад сервер)

Додаткові засоби захисту можливо реалізувати за допомогою базових засобів операційної системи, як лінукс так і віндовс. Це може реалізувати адміністратор без додаткових витрат на програмне та технічне забезпечення.

При підрахунку вартості системи було реалізовано лише підрахунок засобів захисту, без врахування вартості обчислюваних машин, серверів, тощо.

Для реалізації захисту системи необхідно купити: антивірус, фаєрвол, базу даних з підтримкою шифрування, програму для контролю користувачів системи, захист від ддос – атак.

Обладнання, що необхідно для закупівлі, орієнтоване приблизно на 10 користувачів:

- Антивірус: Avast Internet Security 2019
- Файрвол: Cisco RV325-K9-G5
- Захист від ддос атак: рекомендовано використовувати захист, що пропонують компанії, для гарантій захисту.
- Програма для контролю за користувачами: LanAgent
- Флешки з шифруванням: iStorage datAshur Personal

Таблиця 2.3 - Вартість необхідних засобів захисту для системи обробки критичної інформації:

Захист	Прилад	Кількість	Ціні за одиницю	Ціна грн/за рік
Антивірус	Avast Internet Security 2019	1	600	600
Файрвол	Cisco RV325-K9-G5	1	10 000	10 000
Захист від ддос атак	Послуги компанії	1	10 000 (за місяць)	120 000
Програма для контролю за користувачами	<u>LanAgent</u>	10	500	5 000
Флешки з шифруванням	iStorage datAshur Personal	10	2 000	20 000
Загальна сума:				155 600 грн



Дана система забезпечить захист проти зовнішніх атак та зловмисного програмного забезпечення, на жаль, система не буде спроможна протидіяти людському фактору. Через це буде залишатися досить суттєва ймовірність втрати критичної інформації.

Недоліки системи:

- Відсутній захист проти внутрішньої загрози через співробітників компанії
- Відсутній повний захист від дій користувачів в системі, таким чином користувач може стати жертвою соціальної інженерії або внутрішнім агентом.
- Захист проти перехоплення недостатній, стандартне шифрування не завжди може забезпечити достатній захист даних.
- Відсутній захист від копіювання даних та перехвату при роботі з системою

Таким чином дана система може забезпечити достатній рівень безпеки системі обробки критичної інформації організації, однак все ж таки матиме досить велику кількість суттєвих недоліків, що зможуть дати можливість зловмиснику отримати бажану інформацію, не кажучи про досить високу вартість системи.

### **2.3 Запропоновані заходи для забезпечення захисту системи обробки критичної інформації.**

Було виявлено велику кількість проблем у методах захисту під час проведення дослідження. Найбільш вагомі проблеми було виявлено шляхом детального розгляду та аналізу методів захисту. Наприклад проксі – сервер не реалізує шифрування трафіку а лише маскує місцезнаходження користувача у той же час користувач отримує трафік, що може містити як і корисну інформацію так і зловмисні додатки або зловмисний код.

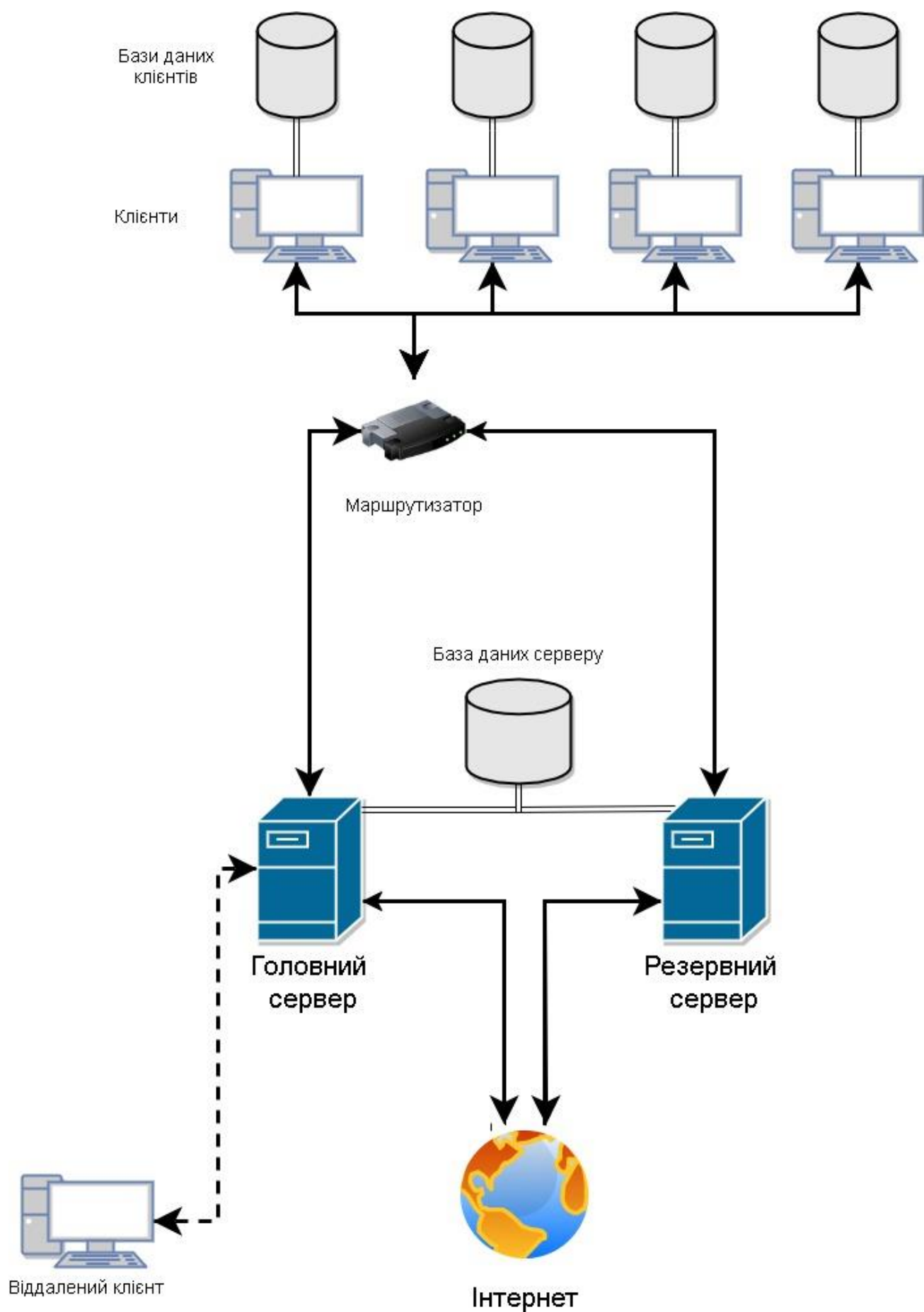


Рисунок 2.1 - Модель захищеної системи обробки критичної інформації

Проблему фільтрації ресурсів та трафіку забезпечує фаєрвол однак він у свою чергу не реалізує перевірку завантажень користувача, таким чином не реалізується захист повноцінно та не може забезпечити захист.

Також фаєрволи не забезпечують безпеки проти внутрішніх атак, адже працюють на захист проти зовнішніх загроз.

Антивіруси також не можуть забезпечити належного захисту, оскільки величезна база даних вірусів, що постійно поповнюється просто не спроможна на справитися з новими загрозами, а працює використовуючи базу вже знайдених загроз. Таким чином антивіруси також не спроможні реалізувати повноцінний захист користувачів.

Для забезпечення надійної захищеності системи обробки критичної інформації необхідно створити систему методів та засобів по забезпеченню захисту, що забезпечить надійний захист систем обробки інформації.

Для системи буде використовуватися наступні засоби захисті:

- Шифрування при передачі та зберіганні інформації
- Фільтр для аналізу та фільтрації отриманих даних
- Захищений інтерфейс для користування мережею
- Сервер для з'єднання клієнта та мережі інтернет
- Збереження даних у шифрованому виді
- Контроль за діями користувачів
- Можливість роботи через бездротовий зв'язок
- Фільтр даних, які будуть циркулювати в системі під час роботи користувачів
- Дублювання критичних компонентів системи
- Підключення приладів по ідентифікаторах
- Використання маршрутизаторів для з'єднання машин користувачів із сервером
- Спеціалізоване обладнання для забезпечення захисту приміщення в якому будуть знаходитися компоненти системи

### **2.3.1 Шифрування при передачі та зберіганні даних**

Зазвичай при використанні гібридного шифрування використовують асиметричне шифрування для передачі ключа, та симетричне для шифрування повідомлення. Саме така система реалізовується оскільки необхідно було поєднати швидкість та якість шифрування задля забезпечення захисту критичної інформації.

Я вирішив використовувати трохи інший підхід та реалізувати систему на двох алгоритмах асиметричного шифрування. Це обумовлено не великим обсягом інформації яка буде передаватися, що у свою чергу значно посилить захист та не буде впливати на швидкодію передачі даних.

Таким чином можливо забезпечити значно більший захист даних, що передаються та зберігається у системі без ризиків сильного сповільнення роботи користувачів та всієї системи загалом.

### **2.3.2 Фільтр для реалізації аналізу та фільтрації отриманих даних сервером**

Під час аналізу існуючих методів захисту я звернув увагу що існує велика кількість фільтрів трафіку по різних критеріям, та проксі серверам, що забезпечують змінення місцезнаходження користувачів.

Однак проаналізувавши дані методи я зрозумів, що доцільніше було б використовувати такий фільтр даних, що надходитимуть користувачеві, що й сам користувач не зможе ненароком здійснити дії, котрі можуть йому нашкодити.

Фільтр буде працювати наступним чином: по перше фільтрувати дані, що надходитимуть, потім виділяти лише необхідну інформацію (текст, посилання, необхідні листи). Після фільтрації та перевірки даних на наявність коду зломисника, буде реалізовано їх шифрування гібридною криптосистемою та передача до клієнта, що виконував запит. Після чого клієнт отримає у своєму

додатку дані, що буде йому передано не переживаючи за свою безпеку та навіть необачність.

Даний фільтр увібрав у себе надійну безпеку та простоту в експлуатації. Даний засіб безпеки дозволить ізолювати локальну мережу та запобігти витоку критичної інформації.

### **2.3.3 Захищений інтерфейс для клієнта**

Даний інтерфейс безпечний дозволяє пошук інформації в інтернеті та використання пошти. Інтерфейс буде встановлено на клієнті. Дані при передачі будуть шифруватися та передаватися на сервер. Отримана відповідь буде розшифровуватися та виводитися на екран користувача. Інтерфейс буде підтримувати лиш текстові формати та отримувати відповідно також текст. Таким чином при використанні даним застосунком користувач нічим не ризикує. Дані на клієнті будуть зберігатися у шифрованому вигляді.

### **2.3.4 Сервер для з'єднання клієнта та мережі інтернет**

На сервері буде встановлено фільтр що фільтруватиме вхідні та вихідні дані. Гібридна криптосистема для шифрування та розшифрування даних та база з даними про історію з запитами користувачів.

Пошук даних у мережі буде реалізовуватися за допомогою пошукової системи Google. Для зв'язку з клієнтами буде реалізовано дротове з'єднання з резервним каналом передачі даних.

### **2.3.6 Контроль за діями користувачів**

Даний засіб захисту системи необхідний для контролю дій користувачів та можливості створення тайм лайну при необхідності та аналізувати дані з корками

що призвели до певних дій. Таким чином можна буде модернізувати та впроваджувати нововведення для покращення взаємодії з споживачем та прискорення роботи сієї системи. За допомогою даного засобу можливо буде постійно вдосконалювати та пришвидшувати роботу споживачів не кажучи вже про можливість відслідковування та виявлення зловмисних дій, що можуть намагатися зробити користувачі.

Контроль за діями користувачів система буде реалізовувати шляхом реєстрації кожної дії та події а при необхідності повідомляти про потенційно небезпечні дії.

### **2.3.7 Можливість роботи через бездротовий зв'язок**

За допомогою впровадження шифрування можливо реалізувати роботу через бездротовий в'язок, точніше віддалено. Дане введення використовується через швидкий та інтенсивний розвиток бездротового з'єднання та необхідності час від часу віддалено пересилати чи отримувати дані.

Дане введення значно пришвидшить реакцію та роботу через систему. Звісно для віддаленого користування буде окремо готуватися мишина, на якій буде реалізовувати робота з системою обробки критичної інформації. Функціонал буде урізаний, це обумовлено необхідністю захисту системи від зовнішньої загрози та неможливістю впливати на систему через даний пристрій.

Таким чином можливо буде налаштувати зв'язок на досить великій відстані й зберегти конфіденційну інформацію та систему в безпеці.

### **2.3.8 Фільтр даних, які будуть циркулювати в системі під час роботи користувачів**

Фільтр даних буде реалізовувати фільтрацію інформації, що буде передаватися системою користувачам під час роботи в мережі та з поштою. Даний

підхід не дасть можливості реалізовувати атаки направлені на використання браузерів та запуск скриптів й інших подібних атак.

Даний підхід забезпечить потужний захист системи від можливих атак з використанням соціальної інженерії та зловмисного програмного забезпечення.

Дані будуть фільтруватися на сервері а вже після передаватися на клієнта, тобто користувачу.

### **2.3.9 Дублювання критичних компонентів системи**

Для забезпечення відмово стійкості системи продумано дублювання та резервування критичних компонентів системи, таких як, сервер, бази даних, додаткові машини для роботи з системою.

Даний захист забезпечить відмово стійкість та збереження даних при знищенні чи поломці основного компонента. Дана міра необхідна для збереження даних про дії користувачів в системі, збереження їх даних та запобігти втраті критичної інформації.

## **Висновки до розділу 2**

Проаналізувавши сучасні методи захисту інформації можна зробити висновок, що вони не забезпечують достатнього захисту користувачів та їх даних та потребують модифікацій та удосконалень. Дуже висока вартість на послуги та засоби захисту через що деякі фірми не можуть собі дозволити їх використання та замінюють дешевшим обладнанням, що значно впливає на рівень захисту системи.

Була виявлена необхідність моделювання системи, що дозволить забезпечити безпеку локальній мережі та безпечне використання мережі інтернет. Тому було запропоновано систему котра врахувала переваги існуючих систем та нівелювала їх недоліки.

Для моделювання даної системи будуть використовуватися сучасні методи захисту, що були розглянуті, та будуть запропоновані вдосконалення їх властивостей в залежності від цільового призначення та потреб системи. Такі методи захисту як: шифрування при передачі даних, шифрування при зберіганні даних, резервування каналів зв'язку, фільтр для аналізу та фільтрації отриманих даних, контроль за діями користувачів, фільтр даних, які будуть циркулювати в системі під час роботи користувачів, дублювання критичних компонентів системи, підключення приладів по ідентифікаторах, використання маршрутизаторів для з'єднання машин користувачів із сервером.



### **3 СТВОРЕННЯ МОДЕЛІ ЗАХИЩЕНОЇ СИСТЕМИ ОБРОБКИ КРИТИЧНОЇ ІНФОРМАЦІЇ.**

Проаналізувавши перші два розділи стає зрозумілим, що на сьогоднішній день існуючі методи та засоби захисту не справляються з поставленим завданням.

Було проаналізовано та запропоновано оптимальне рішення по вирішенню проблеми викрадення конфіденційних даних користувачів під час роботи в мережі інтернет. При плануванні даної системи буде враховано всі переваги сучасних методів та засобів захисту, що використовуються при роботі в мережі інтернет та запропоновано вирішення їх недоліків.

Таким чином буде розроблено систему по забезпеченню конфіденційності даних і безпечної роботи в мережі інтернет, яка увібрала в себе усі переваги сучасних методів та засобів захисту й забезпечить оптимальне рішення для забезпечення безпечної роботи в мережі та конфіденційності даних користувача.

#### **3.1 Модель системи**

Модель було розроблено враховуючи актуальність та сучасність на сьогоднішній день методів захисту. Було враховано основні вразливості та загрози, що виникають під час роботи в мережі. Дану проблему було розглянуто не лише як захист від зовнішніх загроз а й захист від внутрішніх.

При розробці даної моделі використано наступні компоненти та методи захисту:

- Шифрування при передачі та зберіганні інформації
- Фільтр для аналізу та фільтрації отриманих даних
- Захищений інтерфейс для користування мережею
- Сервер для з'єднання клієнта та мережі інтернет

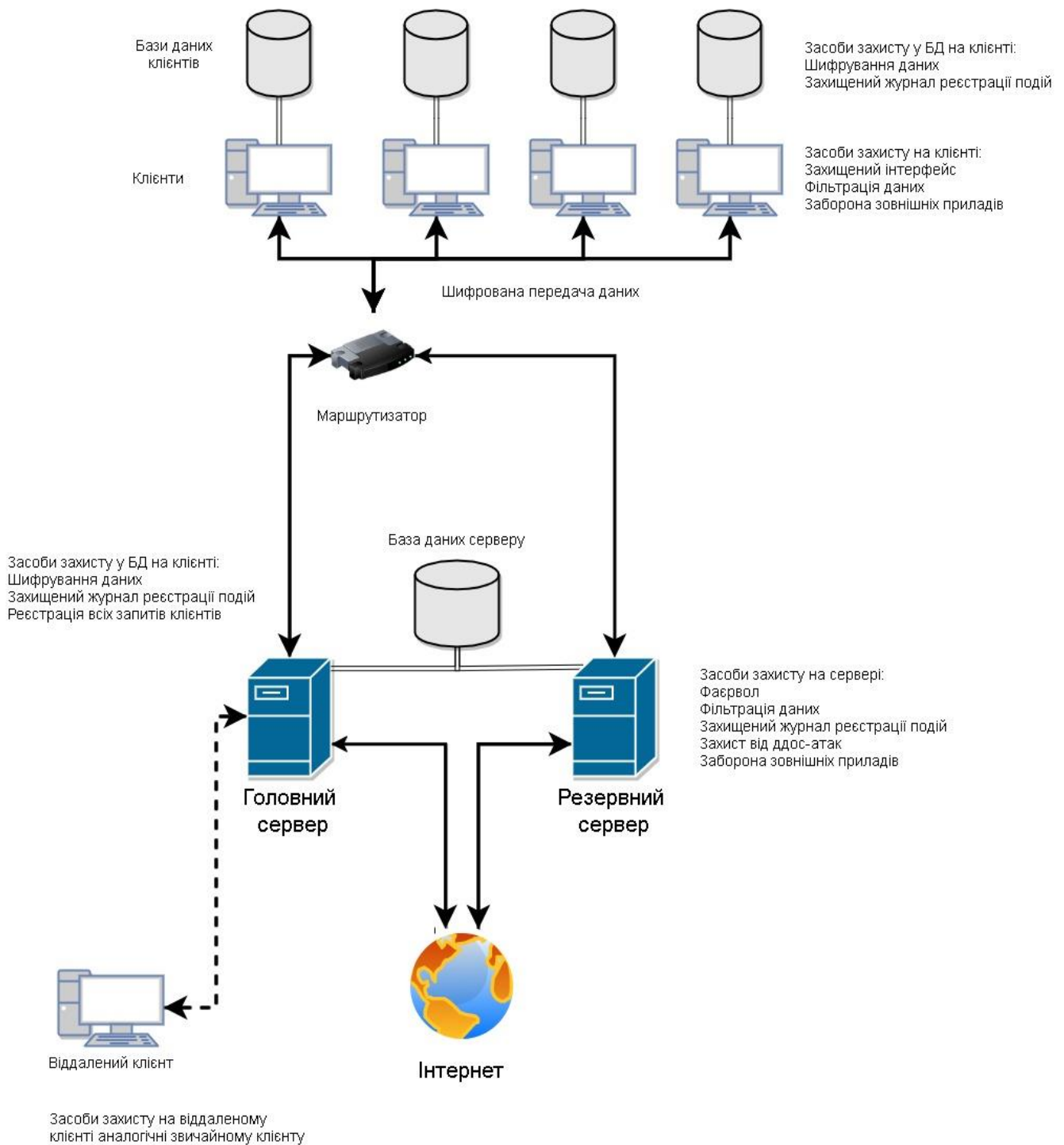


Рисунок 3.1 – Схема передачі даних в системі обробки критичної інформації

- Збереження даних у шифрованому виді
- Контроль за діями користувачів
- Можливість роботи через бездротовий зв'язок
- Фільтр даних, які будуть циркулювати в системі під час роботи користувачів

- Дублювання критичних компонентів системи
- Підключення приладів по ідентифікаторах
- Використання маршрутизаторів для з'єднання машин користувачів із сервером
- Спеціалізоване обладнання для забезпечення захисту приміщення в якому будуть знаходитися компоненти системи

Дана система увібрала в себе переваги сучасних рішень по забезпеченню безпеки роботи в мережі та протидії зловмисникам в отриманні конфіденційної інформації через мережу. Система спроможна забезпечити надійну роботу та безпеку конфіденційних даних користувачів від різноманітних загроз.

Даний склад системи було створено для забезпечення максимальної протидії спробам реалізації атак, направлених на користувачів. Вибір засобів захисту реалізовувався на основі їх технічних характеристиках та можливості поєднання з іншими засобами захисту.

### **3.1.1 Сервер**

Сервер забезпечує роботу та основну безпеку всієї системи. На ньому встановлено фаєрвол, антивірус, фільтр даних та систему гібридного шифрування/розшифрування.

Дані передаються між клієнтом та сервером по захищеному каналу передачі. За захист каналу відповідає гібридна криптосистема. Дані шифруються перед передачею та розшифровуються при їх використанні. У базі даних дані зберігаються в зашифрованому виді.

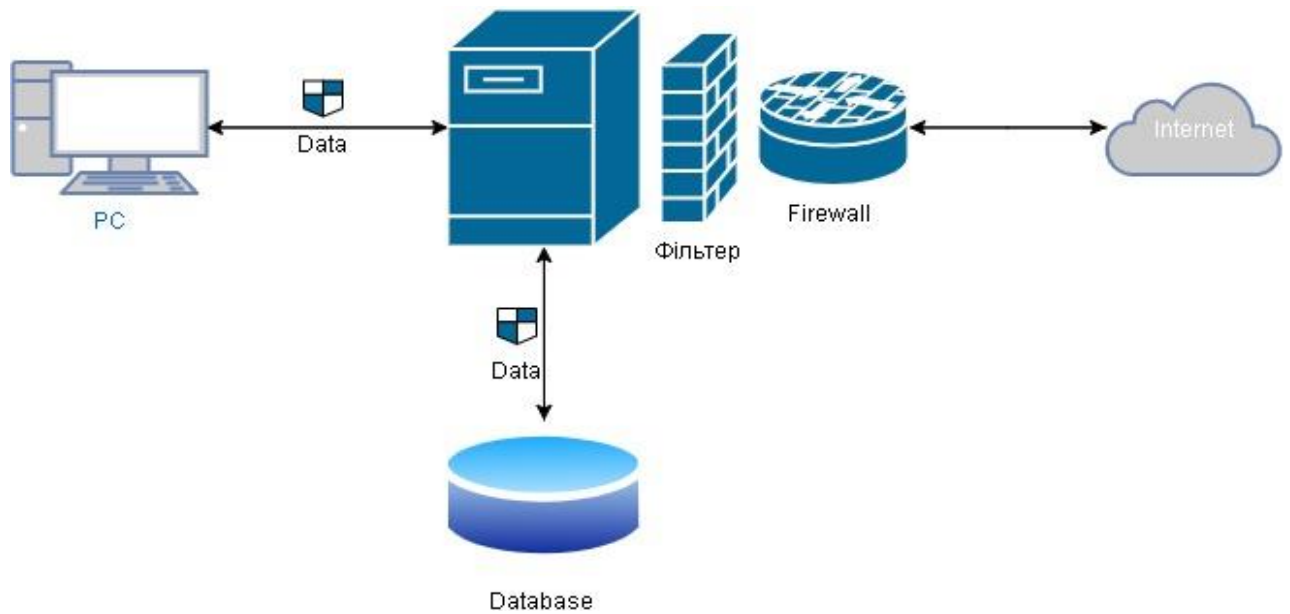


Рисунок 3.2 – Схема засобів захисту сервера

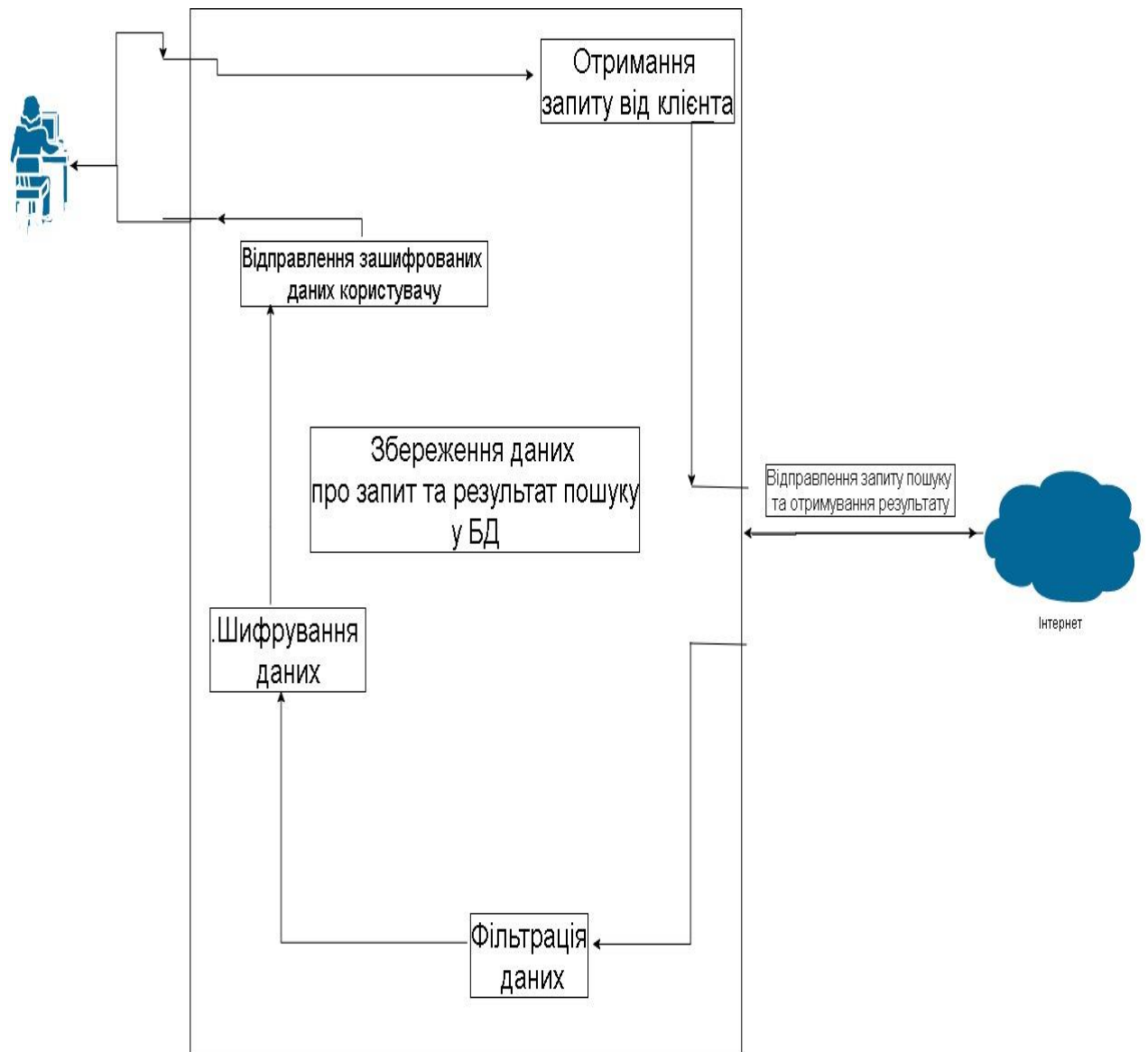


Рисунок 3.3 – Схема циркуляції даних на сервері

Сервер з клієнтом з'єднано кабелем Ethernet з резервуванням каналу передачі даних. Дані на клієнті та сервері зберігаються в зашифрованому виді в базі даних.

Такий підхід забезпечує безпечну передачу даних без ризиків при перехваті чи прослуховуванні трафіку.

Завдяки використанню гібридного шифрування навіть при збереженні інформації можна не хвилюватися за копіювання бази даних чи навіть ін'єкцій до бази даних, тому даний засіб захисту дуже ефективний.

Завдяки такому підходу до проектування серверу реалізовується ще один засіб по забезпеченню захисту системи – захист проти сканування та подальшого моделювання компонентів системи. Даний захист забезпечує захищеність компонентів системи проти сканування та проектування моделі системи й виявлення слабких сторін.

### **3.1.2 Клієнт**

Клієнт дозволяє реалізовувати роботу в системі користувачам. На клієнті встановлено систему шифрування для зберігання та передачі даних, систему розшифрування для реалізації читання та перегляду отриманої інформації, інтерфейс для роботи в мережі та листування.

База даних, встановлена на клієнті, реалізовуватиме зберігання даних та інформації про дії користувачів, тобто повний контроль над кожною дією користувача.

Таким чином користувач може реалізовувати пошук в мережі інтернет та роботу з базою даних та поштою без ризику підхопити зловмисне програмне забезпечення. Основний захист проти зовнішніх атак лягає на серверну частину.

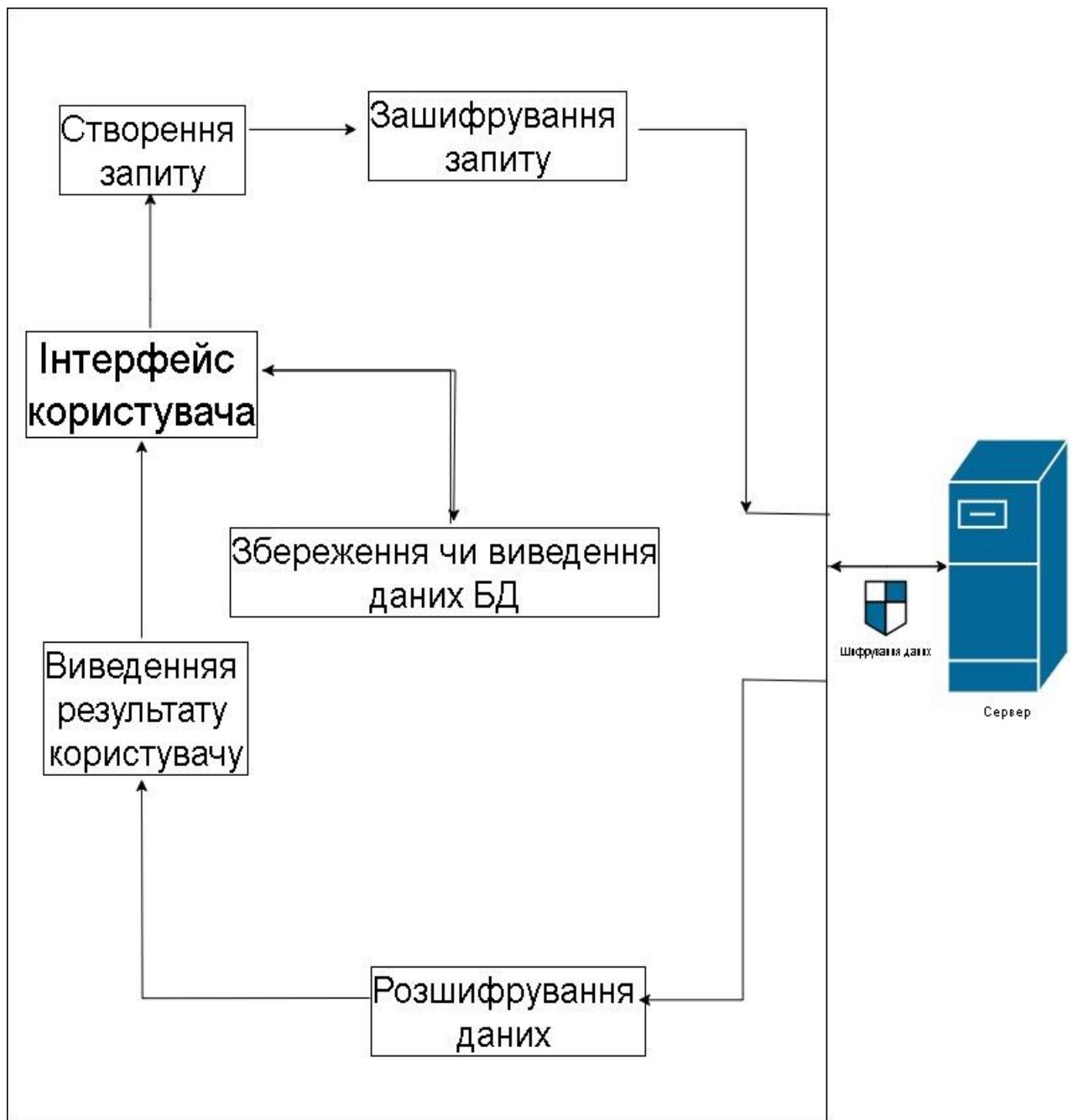


Рисунок 3.4 - Схема циркуляції даних на клієнті

База даних, встановлена на клієнті, реалізовуватиме зберігання даних та інформації про дії користувачів, тобто повний контроль над кожною дією користувача.

Таким чином користувач може реалізовувати пошук в мережі інтернет та роботу з базою даних та поштою без ризику підхопити зловмисне програмне забезпечення. Основний захист проти зовнішніх атак лягає на серверну частину.



Рисунок 3.5 – Схема засобів захисту клієнта

На клієнті встановлено гібридну криптосистему для розшифрування та шифрування даних, що будуть передаватися. Програма, в якій буде користувач взаємодіяти з сервером та криптосистемою, також встановлена на клієнті.

### 3.1.3 Віддалений клієнт

Суть використання віддаленого клієнта полягає в можливості віддалено підключитися до системи та отримувати чи надсилати інформацію. Дане підключення стане можливим за допомогою реалізації подвійного асиметричного шифрування.

Схема циркуляції даних на віддаленому клієнті буде аналогічній схемі циркуляції даних на клієнті.

Для функціонування та можливості підключення до системи необхідно буде встановити на клієнт: криптосистему для шифрування та дешифрування, інтерфейс користувача та фільтр. Даного поєднання буде достатньо для забезпечення роботи на відстані. Особливо враховуючи, урізаний функціонал для даного клієнта: неможливість передавати великі дані, а лише текстові та отримання необхідних даних.

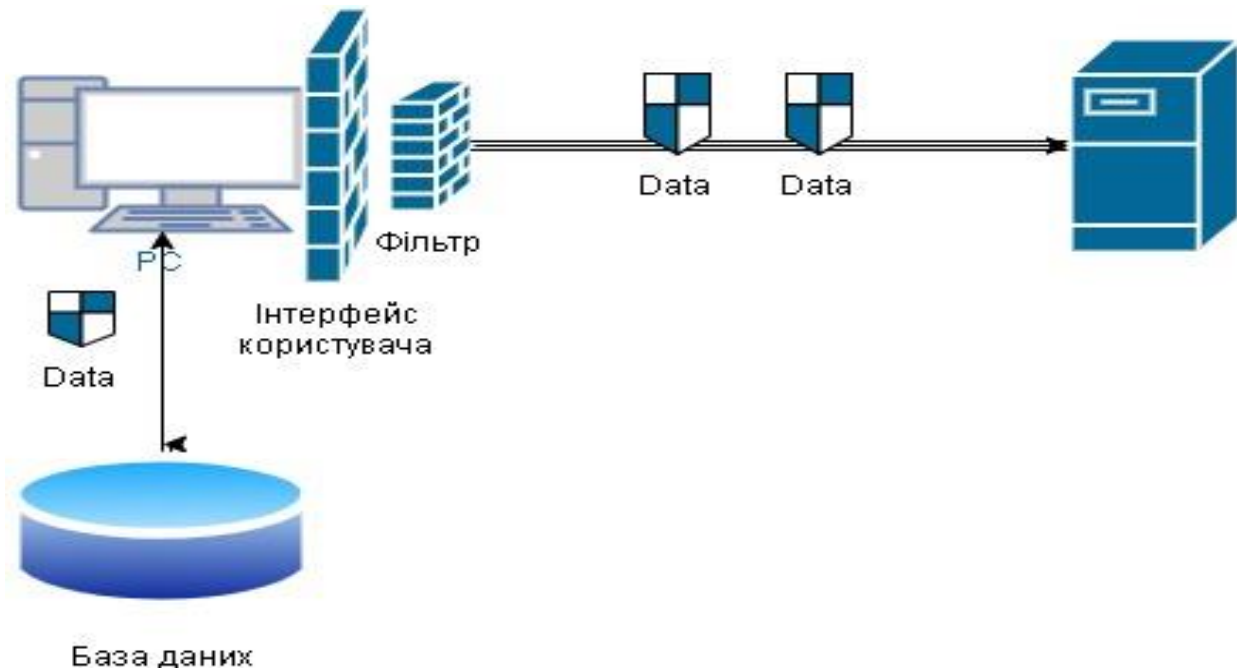


Рисунок 3.6 – Схема засобів захисту на віддаленому клієнті

Тобто для віддаленого клієнта існує ряд обмежень стосовно підключення та роботи з системою. Повноцінної роботи з системою не буде відбуватися, клієнт зможе отримувати та відправляти текстові повідомлення, передивлятися свої дані на основному робочому місці, однак не зможе нічого копіювати або скачувати.

### 3.2 Засоби захисту, їх опис

Після ретельного огляду та аналізу сучасних методів та засобів захисту було зроблено висновок, що більшість з них можна використовувати для захисту в системах обробки критичної інформації, однак досить суттєву їх кількість слід модернізувати та поєднати з іншими засобами захисту, для покращення та посилення загального рівня безпеки усієї системи та її компонентів. Таким чином ми досягли високого рівня захищеності всієї системи включаючи окремі компоненти та забезпечили безпечну та впевнену роботу з мережею.

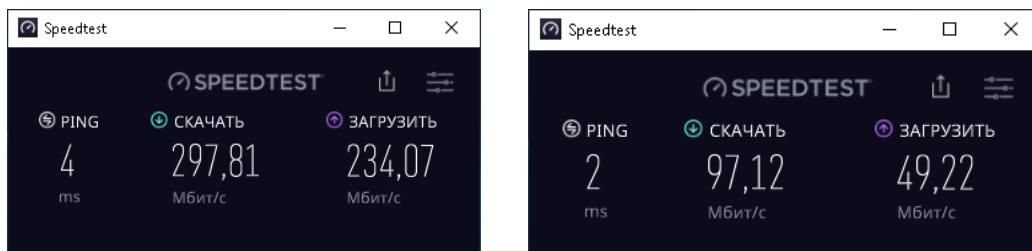


### 3.2.1 Резервування каналів зв'язку

Під час роботи з критичною інформацією необхідно своєчасно та точно її передавати або обробляти. Для цього необхідно реалізувати швидкісну та надійну передачу даних. Через це необхідно реалізовувати резервування каналів зв'язку.

Резервування каналів зв'язку полягає в використанні резервного каналу, що забезпечить зв'язок з сервером та реалізує резервне з'єднання при виведенні з ладу основного каналу передачі.

Я пропоную використовувати дротову передачу як основну та резервну передачу. Дротовий зв'язок буде реалізовано за допомогою кабелю Ethernet через фізичні властивості даного типу зв'язку.



Ethernet

Wi-fi

Рисунок 3.7 - Порівняння швидкості роботи кабелю Ethernet та Wi-fi

Перевірка швидкості зв'язку з мережею інтернет по дротовому та бездротовому каналу передачі очевидно, що бездротовий зв'язок програє дротовому, ще й досить суттєво.

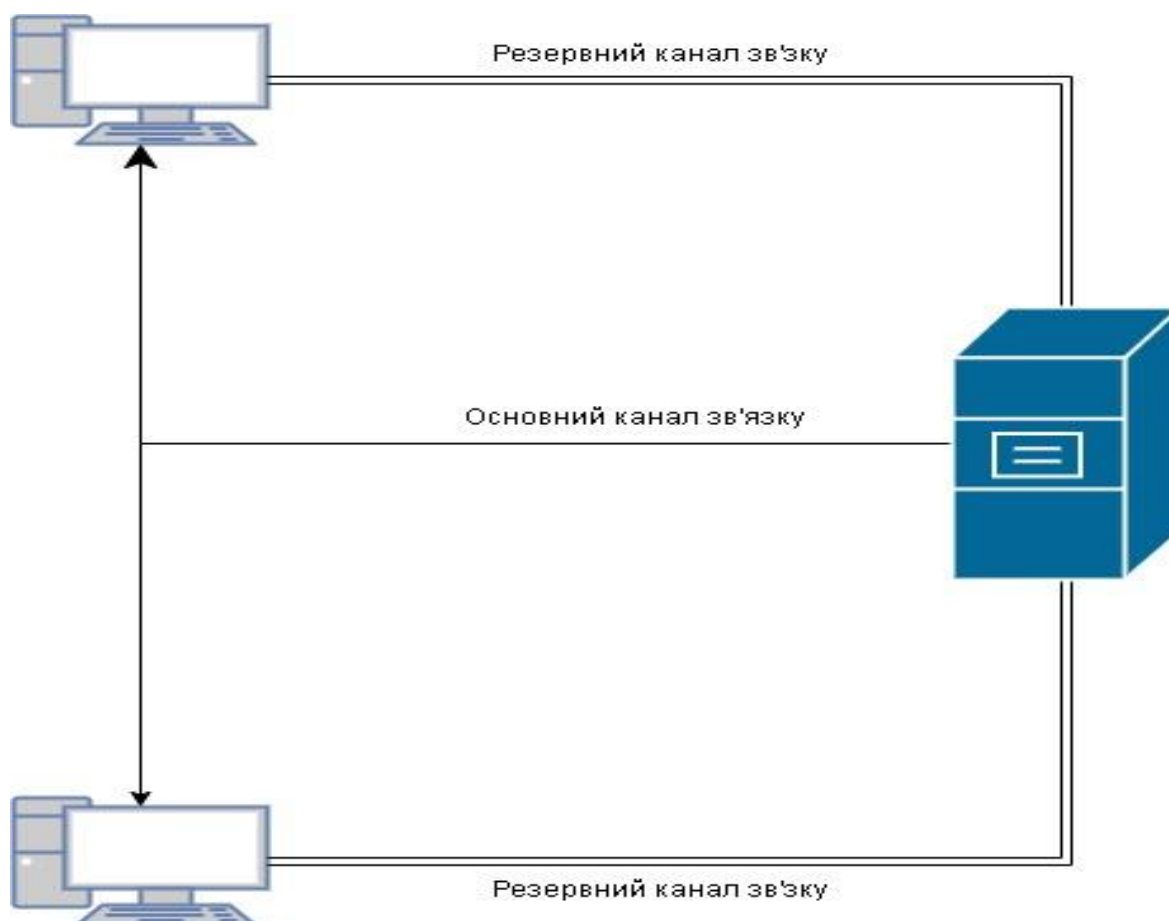


Рисунок 3.8 - Резервування каналу зв'язку

Окрім швидкості передачі інформації Wi-fi мережа має істотний недолік – радіус дії, що може досягати меж приміщення, в якому будуть працювати з критичною інформацією, а це у свою чергу може призвести до витіку критичної інформації.

При втраті зв'язку через основний канал зв'язок буде працювати використовуючи резервний канал зв'язку. Даний захист буде передавати інформацію щодо несправності основного каналу зв'язку у випадку втрати його функціональності.

### 3.2.2 Контроль трафіка

Даний захист було вирішено використовувати для тимчасових перевірок роботи співробітників та їх дій з системою, виявлення можливих спроб компрометувати чи виведення з ладу системи чи її компонентів.

Контроль трафіка буде забезпечуватися за допомогою збереження даних про історію пошуку користувачів та перелік посилань, що було їм надано для обробки. Дані будуть зберігатися для керівників, щоб було реалізовано при необхідності відслідковування дій користувачів та можливість побудови повноцінної тайм лайну їх дій при необхідності.

Дані зберігаються в базі даних на сервері та раз на годину дублюються на базу даних для тривалого зберігання, де у подальшому й відбувається їх зберігання. Тобто на сервері відбувається тимчасове зберігання даної інформації, після чого вона очищується.

Дана система може реалізовувати відключення функції контролю трафіка для забезпечення анонімності використання мережі. Таким чином буде неможливо виявити що за користувач використовував дану систему та які запити реалізовував.

### 3.2.3 Збереження даних у шифрованому виді

Було вирішено зберігати критичну інформацію та дані в шифрованому виді для захисту від копіювання жорстких дисків або бази даних. Навіть за умови реалізації контролю доступу приладів до системи існує вірогідність копіювання працівниками. Таким чином скопійована інформація не буде мати вартості й не зможе принести збитків компанії.

	sitename	score
	Фільтр	Фільтр
1	e7006c8cc9ab7110da7ee566de5d...	NULL
2	9700b93abe09b7197d29eef68823f...	NULL
3	70040961d9b5e8e7787de0da0307...	NULL

e7006c8cc9ab7110da7ee566de5d56d2d926c6b1c0fe352728c78693048094365c7804b53f594bd34461b24a5425dd5951ef2b60e088ae2af8b6f0546ce351b0d178d7e9b36474edd6ca0241368064c9cee1524be34cf27a65e9024e53b98a3fdf87781977f28b556b56da85bdeee1663fb76702a6a7814bfe026876534d79d3

Рисунок 3.9 - Приклад зберігання інформації в базі даних

Збереження даних відбувається за допомогою бази даних. Дані у базі зберігаються в шифрованому виді. Користувачі під час роботи можуть зберігати всі необхідні дані для подальшого використання локально в базі даних та отримати дані в будь – який момент часу.

### 3.2.4 Захищений інтерфейс для користування мережею

Судь даного захисту полягає у використанні такого інтерфейсу користувача, що зробить неможливим загрозу системі обробки критичної інформації через дії користувача та помилкові відвідування потенційно небезпечних ресурсів.

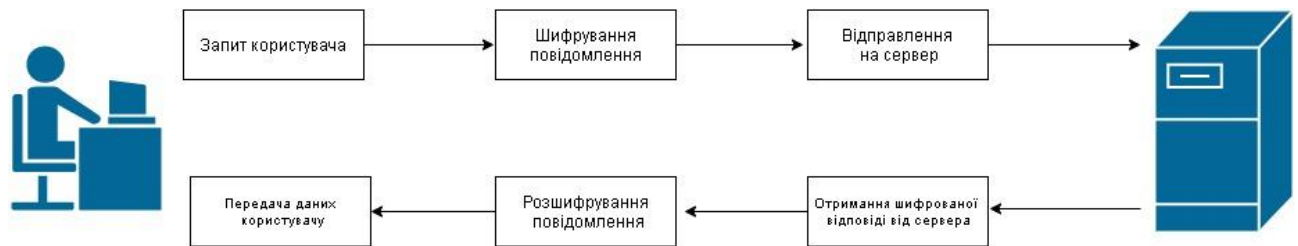


Рисунок 3.10 - Схема роботи інтерфейсу

Фаєрвол та більшість систем безпеки не можуть забезпечити захист проти загроз направлених на неуважність людей та незнання правил безпеки на підприємстві, тому використання звичайних браузерів може стати загрозою для корпорації. Через цю причину було прийняте рішення використовувати даний засіб. Після отримання наприклад сторінки браузера відбувається повна фільтрація даних від непотрібних даних, щоб залишилася лише важлива інформація: текст, зображення тощо. Таким чином можливо реалізувати пошук в мережі інтернет без ризику втрати секретної інформації через перехід по небезпечному посиланню чи отриманні зловмисного коду чи скрипту.

Сам підхід та ідея дозволяє робити не лише інтерфейси для користування мережею та передачі даних а й для систем безпеки як корпорацій так і приватного використання, наприклад, пункт охорони в приватному маєтку.

### 3.2.5 Впровадження гібридного шифрування

Гібридна криптосистема - використовує переваги симетричної і асиметричної криптографії. Симетричний ключ використовується для

шифрування даних, а асиметричний - для шифрування самого симетричного ключа.

Дана гібридна система працює наступним чином:

- для симетричного алгоритму генерується випадковий сеансовий ключ.
- використовується симетричний алгоритм для шифрування повідомлення.
- відправка повідомлення, зашифроване симетричним алгоритмом,
- відправка ключа зашифрованого асиметричним алгоритмом.
- одержувач спочатку розшифровує ключ за допомогою свого секретного ключа, а потім отримує і все повідомлення.

### 3.2.5.1 Криптосистема Рабіна

Основні причини вибору даної криптосистеми:

- Простота реалізації
- Безпека
- Контроль цілісності

Простота реалізації: однією головних причин використання саме цієї криптосистеми являється простота її реалізації.

Безпека: перевага криптосистеми Рабіна полягає в тому, що випадковий текст може бути відновлений повністю від зашифрованого тексту лише за умови, що дешифрувальник здатний до ефективної факторизації відкритого ключа  $n$ .

Контроль цілісності: буде реалізовуватися за допомогою цифрового підпису, який нам дозволяє використовувати асиметрична криптографія.

Необхідні умови для надійної роботи даного шифрування: генерування великих простих чисел  $p$ ,  $q$ , кожне виду  $4k + 3$ , та форматування вхідних повідомлень.

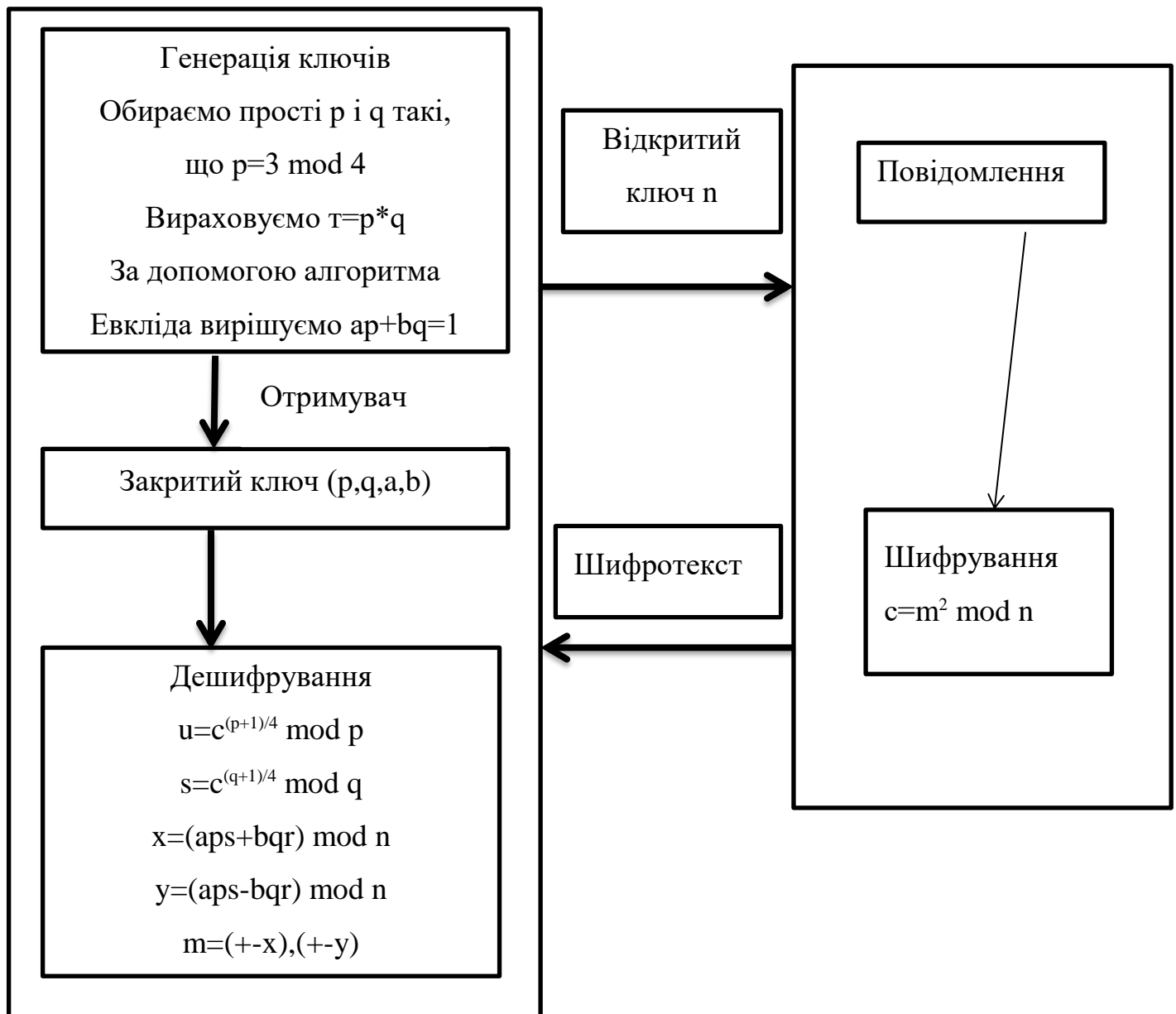


Рисунок 3.11 - Схема шифрування Рабина

Генерування двох великих простих чисел  $p$ ,  $q$ , кожне виду  $4k + 3$ , та обчислювання  $n = pq$ .

Отримуємо:  $p$ ,  $q$  є секретним ключем, а число  $n$  – відкритим ключем.

### 3.2.5.2 Система RSA

Система RSA в створеній моделі використовується для реалізації шифрування асиметричного та симетричного ключа при їх передачі.

Вибір даної криптосистеми обумовлено її надійністю, поширенням та простотою реалізації. Дана система перевірена роками використання та використовується й на сьогоднішній день, що свідчить про її надійність та стійкість.

Для початку необхідно згенерувати відкритий і секретні ключі:

- Візьмемо два великих простих числа  $p$  and  $q$ .
- Визначимо  $n$ , як результат множення  $p$  on  $q$  ( $n = p * q$ ).
- Виберемо випадкове число, яке назвемо  $d$ .
- Це число повинне бути взаємно простим з результатом множення  $(p-1) * (q-1)$ .
- Визначимо таке число  $e$ , для якого є істинним наступне співвідношення  $(e * d) \bmod ((p-1) * (q-1)) = 1$ .
- Назвемо відкритим ключем числа  $e$  і  $n$ , а секретним -  $d$  і  $n$ .

Для того, щоб зашифрувати дані з відкритого ключу  $\{e, n\}$ , необхідно наступне:

- розбити шифруємий текст на блоки, у вигляді числа  $M(i) = 0, 1, 2, \dots, n-1$ .
- зашифрувати текст, що розглядається як послідовність чисел  $M(i)$  за формулою  $C(i) = (M(i) ^ e) \bmod n$ .

Щоб розшифрувати ці дані, використовуючи секретний ключ  $\{d, n\}$ , необхідно виконати наступні обчислення:  $M(i) = (C(i) ^ d) \bmod n$ . В результаті буде отримано безліч чисел  $M(i)$ , які представляють собою вихідний текст.

### 3.2.6 Сервер для з'єднання клієнта та мережі інтернет

Одна з найважливіших функцій серверної частини даної моделі – реалізація з'єднання клієнта з мережею інтернет. Даний захист реалізується шляхом передачі запиту з клієнта на сервер, а вже сервер буде від свого імені реалізовувати пошук та роботу в мережі.

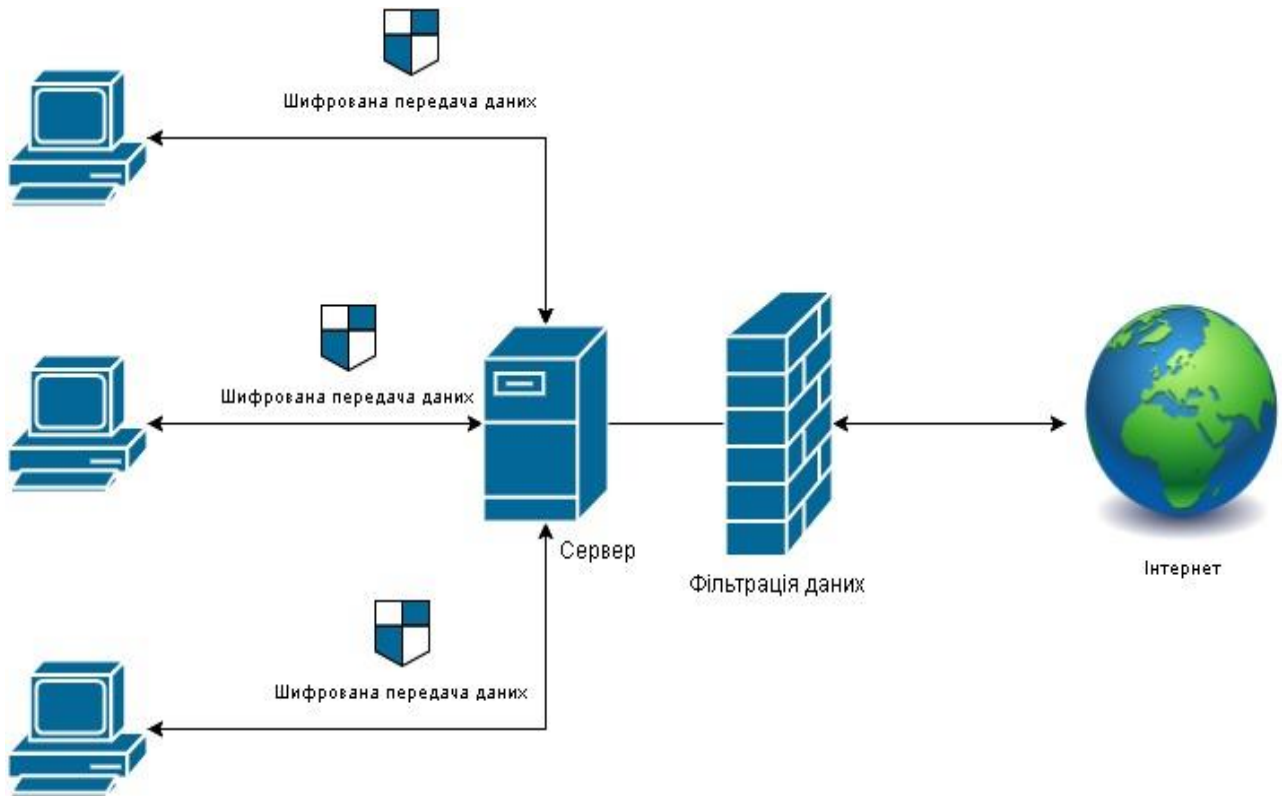


Рисунок 3.12 - Схема з'єднання клієнтів з мережею інтернет

Даний засіб захисту відміно реалізує захист систем обробки критичної інформації від сканування внутрішньої будови мережі. Необхідність у даному засобі захисту полягає в ризиках, що пов'язані з можливістю побудови зломисником внутрішньої моделі системи та реалізації загроз шляхом виявлення та використання вразливостей системи.

### 3.2.7 Контроль за діями користувачів

Для забезпечення контролю за діями користувача можливо використовувати як готове рішення представлені на ринку, так й додаткову функцію в інтерфейсу користувачів, що буде дублювати запити на сервер і отримані відповіді та записувати їх у базу даних в хронологічній послідовності для можливості побудови тайм лайну при виникненні якихось проблем чи помилок.



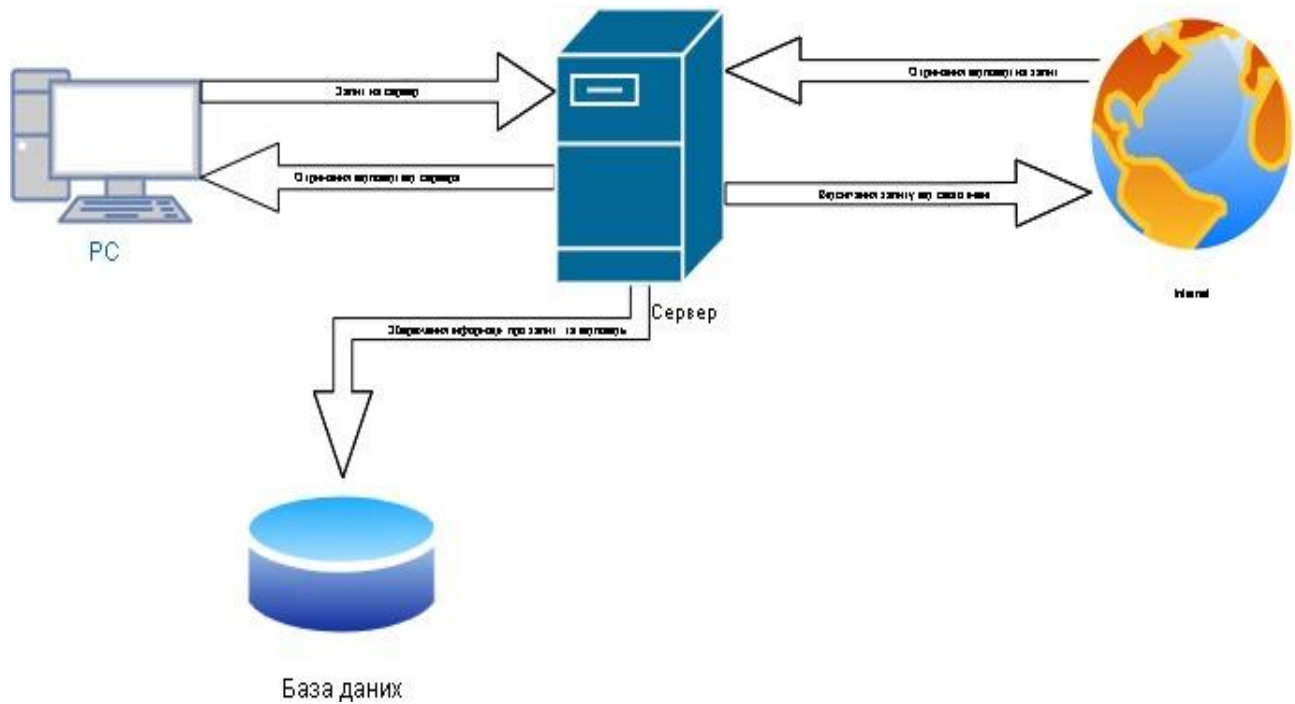


Рисунок 3.13 - Схема дублювання даних про дії користувача

Даний захист встановлено на сервері системи та клієнті, таке рішення обумовлено тим, щоб не навантажувати систему додатково на постійні запити з даними про дії користувачів. Таким чином основні дані про пошук та роботу в мережі інтернет будуть знаходитися в безпеці та цілодобовому доступі, а вже історія дій користувачів на конкретній машині буде на ній же й зберігатися. Для посилення даного засобу захисту можливо налаштувати за необхідністю копіювання даних, про дії користувачів н віддалені сервери, бази даних чи сервіси для зберігання даних у хмарі.

### 3.2.8 Фільтр даних, які будуть циркулювати в системі під час роботи користувачів

При використанні систем обробки критичної інформації в роботі користувачів ключовим ризиком є можливі дії користувачів, тип паче з наявністю доступу до інтернету.

Для коректної роботи варто використовувати два фільтри: для встановлення на машину користувачів та серверну частину. Дані фільтри

створено для перевірки всіх даних, що будуть циркулювати системою та блокуванні при виявленні потенційних загроз.

На клієнті фільтр буде виконувати перевірку, перед відправленням запиту на сервер, на наявність забороненої інформації у запиті та потенційні загрози в потоці даних. На сервері фільтрація даних розрахована на перевірку безпечності отриманої інформації або про наявність додаткового коду в даних. Суть даного засобу захисту полягає в тому, що він забезпечує безпеку пошуку інформації в мережі інтернет та нівелює фактор соціальної інженерії.

Даний засіб фільтрує отриманий потік даних та передає користувачеві лише ті дані, що він шукав, відсіюючи все інше. Таким чином можливо реалізувати безпечний для фірми та співробітника пошук в інтернеті, не переживаючи за можливість вторгнення у систему зловмисного програмного забезпечення шляхом дій користувача у мережі інтернет.

### **3.2.9 Додаткові методи захисту**

В залежності від зовнішніх та внутрішніх факторів у місця впровадження даної системи може знадобитися встановлення додаткових засобів захисту. Для поліпшення роботи системи та забезпечення підвищеної надійності рекомендовано використовувати:

- Контроль доступу до робочих станцій за допомогою облікового запису
- Перевірка на вході на наявність зовнішніх носіїв
- Заклейка камер відеоспостереження на час знаходження на території компанії.
- Перевірка співробітників на детекторі брехні

Наведений перелік при необхідності значно посилить та покращить захист кожного компоненту системи.

### 3.3 Характеристика приміщення

Для забезпечення повноцінного захисту системи обробки критичної інформації варто реалізувати й безпеку приміщення, де буде знаходитися дана система. При використанні подібних систем варто проаналізувати слабкі та сильні сторони приміщення, в якому вони будуть розташовуватися й реалізувати специфікацію приміщення під систему якщо це не було зроблено раніше. Для реалізації даного задуму варто використовувати систему сигналізації та фізичні властивості приміщення, в якому буде розташована система обробки критичної інформації. Таким чином можливо реалізувати захист не лише на програмному рівні від внутрішніх та зовнішніх атак але й від вторгнень на територію й спроби викрадення критичної інформації або й всієї системи.

#### 3.3.1 Використання сигналізації

Для забезпечення захисту приміщення я вирішив використовувати сигналізацію, спроектовану в дипломній роботі бакалавра, що була розроблена на четвертому курсі.

При розробці даної моделі використано наступні методи захисту:

- Датчики зв'язуються з клавіатурою кожну хвилину.
- Захист від глушіння.
- Шифрування при передачі даних.
- Застосування при передачі даних резервних каналів зв'язку.
- Акумулятори, що забезпечать роботу системи за відсутності електроживлення.
- Захист від руйнування або виведення з ладу

Було вирішено посилити засоби захисту сигналізації та реалізувати додаткове шифрування ключа, що буде передаватися при обміні даними

сигналізації та пульту керування. Таким чином буде реалізовано додатковий захист проти перехвату даних та можливості скомпрометувати систему.

Сигналізація складається з наступних приладів, що мають задані технічні характеристики:

- Базовий блок: забезпечує роботу всієї системи та містить GSM модуль для бездротового зв'язку з пультом охорони чи номером власника об'єкту. Для зв'язку використовується кабель Ethernet в якості основного каналу передачі. Канал GSM буде використовуватися в якості запасного зв'язку, за допомогою мобільного інтернету / СМС сповіщення або голосового набору записаного заздалегідь повідомлення.
- Датчики: магнітодатчик, датчик пожежі, датчик руху, сирена, вібраційний датчик, ІК-бар'єр. Дані датчики в забезпечать надійну охорону об'єкту. Датчики працюють по захищеному протоколу та автентифікуються на базовому блоці, щоб не було можливості підміни датчиків.
- Основна настройка приладів відбувається за наступними характеристиками: час перевірки датчиків та клавіатури з базовим блоком кожну 1 хвилина. час перевірки справності всієї апаратури 1 хвилина, під час даної перевірки відправляється інформація стосовно справності системи.
- Основним каналом передачі являється Ethernet, додатковий канал передачі GSM(СМС повідомлення або автодозвон).

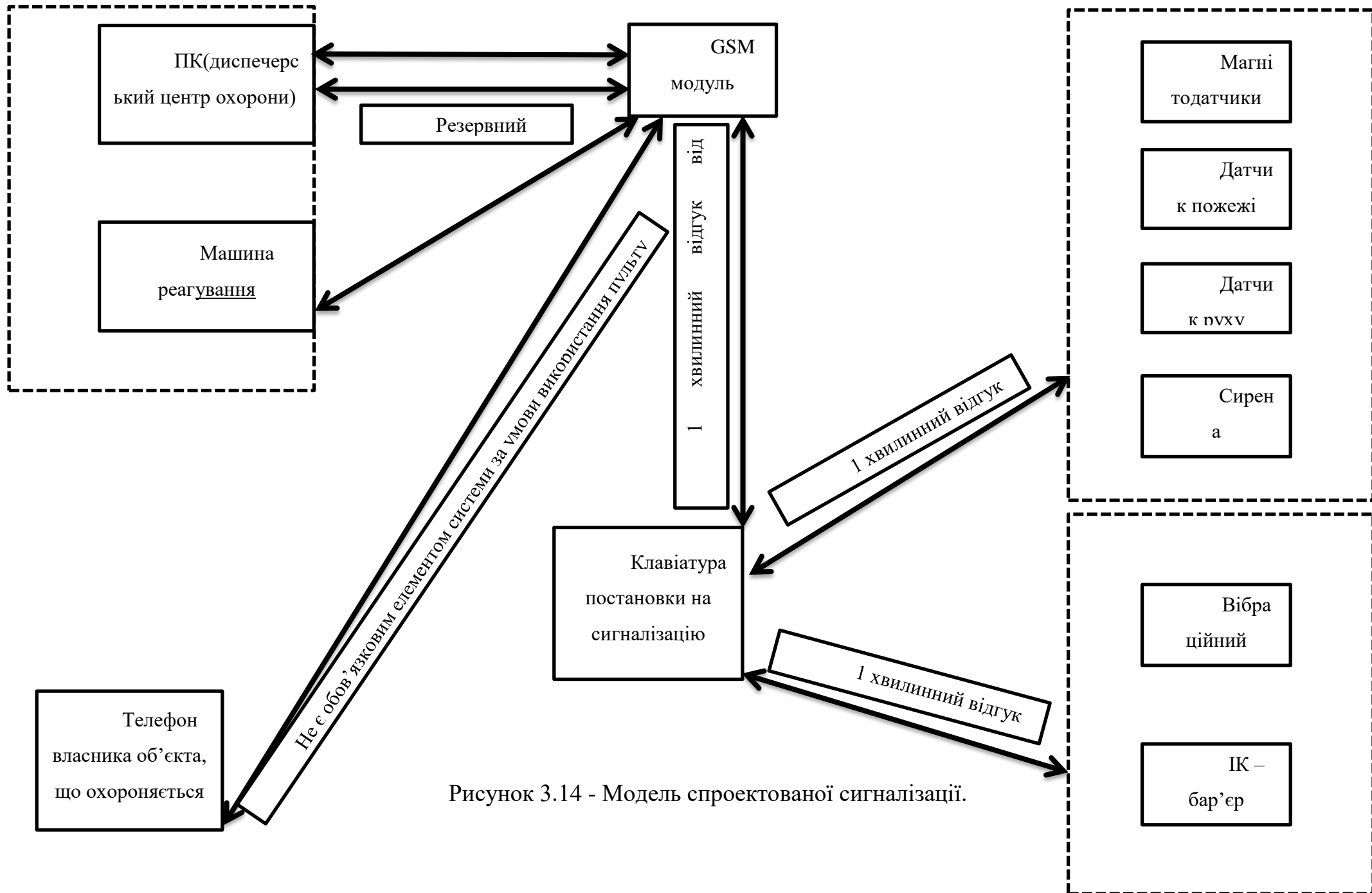


Рисунок 3.14 - Модель спроектованої сигналізації.

Необхідно використовувати в базовій комплектації наступну додаткову апаратуру, що забезпечить більш широкий спектр захисту об'єкту:

- Звукова сирена
- Вібраційний датчик
- Датчик пожежі
- ІК – бар'єр

Додаткова апаратура, яку можна використовувати в залежності від об'єкту:

- Датчик шуму
- Датчик освітленості

При встановленні датчиків варто дотримуватися певних правил, наприклад:

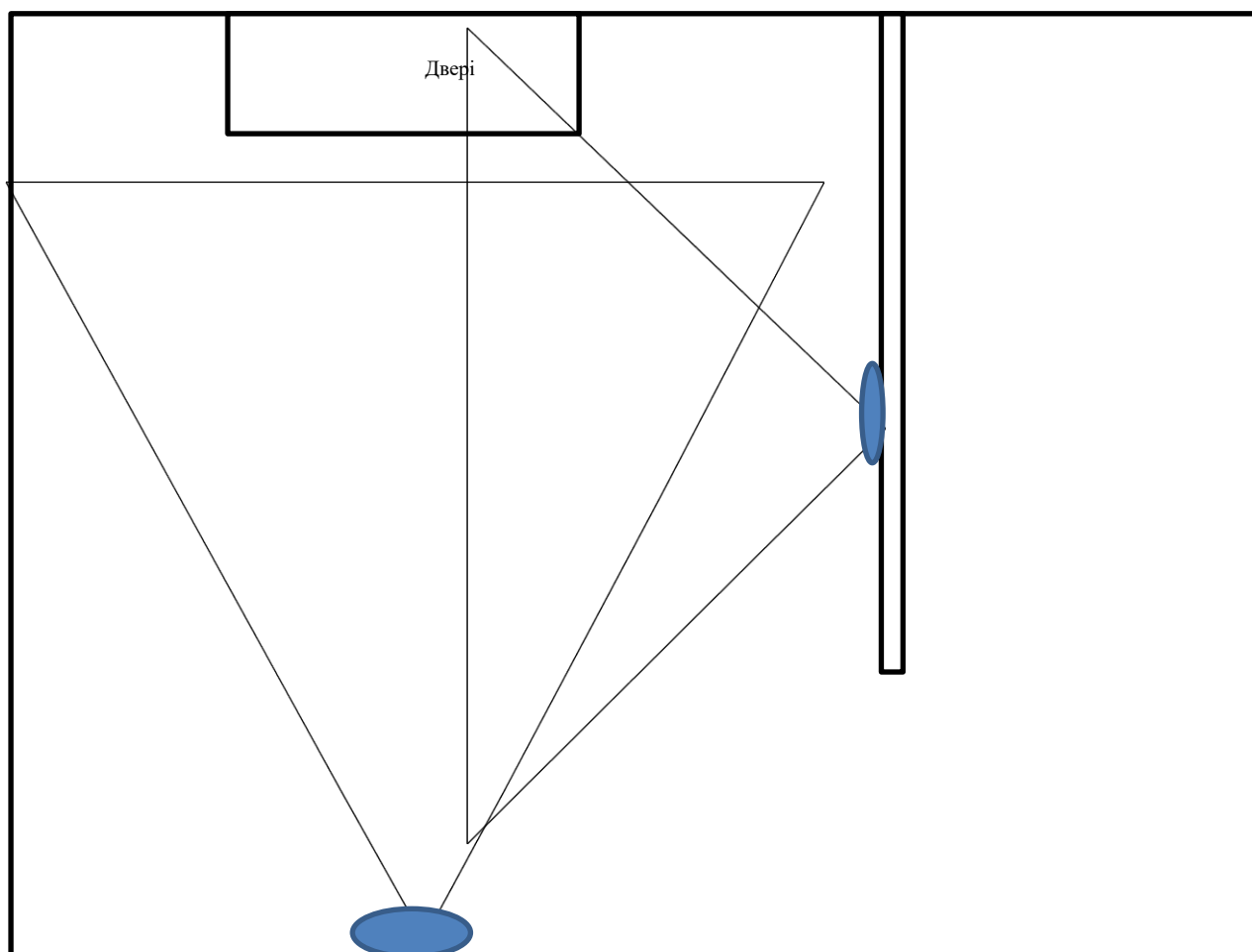


Рисунок 3.15 - Схема встановлення датчиків руху.

### Датчик розбиття скла

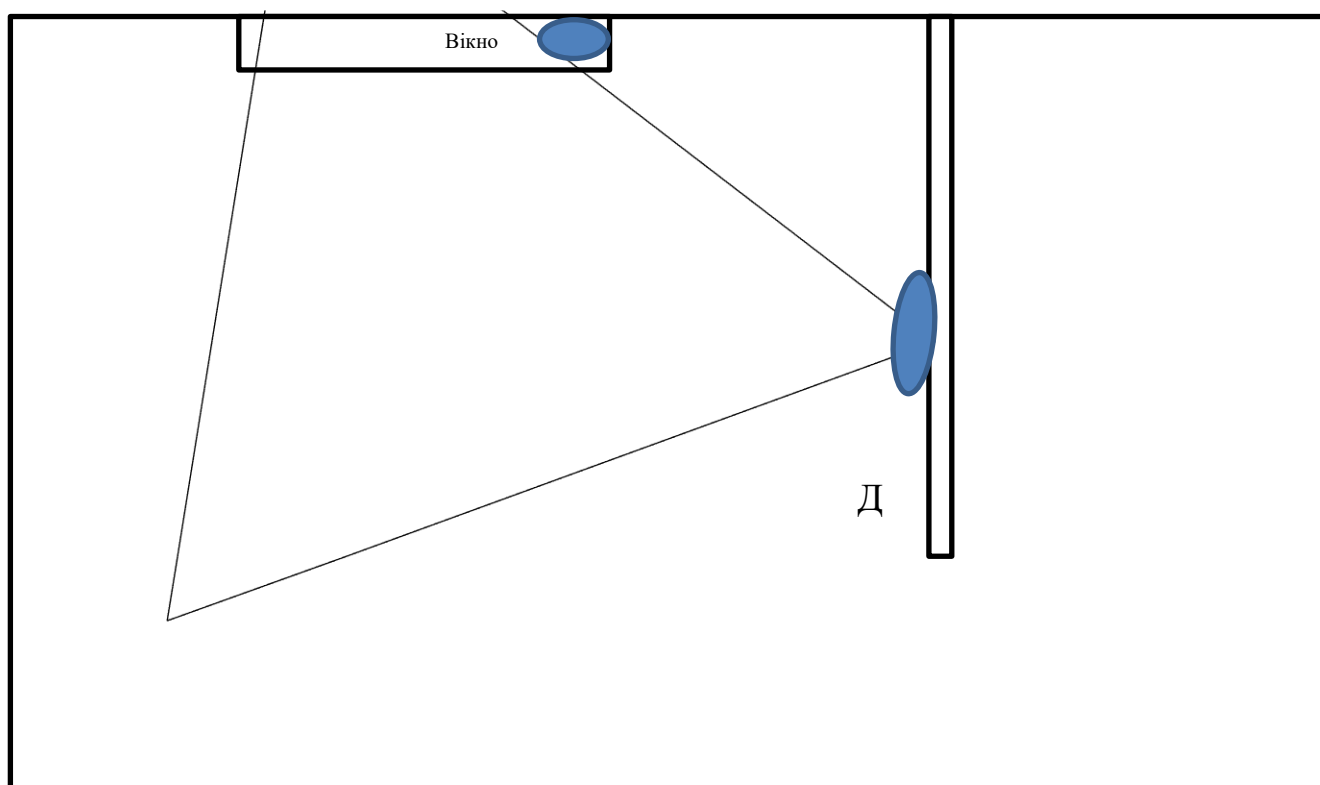


Рисунок 3.16 - Схема встановлення датчиків на вікна

Використовуючи дану сигналізацію можна досягти високого рівня захищеності системи та забезпечити захист системи обробки критичної інформації та її даних від спроб вторгнень в приміщення та реалізації фізичного знищення чи викрадення критичної інформації.

### 3.3.2 Фізичні властивості приміщення

Наша система буде реалізовувати захист системи обробки критичної інформації, тому слід розглянути всі можливі засоби витоку інформації та обрати оптимальне вирішення проблеми можливих каналів витку.

Можливі канали витоку:

- За рахунок вібрацій стін

- По системам вентиляцій
- По опалювальним чи пожежним трубах
- По дротах електромережі
- За допомогою радіозакладок
- Лазерний з'їм акустичної інформації з вікон
- дистанційний з'їм відео інформації
- Побічні електромагнітні випромінювання радіоелектронної техніки

Для реалізації заходів безпеки системи обробки критичної інформації необхідно використовувати наступний захист проти каналів витоку: через вентиляцію, за допомогою дротів електромережі, радіозакладок, дистанційного зйому відеоінформації, побічні електромагнітні випромінювання.

Вартість даних засобів захисту може бути досить високою враховуючи специфічність їх використання, у той же час деякі з них досить доступні для широкого кола використання.

Таблиця 3.1 - Вартість засобів захисту для технічного приміщення.

Назва	Тип захисту	Кількість	Вартість (грн)
Генератор шума DNG-2300	Проти витоку через вентиляцію	1	20 000
М-17	Проти витоку через мережу	1	6 500
СОНАТА-РЗ	Побічні електромагнітні випромінювання	1	27 000
Камери відеоспостереження	Захист проти копіювання даних, порушення кордонів об'єкту, що охороняється	3	$500 \cdot 3 = 1\,500$
Загальна вартість:			55 000 грн



Пошук жучків та радіозакладок краще реалізовувати через фірми, що чим займаються. Вони забезпечують підтримку протягом року та за необхідністю можуть реалізувати навчання співробітників чи їх перевірку.

Дана сума реалізує захист проти витоку інформації, однак варто додати до вартості комплексу захисту ще вартість сигналізації, що розглядалася раніше. На сьогоднішній день вона обійдеться в 13 000 грн.

Тому загальна вартість обладнання приміщення буде приблизно:

Вартість сигналізації + вартість засобів захисту для технічного приміщення =  
 $13\,000 \text{ грн} + 55\,000 \text{ грн} = 68\,000 \text{ грн}$

Загальна вартість на реалізацію заходів захисту приміщення буде складати 68 000 грн.

### **3.4 Захищеність системи від атак**

Створена мною система забезпечує надійний захист проти різноманітного роду атак, оскільки під час її створення було враховано переваги та недоліки сучасних систем та можливі варіанти проникнення у систему та крадіжки інформації. Спроектowana система забезпечить надійну безпеку під час роботи в мережі інтернет та збереження конфіденційних даних.

#### **3.4.1 Атаки соціальної інженерії через мережу**

Суть захисту: спроектована система повністю нівелює вірогідність атак виду соціальної інженерії. Це обумовлено в першу чергу тим, що користувач матиме ряд певних обмежень.

По – перше, під час пошуку інформації користувач не буде взаємодіяти напряму з ресурсом, уся робота буде відбуватися через посередника – програму встановлену на сервері, на клієнті буде лише передаватися запит та отримуватися

відповідь від сервера. Тобто користувач буде отримувати вже сам результат пошуку без необхідності відвідувати величезну кількість сайтів та ризикувати.

Почтові розсилки що можуть містити небезпечну програму чи заражені файли не будуть ні скачуватися ні проглядатися. Нові листи будуть фільтруватися від спаму, а ресурси що міститимуться у базі даних як небезпечні не будуть відвідуватися.

Таким чином загрозу соціальної інженерії в мережі закрито та забезпечено повний захист від можливих дій користувачів по різноманітним причинам.

### **3.4.2 Потенційно небажані програми**

Суть захисту: неможливість встановлювати та скачувати потенційно небажані програми користувачами. Захист проти скачування небажаного програмного забезпечення буде реалізовуватися засобами захисту на сервері, а захист проти інсталяції та переносу на машину користувача шляхом заборони використання зовнішніх носіїв, не зареєстрованих у системі.

Це обумовлено принципом обмеження дій користувача в програмному застосунку. Дана система повністю забезпечує безпеку проти скачування та виконання файлів із зовнішнього невідомого джерела.

### **3.4.3 Захист проти прослуховування трафіку**

Суть захисту: захист забезпечується шляхом шифрування усіх даних, що зберігаються на сервері та повною очисткою інформації про дії користувачів після їх роботи. Дані зберігаються лише в шифрованому вигляді та на сервері.

Інформація, що буде зберігатися під час роботи знаходиться в базі даних локально у шифрованому вигляді та буде розшифровуватися під час роботи для читання та модифікацій.

Варіанти перехоплення даних, що передаються в системі обробки критичної інформації:

- Перехоплення даних всередині компанії
- Перехоплення даних віддаленого клієнта
- Перехоплення даних, що надсилаються в мережу інтернет

Жодне з перерахованих варіантів перехоплення даних не буде нести шкоди ні підприємству ні системі обробки інформації. Наприклад при перехопленні даних всередині корпорації чи при роботі віддаленого клієнта з сервером їх вартість буде дорівнювати нулю, оскільки вони будуть повністю зашифрованными гібридною системою шифрування. А при перехопленні даних при роботі сервера з мережею інтернет дані будуть або безкорисними або також в зашифрованому виді, наприклад при роботі з поштовим сервером.

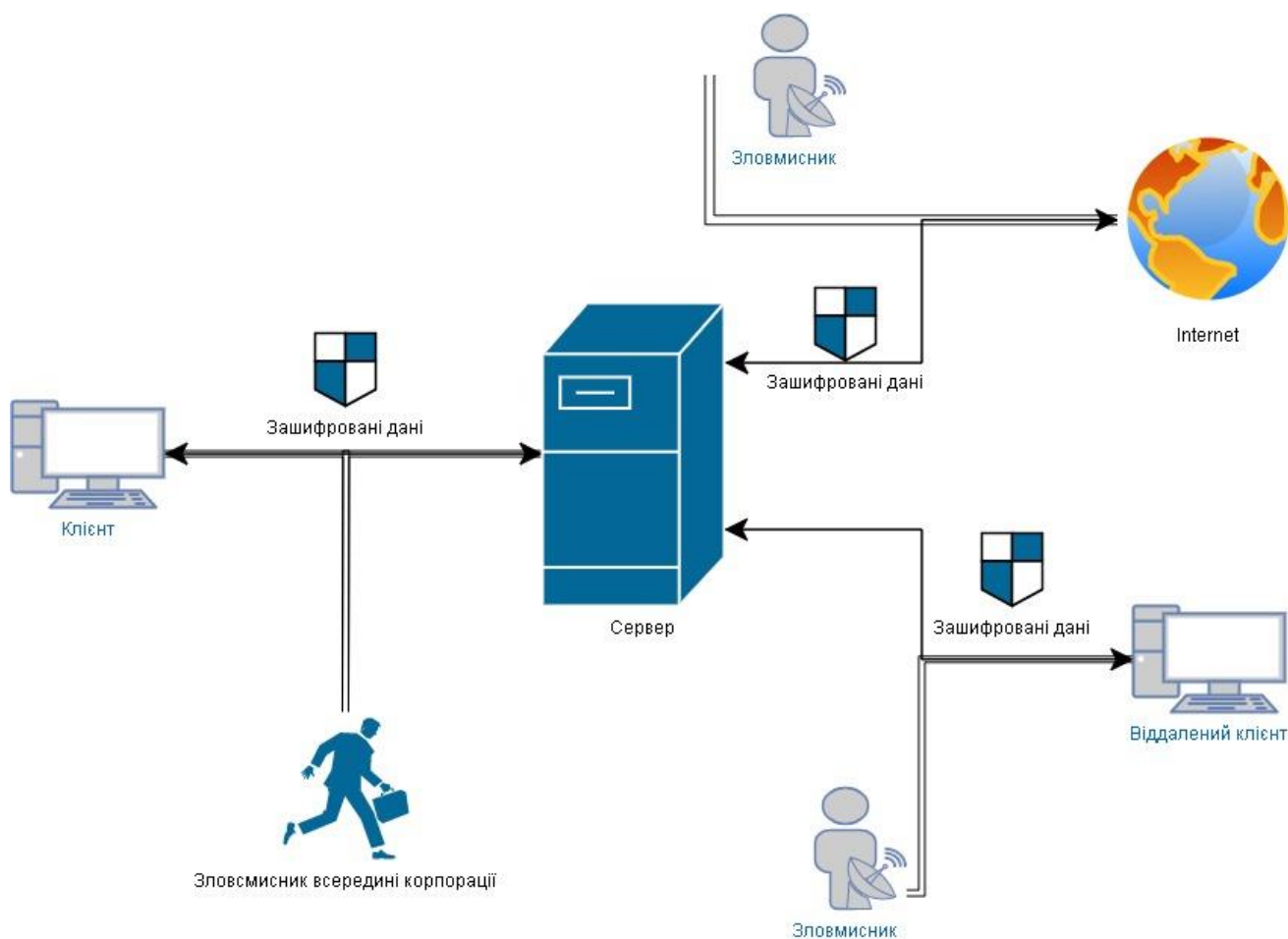


Рисунок 3.17 - Схема прослуховування трафіка

Таким чином процес прослуховування трафіку не буде причиняти шкоди компанії, адже інформація що зможе потрапити до зломисників буде зашифрована й не зможе стати їм у пригоді.

### **3.4.4 Захист проти внутрішніх атак**

Дана система забезпечує захист від внутрішніх атак за допомогою встановлення камер відеоспостереження, шифрування при передачі даних. Шифрування інформації, що зберігається в базі даних не дасть можливості зломиснику скопіювати інформацію, адже для її використання необхідно буде її розшифрувати.

Можливі внутрішні атаки: копіювання даних персоналом, фізичне проникнення на об'єкт тощо.

Захист приміщення від різноманітних можливих витоків інформації таких як: електромагнітне випромінювання, вентиляція, мережеві кабелі тощо, повністю унеможлиблює можливості витоку критичної інформації.

Слід додержуватися даних правил та рекомендацій стосовно реалізації захисту системи обробки критичної інформації, адже лише при використанні даних рекомендацій та критеріїв підбору апаратури можлива реалізації повноцінного захисту системи.

### **3.4.5 Захист проти зовнішніх атак**

Система повністю захищена від зовнішніх атак за допомогою використання фаєрвола, фільтра даних, підключення приладів до системи лише через ідентифікатори, зберігання, та передача даних в шифрованому виді.

З технічних заходів щодо забезпечення захисту проти зовнішніх атак: використання жалюзів на вікнах, впровадження захисту проти виток інформації через вентиляцію, мережу електроживлення, електромагнітне випромінювання.

### 3.4.6 Захист проти фізичного проникнення

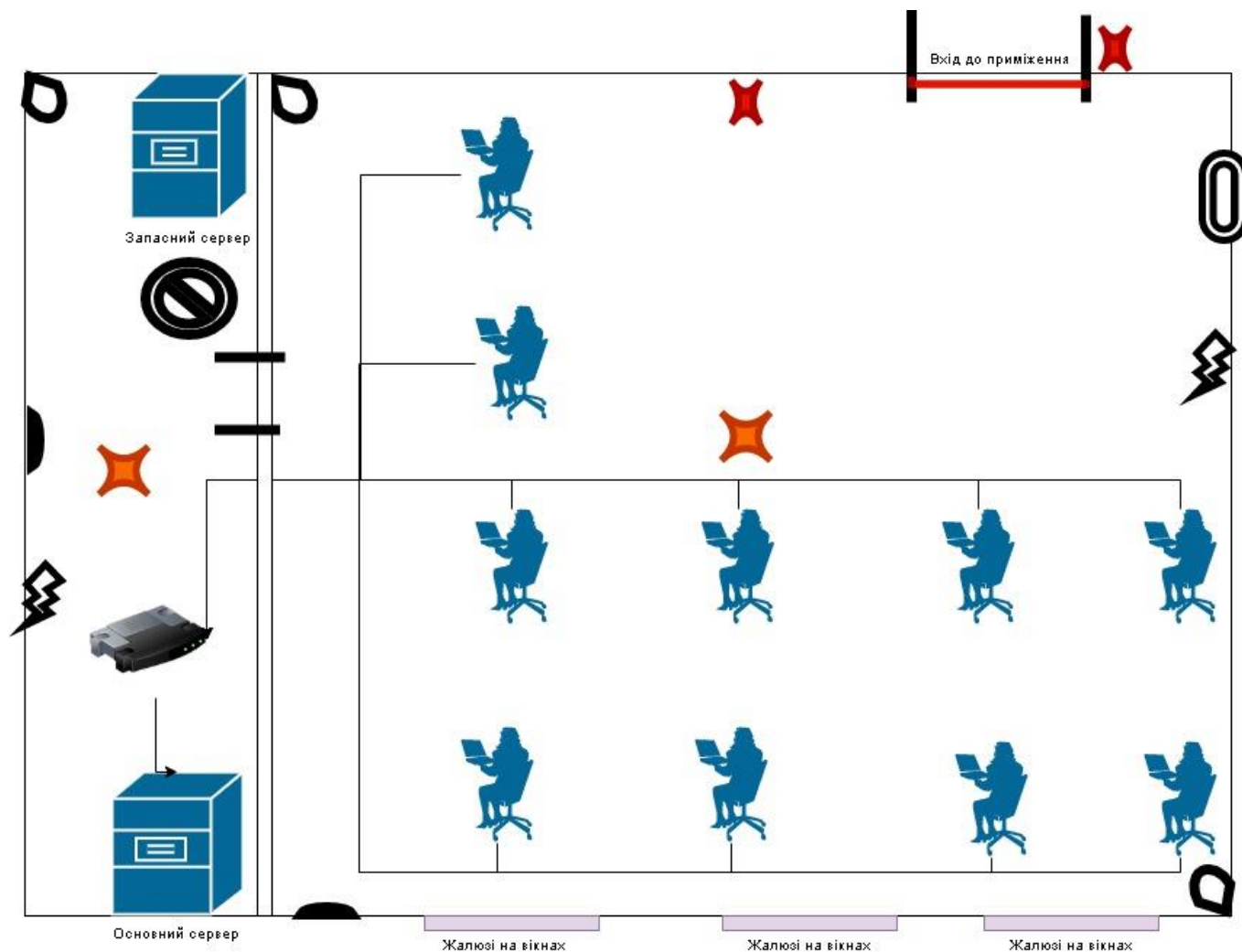


Рисунок 3.18 - Приклад схеми приміщення



Рисунок 3.19 - Умовні позначки до схеми 3.18

Захист проти фізичного проникнення буде забезпечуватися за допомогою камер відеоспостереження, датчиків руху, вібраційних датчиків, ік-бар'єру, захисту проти витоку електромагнітного випромінення, вентиляцію мережу та сигналізації, що буде реалізовувати моніторинг приміщення, та до якої будуть підключені наступні датчики: руху, вібраційний датчик, ік бар'єр, датчик пожежі, звукова сирена, що сповіщатиме про вторгнення. . Дані засоби захисту спроможні забезпечити як захист від вторгнення так і виявлення проникнення.

Враховуючи специфікації приміщення та сигналізації можна зробити висновок, що система обробки критичної інформації буде в повній безпеці.

### **3.5 Аналіз результатів дослідження**

Аналізуючи результати дослідження можна прийти висновків, що було створено захищену модель системи обробки критичної інформації та комплекс необхідних засобів для реалізації повноцінного захисту від різноманітних типів та видів атак.

#### **3.5.1 Засоби захисту, що використовуються для роботи з системою.**

При побудові системи враховано недоліки та слабкі сторони існуючих методів та засобів по забезпеченню безпечної роботи в мережі, що забезпечать надійність та стійкість протидії різноманітним видам атак та загроз як зовнішнього так і внутрішнього характеру.

В даній системі впровадженні та реалізовані покращення, що забезпечать більшу надійність та стійкість спробам саботажу системи.

Для роботи з системою можливо використовувати будь – які засоби захисту, адже інтерфейс користувача підтримує кроссплатформеність та зможе інсталюватися на будь – яку платформу в залежності від вимог корпорації.

Таким чином можна використовувати як ноутбук так і портативний комп'ютер. Дана властивість не буде впливати на безпеку системи та окремих її компонентів, адже для кожного подібного приладу буде реалізовуватися персональний підхід для повноцінного та правильного налаштування системи підключення.

Для даної системи рекомендовано використовувати наступні засоби захисту представлені на ринку:

Таблиця 3.2 - Рекомендовані засоби захисту

Захист	Прилад	Кількість	Ціні за одиницю	Ціна грн/за рік
Антивірус	Avast Internet Security 2019	1	600	600
Файрвол	Cisco RV325-K9-G5	1	10 000	10 000
Захист від ддос атак	Послуги компанії	1	5 000 (за місяць)	60 000
Програма для контролю за користувачами	<u>LanAgent</u>	10	500	5 000
Загальна сума:				75 600 грн

В створеній системі не буде використовуватися значна циркуляція трафіку тому для захисту від ддос атак достатнім буде обирання найдешевшого пакету послуг компанії, по захисту від ддос атак. Таким чином можливо значно зекономити кошти та реалізувати достойний захист систему. У зв'язку з використанням шифрування даних при збереженні та передачі відсутня необхідність закупати для персоналу захищені флешки.

### 3.5.2 Вартість системи

Для підрахунку вартості системи було запропоновано порівняльний аналіз вартості необхідних засобів захисту для системи спроектованої у другому розділі та створеній захищеній системі з використанням удосконалених засобів захисту.

При підрахунку вартості комплектуючих створеної системи було отримано наступні результати: 55 000 грн для реалізації захисту в приміщенні де буде розміщатися система обробки критичної інформації та 75 600 грн вартість засобів захисту безпосередньо для впровадження в систему обробки критичної інформації.

Таким чином враховуючи вищезазначене то можна значно зекономити грошові кошти та реалізувати впровадження комплексу технічного захисту в приміщенні, де буде знаходитися система. Економія склала:

$$155\,600 - 75\,600 = 80\,000 \text{ грн}$$

При впровадженні заходів захисту приміщення та засобів захисту можливих каналів витоків інформації було підраховано суму: 55 000 грн.

Якщо відняти дану суму зі зекономлених раніше коштів отримаємо:

$80\,000 - 55\,000 = 25\,000$  грн. економії при впровадженні не лише захисту системи обробки критичної інформації а й при впровадженні обладнання для захисту приміщення.

### 3.5.3 Нововведення та покращення захищеності системи обробки критичної інформації

Для проектування даної системи було створено фільтр, що значно покращив безпеку під час роботи в мережі, у той же час не сповільнивши, як для користування машиною, швидкості роботи.

Було реалізовано дві системи шифрування: гібридне шифрування, для передачі та зберігання великих даних, та подвійне асиметричне, для підвищення безпеки системи при збереженні паролів, та передачі даних на відстані.



Було створено інтерфейс користувача для отримання даних з мережі інтернет без ризику для компанію та користувачів. Таким чином було майже нівельовано ризик соціальної інженерії.

Було впроваджено можливість віддаленої роботи при необхідності із системою без ризиків для останньої.

Реалізовано підбір та побудова комплексу технічних засобів захисту для впровадження у приміщення, де буде знаходитися система обробки критичної інформації.

### **3.5.4 Перспективи розвитку даного проекту**

Дана робота має досить великі перспективи розвитку, через велику варіацію використання. При подальшому дослідженні можливо впроваджувати подібні системи, тобто її спрощені варіанти, для різноманітних завдань та сфер життя.

Наприклад дану систему, а точніше її частину можливо використовувати для обладнання маєтку з використання засобів захисту території. Простота системи та в налаштуванні розширює можливості використання системи на сучасному ринку, адже гнучкість завжди була у тренді та мала високий попит та відповідно дохід.

Дану систему можливо інтегрувати для наступного використання:

- обслуговування маєтку
- обслуговування корпорацій
- для державного призначення
- для налагодження секретного чату або зв'язку на відстані

Дана система може стати в майбутньому, при продовженні досліджень, досить суттєвим конкурентом на ринку не лише для корпорацій та спеціалізованих установ ай для звичайного користувача, для користування у повсякденному житті.

### **Висновки до розділу 3**

Було створено модель захищеної системи обробки критичної інформації для забезпечення конфіденційності даних і безпечної роботи у мережі незалежно від дій користувача. Під час проектування та створення системи було використано наступні методи захисту: шифрування при передачі та зберіганні інформації, фільтр для аналізу та фільтрації отриманих даних, захищений інтерфейс для користування мережею, сервер для з'єднання клієнта та мережі інтернет, збереження даних у шифрованому виді, контроль за діями користувачів, можливість роботи через бездротовий зв'язок, фільтр даних, які будуть циркулювати в системі під час роботи користувачів, дублювання критичних компонентів системи, підключення приладів по ідентифікаторах, використання маршрутизаторів для з'єднання машин користувачів із сервером, спеціалізоване обладнання для забезпечення захисту приміщення в якому будуть знаходитися компоненти системи.

При розробці було вдосконалено наступні методи захисту: застосування гібридної системи шифрування, фільтр даних, які будуть циркулювати в системі під час роботи користувачів, захищений інтерфейс для користування мережею, резервування каналів зв'язку.

Також було розроблено рекомендації стосовно впровадження та підключення системи, щоб забезпечити максимальну ефективність та надійність усієї системи після її встановлення. Дана система забезпечить надійний захист під час роботи з мережею та забезпечить захист критичної інформації.

При підрахунку вартості створеної системи обробки критичної інформації було виявлено значну економію грошей при її впровадженні та можливості забезпечити впровадження на зекономлені кошти системи захисту для приміщення, де буде знаходитися система обробки критичної інформації й отримати економію в розмірі 25 000 грн.

## 4 АНАЛІЗ ВИХОДУ НА РИНОК СТАРТАП ПРОЕКТУ

### 4.1 Опис ідеї стартап проекту

Таблиця 4.1 – Опис ідеї стартап-проекту

<i>Зміст ідеї</i>	<i>Напрямки застосування</i>	<i>Вигоди для користувача</i>
Для забезпечення захисту критичної інформації в системах обробки пропонується модель системи захисту критичної інформації. Дана модель пропонує повне покриття питання захисту систем обробки критичної інформації, включаючи характеристики та настройки, як самої системи так і запобіжних заходів щодо забезпечення її захисту проти фізичних загроз.	1. Використання моделі на підприємствах для забезпечення захисту систем обробки критичної інформації.	1. Забезпечення повного покриття питання захисту критичної інформації 2. Забезпечення повного покриття питання захисту систем обробки критичної інформації. 3. Використання актуальних рекомендацій стосовно засобів захисту систем обробки критичної інформації. 4. Підвищення рівня захищеності систем обробки критичної інформації.
	2. Використання моделі користувачами систем обробки критичної інформації.	1. Отримання вичерпної інформації по забезпеченню захисту системам обробки критичної інформації. 2. Отримання навичок та знань для роботи з системами обробки критичної інформації.

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ n/n	Техніко- економічні характерист ики ідеї	(Потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Конкурент I			
1.	Покриття питань захисту систем обробки критичної інформації.	Забезпечення повного покриття питань захисту систем обробки критичної інформації та оптимізації використання ресурсів для засобів захисту систем обробки критичної інформації.	Забезпечення повного покриття питань захисту, однак нераціональне використання ресурсів.	Недостатність фінансування подальшого аналізу та розвідку систем захисту, поки не буде реалізовано вихід на ринок.	Достатній рівень захисту системи обробки критичної інформації.	Нововведення, модернізація та покращення захисту по забезпеченню захисту систем обробки критичної інформації.

Кінець таблиці 4.2

2.	Технічні	Використання невеликих потужностей у зв'язку з початком виходу на ринок.	Використання великих потужностей в зв'язку з суміжними видами діяльності корпорації.	Малі потужності у зв'язку з початком виходу на ринок	Достатній рівень потужностей для надання послуг.	Менші витрати на підтримання ресурсів.
4.	Масштабовність	Можливість до розширення у випадку виникнення суміжних видів діяльності.	Надання послуг у своїй сфері діяльності.	Необхідно задіювати науково – технічний потенціал.	Процеси виконуються належним чином.	Адаптивність до будь-яких потреб користувача.

## 4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

<i>№ n/n</i>	<i>Ідея проекту</i>	<i>Технології її реалізації</i>	<i>Наявність технологій</i>	<i>Доступність технологій</i>
1.	Модель захищеної системи обробки критичної інформації, що забезпечить повне покриття питання захисту систем.	Для впровадження даного проекту необхідно:  1. Найняти команду спеціалістів для впровадження засобів захисту в систему обробки критичної інформації.	Технології є доступними та стосуються виключно найму персоналу.	Технологія є доступною.
		2. Найняти команду спеціалістів для забезпечення навчання та супроводження впровадженого захисту в систему обробки критичної інформації.	Технології є доступними, стосуються виключно найму персоналу.	Технологія є доступною.
		3. Практична реалізація продукту, та його тестування для забезпечення якості.	Технології є доступними, стосуються найму кваліфікованого персоналу та побудови технічного завдання.	Технологія є доступною

Кінець таблиці 4.3

Обрана технологія реалізації ідеї проекту:

- Найняти команду спеціалістів для впровадження засобів захисту в систему обробки критичної інформації.
- Найняти команду спеціалістів для забезпечення навчання та супроводження впровадженого.
- Практично реалізація продукту.

За результатами аналізу, наведеного вище, було встановлено, що даний проект є технічно реалізованим. Для реалізації необхідно найняти вищенаведений персонал з відповідним рівнем кваліфікації у вищевказаних питаннях. Під час пошуку кандидатів буде проведено ряд інтерв'ю та випробувань для перевірки рівня кваліфікації.

### 4.3 Аналіз ринкових можливостей запуску стартап проекту

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	10
2	Загальний обсяг продаж, грн/ум.од	150 000 ум.од
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Необхідність початкового капіталу та наявність конкуренції

Кінець таблиці 4.4

5	Специфічні вимоги до стандартизації та сертифікації	Необхідно сертифікувати товар згідно постанови вимог до кіберзахисту об'єктів критичної інфраструктури
6	Середня норма рентабельності в галузі (або по ринку), %	Рентабельність проекту складає 119%, що є вищим за показник рентабельності банківського вкладу на 8-10%.

#### 4.4 Розроблення маркетингової програми

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

<i>№ n/n</i>	<i>Потреба, що формує ринок</i>	<i>Цільова аудиторія (цільові сегменти ринку)</i>	<i>Відмінності у поведінці різних потенційних цільових груп клієнтів</i>	<i>Вимоги споживачів до товару</i>
1	- Потреба в підвищенні захисту систем обробки критичної інформації.	- Підприємства та корпорації, які прагнуть оновити чи встановити захищену систему обробки критичної інформації.	- Підвищення рівня стурбованості питаннями безпеки критичної інформації.	- Отримання гарантії захисту критичної інформації



Кінець таблиці 4.5

2	- Потреба в створенні захищеної системи обробки критичної інформації	- Державні установи, що прагнуть встановити захищену систему обробки критичної інформації.	- Необхідність сертифікації захищеної системи обробки інформації відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” для державних та приватних підприємств, працюючих з критичними даними держави ччч громадян України.	- Отримання супровід впровадженої захищеної системи обробки критичної інформації
---	--	--	--	--

Таблиця 4.6 – Фактори загроз

<i>№ n/n</i>	<i>Фактор</i>	<i>Зміст загрози</i>	<i>Можлива реакція компанії</i>
1.	Інтенсивний розвиток сучасних технологій та вірогідність виявлення нових вразливостей засобів захисту, що використовуються.	З розвитком технологій виявляються нові вразливості засобів захисту, що негативно впливає на захищеність системи, тому існує вірогідність виявлення нових загроз в засобах захисту не встигнувши вийти на ринок чи створити базу клієнтів.	При виявленні вразливостей засобів захисту своєчасне реагування та вирішення проблеми.
2.	Недостатність стартового капіталу.	Неможливість подолання бар'єру виходу на ринок через недостатність коштів стартового капіталу	Залучення інвесторів, що забезпечать додатковим капіталом за відсоток майбутнього прибутку компанії.
3.	Наявність конкуренції	Неможливість подолання бар'єру виходу на ринок через велику конкуренцію.	Отримання конкурентої переваги шляхом покращення якості надання послуг.

Таблиця 4.7 – Фактори можливостей

<i>№ n/n</i>	<i>Фактор</i>	<i>Зміст можливості</i>	<i>Можлива реакція компанії</i>
1.	Необхідність забезпечити належного рівня захисту системам обробки критичної інформації відповідно до діючого законодавства.	Модель створено відповідного діючого законодавства враховуючи вимоги до кіберзахисту об'єктів критичної інфраструктури	Забезпечення високого рівня послуг, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.
2.	Підвищення рівня стурбованості безпеки критичної інформації в корпораціях..	Через глобальну інформатизацію, проблема захисту систем обробки критичної інформації для організацій набуває найвищого значення з точки зору впливу на бізнес.	Розповсюдження інформації стосовно важливості захисту критичної інформації організацій та систем обробки критичної інформації.
3.	Необхідність відповідності сучасним законам щодо обробки і зберігання критичної інформації	В зв'язку з турбованістю країн станом інформаційної безпеки – вони впроваджують закони що впливають на процеси керування критичними даними, в результаті цих змін, компаніям потрібно підвищувати рівень захисту систем обробки критичної інформації.	Забезпечення та підтримання високого рівня продукту завдяки потужній науково-технічній базі що закладено з початку роботи проекту.

Таблиця 4.8 - Ступеневий аналіз конкуренції на ринку

<i>Особливості конкурентного середовища</i>	<i>В чому проявляється дана характеристика</i>	<i>Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)</i>
1. Вказати тип конкуренції - монополістична	На ринку багато фірм, проте умови входження на ринок досить легкі.	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.
2. За рівнем конкурентної боротьби - національний	Конкурентна боротьба в межах визначеної країни.	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.
3. За галузевою ознакою - внутрішньогалузева	Конкуренція в межах галузі.	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.
4. Конкуренція за видами товарів: - - товарно-родова	Конкуренція між різноманітними видами товарів, що можуть виконувати схожі функції.	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.

Кінець таблиці 4.8

5. За характером конкурентних переваг - нецінова	Конкуренція за рахунок покращення якості надання послуг	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.
6. За інтенсивністю - марочна	Відсутня необхідність випуску ряду товарів під однією маркою	Забезпечення високого рівня моделі та послуг по встановлені, завдяки відслідковуванню змін в законодавстві України та постійне оновлення засобів захисту моделі внаслідок нововведень у кіберпросторі.

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

	<i>Прямі конкуренти в галузі</i>	<i>Потенційні конкуренти</i>	<i>Постачальники</i>	<i>Клієнти</i>	<i>Товари-замінники</i>
<i>Складові аналізу</i>	Підприємства, що будують комплексні системи захисту інформації.	Потенційними конкурентами можуть виступати проекти, які почнуть пропонувати аналогічні послуги.	Вплив зі сторони постачальників не є застосовним.	Дана послуга стає популярнішою та з кожним роком попит на неї буде збільшуватися	Загроза полягає в тому, що як новому гравцю на ринку можуть не довіряти та обирати товари-замінники.

Кінець таблиці 4.9

<i>Висновки:</i>	Конкуренція буде високою доки не буде реалізовано знайомства користувачів з системою.	Можливості виходу на ринок обґрунтовані рентабельністю проекту, попитом, створеним за разунком підвищення рівня стурбованості суспільства питаннями інформаційної безпеки;	Через велику кількість постачальників вони не зможуть диктувати умови на ринку.	Клієнти не чинять впливу на умови роботи на ринку, вони можуть створювати певний попит відносно до ступеня їх обізнаності в питаннях інформаційної безпеки та розуміння необхідності впровадження систем захисту.	Обмеження роботи на ринку через товари-замінники не буде.
------------------	---	--	---	---	---

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

<i>№ n/n</i>	<i>Фактор конкурентоспроможності</i>	<i>Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)</i>
1.	Повне покриття питання проблеми захищеності систем обробки критичної інформації	Забезпечення повного покриття проблеми захисту систем обробки критичної інформації
2.	Покриття питань захисту критичної інформації.	Забезпечення повного покриття питання захисту критичної інформації
3.	Актуальність рекомендацій стосовно засобів захисту систем обробки критичної інформації.	Забезпечення актуальних рекомендацій стосовно стану захищеності засобів захисту систем обробки критичної інформації.
4.	Репутація виробника	При бездоганній репутації рівень довіри до компанії зростає.
5.	Рівень лояльності до бренду	Чим вище рівень лояльності, тим більше компанія має прихильників та постійних споживачів

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін «назва проекту»

№ n/n	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з даним проектом						
			-3	-2	-1	0	+1	+2	+3
1	Покриття проблеми захищеності систем обробки критичної інформації	18		I		II			
2	Покриття питань захисту критичної інформації.	10			II	I			
3	Актуальність рекомендацій стосовно засобів захисту систем обробки критичної інформації.	19-20	I			II			
4.	Цінотворення інструменту	12	II		I				
5.	Репутація виробника	16						I	II

Умовні позначки позицій конкурентів:

I - конкурент 1

II - конкурент 2

Отже, відповідно до проведеного аналізу можна сказати, що «Метод оцінювання ефективності контролів безпеки» має наступну позицію на ринку:

сильні сторони:

- цінотворення інструменту;
- покриття проблеми захищеності систем обробки критичної інформації;



слабкі сторони:

- лояльність до бренду
- захоплення ринку
- репутація

Таблиця 4.12 – SWOT- аналіз стартап-проекту

<p>Сильні сторони:</p> <ul style="list-style-type: none"> <li>• Цінотворення інструменту на основі модернізації існуючих компонентів об'єднаних в інноваційний продукт, створює умови для низької ціни на етапі виходу на ринок</li> <li>• Покриття проблеми захищеності систем обробки критичної інформації за допомогою нових впроваджень захисту та модернізацію існуючих.</li> </ul>	<p>Слабкі сторони:</p> <ul style="list-style-type: none"> <li>• Так як бренд ще не зарекомендував себе на ринку, а позиції конкурентів сильні це створить перепони</li> <li>• Захоплення ринку відбувається поступово</li> <li>• Лояльність до бренду напрацьовується за рахунок репутації</li> </ul>
<p>Можливості:</p> <ul style="list-style-type: none"> <li>• Можливість зміцнення іміджу</li> <li>• Можливість збільшення обсягів реалізації</li> <li>• Можливість збільшення обсягів продаж за рахунок експансії</li> </ul>	<p>Загрози:</p> <ul style="list-style-type: none"> <li>• Загроза працювати без прибутку скорочення платоспроможного попиту</li> <li>• Загроза втрати споживачів внаслідок підвищення тиску зі сторони конкурентів</li> <li>• Загроза підвищення цін</li> </ul>

Таблиця 4.13 – Альтернативи ринкового впровадження стартап-проекту

<i>№ n/n</i>	<i>Альтернатива (орієнтовний комплекс заходів) ринкової поведінки</i>	<i>Ймовірність отримання ресурсів</i>	<i>Строки реалізації</i>
1.	Підвищувати інформованість суспільства стосовно питань важливості захисту критичної інформації, поширення інформації за допомогою соціальних мереж..	Здобуття конкурентної переваги шляхом покращення популярності та якості продукту.	3-5 місяців

#### 4.5 Розроблення ринкової стратегії проекту

Таблиця 4.14 – Вибір цільових груп потенційних споживачів

<i>№ n/n</i>	<i>Опис профілю цільової групи потенційних клієнтів</i>	<i>Готовність споживачів сприйняти продукт</i>	<i>Орієнтовний попит в межах цільової групи (сегменту)</i>	<i>Інтенсивність конкуренції в сегменті</i>	<i>Простота входу у сегмент</i>
1.	Державні установи та приватні підприємства, де церкуює критична інформація громадян України.	Готовність споживачів до сприйняття продукту обумовлена вимогами законодавства щодо захисту критичної інформації.	Високий попит в зв'язку з високим рівнем захищеності продукту та меншою вартістю.	Інтенсивність конкуренції в сегменті не є високою.	Середня складність входу в сегмент в зв'язку.

Кінець таблиці 4.14

2.	Приватні установи, що вирішили використовувати засоби захисту для систем обробки критичної інформації.	Готовність споживачів до сприйняття продукту обумовлена бажанням підвищення безпеки критичній інформації установи.	Високий попит в зв'язку з високим рівнем захищеності продукту та меншою вартістю.	Інтенсивність конкуренції в сегменті середня.	Середня складність входу в сегмент в зв'язку.
Які цільові групи обрано: державні та приватні установи.					

Таблиця 4.15 – Визначення базової стратегії розвитку

<i>№ п/п</i>	<i>Обрана альтернатива розвитку проекту</i>	<i>Стратегія охоплення ринку</i>	<i>Ключові конкурентоспроможні позиції відповідно до обраної альтернативи</i>	<i>Базова стратегія розвитку*</i>
1.	Кооперування з відомими компаніями з метою отримання взаємовигідних результатів.	Стратегія диференційованого маркетингу	Орієнтованість на вартість товару та ціні властивості з точки зору споживача, які роблять товар кращим за конкурентів.	Стратегія диференціації

Таблиця 4.16 – Визначення базової стратегії конкурентної поведінки

<i>№ n/n</i>	<i>Чи є проект «першопрохідцем» на ринку?</i>	<i>Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?</i>	<i>Чи буде компанія копіювати основні характеристики товару конкурента, і які?</i>	<i>Стратегія конкурентної поведінки*</i>
	<i>Дана послуга не являється першопрохідцем на ринку, існує ряд суміжних послуг.</i>	<i>Передбачується утворення власного кола споживачів, однак існує вірогідність переходу частини споживачів від конкурентів.</i>	<i>Компанія не буде копіювати характеристики товару конкурента.</i>	<i>Створення власного кола споживачів, чия діяльність базується на забезпеченні безпеки систем обробки критичної інформації.</i>

Таблиця 4.17 – Визначення стратегії позиціонування

<i>№ n/n</i>	<i>Вимоги до товару цільової аудиторії</i>	<i>Базова стратегія розвитку</i>	<i>Ключові конкурентоспроможні позиції власного стартап-проекту</i>	<i>Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)</i>
1.	Простота виоритсання Простота впровадження Супровідь продукту	Стратегія диференціації	Вигоди, які пропонуються в даному проекті, конкурентні фактори (див. табл. 4.18)	Унікальність Захищеність Модернізація

#### 4.6 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 18 потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.18 – Визначення ключових переваг концепції потенційного товару.

<i>№ n/n</i>	<i>Потреба</i>	<i>Вигода, яку пропонує товар</i>	<i>Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)</i>
1.	Потреба в захисті систем обробки критичної інформації.	Забезпечення надійного захисту систем обробки критичної інформації.	Модернізація систем обробки критичної інформації посиленими засобами захисту.

Таблиця 4.19 – Визначення меж встановлення ціни

<i>№ n/n</i>	<i>Рівень цін на товари-замінники</i>	<i>Рівень цін на товари-аналоги</i>	<i>Рівень доходів цільової групи споживачів</i>	<i>Верхня та нижня межі встановлення ціни на товар/послугу</i>
	15 000 – 18 000	20 000	Високий або середній	10 000 – 15 000

Таблиця 4.20 – Опис трьох рівнів моделі товару

<i>Рівні товару</i>	<i>Сутність та складові</i>		
I. Товар за задумом	Захищена система обробки критичної інформації. Реалізовує повноцінну безпеку системам обробки критичної інформації на програмному та фізичному рівнях.		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1. Висорий рівень захисту	М	
	2. Простота використання	М	
	3. Актуальність		
	Якість: стандарти, нормативи, параметри тестування тощо		
	Пакування: Надання користувачу підтримки, персональний підхід до кожного.		
	Марка: Secure your info -		
III. Товар із підкріпленням	До продажу популяризація критичної інформації, виступи / публікації; проведення демонстрації всього обсягу надання послуги.		
	Після продажу розвиток суміжних видів діяльності, підвищення зацікавості аудиторії		
За рахунок чого потенційний товар буде захищено від копіювання:			
в зв’язку зі специфікою надання послуг питання про захист полягатиме в патенуванні захищеної систем обробки критичної інформації. Захист від копіювання моделі сиистеми полягатиме в захисті інтелектуальної власності			

Таблиця 4.21 – Формування системи збуту

<i>№ n/n</i>	<i>Специфіка закупівельної поведінки цільових клієнтів</i>	<i>Функції збуту, які має виконувати постачальник товару</i>	<i>Глибина каналу збуту</i>	<i>Оптимальна система збуту</i>
1.	Мінімальна кількість посередників	Організація широкої мережі збуту та популяризація товару	Прямий канал збуту	Залучення компаній – партнерів для організації ефективного збуту

Таблиця 4.22. – Концепція маркетингових комунікацій

<i>№ n/n</i>	<i>Специфіка поведінки цільових клієнтів</i>	<i>Канали комунікацій, якими користуються цільові клієнти</i>	<i>Ключові позиції, обрані для позиціонування</i>	<i>Завдання рекламного повідомлення</i>	<i>Концепція рекламного звернення</i>
1.	Вимоги до зручності використання	Інформаційні мережі	Адаптація до вимог замовника	Донесення переваг моделі до цільових клієнтів	Рекламне повідомлен ня має демонструв ати основні визначені переваги проекту.
2.	Вимоги до повноцінного захисту системи	Інформаційні мережі	Адаптація до вимог замовника	Донесення переваг моделі до цільових клієнтів	

#### **Висновки до розділу 4**

Було проведено технологічний аудит ідеї проекту, аналіз ринкових можливостей для запуску, цільової аудиторії, потенційних клієнтів. Проведено порівняльний аналіз з конкурентами на основі специфіки діяльності, та переваг.

Підсумовуючи, можна зробити висновок, що вихід на ринок буде затруднений специфікою проекту та через протидію зі сторони основних гравців ринку. Але при поступовому введенні продукту на ринок, він завоює міцні позиції та покаже високі показники прибутку, залишаючи за собою можливості для масштабування.



## ВИСНОВКИ

Результатом виконання дипломної роботи є реалізація побудови моделі захищеної системи обробки критичної інформації, що забезпечить надійну роботу та захист критичній інформації.

Для реалізації захищеної передачі даних по незахищеному середовищу та можливості використовувати мережу інтернет було реалізовано подвійне асиметричне шифрування. Для реалізації цього засобу захисту було реалізовано криптосистему Рабіна та RSA.

Було реалізовано додатковий засіб захисту – фільтр даних, що додатково перевіряє дані, які будуть надходити на сервер та клієнт, після фільтрації вони відображаються в інтерфейсі користувача. Інтерфейс було реалізовано для захисту системи від можливих непідконтрольних дій користувачів системи, для забезпечення захисту від фактору соціальної інженерії.

Для зберігання та передачі даних всередині системи обробки критичної інформації було впроваджено гібридну систему шифрування, де для шифрування тексту використовується симетричне шифрування а для шифрування ключа асиметричне. Також було додано можливість реалізовувати віддалену роботу з системою за допомогою впровадженого подвійного асиметричного шифрування.

Було розроблено рекомендації стосовно специфікації приміщення в якому буде знаходитися система обробки критичної інформації. Для реалізації додаткового захисту системи було використано систему бездротової GSM сигналізації, спроектованої на четвертому курсі в дипломній роботі бакалавра.

Під час перевірки надійності даної системи було отримано наступні результати: дана система ефективно протидіє загрозам прослуховування трафіку, внутрішнім загрозам, загрозам соціальної інженерії та прямим проникненням на об'єкт.

Було реалізовано підрахунок приблизної вартостів провадження засобів захисту для системи обробки критичної інформації, зі сторони системи та

приміщення, де вона буде знаходитися заради створення системи захисту за оптимальну ціну.

На підставі отриманих висновків необхідне подальше дослідження проблеми вразливості систем обробки критичної інформації.

Подальші дослідження слід направити на розробку прискореної криптосистеми шифрованої передачі критичних даних без втрат захищеності. У вдосконаленні методів та засобів захисту критичної інформації. Також слід реалізувати модернізацію технічних засобів захисту, для приміщення в якому буде знаходитися системи обробки критичної інформації та її складові, це обумовлено їх високою вартістю, що впливає у свою чергу на безпеку системи.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури [Електронний ресурс] Режим доступа: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF>
2. НОРМАТИВНИЙ ДОКУМЕНТ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ [Електронний ресурс] Режим доступа: [http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art\\_id=101870&cat\\_id=89734&ctime=1344501089407](http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407)
3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] Режим доступа: <https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf>
4. Методи соціальної інженерії [Електронний ресурс] Режим доступа: <https://www.a1qa.ru/blog/sotsialnaya-inzheneriya-ili-ataki-na-chelovecheskiy-faktor/>
5. PUP програми [Електронний ресурс] Режим доступа: <http://talkdevice.ru/pup-optional-chto-eto-za-virus.html>
6. Бімотеричні засоби захисту [Електронний ресурс] Режим доступа: <https://www.osp.ru/os/2012/10/1303312/>
7. Переваги використання брандмауера [Електронний ресурс] Режим доступа: <https://studfile.net/preview/5043913/page:2>
8. Переваги та недоліки антивірусів [Електронний ресурс] Режим доступа: <https://kamchadal.wordpress.com/>
9. Види антивірусів [Електронний ресурс] Режим доступа: <http://soft-ru.org/articles/Vidy-antivirusov-polifagi-revizory-blokirovwiki.php>
10. Брандмауер [Електронний ресурс] Режим доступа: <https://studfile.net/preview/5043913/page:2/>

11. SQL Injection найнебезпечніший вид вразливості [Електронний ресурс]  
Режим доступу: [https://acribia.ru/articles/why\\_sql\\_injection\\_is\\_the\\_most\\_dangerous\\_type\\_of\\_vulnerability](https://acribia.ru/articles/why_sql_injection_is_the_most_dangerous_type_of_vulnerability)
12. Ідентифікація особистості в мережі інтернет [Електронний ресурс] Режим доступу: <https://moluch.ru/archive/110/26935>
13. Інтернет в Україні [Електронний ресурс] Режим доступу: [https://project.liga.net/projects/eastern\\_threat](https://project.liga.net/projects/eastern_threat)
14. Анонімність в інтернеті, як стати анонімом в мережі [Електронний ресурс]  
Режим доступу: <https://vkoshelek.com/anonimnost-v-internete-10-sposobov>
15. НД ТЗІ 1.1-002-99 [Електронний ресурс] Режим доступу: [http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=15FDA2B2745B1390AC937214804F2E76?showHidden=1&art\\_id=102089&cat\\_id=89734&ctime=1344502332348](http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=15FDA2B2745B1390AC937214804F2E76?showHidden=1&art_id=102089&cat_id=89734&ctime=1344502332348)
16. Контроль дій користувачів [Електронний ресурс] Режим доступу: <http://www.infobezpeka.com/products/insider/?view=3>
17. Антивірус norton [Електронний ресурс] Режим доступу: <https://us.norton.com/products?>

**ДОДАТКИ**

## Додаток А

```

{
    SQLiteConnection.CreateFile("TestDB.db");
}

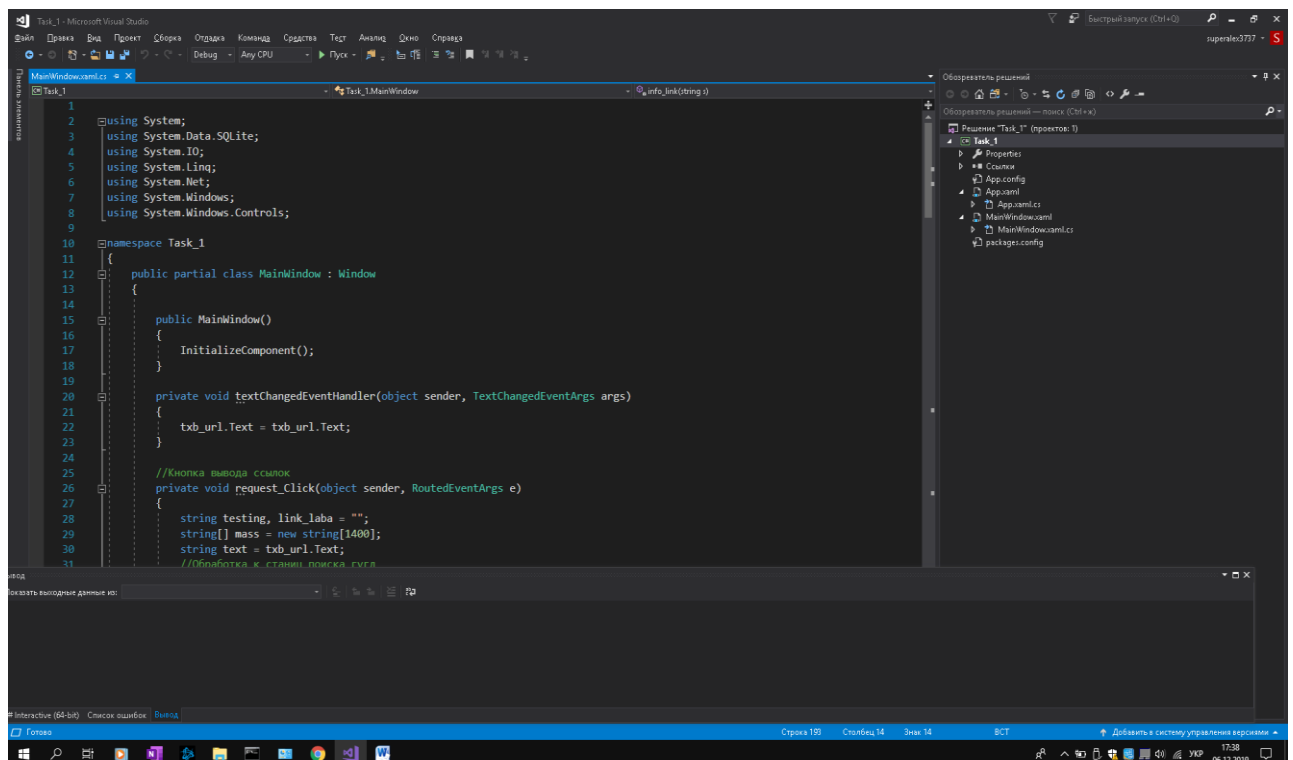
//Подключение к БД
using (SQLiteConnection Connect = new SQLiteConnection("Data Source=TestDB.db; Version=3;"))
{
    // Создать таблицу, если её нет
    string commandText = "CREATE TABLE IF NOT EXISTS [dbTableName] ( [id] INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, [link_info] VARCHAR(50), [link_text] NVARCHAR(128))";
    SQLiteCommand Command = new SQLiteCommand(commandText, Connect);
    Connect.Open(); // Открыть соединение
    Command.ExecuteNonQuery(); // Выполнить запрос
    Connect.Close(); // Закрыть соединение
}

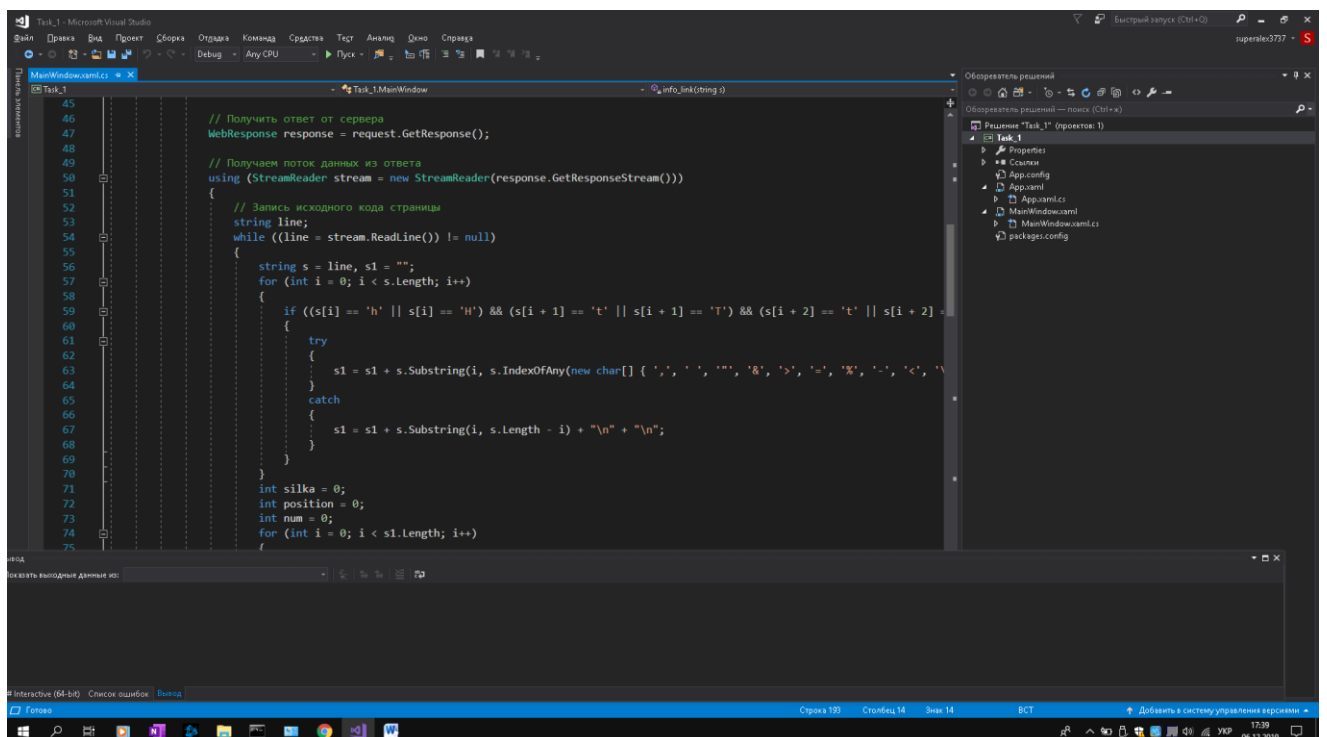
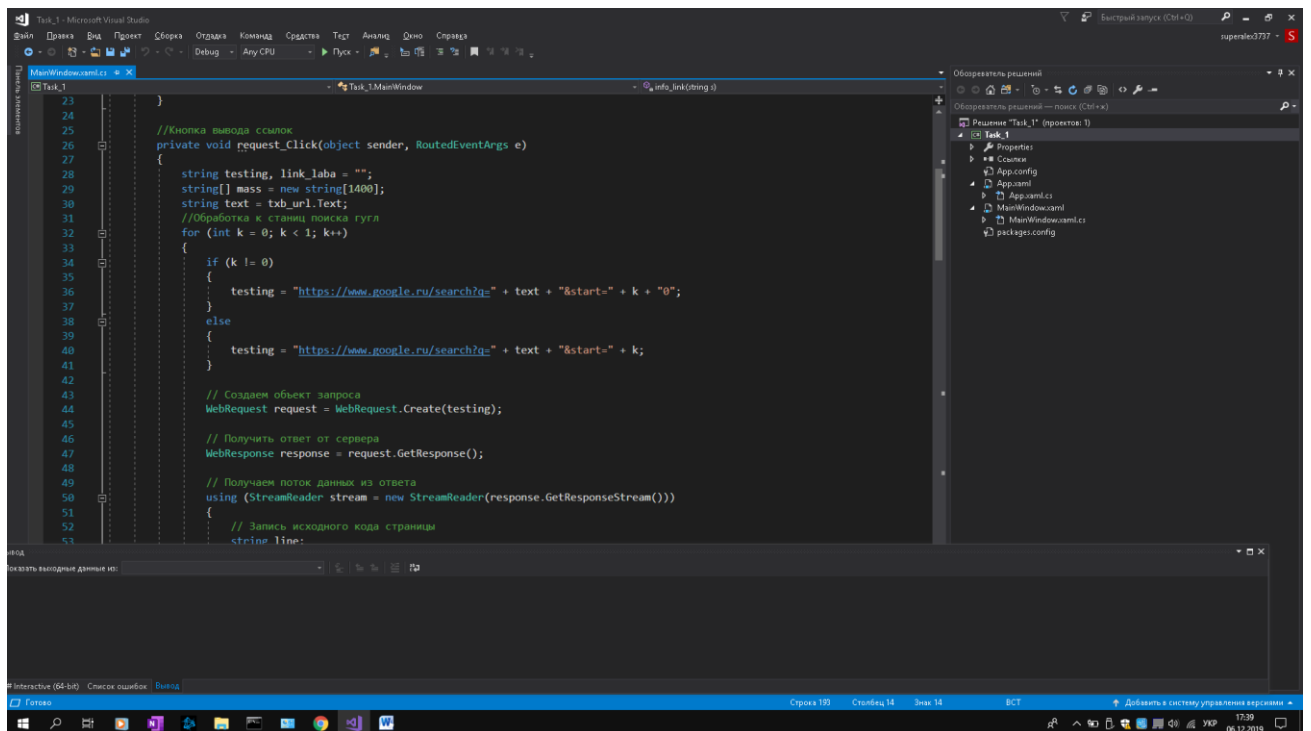
// Записываем информацию в базу данных
using (SQLiteConnection Connect = new SQLiteConnection("Data Source=TestDB.db; Version=3;"))
{
    string commandText = "INSERT INTO [dbTableName] ([link], [link_info], [link_text]) VALUES(@link, @link_info, @link_text)";
    SQLiteCommand Command = new SQLiteCommand(commandText, Connect);
    Command.Parameters.AddWithValue("@link", link);
    Command.Parameters.AddWithValue("@link_info", link_info);
    Command.Parameters.AddWithValue("@link_text", link_text);
    Connect.Open();
    Command.ExecuteNonQuery();
    Connect.Close();
}

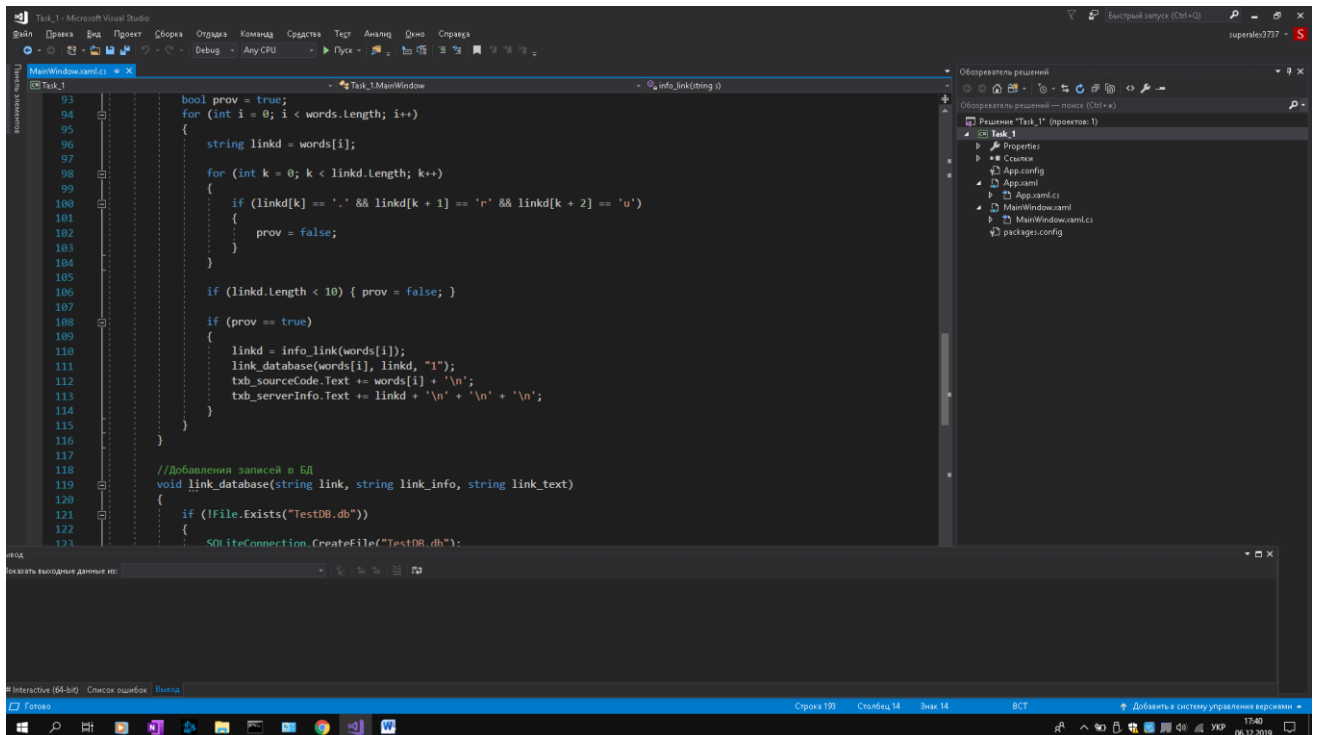
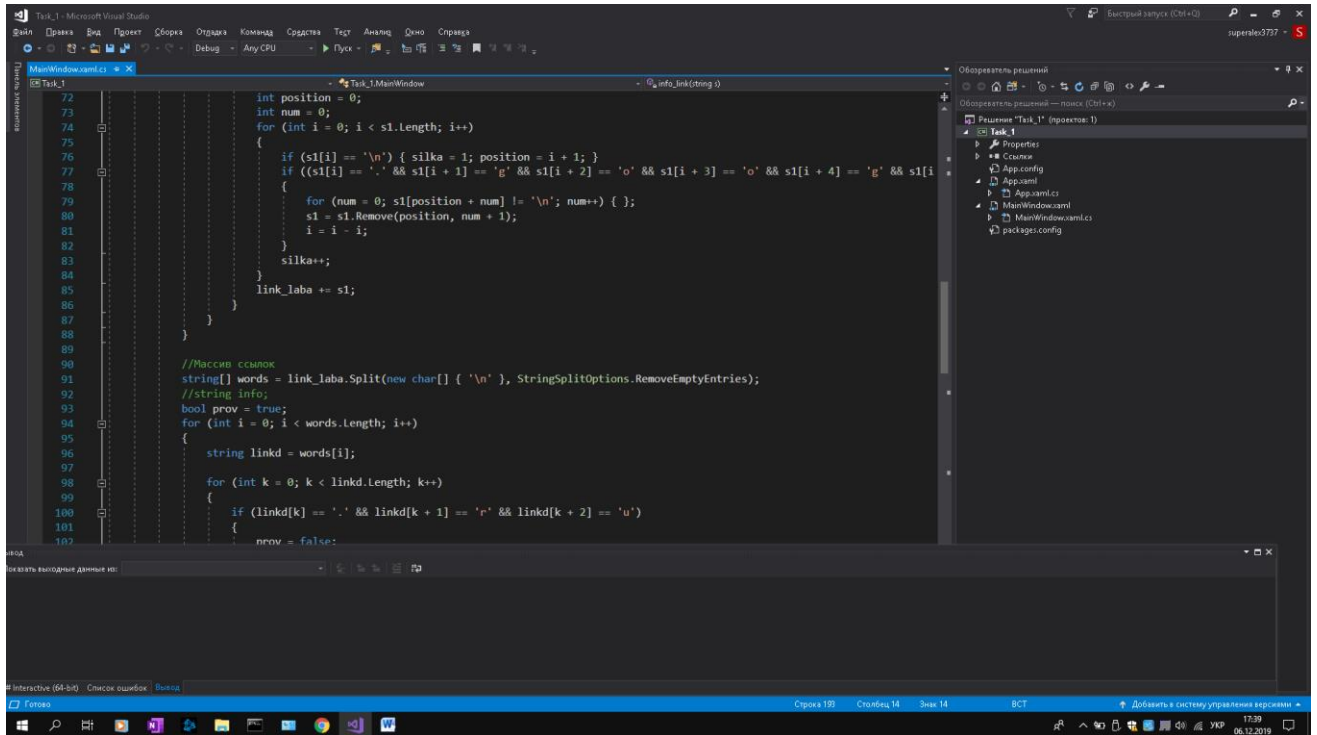
//Планшета о сервере

```

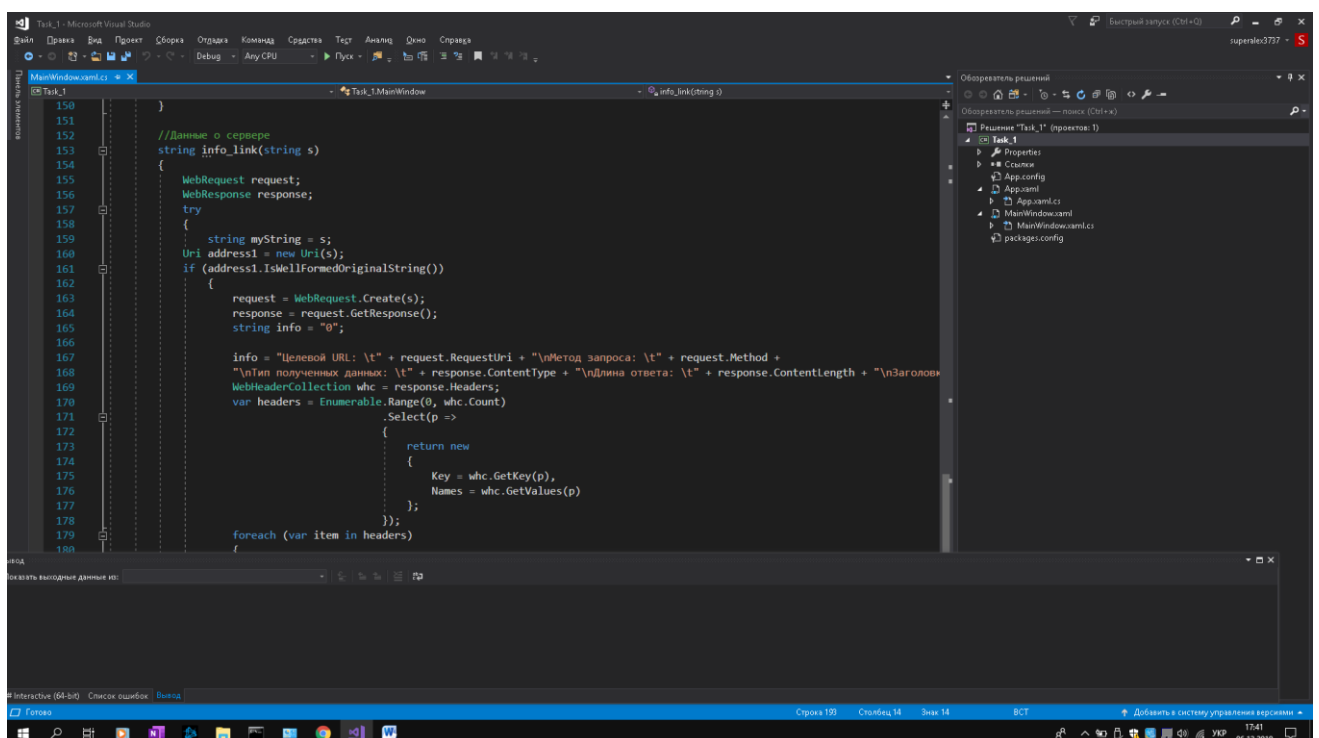
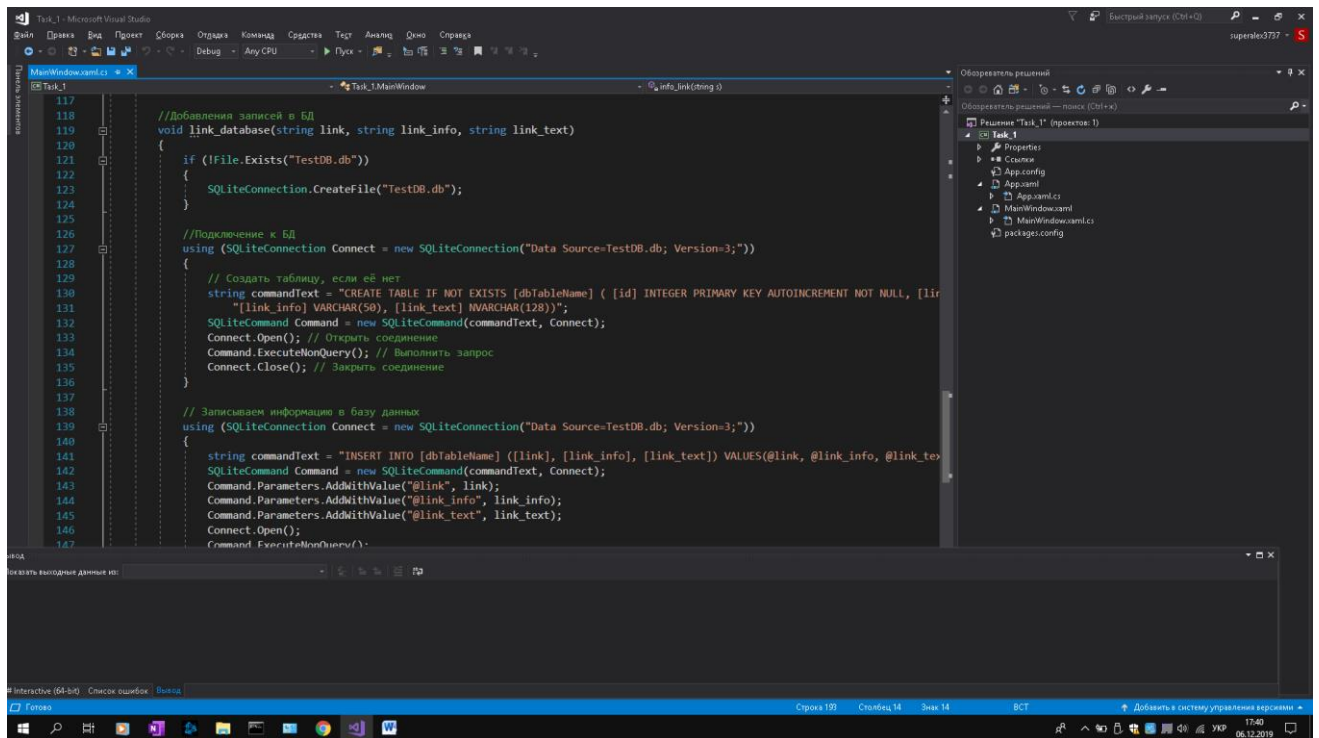
## Додаток Б

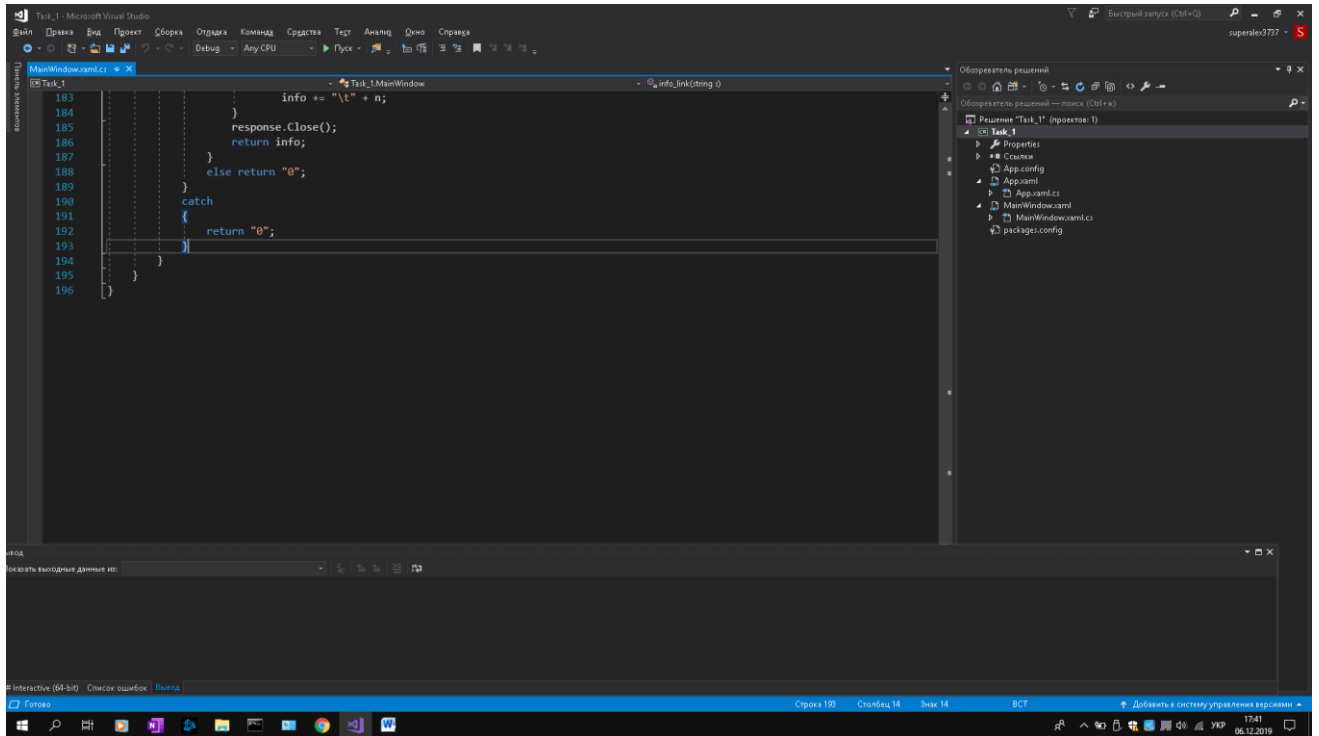




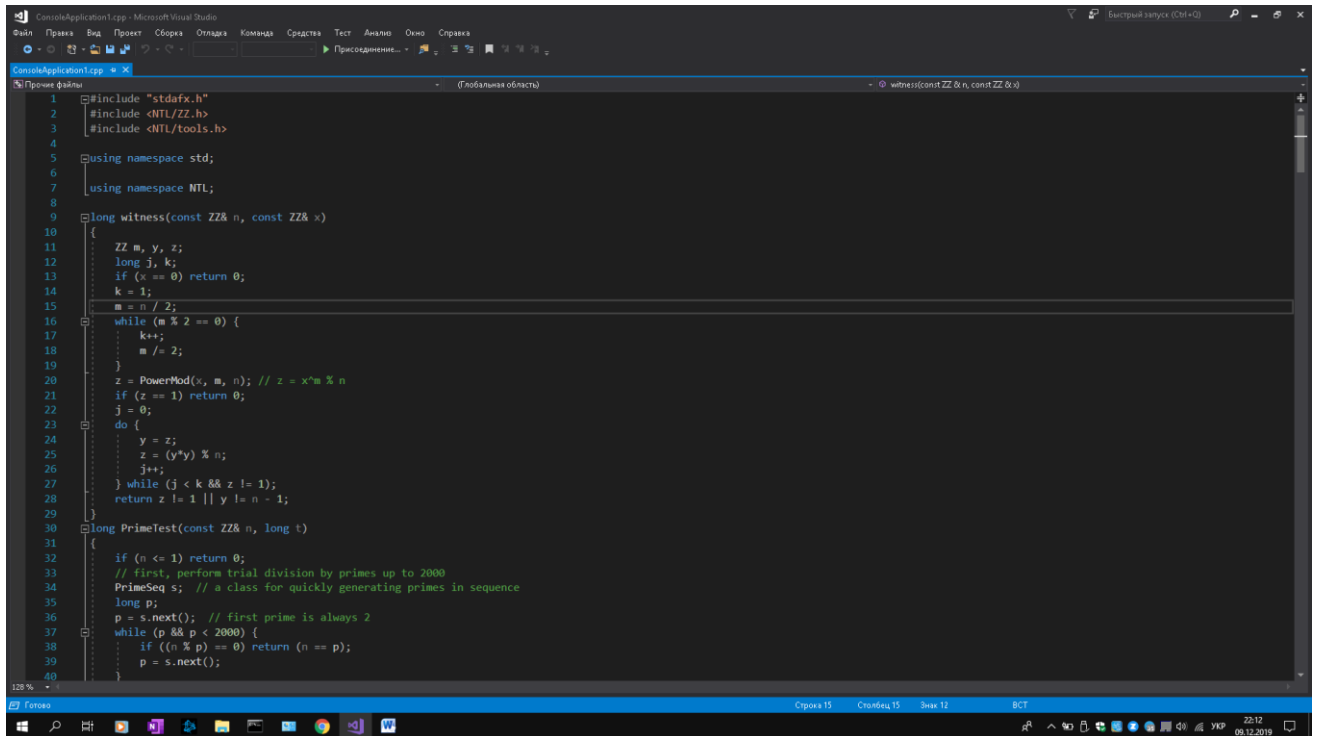








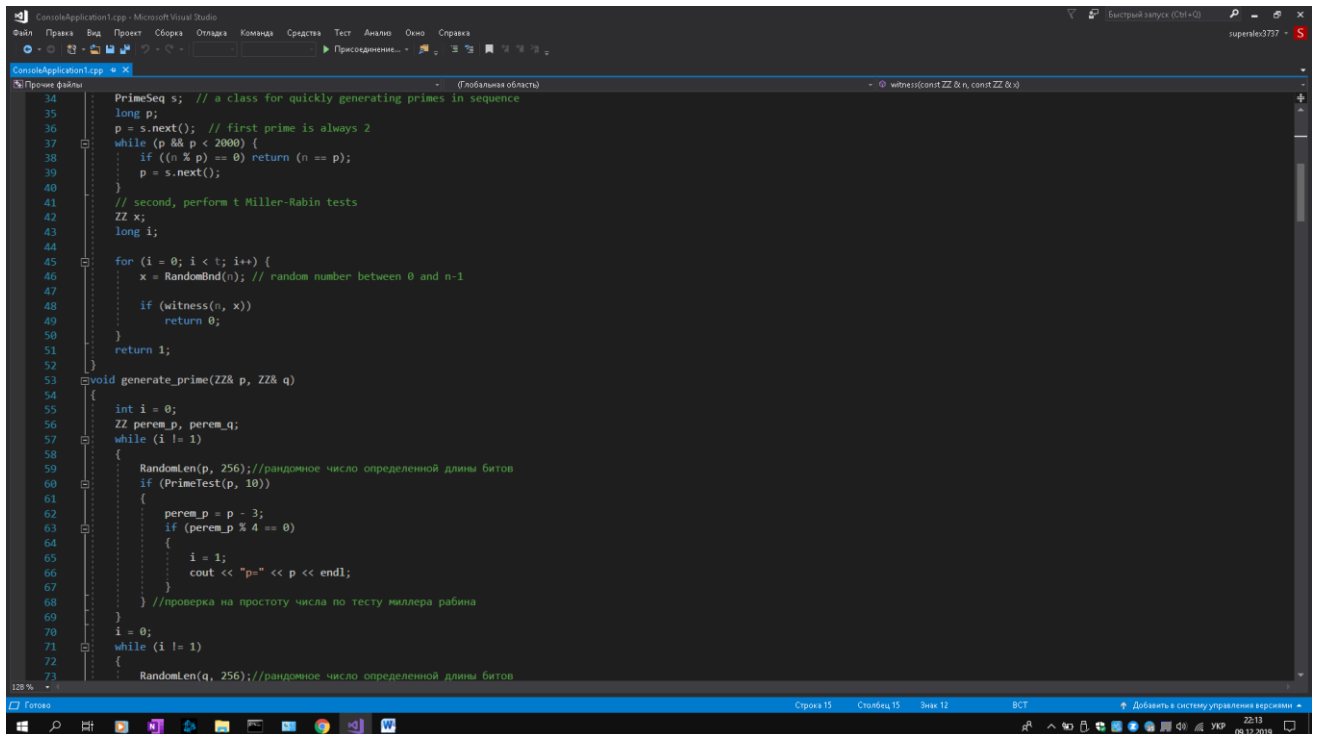
## Додаток В



```

1  #include "stdafx.h"
2  #include <NTL/ZZ.h>
3  #include <NTL/tools.h>
4
5  using namespace std;
6
7  using namespace NTL;
8
9  long witness(const ZZ& n, const ZZ& x)
10 {
11     ZZ m, y, z;
12     long j, k;
13     if (x == 0) return 0;
14     k = 1;
15     m = n / 2;
16     while (m % 2 == 0) {
17         k++;
18         m /= 2;
19     }
20     z = PowerMod(x, m, n); // z = x^m % n
21     if (z == 1) return 0;
22     j = 0;
23     do {
24         y = z;
25         z = (y*y) % n;
26         j++;
27     } while (j < k && z != 1);
28     return z != 1 || y != n - 1;
29 }
30
31 long PrimeTest(const ZZ& n, long t)
32 {
33     if (n <= 1) return 0;
34     // first, perform trial division by primes up to 2000
35     PrimeSeq s; // a class for quickly generating primes in sequence
36     long p;
37     p = s.next(); // first prime is always 2
38     while (p && p < 2000) {
39         if ((n % p) == 0) return (n == p);
40         p = s.next();
41     }
42 }

```



```

34 PrimeSeq s; // a class for quickly generating primes in sequence
35 long p;
36 p = s.next(); // first prime is always 2
37 while (p && p < 2000) {
38     if ((n % p) == 0) return (n == p);
39     p = s.next();
40 }
41 // second, perform t Miller-Rabin tests
42 ZZ x;
43 long i;
44 for (i = 0; i < t; i++) {
45     x = RandomBnd(n); // random number between 0 and n-1
46     if (witness(n, x))
47         return 0;
48 }
49 return 1;
50
51 void generate_prime(ZZ& p, ZZ& q)
52 {
53     int i = 0;
54     ZZ perem_p, perem_q;
55     while (i != 1)
56     {
57         RandomLen(p, 256); // случайное число определенной длины битов
58         if (PrimeTest(p, 10))
59         {
60             perem_p = p - 3;
61             if (perem_p % 4 == 0)
62             {
63                 i = 1;
64                 cout << "p=" << p << endl;
65             }
66         } // проверка на простоту числа по тесту миллера рабина
67     }
68     i = 0;
69     while (i != 1)
70     {
71         RandomLen(q, 256); // случайное число определенной длины битов
72     }
73 }

```

```

67     }
68     } //проверка на простоту числа по тесту миллера рабина
69 }
70 i = 0;
71 while (i != 1)
72 {
73     Randomen(q, 256); //рандомное число определенной длины битов
74     if (Primestest(q, 10) && q != p)
75     {
76         perem_q = q - 3;
77         if (perem_q % 4 == 0)
78         {
79             i = 1;
80             cout << "q=" << q << endl;
81         }
82     } //проверка на простоту числа по тесту миллера рабина
83 }
84 }
85 void encryption(ZZ& n, ZZ& x, ZZ& y, ZZ& c1, ZZ& c2)
86 {
87     int perem;
88     MulMod(y, x, x, n);
89     c1 = x % 2;
90     perem = Jacobi(x, n);
91     if (perem == 1) c2 = 1;
92     if (perem != 1) c2 = 0;
93     cout << endl << endl << "y=" << y << endl;
94     cout << "c1=" << c1 << endl;
95     cout << "c2=" << c2 << endl << endl;
96 }
97 void decryption(ZZ& p, ZZ& q, ZZ& y, ZZ& n)
98 {
99     ZZ s1, s2, u, v, perem, perem1, M1, M2, M3, M4, i, y1, y2;
100     perem = (p + 1) / 4;
101     perem1 = (q + 1) / 4;
102     y1 = y % p;
103     PowerMod(s1, y1, perem, p);
104     cout << "s1=" << s1 << endl;
105     y2 = y % q;
106     PowerMod(s2, y2, perem1, q);
107 }

```

```

95     cout << "c2=" << c2 << endl << endl;
96 }
97 void decryption(ZZ& p, ZZ& q, ZZ& y, ZZ& n)
98 {
99     ZZ s1, s2, u, v, perem, perem1, M1, M2, M3, M4, i, y1, y2;
100     perem = (p + 1) / 4;
101     perem1 = (q + 1) / 4;
102     y1 = y % p;
103     PowerMod(s1, y1, perem, p);
104     cout << "s1=" << s1 << endl;
105     y2 = y % q;
106     PowerMod(s2, y2, perem1, q);
107     cout << "s2=" << s2 << endl;
108     XGCD(i, u, v, p, q);
109     u = u * p % s2;
110     v = v * q % s1;
111     u = u % n;
112     v = v % n;
113     M1 = u + v;
114     M1 = M1 % n;
115     cout << "M1=" << M1 << endl;
116     M2 = u - v;
117     M2 = M2 % n;
118     cout << "M2=" << M2 << endl;
119     M3 = v - u;
120     M3 = M3 % n;
121     cout << "M3=" << M3 << endl;
122     M4 = (u + v) % (-1);
123     M4 = M4 % n;
124     cout << "M4=" << M4 << endl;
125 }
126 void podpis(ZZ& x, ZZ& n, ZZ& s, ZZ& p, ZZ& q)
127 {
128     ZZ s1, s2, u, v, perem, perem1, M1, M2, M3, M4, i, y1, y2, x1;
129     perem = (p + 1) / 4;
130     perem1 = (q + 1) / 4;
131     y1 = x % p;
132     PowerMod(s1, y1, perem, p);
133     //cout << "s1=" << s1 << endl;
134     y2 = x % q;

```

```

140  u = u % n;
141  v = v % n;
142  M1 = u + v;
143  M1 = M1 % n;
144  //cout << "M1=" << M1 << endl;
145  M2 = u - v;
146  M2 = M2 % n;
147  //cout << "M2=" << M2 << endl;
148  M3 = v - u;
149  M3 = M3 % n;
150  //cout << "M3=" << M3 << endl;
151  M4 = (u + v)*(-1);
152  M4 = M4 % n;
153  //cout << "M4=" << M4 << endl;
154  s = M1;
155  cout << "s=" << s << endl;
156  }
157  void proverka_podpisi(ZZ& x1, ZZ& s, ZZ& n)
158  {
159      MulMod(x1, s, s, n);
160      cout << "x1=" << x1 << endl;
161  }
162  void protokol(ZZ& p, ZZ& q, ZZ& n)
163  {
164      ZZ x, z, y;
165      RandomLen(x, 256);
166      SqrMod(y, x, n);
167      SqrMod(y, y, n);
168      cout << "Alice generate y=" << y << endl;
169      cout << "Alice sent y Bob..." << endl;
170      ZZ s1, s2, u, v, perem, perem1, M1, M2, M3, M4, i, y1, y2;
171      perem = (p + 1) / 4;
172      perem1 = (q + 1) / 4;
173      y1 = y % p;
174      PowerMod(s1, y1, perem, p);
175      y2 = y % q;
176      PowerMod(s2, y2, perem1, q);
177      XGCD(i, u, v, p, q);
178      u = u * p*s2;
179      v = v * q*s1;

```

```

182  M1 = u + v;
183  M1 = M1 % n;
184  cout << "M1=" << M1 << endl;
185  M2 = u - v;
186  M2 = M2 % n;
187  cout << "M2=" << M2 << endl;
188  M3 = v - u;
189  M3 = M3 % n;
190  cout << "M3=" << M3 << endl;
191  M4 = (u + v)*(-1);
192  M4 = M4 % n;
193  cout << "M4=" << M4 << endl;
194  perem = Jacobi(M1, n);
195  if (perem == 1) {
196      z = M1;
197      //cout << "Jacobi(M1, n)=" << perem << endl;
198  }
199  else
200  {
201      perem = Jacobi(M2, n);
202      if (perem == 1) {
203          z = M2;
204          //cout << "Jacobi(M2, n)=" << perem << endl;
205      }
206      else
207      {
208          perem = Jacobi(M3, n);
209          if (perem == 1) {
210              z = M3;
211              //cout << "Jacobi(M3, n)=" << perem << endl;
212          }
213          else
214          {
215              perem = Jacobi(M4, n);
216              if (perem == 1) z = M4;
217              //cout << "Jacobi(M4, n)=" << perem << endl;
218          }
219      }
220  }
221  }

```

```

290
291 int main()
292 {
293     ZZ n, p, q, x, m, r, peremena, peremena1, y, c1, c2, perem, perem1, s, x1, x_alice, y_alice;
294     int l;
295     y = 1;
296     cout << endl << "-----generate_prime-----" << endl;
297     generate_prime(p, q); // генерируем протсые числа
298     n = p * q;
299     cout << "n=" << n << endl; // образуем n
300     l = NumBytes(n);
301     l = 8 * (l - 8);
302     Randomlen(m, 256); cout << "m=" << m << endl;
303     power(peremena1, 2, l); //
304     mul(peremena1, peremena1, 255); //
305     power(peremena, 2, 64); // Процесс генерации второй части сообщения
306     mul(peremena, peremena, m); //
307     add(x, peremena1, peremena);
308     perem = 0;
309     perem1 = 1;
310     while (perem != perem1)
311     {
312         Randomlen(r, 64);
313         add(x, x, r);
314         perem = Jacobi(x, p);
315         if (perem <= 0) perem = 2;
316         perem1 = Jacobi(x, q);
317         if (perem1 <= 0) perem1 = 3;
318     }
319     cout << "Jacobi(x, p) = " << perem << endl;
320     cout << "Jacobi(x, q) = " << perem1 << endl;
321     cout << "x=" << x << endl;
322     cout << endl << "-----encryption-----" << endl;
323     encryption(n, x, y, c1, c2); // Шифруем наше сообщение
324     cout << endl << "-----podpis-----" << endl;
325     podpis(x, n, s, p, q);
326     cout << endl << "-----decryption-----" << endl;
327     decryption(p, q, y, n); // Дешифруем наше сообщение
328     cout << endl << "-----proverka_podpis-----" << endl;
329     proverka_podpis(x1, s, n);

```