Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)
Навчально-науковий інститут інформаційних технологій та робототехніки
(повна назва факультету)
Кафедра комп'ютерних та інформаційних технологій і систем
(повна назва кафедри)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**
**до дипломного проекту (роботи)**
магістра
(освітньо-кваліфікаційний рівень)

на тему

# «АНАЛІЗ СТАНУ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ВДОСКОНАЛЕННЮ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ З ВИКОРИСТАННЯМ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ»

Виконав: студент групи д6ТН

спеціальності 122 Комп'ютерні науки
(шифр і назва напряму)
Пенц Володимир Федорович
(прізвище та ініціали)

Керівник к.т.н.,доц. Брусенцев В.О.
(прізвище та ініціали)

Полтава – 2024 року

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ**

**КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ**

**КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА**
**спеціальність 123 «Комп'ютерна інженерія»**

**на тему**

# «АНАЛІЗ СТАНУ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ВДОСКОНАЛЕННЮ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ З ВИКОРИСТАННЯМ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ»

**Студента групи д6ТН Пенца Володимира Федоровича**

Керівник роботи
кандидат технічних наук, доцент
Брусенцев В.О.

Завідувач кафедри
кандидат фізико-математичних наук,
Двірна О. А.

Полтава – 2024

# РЕФЕРАТ

Пояснювальна записка містить: 66 сторінок, 27 малюнків, 9 таблиць, 24 джерел.

**Об’єкт дослідження:** аналіз стану та розробка рекомендацій по вдосконаленню системи захисту інформації на підприємстві з використанням криптографічних алгоритмів.

**Мета роботи:** проаналізувати стан та розробити рекомендації щодо систем комплексного захисту інформації на підприємстві та розробка системи шифрування файлів та повідомлень.

**Методи:** аналіз стану та розробка рекомендацій по вдосконаленню системи захисту інформації на підприємстві з використанням криптографічних алгоритмів.

**Ключові слова:** захист інформації, інформаційна безпека, безпека інформації, комплексні методи захисту інформації, методи захисту інформації, криптографія, криптологія, крипоаналітика.

# ABSTRACT

The explanatory note contains: 66 pages, 27 figures, 9 tables, 24 sources.

**Object of research**: analysis of the state and development of recommendations for improving the information protection system at the enterprise using cryptographic algorithms.

**Purpose of work**: to analyze the state and develop recommendations for comprehensive information protection systems at the enterprise and develop a file and message encryption system.

**Methods**: analysis of the state and development of recommendations for improving the information protection system at the enterprise using cryptographic algorithms.

**Keywords**: information protection, information security, information security, comprehensive information protection methods, information protection methods, cryptography, cryptology, cryptanalysis.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

**ІБ –** Інформаційна безпека.

**ЗІ –** Захист інформації.

**СЗІ –** Системи захисту інформації.

**ІС –** Інформаційна система.

**ІБ –** Інформаційна безпека.

**ДТ** – Державна таємниця.

**СУІБ** – Система управління інформаційною безпекою.

**СУБД** – Система управління базами даних.

**ПЗ** – Програмне забезпечення.

**ПК** – персональний комп’ютер.

# ВСТУП

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації. З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних жертв, у тому числі й людським. Тому конфіденційності (тобто нерозголошенню інформації) в перших системахбезпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування. Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням сьогодні стає захист інформації в комп'ютерних мережах. Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будьякої діяльності.

Принцип сучасного захисту інформації можна виразити так - пошук оптимального співвідношення між доступністю й безпекою. Повністю захищений комп'ютер - це той, який знаходиться під замком у броньованій кімнаті в сейфі, не підключений ні до якої мережі (навіть електричної) і виключений. Такий комп'ютер має абсолютний захист, однак використати його не можна. У цьому прикладі не виконується вимога доступності інформації. "Абсолютності" захисту заважає не тільки необхідність користуватися захищеними даними, але й ускладнення систем, що захищають. [1]

# РОЗДІЛ 1
# РОЗГЛЯД ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПОСТАНОВКА ЗАДАЧІ

## 1.1 Основні поняття, що до захисту інформації

«За́хист інформа́ції — сукупність методів і засобів, що забезпечують цілісність, конфіденційність, доступність і спостереженість інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації».-[2]

«Цілісність — неможливість модифікації інформації неавторизованим користувачем» - [2].

«Конфіденційність — інформація не може бути отримана неавторизованим користувачем» - [2].

«Доступність — полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого інтервалу часу» - [2].

«Спостережність – це властивість інформації, яка полягає в тому, що процес її обробки має безперервно знаходитись під контролем органу, що керує захистом» - [2].

«Загроза – це потенційно можлива несприятлива дія на інформацію, що призводить до порушень хоча б однієї з наведених властивостей» - [2].

**Засоби захисту інформації**

«Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у декілька груп:

- законодавчі;
- організаційні;
- технічні;
- апаратні;

- програмні;
- морально-етичні» - [2].

**«Законодавчі засоби захисту** — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення» - [2].

**«Організаційні засоби захисту** інформації регламентують управління доступом до інформації, діяльністю персоналу, а також порядоком взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки» - [2].

**«Технічні засоби захисту** — це різного роду механізми, спорудження і матеріали, призначені для захисту від несанкціонованого фізичного доступу» - [2].

**«Апаратні засоби захисту** — це фізичні пристрої та компоненти, які забезпечують безпеку інформаційних систем на апаратному рівні» - [2].

**«Програмні засоби захисту** забезпечують автентифікації та авторизацію користувачів, криптографічний захист інформації, захист від комп'ютерних вірусів та інші види захисту на рівні програм» - [2].

**«Морально-етичні засоби захисту** — норми поведінки, які традиційно склались в компанії. Ці норми мають рекомендаційних характер і не затверджені в законодавчому порядку. Морально-етичні норми бувають як неписаними, так і оформленими в деякі письмові рекомендації» - [2].

«Отже захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації» - [1].

**«Інформація** – це результат відображення та обробки в людській свідомості різноманіття навколишнього світу, відомостей про предмети, що оточують людину, явища природи, діяльність інших людей і т.д. Технічний захист інформації – охоплює організацію, розробку, впровадження та функціонування технічних методів та засобів захисту інформації, але не

шляхом шифрування. Криптографічний захист інформації – охоплює організацію, розробку, впровадження та функціонування криптографічного захисту інформації» - [1].

**«Інформаційна безпека** – багатогранна, можна навіть сказати, багатовимірна область діяльності, в якій успіх може принести тільки систематичний, комплексний підхід» - [2].

«Інформаційна безпека представляє собою складну та многогранну сферу, де успіх можливий лише завдяки систематичному та комплексному підходу.

Суб'єкти, які використовують інформаційні системи, мають різні цілі та інтереси, які можна поділити на такі категорії: забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів та інфраструктури, що її підтримує» [2].


Рисунок.1.1 Основні складові інформаційної безпеки

«Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. [4] Із цього погляду основними випадками порушення безпеки інформації можна назвати такі:

- несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в 1С правил розмежування доступу; [4]

- витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї; [4]
- втрата інформації — дія, внаслідок якої інформація в 1С перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі; [4]
- підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в 1С; [4]
- блокування інформації — дії, наслідком яких є припинення доступу до інформації; [4]
- порушення роботи ІС — дії або обставини, які призводять до спотворення процесу обробки інформації. Причини настання зазначених випадків такі: збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо); [4]
- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо); [4]
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1С, спричинення витоку інформації); [4]
- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо); [4]

- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією)» - [4].

Починаючи з 1992 року, основні зусилля з організації заходів у сфері інформаційної безпеки докладались Міністерством оборони США в рамках концепції “Інформаційного протиборства”, що орієнтована на вирішення завдань боротьби з системами управління воєнними силами супротивника на різноманітних рівнях і забезпечення безпеки та ефективності інформаційних систем армії США. Подальший розвиток ця концепція отримала в 1996 році у вигляді польового статуту армії США “Інформаційні операції”. В цілому ж початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати директиви адміністрації президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) “Захист критично важливої інфраструктури” 1998 року. На цьому документі базується підписаний Б. Клінтоном на початку 2000 року Загальнонаціональний план захисту інформаційних систем, який визначає основні напрями діяльності держави та всього суспільства у сфері забезпечення інформаційної безпеки. Також у лютому 2003 року адміністрацією Джорджа Буша молодшого була опублікована Національна стратегія досягнення безпеки в кіберпросторі (National Strategy to Secure Cyberspace), в якій викладено п’ять пріоритетів діяльності США із забезпечення інформаційної безпеки та основних завдань у рамках цих пріоритетів на середньострокову та довгострокову перспективу. Фактично ці документи можуть вважатися офіційною загальнонаціональною політикою США у сфері інформаційної безпеки, на основі якої будується система діяльності державної влади та структура державних органів, які забезпечують інформаційну безпеку в державі. Відповідно до стратегії інформаційної безпеки основними державними пріоритетами у цій сфері є: Становлення та розвиток національної системи реагування на події у сфері інформаційної безпеки. Реалізація комплексної системи заходів із зменшення загроз інформаційної безпеки. Забезпечення підготовки спеціалістів у сфері

комп’ютерної безпеки та відповідального ставлення всього населення до питань захисту інформації. Забезпечення захисту інформаційних систем, які мають відношення до державних органів. Розвиток різних форм кооперації (у тому числі й міжнародних) у сфері забезпечення інформаційної безпеки [5].

**Законодавча база захисту інформації.** В Україні існує певна кількість законодавчих актів пов'язаних з інформацією та з її захистом яка стосується даної фірми:

- Закон України «Про інформацію»;
- Закон України "Про доступ до публічної інформації"
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (договір про нерозголошення);
- Закон України «Про державну таємницю»;
- Закон України про Національну програму інформатизації;
- Закон України «Про захист персональних даних» (політика конфіденційності);
- Закон України «Про авторське право і суміжні права» (інтелектуальна власність);
- Закон України «Про охорону праці» (політика охорони праці та техніки безпеки);
- також сюди відносяться внутрішні накази та розпорядження компанії.

«Закон України «Про інформацію» встановлює, що кожен має право на вільне одержання, використання, поширення, зберігання та захист інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб» - [4].

«Закон України «Про доступ до публічної інформації» визначає порядок здійснення та забезпечення права кожного на доступ до інформації, яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників

публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес» - [4].

«Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює правовідносини, пов'язані із захистом інформації, яка обробляється в інформаційно-телекомунікаційних системах. Він визначає основні принципи захисту інформації, права та обов'язки власників, користувачів інформації. Метою цього закону є забезпечення конфіденційності, цілісності та доступності інформації в умовах використання автоматизованих систем. Відповідно до цього закону складається договір про нерозголошення» - [5].

«Закон України «Про доступ до публічної інформації» – визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес» - [6].

«Закон України «Про державну таємницю» визначає, які відомості є державною таємницею, і встановлює правила їхнього захисту. Доступ до такої інформації надається лише особам з відповідним рівнем допуску, а її розголошення може завдати шкоди національній безпеці. Закон передбачає відповідальність за порушення правил охорони державної таємниці» - [7].

«Закон України «Про Національну програму інформатизації» регулює процес розробки та реалізації національної програми, спрямованої на розвиток інформаційного суспільства в Україні. Основна мета закону – створення умов для ефективного використання інформаційних ресурсів для розвитку економіки, науки, освіти, культури та інших сфер суспільного життя» - [8].

«Політика конфіденційності – Закон України «Про захист персональних даних», який регулює порядок збирання, обробки, зберігання та захисту персональних даних фізичних осіб. Політика повинна інформувати клієнтів про їхні права, мету збору даних і заходи безпеки, які використовуються для захисту їх персональної інформації» - [9].

«Інтелектуальна власність – Закон України «Про авторське право і суміжні права». Підзаконний акт, який регулює питання авторського права на створені дизайни, візуальні продукти та інші інтелектуальні продукти компанії. Він повинен дотримуватися положень Закону України "Про авторське право і суміжні права" і визначати, хто володіє правами на результати творчої діяльності: компанія чи співробітники» - [10].

«Політика охорони праці та техніки безпеки – Закон України «Про охорону праці». Цей підзаконний акт регулює питання безпеки на робочому місці, заходи щодо захисту здоров'я працівників, а також дотримання вимог Закону України "Про охорону праці". Він визначає правила використання обладнання та робочих місць, а також порядок дій у разі нещасних випадків» - [11].

**Зарубіжні законодавчі акти щодо ЗІ**

«Захист інформації є проблемою не лише національного, але й міжнародного масштабу, що вимагає спільних зусиль та стандартів. У світі існує ряд міжнародних законодавчих актів, які регулюють захист інформації у різних аспектах.

Одним з найважливіших міжнародних документів є Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, що була прийнята Радою Європи в 1981 році. Ця Конвенція встановлює загальні принципи та правила захисту персональних даних, які обробляються з використанням інформаційних технологій. Вона також передбачає міжнародне співробітництво та контроль у цій сфері» - [4].

«Іншим важливим міжнародним документом є Конвенція про кіберзлочинність, що була прийнята Радою Європи в 2001 році. Ця Конвенція є першим міжнародним договором, який визначає кримінальну відповідальність за різні види злочинів, що скоюються в кіберпросторі, такі як незаконний доступ, пошкодження даних, порушення авторських прав, дитяча порнографія, шахрайство тощо. Конвенція також містить положення про міжнародну

правову допомогу та співробітництво у розслідуванні та попередженні кіберзлочинів» - [4]

Ці та інші міжнародні законодавчі акти щодо захисту інформації спрямовані на гармонізацію правового режиму інформації, забезпечення її безпеки, конфіденційності та цілісності, а також сприяють міжнародному діалогу та співробітництву у цій сфері. [4]

## 1.2 Вірусні загрози та боротьба з ними.

**«Комп'ютерний вірус** — комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макровіруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. [7] Розробники вірусного програмного забезпечення використовують засоби соціальної інженерії і інформацію про вразливості цільового ПЗ, щоб заражати системи і розповсюджувати вірус. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ - програми-шпигуни чи навіть спам» - [7].

«За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363). Приклади вірусів: Neshta, Staog, Archiveus» - [7].

**«Прийнято розділяти віруси за:**

- об'єктами, які вражаються (файлові віруси, завантажувальні віруси, анти-антивірусні віруси, скриптові віруси, макровіруси, мережеві черв'яки);

- способом зараження (перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси, віруси, що вражають вихідний код програм);
- операційними системами і платформами, які вражаються (DOS, Microsoft Windows, Unix, Linux, інші);
- активністю (резидентні віруси, нерезидентні віруси);
- технологіями, які використовуються вірусом (нешифровані/шифровані віруси, поліморфні віруси, стелс-віруси (руткіт і буткіт);
- деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси);
- мовою, якою написаний вірус (асемблер, високорівнева мова програмування, скриптова мова, інші). [7]

Здебільшого, все це в минулому. Зараз основні ознаки — самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус» - [7].

**«Антивірусні програми діляться на певні типи:**

1 Програми-детектори – ті, які допомагають знайти віруси в оперативній пам'яті або ж на носіях інформації, при цьому програми-детектори знайдені віруси не лікують [7].

2 Програми-доктора – програми, які на відміну від попереднього виду, не тільки знаходять вірус, але і лікують заражений файл, повертаючи його в початковий стан [7].

3 Програми-ревізори – такі програми мають властивість запам'ятовувати файл або системну область диска в його початковому стані, і пізніше порівнювати поточний стан з вихідним. При порівнянні файлу враховуються багато параметрів файлу, тому сховатися вірусу такі програми не залишають шансу [7].

4 Програми-фільтри – призначені для виявлення підозрілих дій в роботі комп'ютера. При спробі активізації вірусу програма може блокувати його роботу [7].

5 Вакцини – такі програми, які відразу запобігають зараженню різних файлів. Варто застосовувати такі програми, якщо програми-доктора відсутні. Але варто врахувати, що «вакцинація» можлива тільки проти вже відомих вірусів» - [7] .

## 1.3 Постановка задачі

**Об’єкт дослідження:** аналіз стану та розробка рекомендацій по вдосконаленню системи захисту інформації на підприємстві з використанням криптографічних алгоритмів.

**Мета роботи:** проаналізувати стан та розробити рекомендації щодо систем комплексного захисту інформації на підприємстві та розробка системи шифрування файлів та повідомлень.

**Методи:** аналіз стану та розробка рекомендацій по вдосконаленню системи захисту інформації на підприємстві з використанням криптографічних алгоритмів.

На основі законодавчих бази України необхідно розробити систему захисту інформації на підприємстві. Для цього необхідно розробити:

1. Організаційні засоби захисту інформації;
   - мандатна модель доступу Бела – Лападули;
   - матриця доступу;
   - засоби доступу до інформації.
2. Технічні апаратні і програмні засоби інформації.
3. А також розробити програму криптографічного захисту на основі шифрування Triple DES, де є можливість зашифрувати та дешифрувати інформацію та файли.

# РОЗДІЛ 2
# РОЗРОБКА СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

## 2.1 Загальні відомості про підприємство

**SPHERE** – IT компанія, що спеціалізується на Розроці програмного забезпечення та web-дизайні.

Сайт: https://www.sphere.com

Адреса:м. Полтава вул. Котляревського 2

Тел. +3809888*****

Рисунок 2.1 – Загальний вигляд логотипу підприємства

Використовуючи багаторічний досвід у сфері просування сайтів, ми вивели в ТОП пошукових систем тисячі запитів. Приклади та відгуки про пошукове просування у висококонкурентних нішах ви можете побачити на нашому сайті. https://www.sphere.com

Створені нами сайти багато років успішно працюють, сприяючи ефективному розвитку бізнесу наших клієнтів.

Наші сертифіковані спеціалісти виконають професійне налаштування контекстної реклами, завдяки чому ви отримуєте зацікавлених клієнтів вже першого дня після запуску рекламних кампаній.

І ще багато цікавих та корисних рішень для вашого бізнесу на нашому сайті https://www.sphere.com

**Розробка сайтів**

Ми створимо сучасний, індивідуальний, красивий, що презентує ваші вигоди сайт, побудований по вирві продажів, із зручною функціональною адмін панеллю, на який дорівнюватимуть конкуренти. Час створення 1 місяць. За потреби сайт можна створити і швидше, питання обговорюється окремо.

**SEO**

Просування сайту за запитами, що цікавлять, на першій сторінці (ТОП-10) органічної видачі пошукових систем. За статистикою переважна частина комерційно орієнтованих відвідувачів приходить на сайт із пошукових систем. Також 95% користувачів довіряють і роблять покупки на першій сторінці пошукових систем (ТОП-10). Завдяки якісній оптимізації сайт буде знаходитися в ТОП-10 Google і Яндекс, за необхідними ключовими словами, і залишиться там кілька років, навіть якщо припинити роботи, збільшитися відвідуваність сайту, піде постійний цільовий трафік споживача на сайт і з'являться нові клієнти.

**Контекстна реклама в GOOGLE ADS**

Найпотужніший інструмент швидкого залучення нових клієнтів у бізнес! РК дозволить сайту, за багатьма оголошеннями, вже завтра бути на першій сторінці (у ТОПі). Допоможе збільшити обсяги інтернет-продажів, кількість дзвінків до офісу, залучити нових відвідувачів на сайт та сформувати постійну аудиторію. Створимо групу оголошень з унікальними торговими пропозиціями за інтересами кінцевого споживача на підставі частотності та конкуренції ключових слів, що вбиваються. Багато ваших конкурентів вже давно налаштували та користуються цим каналом залучення клієнтів (достатньо подивитися видачу за запитами). Вони щодня борються і забирають тих клієнтів, хто вже сьогодні потребує ваших послугах/товарах, і готовий купувати, себе.

**Банерна реклама**

Ремаркетинг - це інструмент взаємодії з вашими користувачами повторно, всі, хто перейдуть з будь-якого каналу до вас на сайт, бачитимуть у пошуку або на сайтах партнерах вашу націлену банерну рекламу (з закликами, вигодами, знижками), що мотивує користувачів, які не визначилися, зробити замовлення у вас, а не у конкурентів. Контекстно-медійна мережа Google дозволяє звертатися до потенційних клієнтів, коли вони переглядають улюблені сайти або відео на

YouTube, перевіряють пошту в Gmail або використовують мобільні сайти та програми тощо.

**Таргетинг**

На даний момент сумарна унікальна аудиторія Instagram та Facebook в Україні понад 11 мільйонів активних користувачів та постійно зростає. Понад 60% користувачів використовують Instagram та Facebook щодня. Сенс її – у показі реклами велику кількість користувачів на їхніх гаджетах, у певному регіоні. Після налаштування, через 3-5 днів реклама показуватиметься десяткам чи сотням тисяч людей у стрічці Instagram та Facebook за заданими параметрами, стать, вік, регіон.

**Просування і розкрутка профілю**

Розкрутка - це не банальна купівля ботів, а продумана стратегія на місяці вперед, яка дає якісного теплого або гарячого передплатника та сарафан надовго. Ми збільшимо кількість цільових передплатників вашого облікового запису, створюючи та додаючи унікальний, привабливий та потрібний контент, заздалегідь продумуючи стратегію. Наші фахівці знайдуть Цільову Аудиторію – по необхідному регіону, захопленням, хеш-тегам, майданчикам, видом діяльності. Під кожною фотографією застосовуватимемо правильні хеш-теги. Ми будемо створювати списки передплатників інших облікових записів, які займаються різною діяльністю, і робитимемо систематичну підписку на них. Проводитимемо рекламу облікового запису в тематичних пабликах з великою кількістю передплатників. Щоденний моніторинг облікового запису. Весь контент, що додається, може дублюватися в facebook.

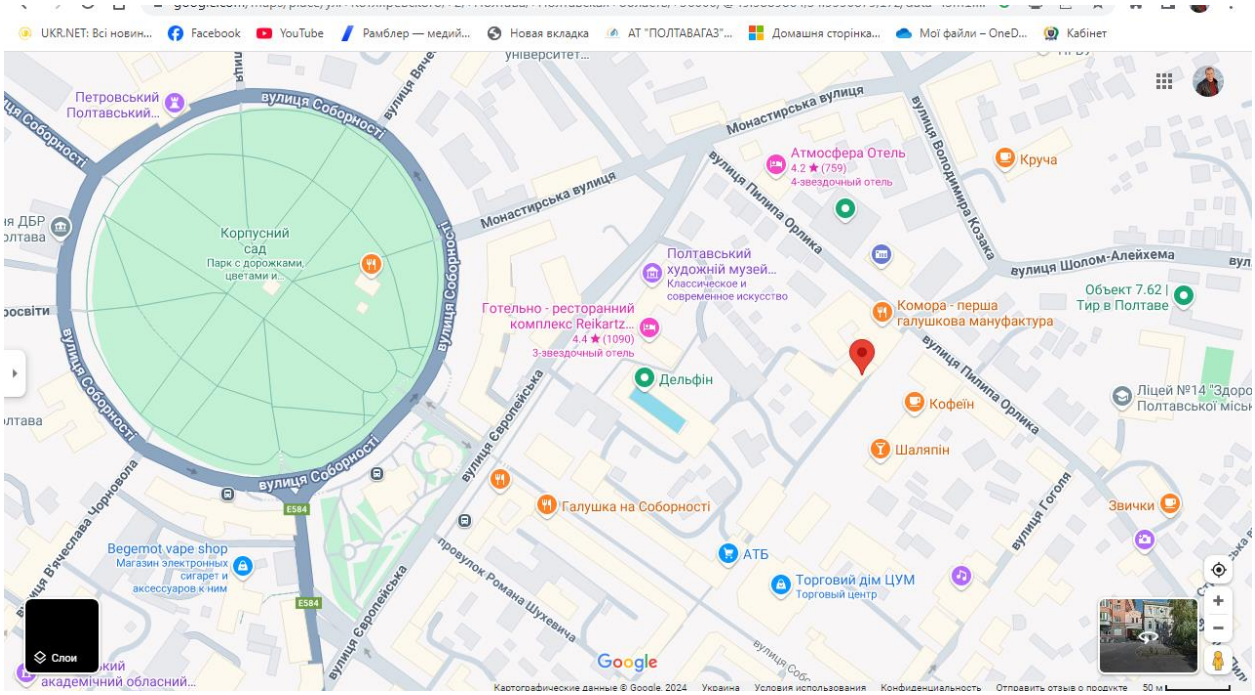



Рисунок 2.2 –Місцезнаходження офісу «SPHERE»

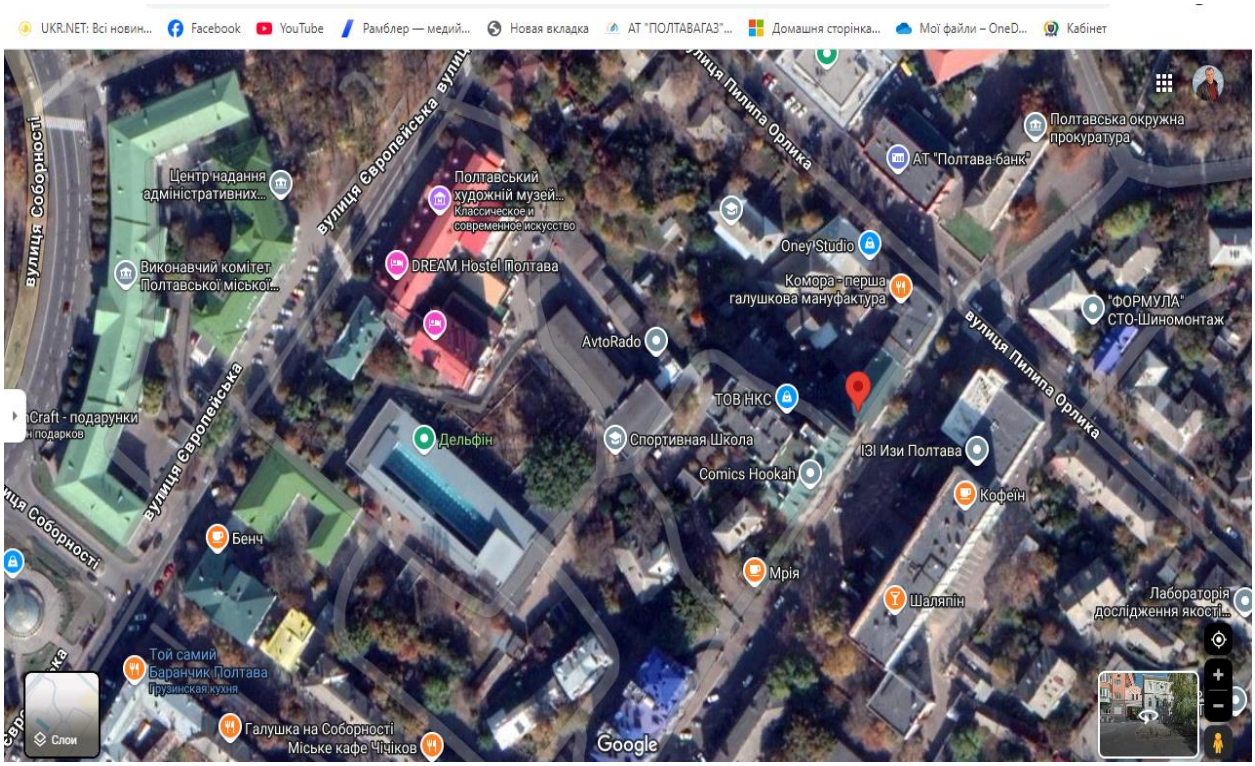



Рисунок 2.3 –Місцезнаходження офісу (2) «SPHERE»

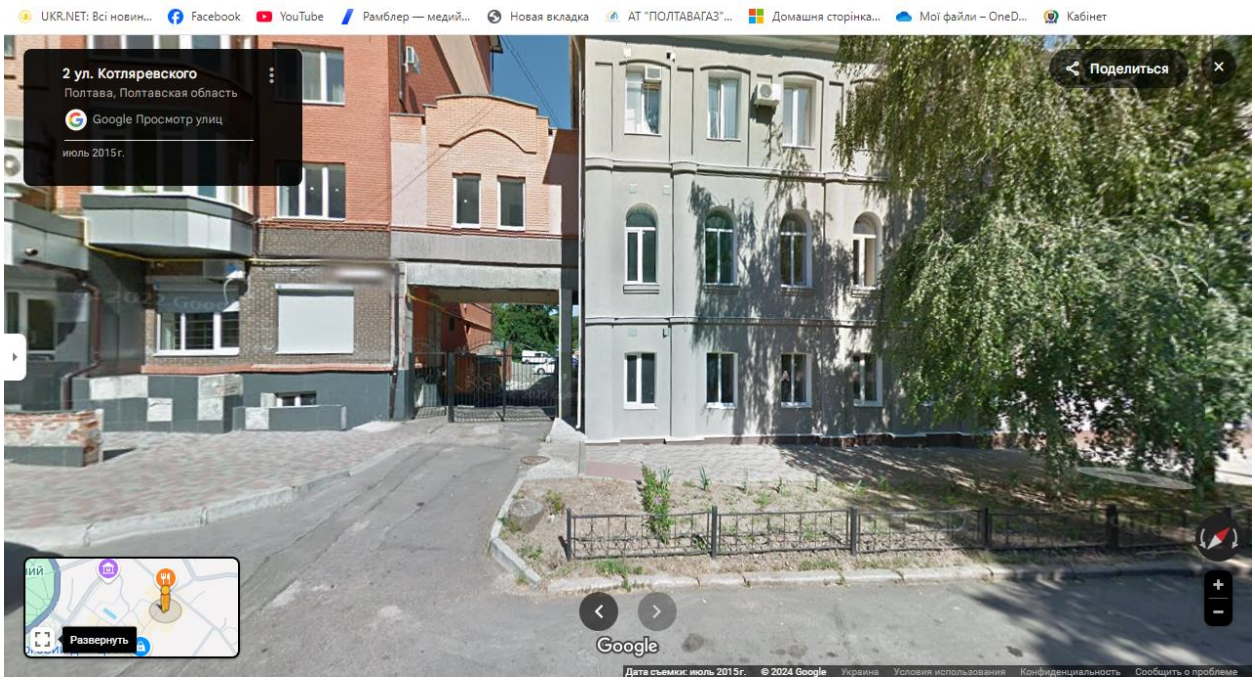



Рисунок 2.4 – Загальний вигляд офісного приміщення підприємства «SPHERE»

Рисунок 2.5 – Загальний вигляд робочих місць підприємства «SPHERE»

Рисунок 2.6 – Загальний вигляд робочих місць підприємства «SPHERE»

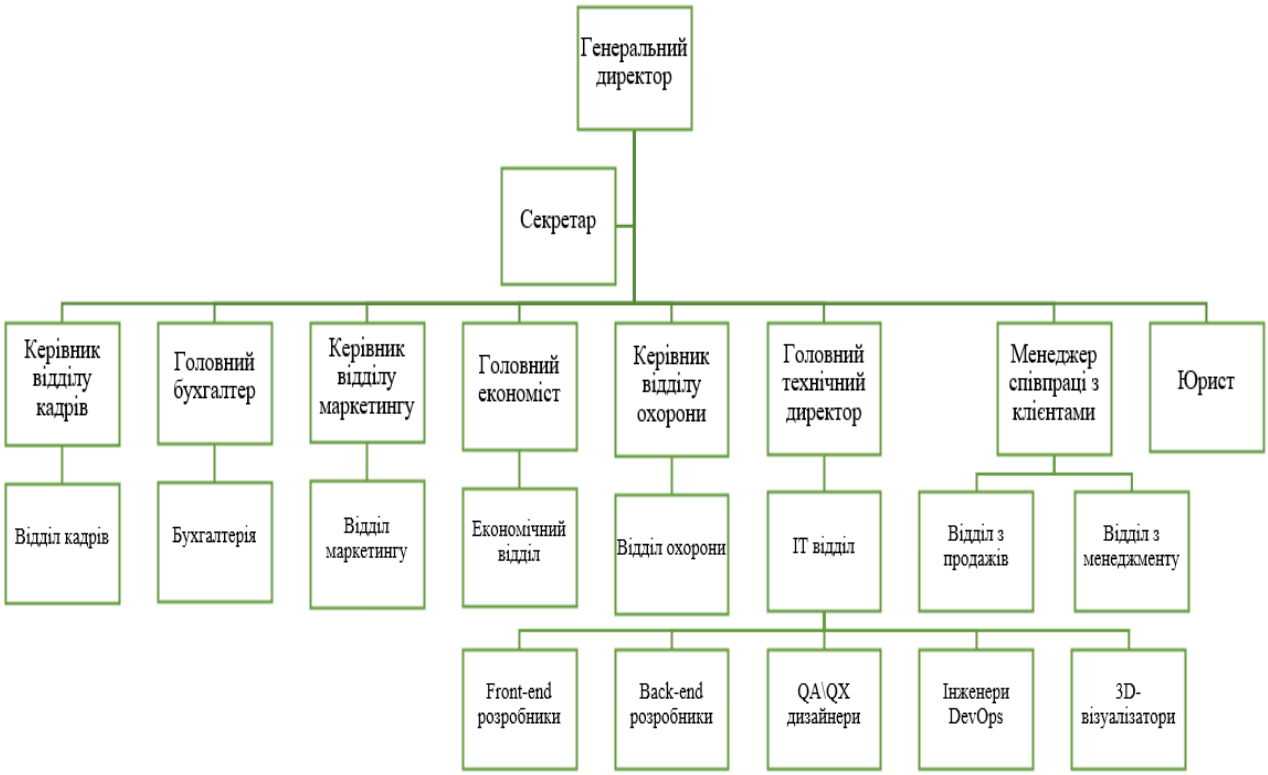



Рисунок 2.7 – Організаційна структура підприємства «SPHERE»

**Схематичний план будівлі**

Офіс компанії Sphare містить 2 поверхи. Перший з яких містить 14 одиниць моноблоків та 6 принтерів. Другий поверх містить 25 одиниць моноблоків та 4 одиниці принтерів. Тобто загально компанія володіє 39 комп’ютерами, що пов’язані мережею. Офіс компанії з двох поверхів складає 312 м$^2$. Також зазначений фасад будівлі.


Рисунок 2.8 – План першого поверху будівлі та розміщення техніки у ньому

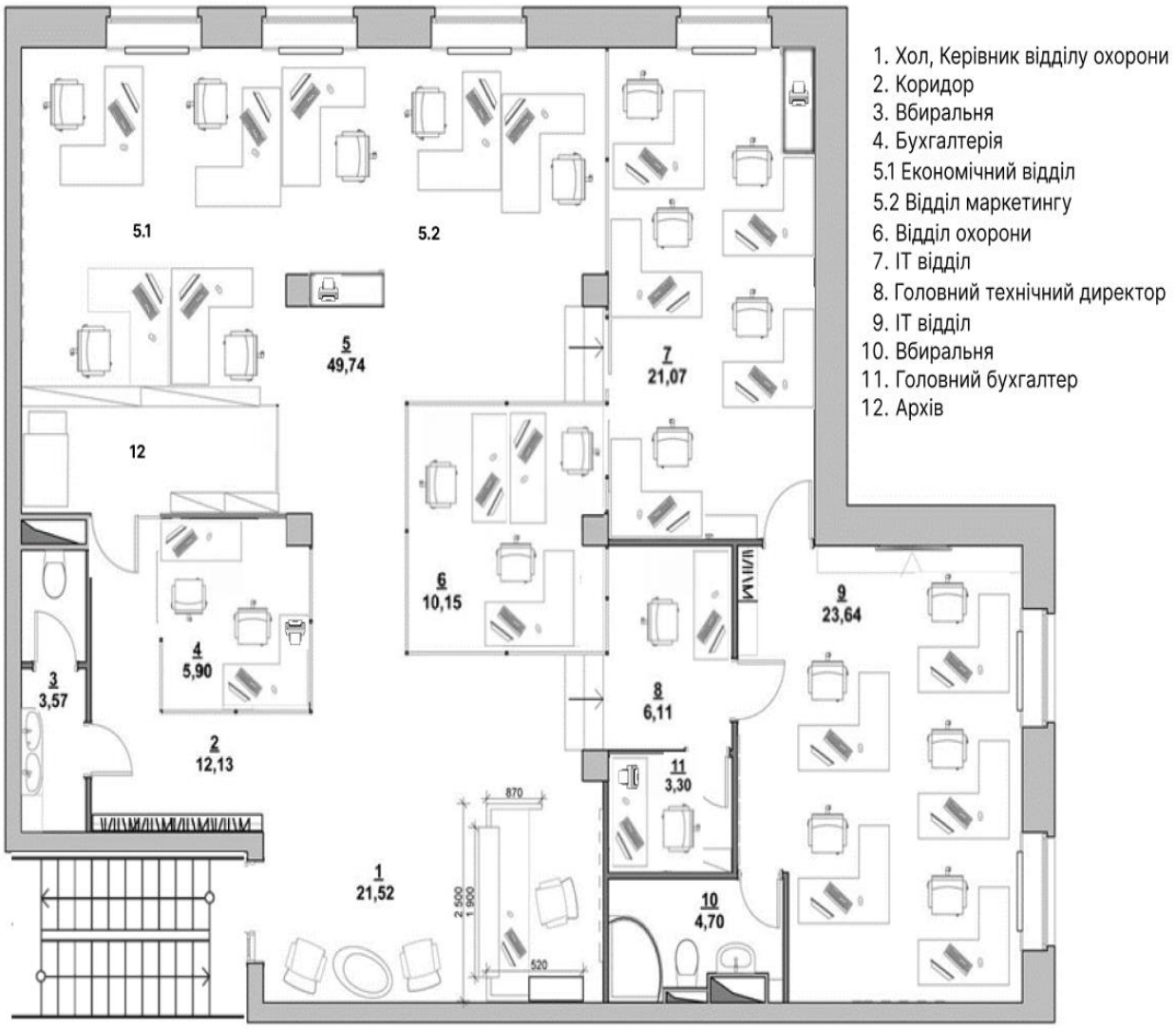



Рисунок 2.9 – План другого поверху будівлі та розміщення техніки у ньому

## 2.2. Вимоги до організації захисту інформації

**Керуючись постановою Кабінету міністрів України № 373**. «Потрібно виконувати наступні вимоги до забезпечення захисту інформації в системі:

1. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення [15].

2. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження [15].

3. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися [15].

4. Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [15].

5. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися [19].

6. У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки службової інформації або позбавлення його такого права [15].

7. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються розпорядником інформації, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством [15].

8. Порядок підключення систем, в яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається законодавством» - [15].

9. Згідно вимоги до забезпечення захисту інформації в системі було створено матрицю доступу (Табл. 2.1) для наочного зображення доступу до інформації у кожного з користувачів.

## 2.3 Розмежування доступу

Розмежування доступу полягає в тому, щоб кожному зареєстрованому користувачу надати можливість доступу до інформації в межах його повноважень. Для кожного користувача встановлюються його повноваження щодо файлів, каталогів.

Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів комп’ютерної системи, а елементами матриці виступають дозволені або заборонені режими доступу. [12]

У моєму прикладі, матриця доступу є таблицею, що використовується для визначення прав доступу різних відділів або користувачів до певних типів інформації у системі. У цій таблиці кожен рядок представляє відділ або користувача, а кожен стовпець – вид інформації (загальна, особиста, фінансова). Символи «+» та «-» вказують, чи має конкретний відділ доступ до певної інформації. Якщо є «+», доступ дозволений, а якщо «-», доступ заборонений. Це допомагає контролювати, хто і до яких ресурсів або даних може отримувати доступ. Також зазначено рівень секретності інформації у кожному відділі: нетаємна, таємна, для службового користування. Таємна інформація – це найвищий доступ, нетаємна – може використовуватися за межами компанії, для службового користування – частковий доступ до важливої інформації певним особам чи відділам.

Матриця доступу (Табл. 2.1) є загальним зображенням доступу в компанії. Натомість модель Бела – ЛаПадули (Табл. 2.2) є більш точною.

«Модель Бела – ЛаПадули – модель контролю та керування доступом, яка заснована на мандатній моделі керування доступом. У моделі аналізуються умови, при яких неможливе утворення інформаційних потоків від суб'єктів з вищим рівнем доступу до суб'єктів з нижчим рівнем доступу» - [13].

У таблиці з моделлю Бела – ЛаПадули визначаються види інформації для кожного відділу чи особи за такими параметрами як: читання, частковий доступ, немає доступу та повний доступ.

Таблиця 2.1 – Рівні таємності підприємства

| **Гриф секретності** | **Інформація** |
|---|---|
| Несекретно | Довідкова технічна інформація |
| Для службового користування | Комерційна інформація |
| Інформація з обмеженим доступом | Сховище керівництва, сховище бухгалтерії, персональні дані працівників |
| Секретно | Угоди, банківські рахунки, фонд заробітної плати |
| Абсолютно секретно | Розробки конструкторського бюро, банківські рахунки, патенти |

Таблиця 2.2 – Матриця доступу

| **Види інформації** / **Відділи** | **Загальна інформація** | **Особиста інформація** | **Фінансова інформація** | **Економічна інформація** | **Правова інформація** | **Технічна інформація** |
|---|---|---|---|---|---|---|
| Генеральний директор | + | + | + | + | + | + |
| Секретар | + | - | - | - | - | - |
| Керівник відділу кадрів | + | + | - | - | + | - |
| Відділ кадрів | + | + | + | - | - | - |
| Головний бухгалтер | + | + | + | - | + | - |
| Бухгалтерія | + | + | + | - | - | - |
| Головний економіст | + | - | - | + | + | - |
| Економічний відділ | + | - | - | + | - | - |
| Відділ маркетингу | + | - | - | - | - | - |
| Керівник відділу охорони | + | - | - | - | + | - |
| Відділ охорони | + | - | - | - | - | - |
| Головний технічний директор | + | + | - | - | + | + |
| ІТ відділ | + | - | - | - | - | + |
| Менеджер співпраці з клієнтами | + | + | - | - | - | + |
| Відділ з продажів | + | - | - | - | - | - |
| Відділ з менеджменту | + | - | - | - | - | - |
| Юрист | + | - | - | - | + | - |
| Рівень секретності інформації | Н | Т | ДСК | ДСК | Т | ДСК |

Н – нетаємна; Т – таємна; ДСК – для службового користування

Модель Белла–ЛаПадули являє собою підхід до контролю доступу, який базується на мандатній моделі. Вона розглядає ситуації, де передача інформації від суб'єктів з вищим рівнем доступу до тих, хто має нижчий рівень, не можлива. Такий метод управління доступом застосовується для баз даних із фіксованою структурою інформації, що характерно для деяких державних та військових організацій. Головна ідея моделі полягає в тому, що кожному інформаційному об'єкту надається певний рівень секретності (наприклад, "Абсолютно секретно", "Секретно", "Для службового користування"), а користувачам присвоюється відповідний рівень доступу, сумісний із цими рівнями секретності. [13]

Таблиця 2.2 – Мандатна модель доступу Бела – ЛаПадули

| **Види інформації** / **Відділи** | **Загальна інформація** | **Особиста інформація** | **Фінансова інформація** | **Економічна інформація** | **Правова інформація** | **Технічна інформація** |
|---|---|---|---|---|---|---|
| Генеральний директор | П | ЧС | Ч | Ч | Ч | Ч |
| Секретар | П | ЧС | Н | Ч | Н | Ч |
| Керівник відділу кадрів | Ч | П | Н | Н | Ч | Н |
| Відділ кадрів | Ч | П | П | Н | Ч | Н |
| Головний бухгалтер | Ч | П | П | ЧС | Ч | Н |
| Бухгалтерія | Ч | Н | П | ЧС | Ч | Н |
| Головний економіст | Ч | Н | Н | П | Н | Н |
| Економічний відділ | П | Н | Н | П | Н | Н |
| Відділ маркетингу | Ч | Н | Н | П | Н | Н |
| Керівник відділу охорони | Ч | Н | Н | Н | Ч | Н |
| Відділ охорони | Ч | Н | Н | Н | Н | Н |
| Головний технічний директор | Ч | Ч | Н | Н | Ч | П |
| ІТ відділ | Ч | Н | Н | Н | Н | П |
| Менеджер співпраці з клієнтами | Ч | ЧС | Н | Н | Н | Н |
| Відділ з продажів | Ч | Н | ЧС | Ч | Н | Н |
| Відділ з менеджменту | Ч | Н | Ч | Н | Н | Н |
| Юрист | Ч | ЧС | Н | Н | П | Н |

Ч – читання;

ЧС – частковий доступ;

Н – немає доступу;

П – повний доступ

«Логування є важливим процесом, який полягає у зборі та збереженні даних про події, що відбуваються в інформаційній системі. Кожен сервіс реєструє свій набір подій, які поділяються на зовнішні, внутрішні та клієнтські. Зовнішні події ініціюються іншими сервісами, внутрішні пов’язані із внутрішніми процесами самого сервісу, а клієнтські викликані діями користувачів або адміністраторів. [14]

Аудит кібербезпеки доповнює логування як системний процес аналізу стану захищеності компанії на основі визначених критеріїв. Його метою є забезпечення об’єктивної оцінки ефективності заходів безпеки. Завдяки поєднанню логування й аудиту можна вирішувати низку важливих завдань.

1. Це контроль за діями користувачів і адміністраторів. Розуміння, що всі дії реєструються, є потужним стримуючим фактором для потенційних порушників. До того ж фіксація кожної дії підозрілих осіб допомагає не лише у розслідуванні інцидентів, а й у відновленні змін, що порушують цілісність даних. [14]

2. Логування дозволяє аналізувати послідовність подій, що є ключовим для виявлення слабких місць у захисті, ідентифікації винних та оцінки завданих збитків. Це також забезпечує можливість відновлення системи до нормального функціонування. По-третє, за допомогою аудиту можна вчасно виявляти спроби порушення безпеки. Активний аудит дозволяє миттєво реагувати на загрози, а періодичний — фіксувати вразливості навіть через певний час. І нарешті, результати логування та аудиту надають цінну інформацію для вдосконалення системи. Це дозволяє усувати вузькі місця в конфігурації, покращуючи загальну доступність сервісів. [14]

Важливу роль відіграє обліковий запис, який є засобом ідентифікації користувачів і надання доступу до персональних налаштувань. Для входу зазвичай потрібні логін і пароль, які зберігаються у зашифрованій або хешованій формі для забезпечення безпеки. Додатково можуть використовуватися методи аутентифікації, такі як ключі доступу, одноразові

паролі або контрольні запитання. Крім того, обліковий запис часто містить додаткові дані, наприклад, ім’я та прізвище користувача» - [14].

Таким чином, логування, аудит та використання облікових записів є ключовими елементами ефективної системи кібербезпеки, що забезпечують захист даних, моніторинг подій та своєчасне реагування на потенційні загрози.

Таблиця 2.3 – Приклад облікових записів користувачів

| **Кабінет** | **Логін(назва комп’ютера)** | **Пароль** |
|---|---|---|
| Генеральний директор | gender | Gender001 |
| Секретар | secret | Secret002 |
| Керівник відділу кадрів | kerviddilkadr | Kerviddilkadr003 |
| Головний бухгалтер | golbuh | Golbuh004 |
| Головний економіст | goleco | Goleco005 |
| Керівник відділу охорони | golprotect | Golprotect006 |
| Головний технічний директор | admin | Admin007 |
| Менеджер співпраці з клієнтами | managcoop | Managcoop008 |
| Відділ кадрів | viddilkadr1 | viddilkadr100 |
| Відділ кадрів | viddilkadr2 | viddilkadr200 |
| Бухгалтерія | buh1 | buh100 |
| Відділ маркетингу | market1 | market100 |
| Економічний відділ | eco1 | eco100 |
| Відділ охорони | protect1 | protect100 |
| Відділ охорони | protect2 | protect200 |
| ІТ відділ | it1 | it100 |
| ІТ відділ | it2 | it200 |
| Відділ з продажів | sales1 | sales100 |
| Відділ з менеджменту | managem1 | managem100 |
| Юрист | yur | Yur001 |

«Обліковий запис користувача є ключовим елементом у сучасних інформаційних системах, що дозволяє ідентифікувати та персоналізувати доступ до ресурсів, даних і послуг. Його створення є невід'ємною складовою будь-якої цифрової платформи, яка забезпечує багаторівневий контроль доступу та конфіденційність. [17]

Основна мета облікового запису — надати користувачу унікальне середовище роботи, де зберігаються його особисті дані, налаштування та історія взаємодії із системою. Зазвичай обліковий запис складається з унікального ідентифікатора (наприклад, ім'я користувача або електронна пошта) та засобів аутентифікації, таких як пароль. [17]

Обліковий запис також є основою для відстеження дій користувача в системі. Адміністратори можуть контролювати, хто має доступ до певних ресурсів, моніторити активність і, при потребі, обмежувати чи скасовувати доступ. Це особливо важливо в корпоративному середовищі, де безпека даних є пріоритетом. [17]

З іншого боку, обліковий запис може стати об’єктом атак, якщо не дотримуватися базових правил безпеки. Використання слабких паролів, відсутність багатофакторної автентифікації чи невчасне оновлення системи можуть спричинити несанкціонований доступ до облікового запису. Тому важливо використовувати складні паролі, регулярно їх змінювати та активувати додаткові рівні захисту» - [17].

## 2.4 Інженерний підхід до захисту інформації

Встановлення камер спостереження, броньованих дверей, датчиків руху та інших засобів захисту регулюється законами України, спрямованими на забезпечення безпеки, захисту інформації та захисту прав людини. Закон України «Про захист інформації в інформаційно-комунікаційних системах» передбачає технічні та організаційні заходи, серед яких відеоспостереження та системи контролю доступу. Також згідно закону України «Про захист

персональних даних» потрібно повідомити про ведення відеоспостереження. Закон України «Про охорону праці» забезпечує безпечні умови праці, що можуть включати інсталяцію засобів безпеки, таких як датчики руху та броньовані двері.

Офіс компанії Sphare містить 2 поверхи. Перший з яких містить 14 одиниць моноблоків та 6 принтерів. Другий поверх містить 25 одиниць моноблоків та 4 одиниці принтерів. Тобто загально компанія володіє 39 комп’ютерами, що пов’язані мережею.

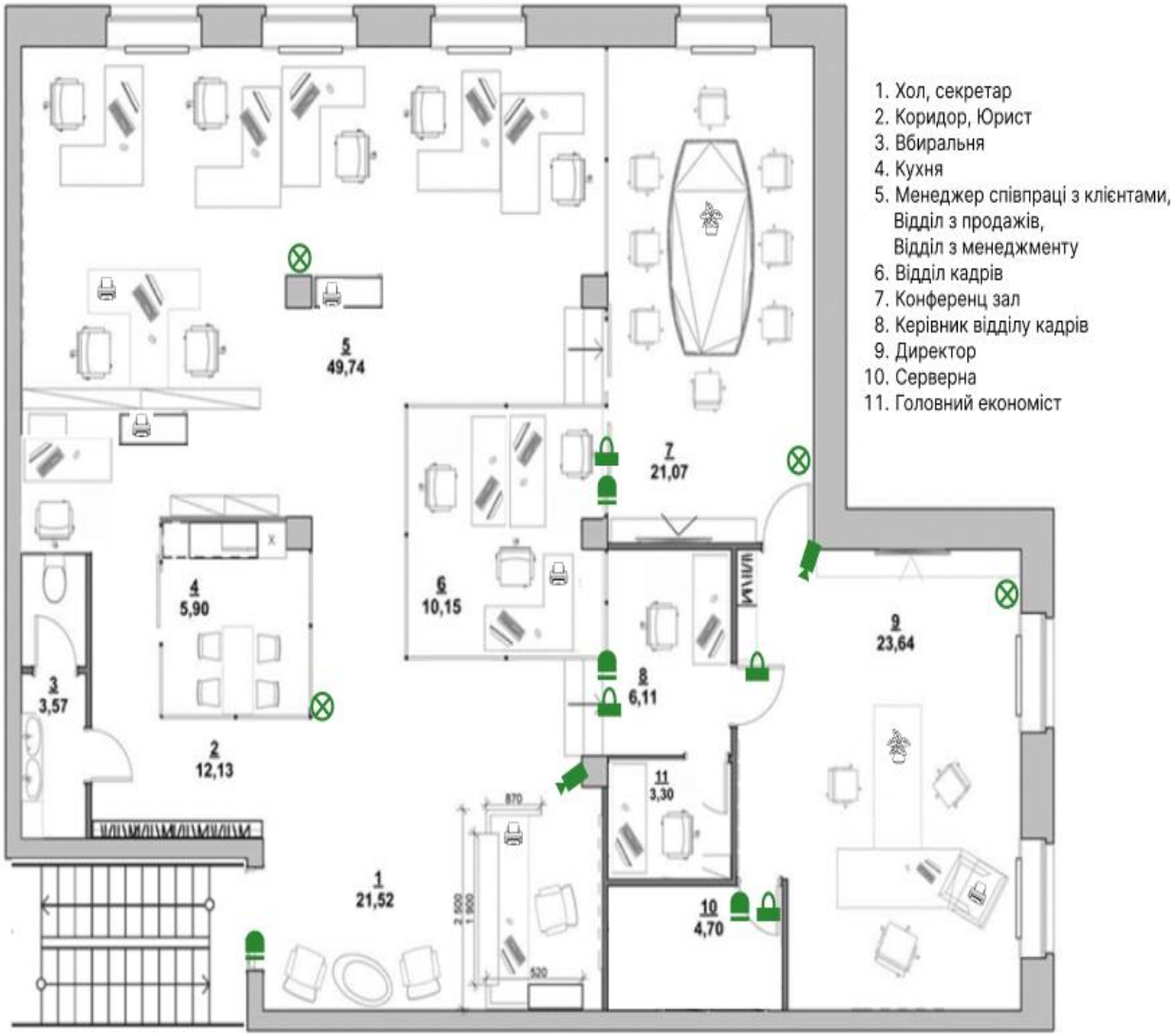



Рисунок 2.10 – План першого поверху будівлі з позначенням засобів доступу до відділів та розміщення техніки у ньому

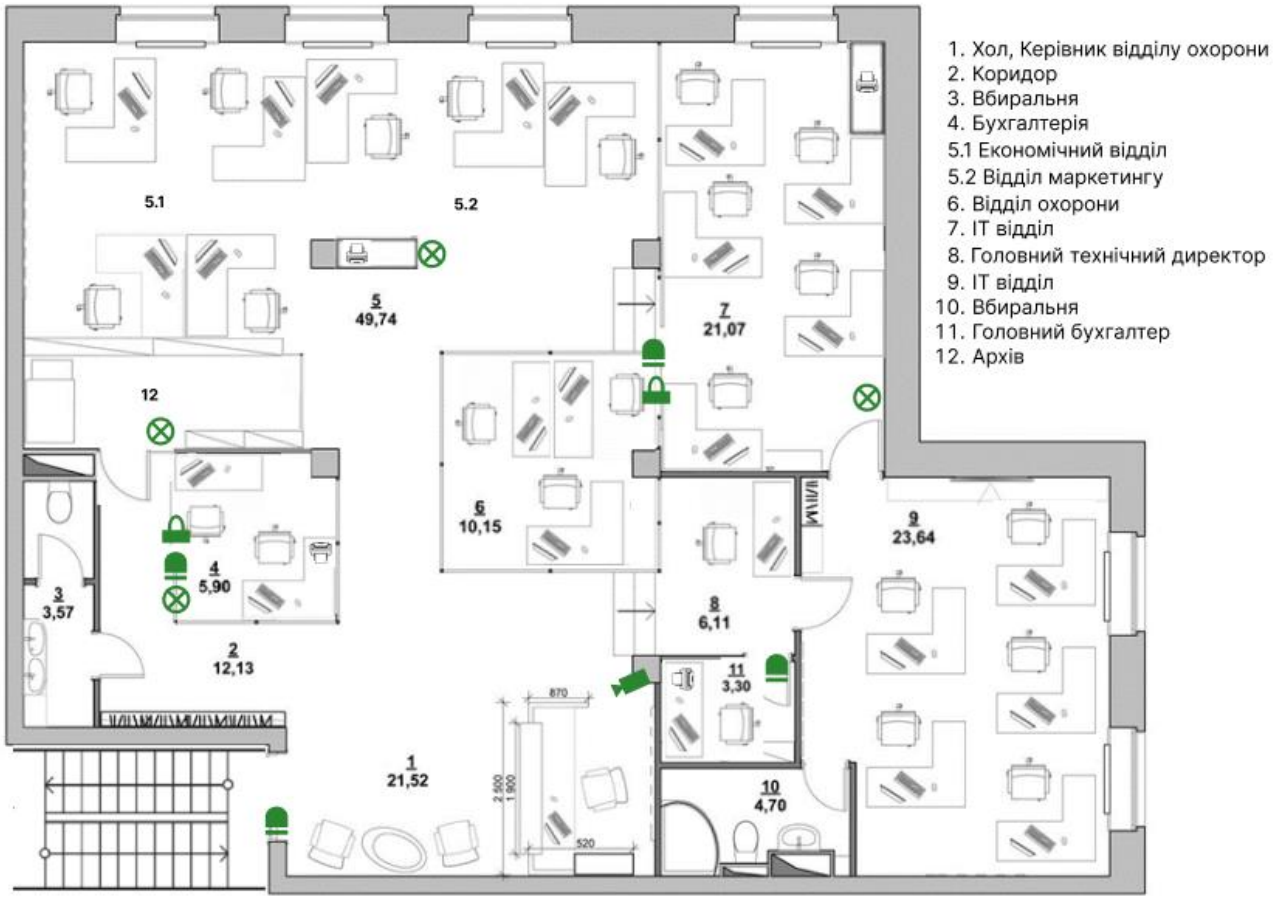
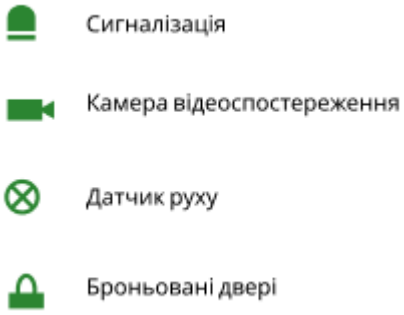



Рисунок. 2.11 – План другого поверху будівлі з позначенням засобів доступу до відділів та розміщення техніки у ньому



Таблиця 2.4 – Апаратне забезпечення засобами доступу до будівлі

| | **Найменування** | **Характеристики** |
|---|---|---|
|  | IP-камера відеоспостереження TP-LINK Tapo C320WS | Для вулиці<br>Запис звуку<br>Можливість нічної зйомки<br>Розумна<br>Тип – бездротові<br>Роздільна здатність – 4 Мп<br>Інфрачервона підсвітка до 30 м<br>Роздільна здатність відео – 2560x1440<br>Фокусна відстань – 3.18 мм<br>Розміри – 142.3 x 103.4 x 64.3 мм<br>Максимальний обсяг карти пам'яті – 256 ГБ |
|  | Датчик руху настінний EUROELECTRIC ST-16 | Тип – інфрачервоні<br>Тип монтажу – накладні<br>Напруга – 220 В<br>Потужність – 1000 Вт<br>Відстань виявлення – 12 м<br>Кут виявлення – 110°<br>Габарити, см – 7.2 x 6 x 7.7<br>Вологозахищені<br>Затримка вимкнення – сек/12 хв |

| | | |
|---|---|---|
|  | Комплект охоронної сигналізації Ajax StarterKit 2 White (000023480) | Вид – бездротові<br>Максимальна кількість користувачів – 199<br>Канали зв'язку – Ethernet<br>Час доставки сигналу тривоги – 0,15 с<br>Резервний акумулятор – Li-Ion 3 А·год – до 15 години автономної роботи<br>Комплектація:<br>Hub 2 – інтелектуальна централь другого покоління<br>MotionProtect – бездротовий датчик руху<br>DoorProtect – бездротовий датчик відкривання<br>SpaceControl – бездротовий брелок |
|  | Броньовані двері Моноліт Класик, 207х96, Бетон | Броньовані<br>Товщина полотна – 95 мм<br>Комплектація:<br>Замок основний фіксуючий– CISA REVOLUTION PRO<br>Замок додатковий верхній – MOTTURA J52<br>Розмір – 960 мм х 2070 мм |

Таблиця 2.5 – Вартість апаратного забезпечення засобами доступу до будівлі

| **Застосунок** | **Кількість** | **Вартість за одиницю, грн** | **Вартість всього, грн** |
|---|---|---|---|
| Камера відеоспостереження | 3 | 2499 | 7497 |
| Датчик руху | 7 | 482 | 3 374 |
| Комплект охоронної сигналізації (сигналізація та датчики руху) | 8 | 12 099 | 96792 |
| Броньовані двері | 6 | 75 000 | 450 000 |
| **Всього** | | | 557663 |

У комплект охоронної сигналізації вже входить датчик руху. Тому в кількість датчиків не входять ті, які розташовані у кімнатах бухгалтерії, серверної, відділу охорони (де вже розташований комплект сигналізації).

## 2.5 Програмні засоби захисту інформації

**Антвірусні програми**


Рис. 2.12 – Кращі антивіруси 2024 року.

Перед вибором антивірусу для компанії я переглянула топ найкращих антивірусів світу та України та описала про кожного з них.

1. **Bitdefender**

«Платний (є безкоштовна версія з обмеженим функціоналом)

З переваг: високий рівень захисту від нових загроз, мінімальний вплив на продуктивність, наявність функцій для захисту від фішингу та шкідливих програм.

Із недоліків, що платні версії мають більш складні налаштування та інтерфейс» -[19].

Країна виробника: Румунія

2. **Panda**

«Платний та безкоштовний

З переваг: простота у використанні, хмарна технологія для швидкого виявлення загроз, додаткові функції захисту приватності.

Із недоліків: деякі платні функції обмежені в безкоштовній версії, хмарна технологія може вимагати стабільного інтернет-з'єднання» - [19].

Країна виробника: Іспанія

3. **Avira**

«Платний та безкоштовний

Переваги: легкий у використанні, високий рівень захисту від шкідливих програм, безкоштовна версія з хорошим базовим захистом.

Недоліки: додаткові функції, наприклад, VPN, доступні лише в платній версії, безкоштовна версія має обмежену кількість функцій» - [19].

Країна виробника: Німеччина

4. **Norton 360**

«Платний

Переваги: багатофункціональний захист з батьківським контролем, VPN, моніторинг темної мережі та інші інструменти безпеки.

Недоліки: висока вартість, може бути дещо важким для новачків через велику кількість функцій» - [19]

Країна виробника: США

5. **Avast Free Antivirus**

«Безкоштовний та платний

Переваги: безкоштовна версія з хорошим рівнем захисту від вірусів і шкідливих програм, легкий інтерфейс та інструменти для оптимізації ПК.

Недоліки: рекламні повідомлення в безкоштовній версії, відсутність деяких функцій у порівнянні з платною версією» - [19]

Країна виробника: Чехія

6. **Windows Defender**

«Безкоштовний (вбудований в Windows)

Переваги: безкоштовний, не займає багато системних ресурсів, інтегрований у Windows, автоматично оновлюється.

Недоліки: не має розширених функцій, таких як VPN чи батьківський контроль, може не вистачити захисту від нових загроз у порівнянні з платними антивірусами» - [19].

Країна виробника: США

7. **AVG Internet Security**

«Платний (є безкоштовна версія з обмеженим функціоналом)

Переваги: добре справляється з виявленням шкідливих програм і фішингових атак, є додаткові інструменти для оптимізації ПК та захисту в Інтернеті.

Недоліки: додаткові функції, такі як захист від шкідливих вебсайтів та вірусів у реальному часі, доступні лише в платній версії» - [19]

Країна виробника: Чехія


Рисунок 2.13 – Рейтинг антивірусів 2024 року.

Запропоновано обрати Bitdefender GravityZone Business Security, бо це потужне, ефективне та надійне рішення, яке не тільки надає високий рівень захисту від кіберзагроз, але й відповідає специфічним вимогам моєї компанії в плані масштабованості, управління та продуктивності. Хоч антивірус є платним він повністю відповідає поставленим перед ним задачам.

Bitdefender GravityZone Business Security – це потужне антивірусне рішення, яке забезпечує всебічний захист від вірусів, шпигунських програм та рансомвару. Воно використовує технології штучного інтелекту для виявлення загроз у реальному часі. [19]

Антивірус автоматично оновлює бази даних, що гарантує актуальний захист від нових загроз. Програмне забезпечення оптимізоване для роботи з мінімальним навантаженням на системні ресурси, що забезпечує високу продуктивність комп'ютерів. Bitdefender пропонує централізоване управління через хмарну консоль, що полегшує адміністрування. Додаткові функції включають захист від рансомвару та веб-фільтрацію для блокування небезпечних сайтів. Програма легко налаштовується та розгортається, що робить її підходящою для будь-якого бізнесу. Це рішення є надійним вибором для компаній, так як я прагну забезпечити високий рівень кібербезпеки. [19]

Зазначене програмне забезпечення, що буде потребувати компанія для роботи. Також, для забезпечення безпечного користування в мережі куплено Румунський антивірус Bitdefender GravityZone Business Security. Цей антивірус забезпечує потужний захист від шкідливих програм та інших загроз з використанням машинного навчання та поведінкового аналізу. А так як цей антивірус є досить гарним, брандмауер не потрібний.

Таблиця 2.6 – Вартість програмного забезпечення

| **Найменування** | **Кількість** | **Вартість за 1 од., грн** | **Вартість всього, грн** |
|---|---|---|---|
| Антивірус Bitdefender GravityZone Business Security | 1 | 4610 /на 2 роки | 4610 |
| **Всього** | | | 4610 |

Таблиця 2.7 – Загальні витрати на організацію захисту інформації

| **Складова** | **Вартість, грн** |
|---|---|
| Вартість апаратного забезпечення засобами доступу до будівлі | 557663 |
| Програмне забезпечення компанії | 4610 |
| Всього | 56273 |

# РОЗДІЛ 3
# КРИПТОЛОГІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

## 3.1 Особливості криптографічного алгоритму

«Алгоритм шифрування Triple DES (3DES) – симетричний блоковий шифр, створений Уітфілдом Діффі, Мартіном Хеллманом і Уолтом Тачманном в 1978 на основі алгоритму DES з метою усунення головного недоліку останнього – малої довжини ключа (56 біт), який може бути зламаний методом повного. Швидкість роботи 3DES в 3 рази нижче, ніж у DES, але криптостійкість набагато вища. 3DES використовується частіше, ніж DES, який легко зламується за допомогою сьогоднішніх технологій (1998 року організація Electronic Frontier Foundation, використовуючи спеціальний комп'ютер *DES* Cracker, розкрила DES за 3 дні). 3DES є простим способом усунення недоліків DES. Алгоритм 3DES побудований на основі DES, тому для його реалізації можна використовувати програми, створені для DES. Офіційна назва алгоритму, що використовується в стандартах – TDEA або Triple DEA (Triple Data Encryption Algorithm). [22]

Шифр DES є блоковим – перетворення в ньому проводяться блоками по 64 біта. Ключ також 64-бітний, але значущими є тільки 56 біт – кожен 8-й розряд використовувався для контролю парності (шифр розроблявся тоді, коли апаратура була не надто надійної і подібні перевірки були необхідні)» - [22].

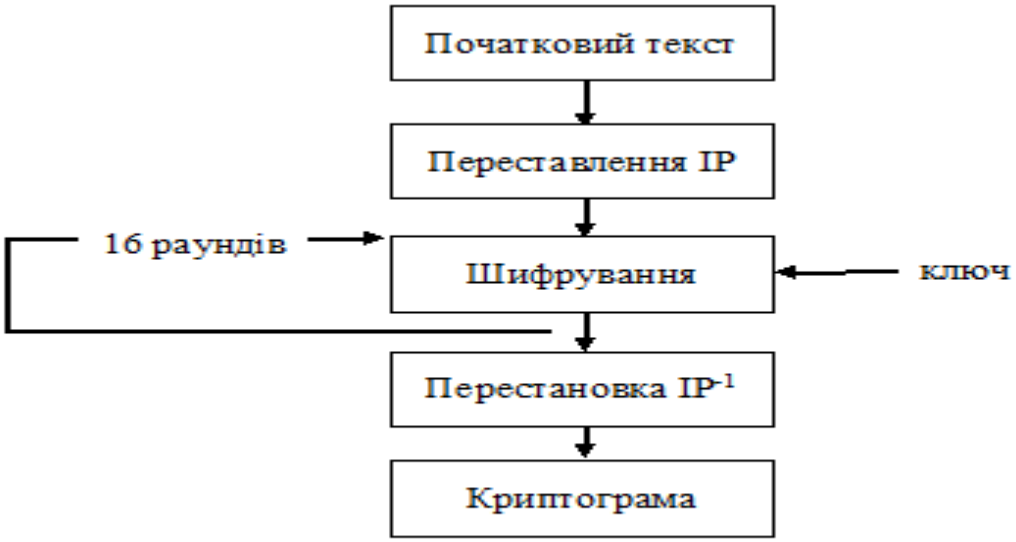



Рисунок 3.1 Узагальнена схема шифру DES

Кінцева перестановка – P $^{1}$ – є зворотною по відношенню до начальной – IP. Шифрування проводиться в 16 раундів.

Існує 3 типи алгоритму 3DES:

DES-EEE3: Шифрується три рази з трьома різними ключами (операція шифрування-шифрування-шифрування).

DES-EDE3: 3DESоперації шифрування-розшифрування-шифрування з трьома різними ключами.

DES-EEE2 та DES-EDE2: Як і попередні, за винятком того, що на першому та третьому кроці використовується однаковий ключ.

Найпопулярніший різновид 3DES – це DES-EDE3, для нього алгоритм виглядає так:

Шифрування:

$$C = E_{k3}(E_{k2}^{-1}(E_{k1}(P)))$$

Розшифровка:

$$P = E_{k1}^{-1}(E_{k2}(E_{k3}^{-1}(C)))$$ [17]

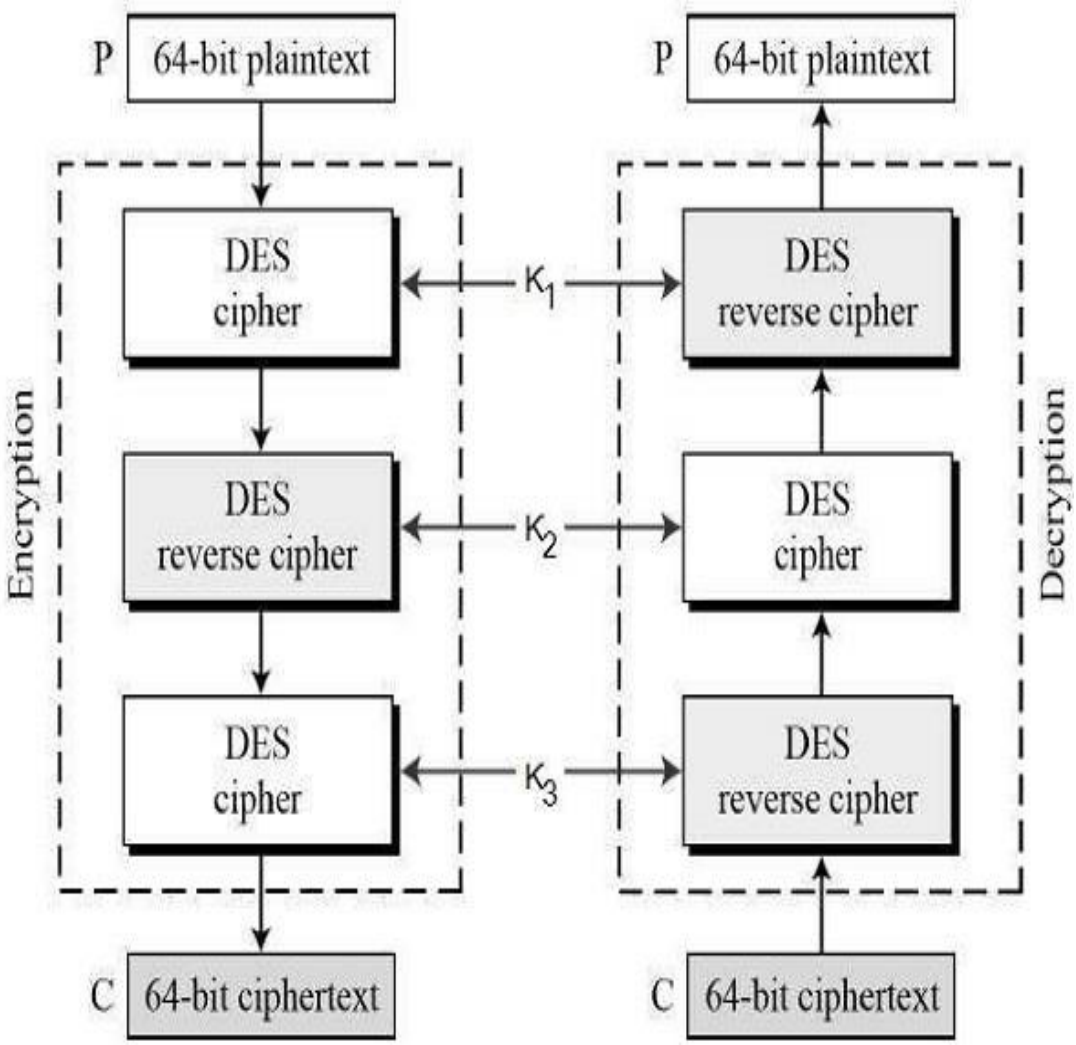



Рисунок 3.2. – Схема шифрування

### 3.2 Представлення розробленого шифратору TRIPLE DES

Реалізація шифратора виконана за допомогою шифру Triple DES на мові програмування C#. Для реалізації використовувався додаток Visual Studio 2022.

Для початку було створено дизайн для вікон, що використовуються у шифраторі, а саме:

- вікно реєстрації, де користувач вводить логін та пароль, відповідно наданий компанією та проходить ідентифікацію відділу (Рис. 2.3);

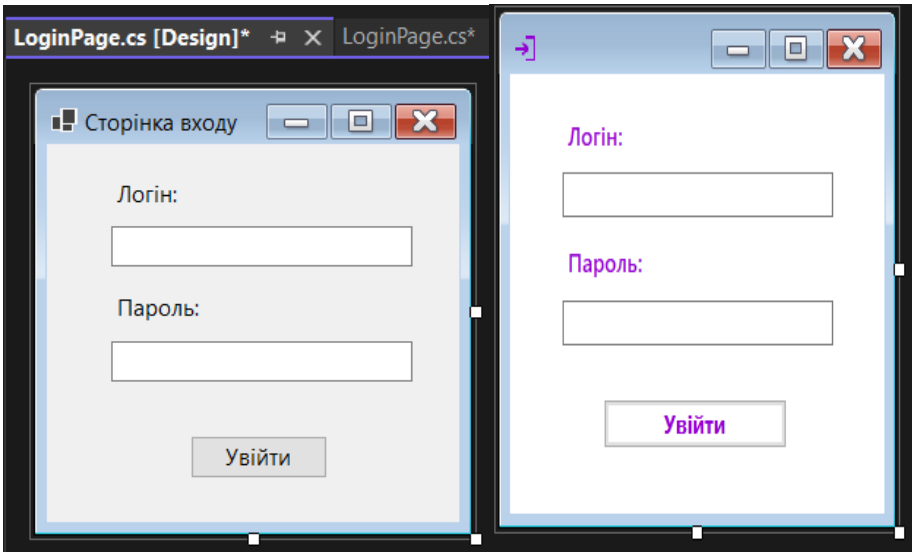



Рисунок 2.3 – Шаблон сторінки входу

- вікно головної сторінки, на яку переходить користувач при натисканні кнопки «увійти» зі сторінки входу. Тут представлений вибір двох кнопок, що хоче зашифрувати/ розшифрувати користувач. Відповідно до цього він переходить на сторінку шифрування або повідомлень або файлів (Рис. 2.4).

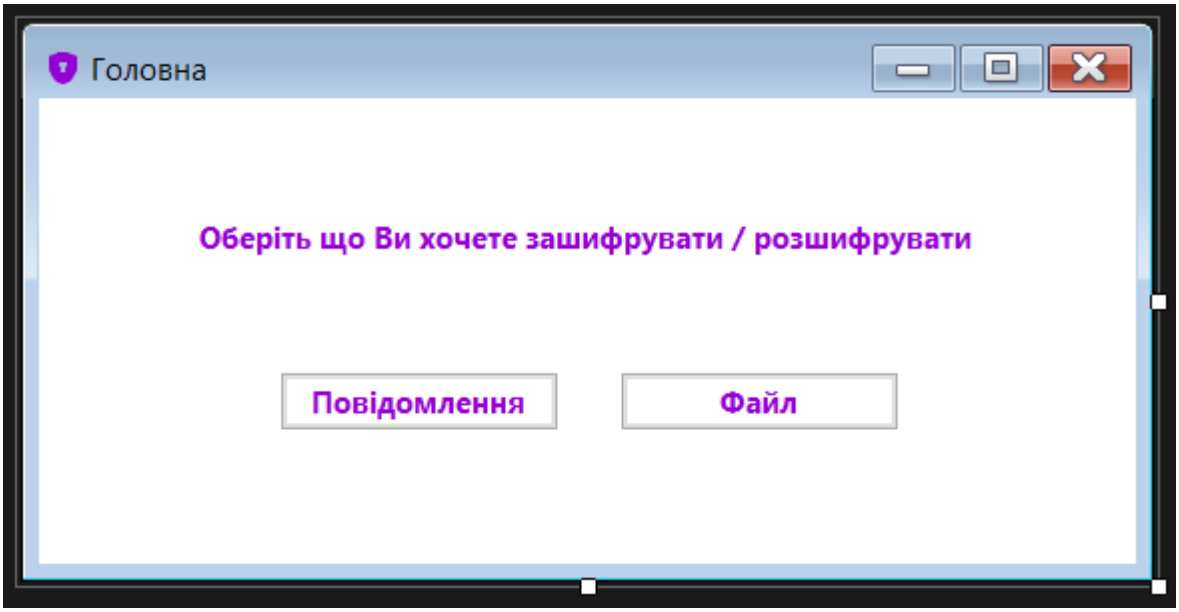



Рисунок 2.4 – Дизайн головної сторінки

- вікно шифрування / дешифрування повідомлень. Тут є поле для вводу повідомлення, поле де буде відображатися результат та відповідно дві кнопки (Рис. 2.5).

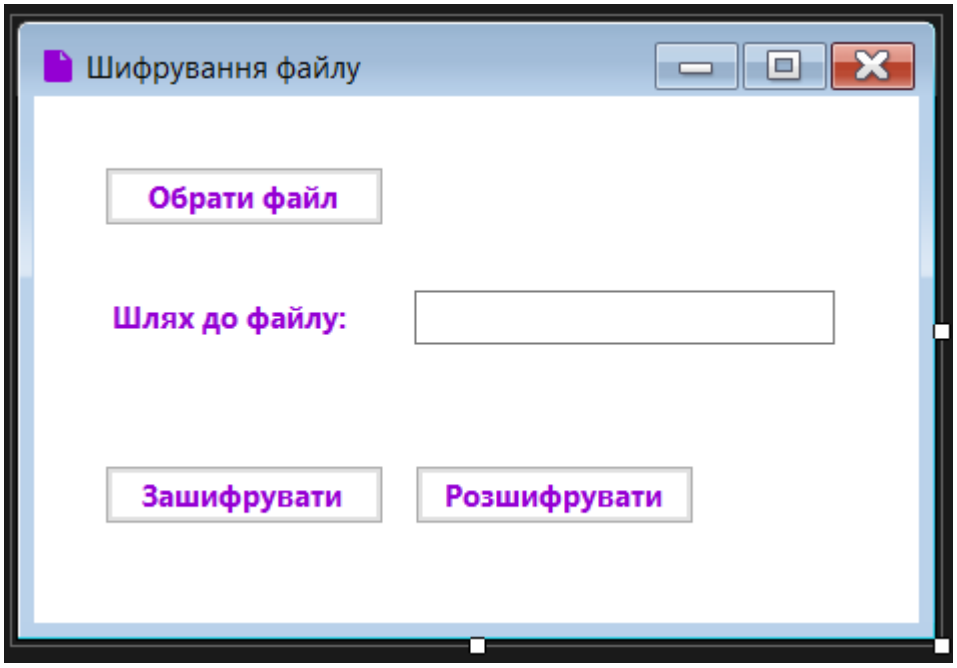



Рисунок 2.5. – Дизайн сторінки шифрування /дешифрування файлу

- Вікно шифрування / дешифрування файлів, тут можна обрати шлях, де розташований файл за допомогою кнопки або введення вручну шляху та дві кнопки (Рис.2.6).

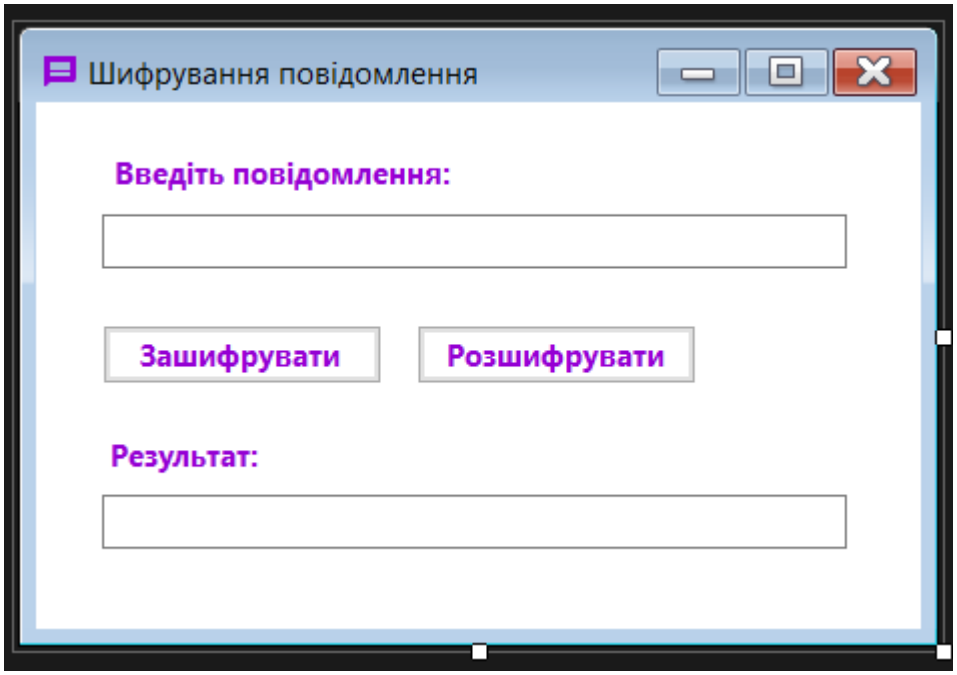



Рисунок 2.6 – Дизайн сторінки шифрування / дешифрування повідомлень

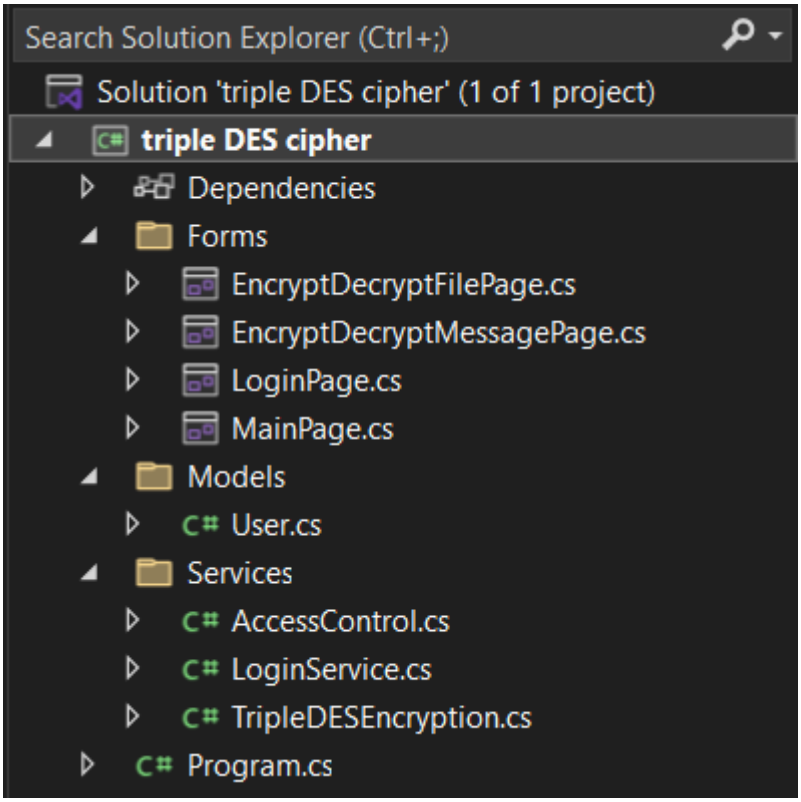
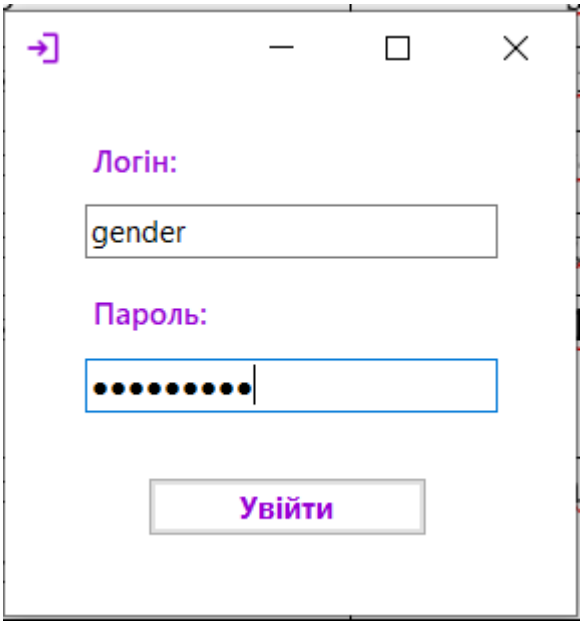



Рисунок 2.7 – Структура проєтку

Для початку користувач вводить логін та пароль, як показано на рис. 10. В прикладі введено дані для входу генерального директора, також можливий вхід для будь-якого співробітника. Якщо реєстрація успішна, програма покаже діалогове вікно з підтвердженням та повідомить, якщо дані для входу невірні (Рис. 2.8). При натисканні «ОК» користувача перенесе на головну сторінку.



| **Кабінет** | **Логін(назва комп'ютера)** | **Пароль** |
|---|---|---|
| Генеральний директор | gender | Gender001 |

Рисунок. 2.8 – Вікно входу та дані

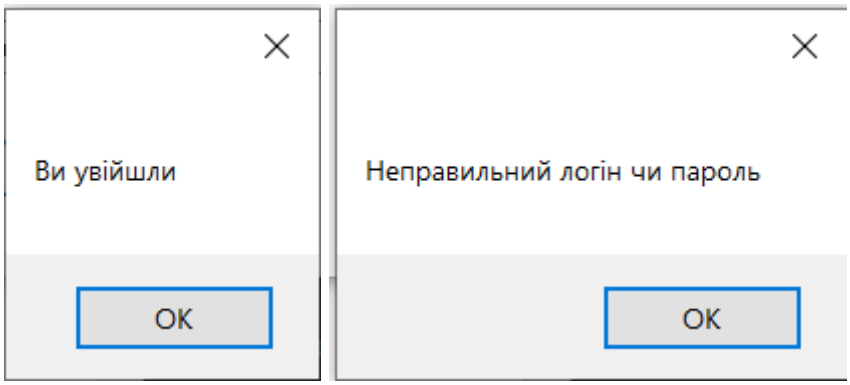



Рисунок 2.9 – Діалогове вікно

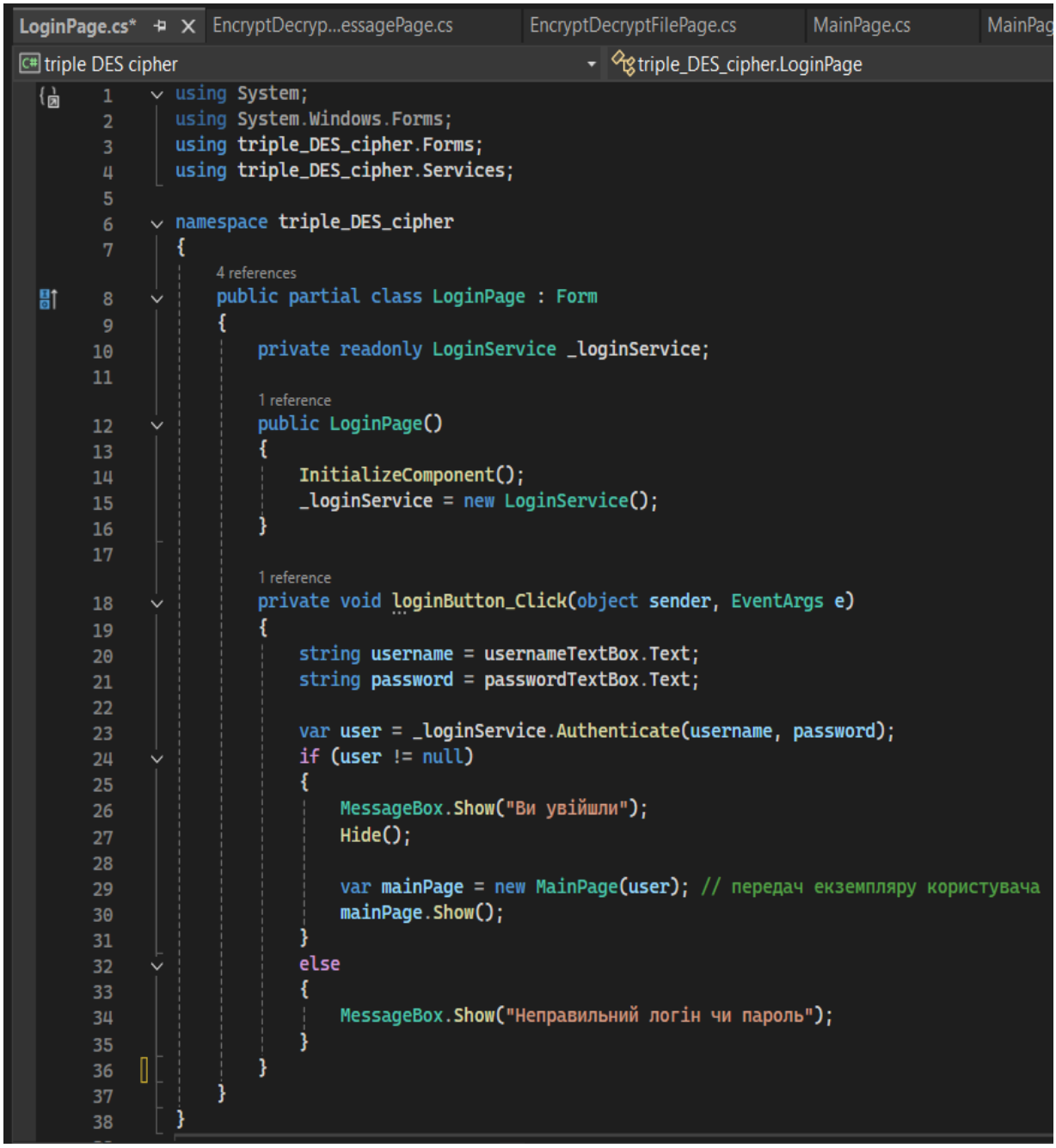



Рисунок 2.10 – Наведений код реалізації сторінки входу

На головній даний вибір лише двох кнопок «Повідомлення» та «Файл» (Рис.2.11). Після вибору користувача перенесе на вибрану сторінку.

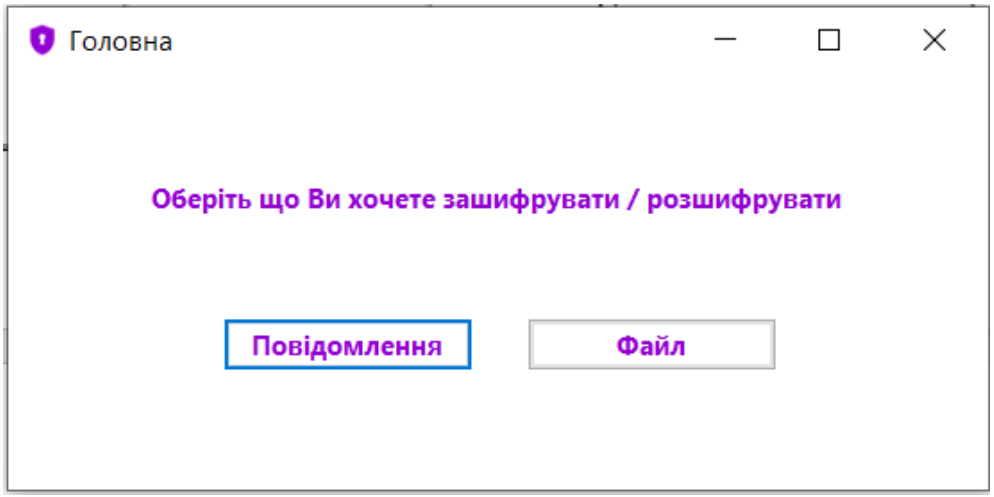



Рисунок 2.11 – Головна сторінка

MainPage.cs | MainPage.cs [Design] | EncryptDecryp...essagePage.cs | EncryptDecryptFilePage.cs

triple DES cipher | triple_DES_cipher.Forms.MainPage

```
1   using System;
2   using System.Collections.Generic;
3   using System.ComponentModel;
4   using System.Data;
5   using System.Drawing;
6   using System.Linq;
7   using System.Text;
8   using System.Threading.Tasks;
9   using System.Windows.Forms;
10  using triple_DES_cipher.Services;
11
12  namespace triple_DES_cipher.Forms
13  {
        4 references
14      public partial class MainPage : Form
15      {
16          private User _currentUser;
            1 reference
17          public MainPage(User currentUser)
18          {
19              InitializeComponent();
20              _currentUser = currentUser;
21          }
            1 reference
22          private void encryptDecryptMessageButton_Click(object sender, EventArgs e)
23          {
24              var messagePage = new EncryptDecryptMessagePage();
25              messagePage.Show();
26          }
27
            1 reference
28          private void encryptDecryptFileButton_Click(object sender, EventArgs e)
29          {
30
31              var filePage = new EncryptDecryptFilePage(_currentUser);
32              filePage.Show();
33          }
34      }
35  }
```

Рисунок 12. – Код головної сторінки

У вікні шифрування повідомлень я показала як можна ввести повідомлення «Вітаю» чи будь-яке інше та зашифрувати (Рис.13). Також можливе дешифрування повідомлення (Рис.14).

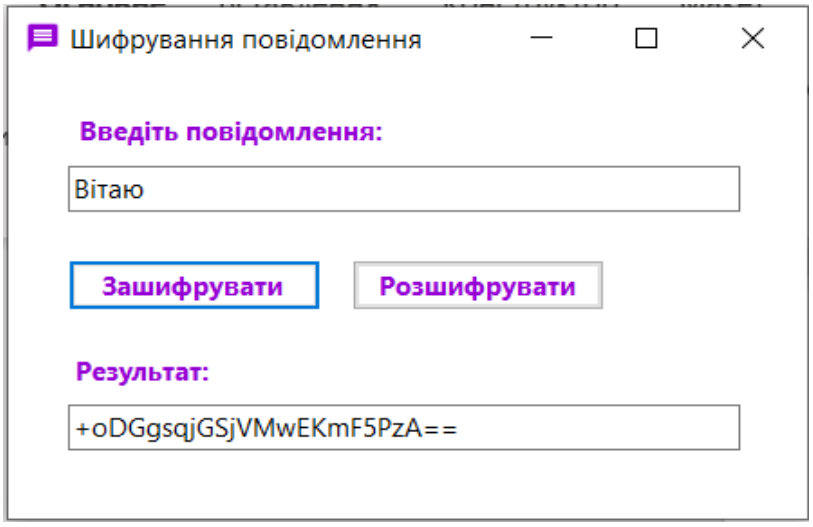



Рисунок 3.13 – Шифрування повідомлень

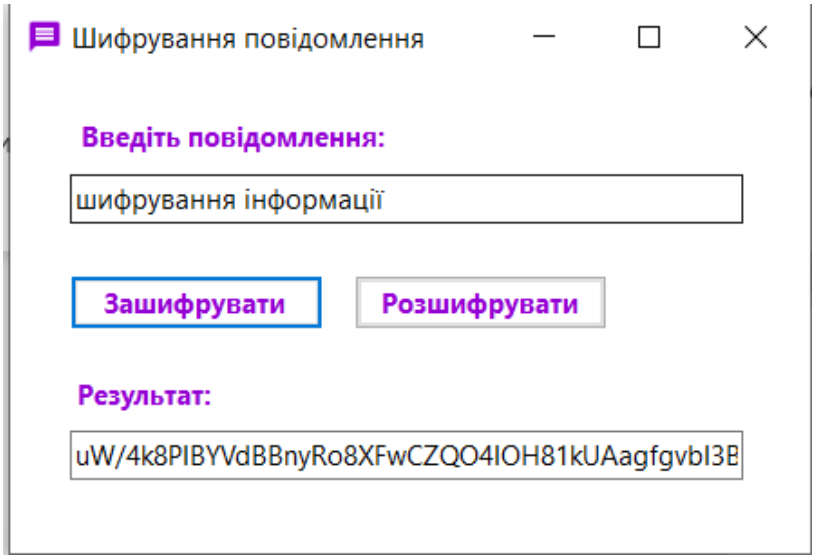



Рисунок 3.14 – Шифрування повідомлень

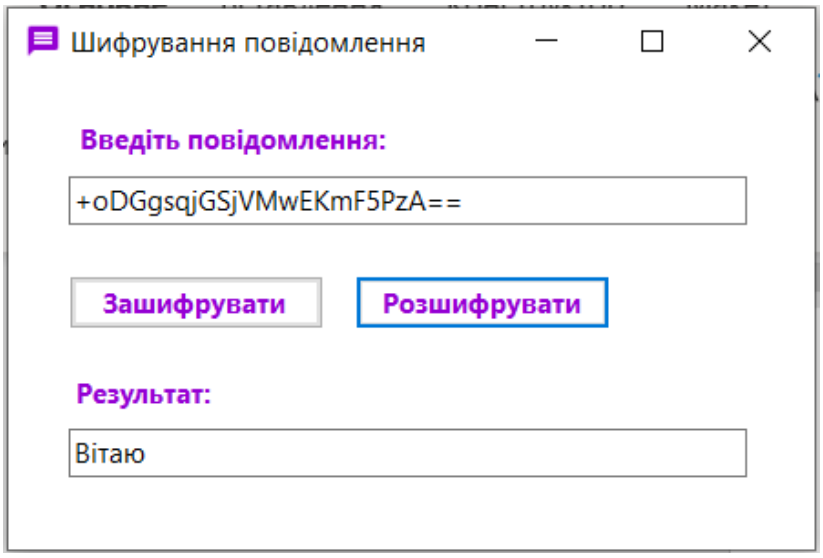



Рисунок 3.15. – Дешифрування повідомлення

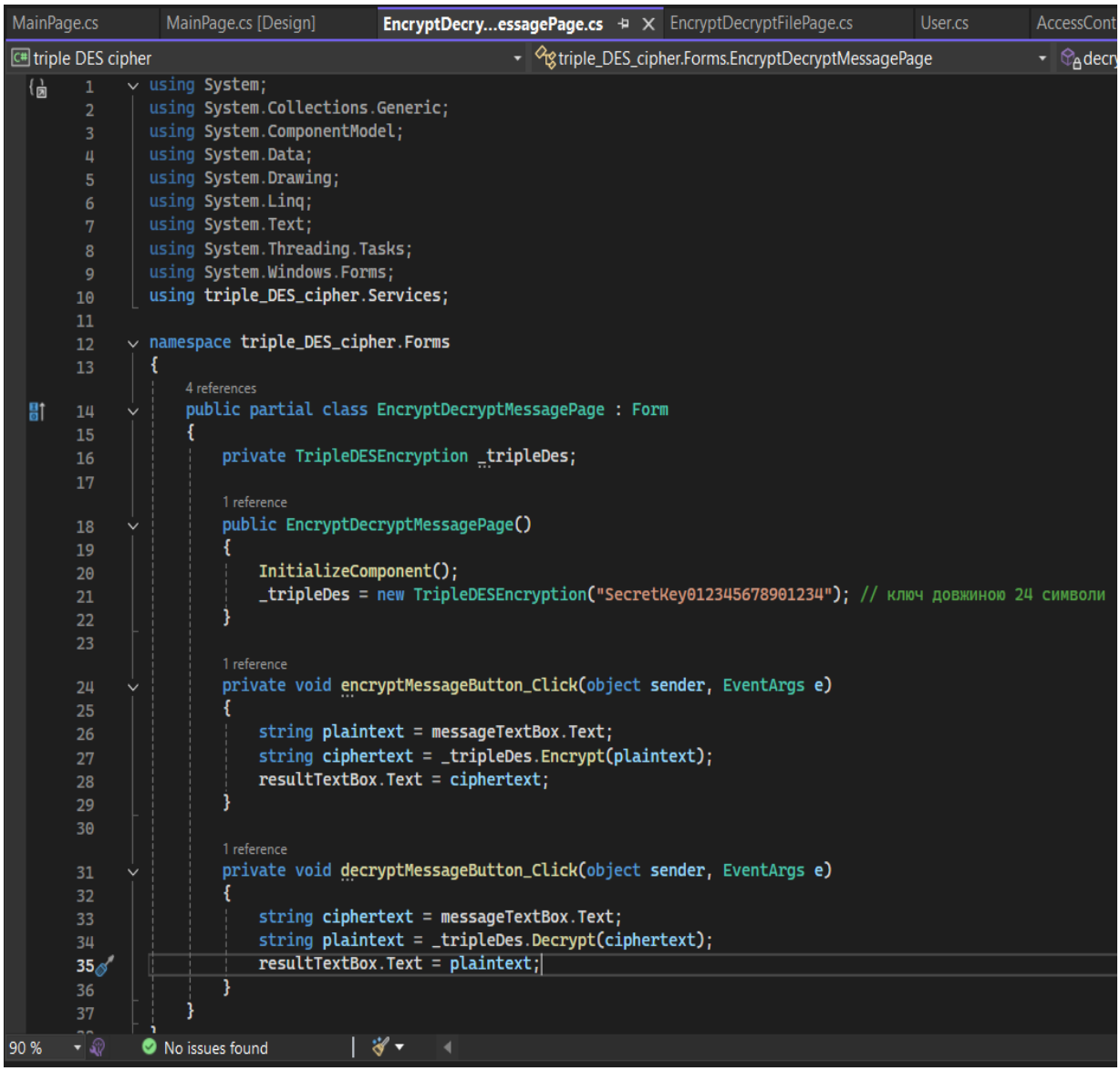



Рисунок 3.16 – Код сторінки шифрування повідомлень

Розглянемо сторінку шифрування файлів (Рис. 3.16). Для перевірки роботи було створено декілька текстових документів, надалі перейменовані, як file1, file2,... При натисканні «Зашифрувати» у нас з'являється діалогове вікно з підтвердженням шифрування (Рис. 3.17). Нижче наведений приклад зашифрованого файлу. При натисканні «Розшифрувати» також відображається діалогове вікно та після натискання «ОК» відкривається файл.

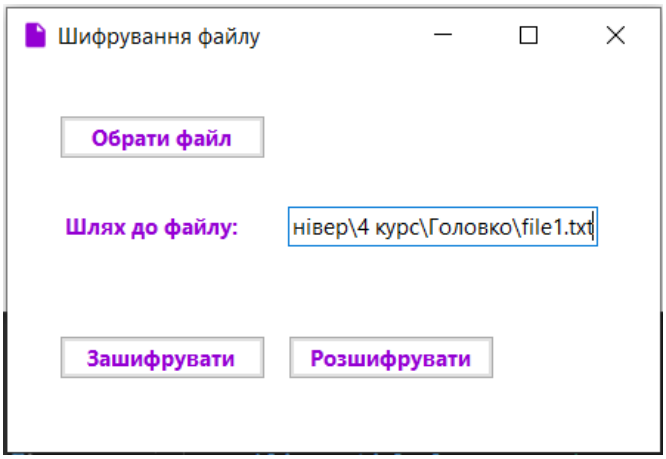



Рисунок 3.16. – Сторінка шифрування файлів

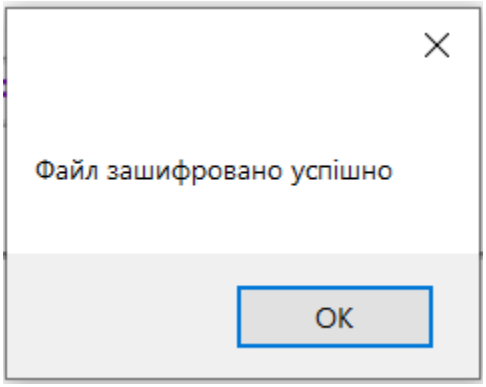



Рисунок 3.17. – Діалогове вікно підтвердження

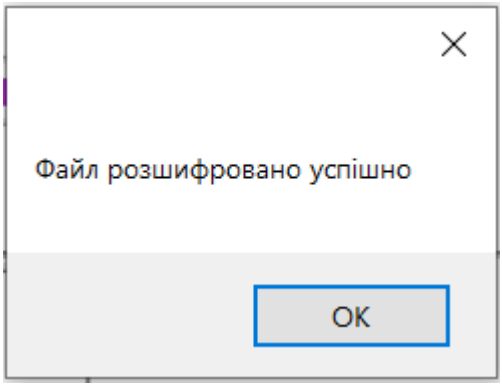



Рисунок 3.18. – Діалогове вікно підтвердження розшифрування

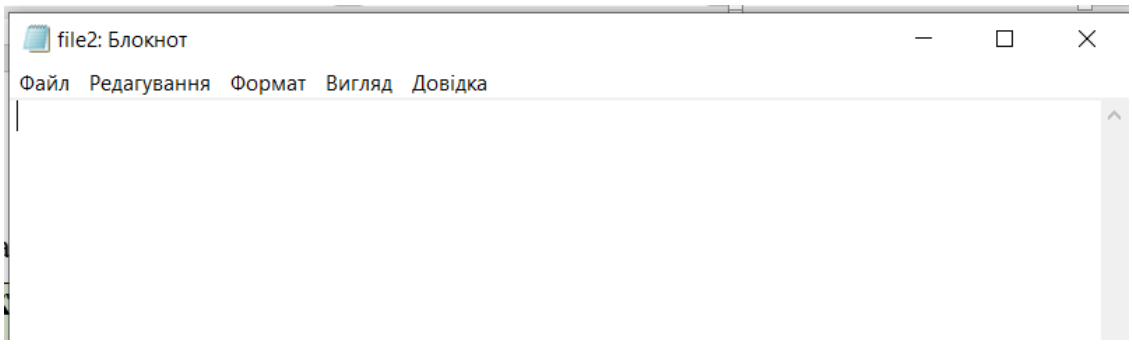



Рисунок 3.20 – Відритий файл розшифрований

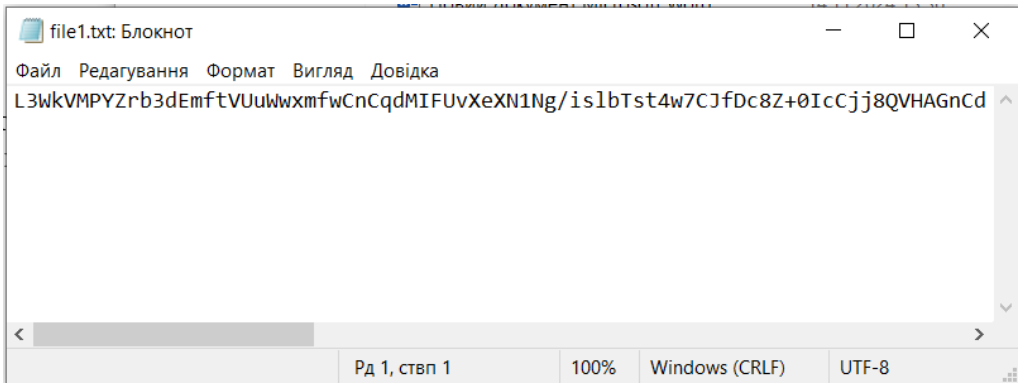



Рисунок 3.21 – Зашифрований файл

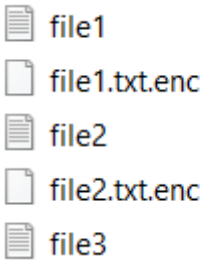
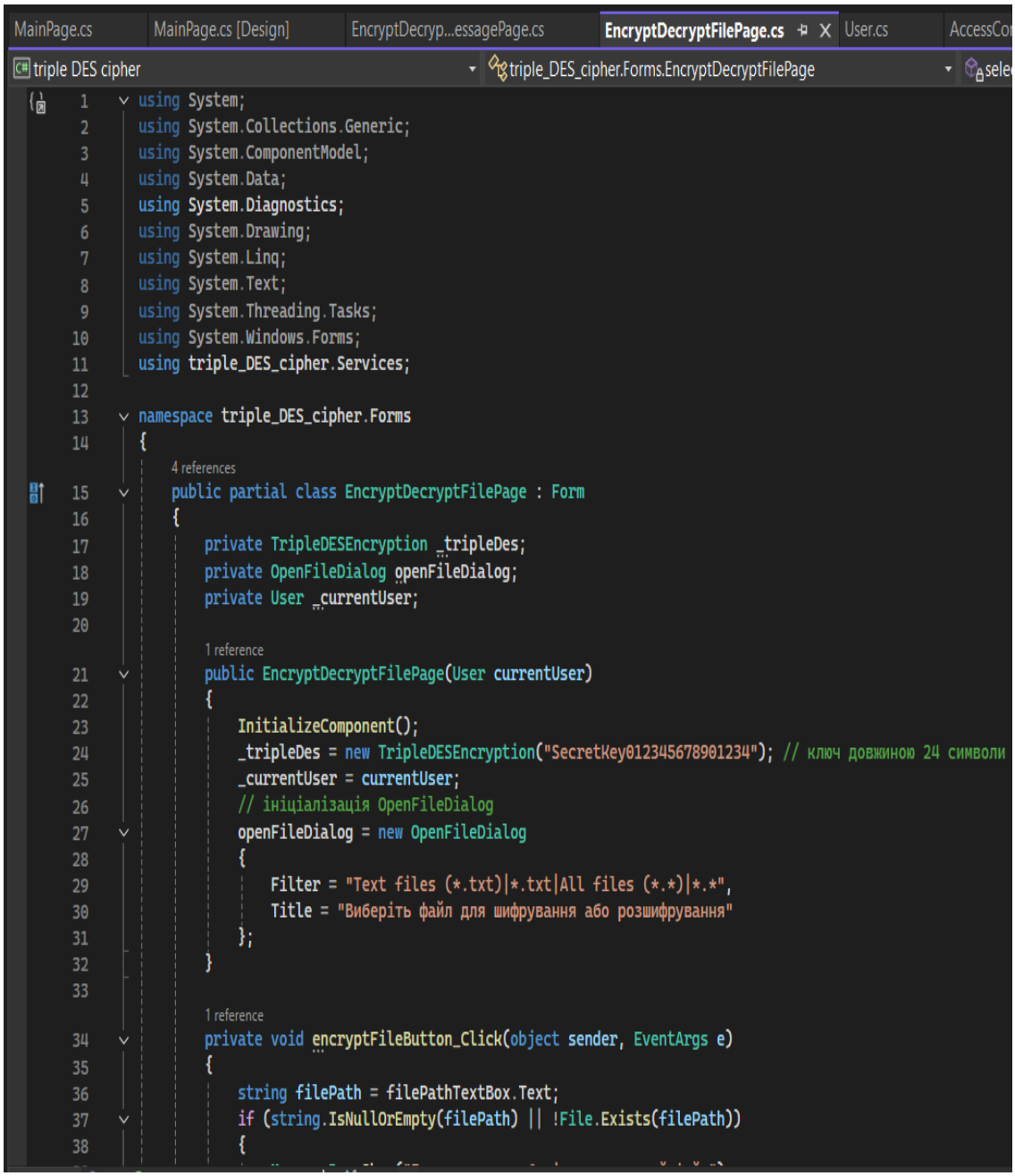
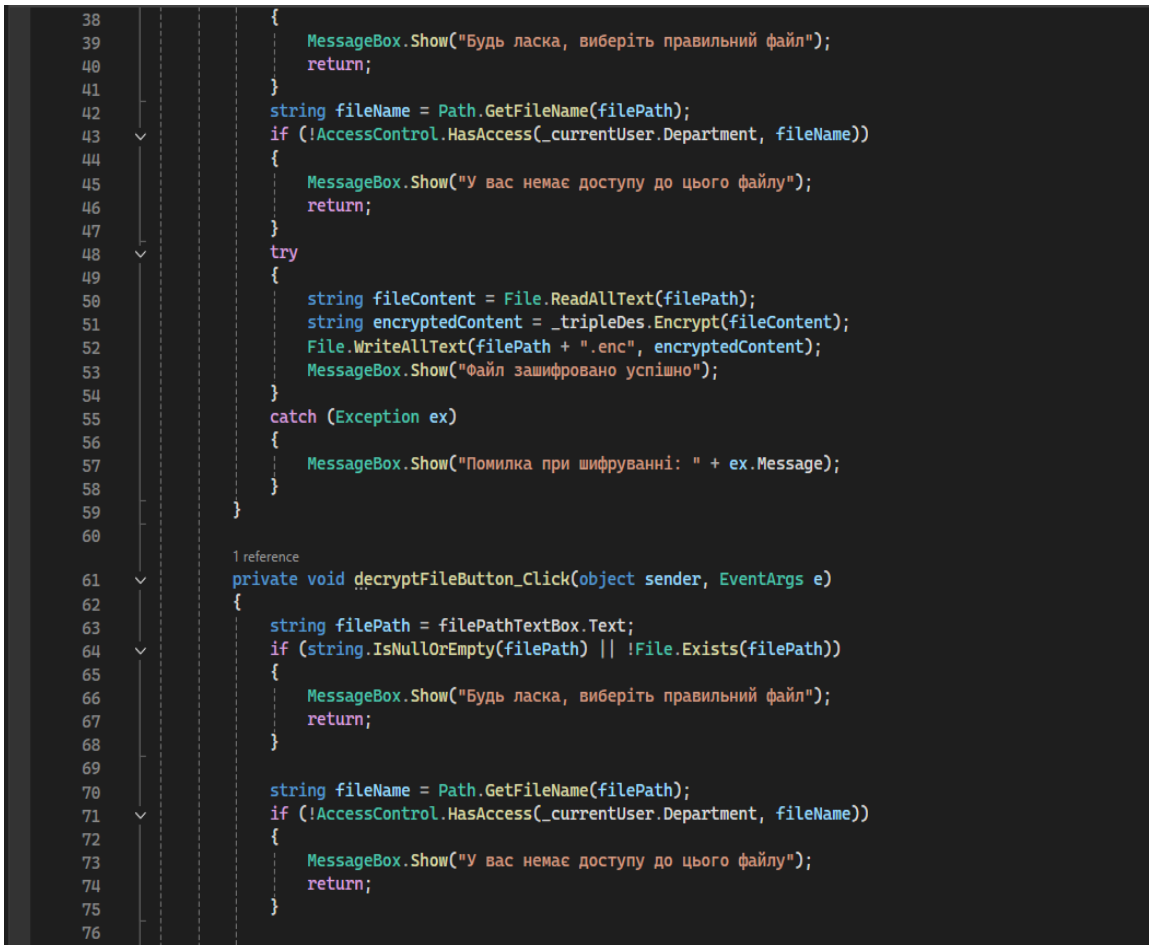



Рисунок 3.22 – Відображення зашифрований та розшифрованих файлів

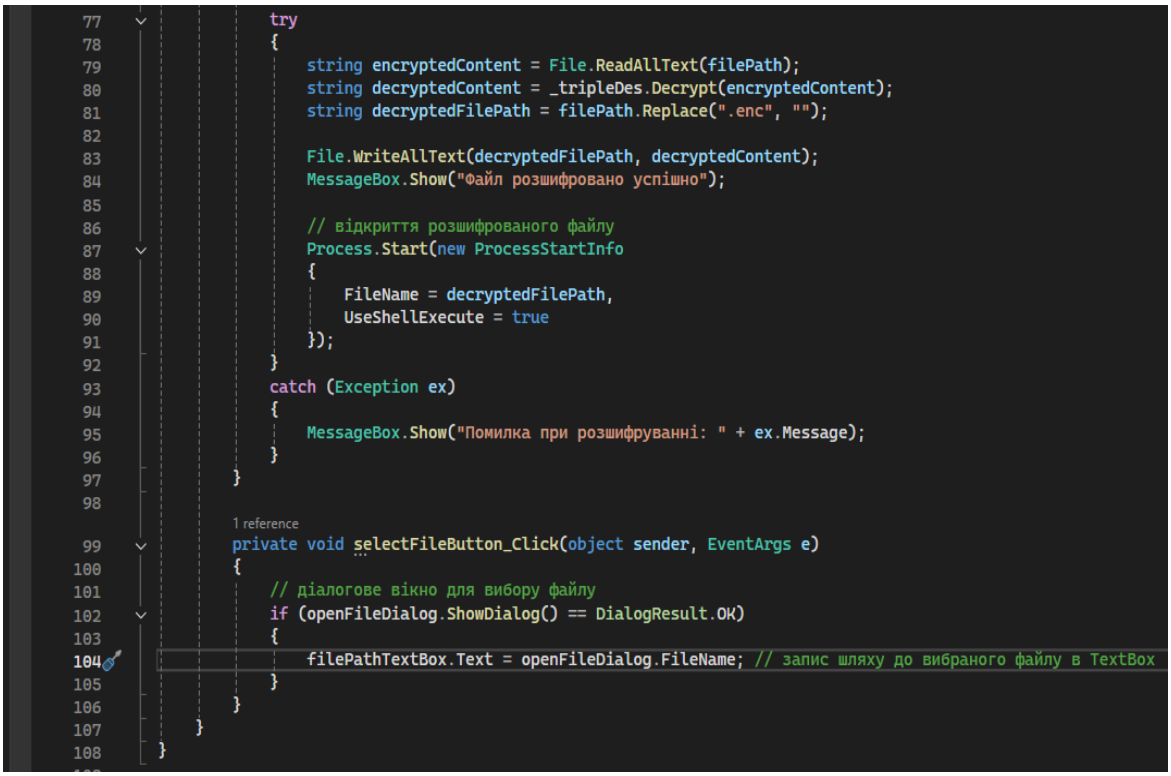

MainPage.cs
MainPage.cs [Design]
EncryptDecryp...essagePage.cs
EncryptDecryptFilePage.cs
User.cs
triple DES cipher
triple_DES_cipher.Forms.EncryptDecryptFilePage
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Diagnostics;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using triple_DES_cipher.Services;
namespace triple_DES_cipher.Forms
{
4 references
public partial class EncryptDecryptFilePage : Form
{
private TripleDESEncryption _tripleDes;
private OpenFileDialog openFileDialog;
private User _currentUser;
1 reference
public EncryptDecryptFilePage(User currentUser)
{
InitializeComponent();
_tripleDes = new TripleDESEncryption("SecretKey012345678901234"); // ключ довжиною 24 символи
_currentUser = currentUser;
// ініціалізація OpenFileDialog
openFileDialog = new OpenFileDialog
{
Filter = "Text files (*.txt)|*.txt|All files (*.*)|*.*",
Title = "Виберіть файл для шифрування або розшифрування"
};
}
1 reference
private void encryptFileButton_Click(object sender, EventArgs e)
{
string filePath = filePathTextBox.Text;
if (string.IsNullOrEmpty(filePath) || !File.Exists(filePath))
{



```
            {
                MessageBox.Show("Будь ласка, виберіть правильний файл");
                return;
            }
            string fileName = Path.GetFileName(filePath);
            if (!AccessControl.HasAccess(_currentUser.Department, fileName))
            {
                MessageBox.Show("У вас немає доступу до цього файлу");
                return;
            }
            try
            {
                string fileContent = File.ReadAllText(filePath);
                string encryptedContent = _tripleDes.Encrypt(fileContent);
                File.WriteAllText(filePath + ".enc", encryptedContent);
                MessageBox.Show("Файл зашифровано успішно");
            }
            catch (Exception ex)
            {
                MessageBox.Show("Помилка при шифруванні: " + ex.Message);
            }
        }

        1 reference
        private void decryptFileButton_Click(object sender, EventArgs e)
        {
            string filePath = filePathTextBox.Text;
            if (string.IsNullOrEmpty(filePath) || !File.Exists(filePath))
            {
                MessageBox.Show("Будь ласка, виберіть правильний файл");
                return;
            }

            string fileName = Path.GetFileName(filePath);
            if (!AccessControl.HasAccess(_currentUser.Department, fileName))
            {
                MessageBox.Show("У вас немає доступу до цього файлу");
                return;
            }
```



```
            try
            {
                string encryptedContent = File.ReadAllText(filePath);
                string decryptedContent = _tripleDes.Decrypt(encryptedContent);
                string decryptedFilePath = filePath.Replace(".enc", "");

                File.WriteAllText(decryptedFilePath, decryptedContent);
                MessageBox.Show("Файл розшифровано успішно");

                // відкриття розшифрованого файлу
                Process.Start(new ProcessStartInfo
                {
                    FileName = decryptedFilePath,
                    UseShellExecute = true
                });
            }
            catch (Exception ex)
            {
                MessageBox.Show("Помилка при розшифруванні: " + ex.Message);
            }
        }

        1 reference
        private void selectFileButton_Click(object sender, EventArgs e)
        {
            // діалогове вікно для вибору файлу
            if (openFileDialog.ShowDialog() == DialogResult.OK)
            {
                filePathTextBox.Text = openFileDialog.FileName; // запис шляху до вибраного файлу в TextBox
            }
        }
    }
}
```

Рисунок 3.23. – Код сторінки роботи з файлами

Проєкт містить класи, код яких не наведений тут. Також є можливість переглянути сторінки розробленого коду дизайну. Весь код шифратора можна переглянути в посиланні на GitHub [16].

# ВИСНОВКИ

У ході виконання кваліфікаційної магістерської роботи було забезпечено комплексний підхід до організації захисту інформації на підприємстві Sphere. Проведені заходи включали впровадження різних механізмів та технологій, спрямованих на створення надійної системи безпеки даних.

А саме:

1. Було реалізовано розмежування доступу до інформаційних ресурсів підприємства. Створення матриці доступу та впровадження мандатної моделі доступу дозволило чітко визначити рівні доступу кожного користувача та встановити відповідні обмеження, що підвищило контроль над інформаційними потоками;
2. Для захисту інформації на різних рівнях були застосовані додаткові заходи. Захист на рівні реєстру та використання паролів забезпечили базову безпеку робочих станцій і запобігли несанкціонованому доступу до системи. Крім того, було створено облікові записи користувачів з різними рівнями привілеїв, що сприяло покращенню управління доступом.
3. З метою захисту від шкідливих програм було обрано та впроваджено антивірусне програмне забезпечення, ретельно проаналізоване з точки зору переваг і недоліків. Це рішення сприяло захисту інформації від загроз, таких як віруси, шпигунські програми та інші шкідливі компоненти.
4. Було розроблено додаток для шифрування даних з використанням алгоритму Triple DES. Цей додаток забезпечив додатковий рівень безпеки шляхом перетворення конфіденційної інформації у зашифрований формат, що суттєво ускладнює можливість несанкціонованого доступу до даних.

У підсумку, всі впроваджені заходи створили надійну систему захисту інформації на підприємстві Sphere, яка враховує сучасні загрози та забезпечує високий рівень безпеки даних як на програмному, так і на фізичному рівнях.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технології захисту інформації. [Електронний ресурс]. – Режим доступу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

2. Захист інформації. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Захист_інформації

3. Законодавчі акти і нормативні документи щодо ЗІ. [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/7475501/page:10/

4. Що таке шкідливе програмне забезпечення? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware

5. Закон «Про інформацію» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0012323-12#Text

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

7. Закон України «Про доступ до публічної інформації» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text

8. Закон України «Про державну таємницю» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

9. Закон України «Про Національну програму інформатизації» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2807-20#Text

10. Закон України «Про захист персональних даних», Президент України Володимир Зеленський офіційне інтернет-представництво [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/2297vi-11567

11. Закон України «Про авторське право і суміжні права» [Електронний ресурс]. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/3792-12#Text

12. Закон України «Про охорону праці» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12#Text

13. ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8:2006»Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів».

14. ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures.

15. ДСТУ ISO/IEC 15946-2:2006 «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2: Електроні цифрові підписи».

16. ISO/IEC 13888-1:2004, IT security techniques – Non-repudiation – Part 1:General.

17. Поняття, сутність, значення захисту інформації. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/publications/?id=102.

18. Засоби захисту інформації. [Електронний ресурс]. – Режим доступу: https://stud.com.ua/94403/informatika/zasobi_zahistu_informatsiyi

19. Антивіруси. [Електронний ресурс]. – Режим доступу: https://blogchain.com.ua/krashii-bezkoshtovnii-antiviry/

20. Комп'ютерні віруси. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/diresideinaction/komp-uterni-virusi-ta-ieh-osnovnaharakteristika

21. Файли проєкту шифратора [Електронний ресурс]. – Режим доступу: https://github.com/Anastasia16-png/Encoder_Triple_DES

22. Курсовий Криптографія DES [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/378802/page:6/

23. Комп'ютерні віруси. Визначення, класифікація і способи захисту [Електронний ресурс] – Режим доступу до ресурсу: http://iteranet.ru/it-

novosti/2013/08/10/kompyuternye-virusy-opredelenie-klassifikaciya-i-sposoby-zashhity/.

24. Brandon G. 37 Shocking Computer Virus Statistics [Електронний ресурс] / Gaille Brandon. – 2017. – Режим доступу до ресурсу: https://brandongaille.com/36-shocking-computer-virus-statistics/.

25. Постанова Кабінету міністрів України [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: http://www.ukrbook.net/zakony/Sfera_inform/Pos_373.pdf.