Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій та робототехніки
(повна назва інституту)

Кафедра комп'ютерних та інформаційних технологій і систем
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра
(рівень вищої освіти)

на тему

Розробка системи захисту інформації для корпоративної мережі на основі сучасних методів шифрування та моніторингу загроз для офісу контакт-центру НП

Виконав: студент 6 курсу, групи 601-ТН
спеціальності
122 Комп'ютерні науки
(шифр і назва спеціальності)
Корчемний Вадим Юрійович
(прізвище та ініціали)
Керівник д.т.н., проф.. Фесенко Т.Г.
(прізвище та ініціали)
Рецензент
(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 122 «Комп'ютерні науки»
на тему

«Розробка системи захисту інформації для корпоративної мережі на основі сучасних методів шифрування та моніторингу загроз для офісу контакт-центру НП»

Студента групи 601-ТН Корчемного Вадима Юрійовича

Керівник роботи доктор технічних наук, професор Фесенко Т.Г.

Консультант кандидат технічних наук, доцент Головко Г.В.

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

Полтава – 2024

РЕФЕРАТ

Пояснювальна записка містить: 81 сторінок, 36 малюнків, 10 таблиць, 25 джерел.

Об'єкт дослідження: розробка системи захисту інформації, орієнтованої на корпоративну мережу, що функціонує в умовах сучасного бізнесу. Дослідження зосереджено на застосуванні передових методів шифрування інформації та засобів моніторингу кіберзагроз, які забезпечують надійний захист даних у офісі контакт-центру компанії «НП».

Мета роботи: детальний аналіз стану інформаційної безпеки у корпоративній мережі та створення ефективної системи захисту інформації. Ця система базується на сучасних методах шифрування, які дозволяють забезпечити високий рівень конфіденційності даних, а також на інструментах моніторингу загроз, що дають змогу виявляти та реагувати на потенційні ризики у найкоротші терміни.

Методи: аналіз сучасного стану інформаційної безпеки та практичні підходи до створення систем захисту даних. Окремо було досліджено моніторинг загроз для забезпечення цілісності інформації та недопущення несанкціонованого доступу до корпоративних ресурсів у середовищі офісу контакт-центру «НП».

Ключові слова: правові, організаційні, технічні, апаратні та програмні методи захисту інформації. Крім того, серед ключових понять виділяються шифрування, криптографія, інформаційна безпека, захист даних та їх збереження. Ці поняття формують основу сучасної системи кібербезпеки і забезпечують її комплексність.

ABSTRACT

The explanatory note contains: 81 pages, 36 figures, 10 tables, 25 sources.

The object of research: development of an information security system focused on a corporate network operating in a modern business environment. The study focuses on the use of advanced information encryption methods and cyber threat monitoring tools that ensure reliable data protection in the office of the NP contact centre.

Work objective: The main goal is to analyse in detail the state of information security in the corporate network and create an effective information security system. This system is based on modern encryption methods that ensure a high level of data confidentiality, as well as on threat monitoring tools that allow identifying and responding to potential risks in the shortest possible time.

Methods: analysis of the current state of information security and practical approaches to creating data protection systems. Separately, we studied threat monitoring to ensure the integrity of information and prevent unauthorised access to corporate resources in the environment of the NP contact centre office.

Keywords: legal, organisational, technical, hardware and software methods of information protection. In addition, the key concepts include encryption, cryptography, information security, data protection and data storage. These concepts form the basis of a modern cybersecurity system and ensure its comprehensiveness.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизована система.

ЗІ – захист інформації, комплекс заходів, спрямованих на запобігання несанкціонованому доступу до інформації.

ІБ – інформаційна безпека, стан захищеності інформації від внутрішніх і зовнішніх загроз.

КСЗІ – комплексна система захисту інформації, сукупність технічних, програмних і організаційних заходів для забезпечення ІБ.

ЛВС – локальна обчислювальна мережа, мережа, що забезпечує обмін інформацією між пристроями в межах обмеженої території.

Twofish – симетричний блоковий алгоритм шифрування, що забезпечує високий рівень криптографічного захисту даних.

ЕЦП – електронний цифровий підпис, спосіб ідентифікації підписанта в електронному документі.

ХЕШ-функція – математична функція, що перетворює вхідні дані у фіксовану строку символів, яка називається хешем.

Несанкціонований доступ (НСД) – доступ до інформації без дозволу на це, що порушує встановлені правила безпеки.

Інформаційна безпека – комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності й доступності інформації.

Криптографія – наука, яка вивчає методи шифрування інформації для забезпечення її захисту.

ЦОД – центр обробки даних, приміщення з обладнанням для зберігання та обробки великого обсягу інформації.

C# – об’єктно-орієнтована мова програмування, яка використовується для створення додатків різного призначення, включаючи засоби криптографічного захисту.

AES – Advanced Encryption Standard, сучасний алгоритм симетричного шифрування, що широко використовується для захисту даних.

MD5 – Message Digest 5, криптографічна хеш-функція, яка створює 128-бітний хеш.

RSA – алгоритм асиметричного шифрування, що базується на складності факторизації великих чисел.

Дані – відомості в будь-якій формі, що підлягають обробці або зберіганню.

Алгоритм шифрування – набір математичних правил для перетворення вихідних даних у зашифрований вигляд.

Сервер – комп’ютер або пристрій, що надає послуги або дані іншим пристроям у мережі.

ВСТУП

Проблема захисту інформації існує вже тривалий час і виникла задовго до появи комп’ютерів. Розвиток технологій, зокрема стрімкий прогрес у сфері комп’ютерних систем, вплинув і на підходи до побудови систем захисту інформації.

Перші системи інформаційної безпеки були орієнтовані переважно на військові потреби, оскільки витік секретних даних міг спричинити серйозні наслідки, включаючи людські втрати. Тому особливу увагу приділяли забезпеченню конфіденційності даних. Одним із ключових засобів, що гарантують нерозголошення інформації, стало повне її шифрування.

У сучасних умовах основний акцент робиться на захист інформації, яка передається та обробляється в комп’ютерних мережах. Інтенсивне впровадження комп’ютерних систем у всі сфери діяльності, постійне збільшення їхньої обчислювальної потужності, а також активне використання локальних і глобальних мереж призвели до зростання ризиків втрати конфіденційної інформації. Сьогодні загрози безпеці даних стали невід’ємною частиною роботи більшості організацій.

Основним принципом сучасного захисту інформації є пошук балансу між її доступністю та безпекою. Абсолютний захист можливий лише за умови, що комп’ютер повністю ізольований: він зберігається у броньованій кімнаті, відключений від усіх мереж, включаючи електроживлення, і не використовується. Проте в такій ситуації вимога доступності інформації не виконується, що робить систему непрактичною. Таким чином, забезпечення оптимального співвідношення між безпекою і доступністю залишається ключовим завданням у розробці систем захисту інформації, незважаючи на їхню зростаючу складність [1].

РОЗДІЛ 1
НОРМАТИВНО-ПРАВОВА БАЗА ТА ПОСТАНОВКА ЗАВДАНЬ ДЛЯ РОЗРОБКИ

Законодавчі заходи у сфері захисту інформації спрямовані на забезпечення виконання чинних у державі нормативно-правових актів або впровадження нових законів, положень, постанов та інструкцій. Їх метою є регулювання юридичної відповідальності посадових осіб, користувачів та технічного персоналу за витік, втрату чи несанкціоновану модифікацію інформації, яка перебуває під їхньою опікою.

Окрему увагу приділено також попередженню дій, які виходять за межі встановлених повноважень, та притягненню до відповідальності сторонніх осіб за навмисні спроби отримати несанкціонований доступ до захищених даних.

Головною метою таких законодавчих заходів є створення умов для запобігання порушенням, стримування потенційних зловмисників та встановлення правової основи для забезпечення інформаційної безпеки.

Крім того, законодавство допомагає формувати культуру відповідального поводження з інформацією, що є важливим чинником у мінімізації ризиків її компрометації.

1.1 Закон України «Про захист персональних даних»

Цей Закон регулює правовідносини, що стосуються захисту та обробки персональних даних, і має на меті забезпечення захисту фундаментальних прав і свобод людини, зокрема права на приватність, у контексті обробки персональної інформації.

Положення Закону поширюються на всі види діяльності, пов'язані з обробкою персональних даних, незалежно від того, чи використовуються для цього автоматизовані засоби повністю або частково.

Водночас дія Закону охоплює обробку даних, що зберігаються у картотеках або призначені для внесення до них, з використанням як автоматизованих, так і ручних методів.

База персональних даних визначається як структурована сукупність упорядкованої інформації про фізичних осіб, що зберігається в електронному вигляді або у формі картотек.

Обробка персональних даних охоплює будь-які операції або їх сукупність, включно зі збиранням, реєстрацією, накопиченням, зберіганням, адаптацією, модифікацією, оновленням, використанням, поширенням (передачею, розповсюдженням, реалізацією), знеособленням і знищенням, зокрема із застосуванням автоматизованих інформаційних систем.

Під персональними даними розуміється інформація або сукупність даних, які стосуються фізичної особи, ідентифікованої або що може бути ідентифікована [2].

1.2 Закон України «Про інформацію»

У цьому Законі наведені терміни використовуються у такому значенні:

1. Документ – це матеріальний носій, який містить інформацію, основними функціями якого є забезпечення її збереження, передачі та можливості відтворення у часі та просторі. Документ може мати як фізичну, так і електронну форму, залежно від способу збереження даних.

2. Захист інформації – це комплекс заходів, який включає правові, адміністративні, організаційні, технічні та інші дії, спрямовані на забезпечення збереження, цілісності та конфіденційності інформації, а також на дотримання встановленого порядку доступу до неї. Метою таких заходів є мінімізація ризиків несанкціонованого доступу, модифікації чи втрати інформації.

3. Інформація – це сукупність даних і/або відомостей, які можуть бути збережені на різних матеріальних носіях, представлені в електронному вигляді

або передані через інформаційні системи. Інформація може бути персональною, комерційною, технічною або державною залежно від її змісту та цінності.

4. Суб'єкт владних повноважень – це орган державної влади, орган місцевого самоврядування чи інша юридична особа, що здійснює управлінські або регуляторні функції згідно із законодавством. До цієї категорії також належать суб’єкти, яким делеговано владні повноваження для виконання певних функцій у межах чинного законодавства.

Дані визначення створюють основу для розуміння ключових понять, які використовуються у сфері інформаційної безпеки та регулювання доступу до інформації [3].

1.3 Закон України про Національну програму інформатизації

У цьому Законі терміни визначаються наступним чином:

1. Адміністрування засобу інформатизації – це управлінська діяльність, яку здійснює власник або технічний адміністратор під час експлуатації засобів інформатизації. Вона спрямована на забезпечення їх ефективного управління та доступності для користувачів інформаційно-комунікаційних систем і технологій.

2. База даних – це організована сукупність даних, що систематично відображає стан об'єктів і зв'язків між ними в конкретній предметній області.

3. Банк даних – це комплекс програмно-апаратних, організаційних і технічних засобів, призначених для централізованого зберігання, обробки та використання даних.

4. Засоби інформатизації – це різноманітні технічні, програмні та системні засоби, включаючи комп’ютери, електронно-обчислювальну техніку, програмне забезпечення, інформаційні системи та їх компоненти, а також електронні комунікаційні мережі, які забезпечують впровадження інформаційно-комунікаційних технологій.

5. Інформаційно-комунікаційні технології – це результат інтелектуальної діяльності, що включає систематизовані знання, технічні рішення, організаційні методи та процедури, спрямовані на збір, обробку, накопичення та використання інформації, а також надання відповідних послуг.

6. Створення засобу інформатизації – це комплекс заходів, до яких належать правові, організаційні, адміністративні й інженерно-технічні дії. Їх здійснює розпорядник або отримувач бюджетних коштів для автоматизації одного чи кількох процесів, включаючи розробку комплексної системи захисту інформації, визначення необхідності таких засобів та їх введення в експлуатацію.

Такі визначення забезпечують єдине розуміння ключових понять, які стосуються інформатизації та інформаційної безпеки, в межах правового регулювання [4].

1.4 Закон України «Про захист інформації в автоматизованих системах»

У цьому Законі терміни використовуються в такому значенні:

1. Автоматизована система (АС) – це комплексна система, яка забезпечує автоматизовану обробку даних. До її складу входять технічні засоби, такі як обчислювальна техніка і засоби зв’язку, програмне забезпечення, а також методи й процедури, що забезпечують виконання завдань обробки даних.

2. Інформація в АС – це всі дані та програми, що використовуються в автоматизованій системі, незалежно від форми їх подання чи способу організації.

3. Обробка інформації – це сукупність операцій, що виконуються з використанням технічних і програмних засобів. До них належать збирання, введення, збереження, запис, перетворення, зчитування, реєстрація, знищення інформації, а також її передача по каналах зв’язку.

4. Захист інформації – це комплекс організаційно-технічних заходів і правових норм, спрямованих на запобігання завданню шкоди власникам інформації або автоматизованої системи, а також користувачам цієї інформації.

5. Несанкціонований доступ – це доступ до інформації, що здійснюється з порушенням правил розмежування доступу, встановлених для конкретної автоматизованої системи.

6. Витік інформації – результат дій, унаслідок яких інформація стає доступною особам або організаціям, які не мають права доступу до неї.

7. Втрата інформації – це дія чи подія, внаслідок якої інформація, що зберігається в АС, стає недоступною для осіб або організацій, які мають законне право на її використання.

Ці визначення формують основу для чіткого розуміння та управління процесами, що стосуються захисту та обробки інформації в автоматизованих системах [5].

1.5 Закон України «Про державну таємницю»

Цей Закон охоплює діяльність органів законодавчої, виконавчої та судової влади, прокуратури, а також інших державних органів, включаючи територіальні підрозділи центральних органів виконавчої влади, що відповідають за митну та податкову політику, які не мають статусу юридичної особи. Закон також поширюється на Верховну Раду та Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи, організації всіх форм власності та об’єднання громадян, які здійснюють діяльність, пов’язану з державною таємницею. Він стосується громадян України, іноземців та осіб без громадянства, що отримали доступ до державної таємниці відповідно до чинного законодавства.

Відомості, передані Україні іншими державами чи міжнародними організаціями, що мають статус таємниці, захищаються відповідно до цього Закону. Якщо міжнародний договір, ратифікований Верховною Радою України, передбачає інші правила захисту таких даних, ніж ті, що визначені цим Законом, діють положення міжнародного договору [6].

1.6 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступуії

Цей нормативний документ з технічного захисту інформації (НД ТЗІ) встановлює концептуальні засади для вирішення завдань захисту інформації в комп’ютерних системах. Він служить основою для розробки нормативних і методологічних матеріалів, які регламентують такі питання:

- встановлення вимог до захисту комп’ютерних систем від несанкціонованого доступу;
- розробка захищених комп’ютерних систем і засобів захисту від несанкціонованого доступу;
- оцінювання рівня захищеності комп’ютерних систем і їх придатності для вирішення завдань споживачів.

Цей документ призначений для постачальників (розробників) і споживачів (замовників, користувачів) комп’ютерних систем, які застосовуються для обробки, включаючи збирання, зберігання, передачу тощо, критичної інформації, що потребує захисту. Також він є корисним для державних органів, які здійснюють нагляд та контроль за обробкою такої інформації [7].

1.7 Закон України «Основи законодавства України про охорону здоров'я»

Кожна людина володіє невід’ємним та непорушним правом на охорону свого здоров’я. Держава та суспільство несуть спільну відповідальність перед нинішніми і майбутніми поколіннями за стан здоров’я населення та збереження генофонду українського народу. Це передбачає пріоритетність охорони здоров’я в державній політиці, поліпшення умов праці, навчання, побуту і відпочинку громадян, розв'язання екологічних проблем, підвищення якості медичної допомоги та популяризацію здорового способу життя.

Основи законодавства України у сфері охорони здоров’я встановлюють правові, організаційні, економічні та соціальні принципи захисту здоров’я громадян. Вони регулюють суспільні відносини у цій сфері з метою гармонійного розвитку фізичних і духовних можливостей людей, забезпечення їхньої високої працездатності та активного довголіття. Також приділяється увага усуненню шкідливих для здоров’я чинників, зниженню рівня захворюваності, попередженню інвалідності та смертності, а також покращенню генетичної спадковості нації.

Охорона здоров’я розглядається як ключовий елемент сталого розвитку суспільства, що впливає на якість життя кожної людини та майбутнє держави [8].

1.8 Криптографічні вимоги

Криптографічні вимоги базуються на шеннонівському підході, який визначає складність дешифрування повідомлень, і сучасній концепції важкорозв'язуваних задач. Основою цих вимог є такі параметри, як трудомісткість отримання відкритого тексту та обсяг інформації, яку потенційно може бути перехоплено. Для електронного цифрового підпису (ЕЦП) визначальним є показник трудомісткості підробки підпису, а для хеш-функцій — складність створення колізій.

Криптографічні вимоги також охоплюють надійнісні характеристики шифрувальних пристроїв, які забезпечують захист інформації навіть за умови відмов обладнання чи перебоїв електроживлення. Особливу увагу приділено вимогам до ключів та іншої криптографічної інформації, включаючи їхню генерацію, зберігання, передачу та знищення.

Організаційно-технічні вимоги стосуються безпеки фізичного середовища, в якому обробляється конфіденційна інформація. До них входять заходи з охорони приміщень, технічних засобів та ключових документів, а також правила використання ключів, умови зберігання та забезпечення доступу до критичних об’єктів. Додатково встановлюються вимоги щодо обладнання приміщень для захисту від акустичних, оптичних та інших витоків інформації, а також регламентується розміщення технічних засобів для мінімізації ризиків несанкціонованого доступу.

Такі комплексні заходи спрямовані на забезпечення високого рівня інформаційної безпеки в умовах сучасних загроз.

1.9 Криптографічний захист інформації

Криптографічний захист інформації охоплює процеси планування, розробки, впровадження та забезпечення функціонування механізмів для захисту даних. Це є ключовим елементом у збереженні інформаційного простору держави від негативних впливів, зокрема, від ворожих дій з боку іноземних держав або неконституційних дій окремих організацій чи осіб, що може мати форму інформаційної війни.

Інформаційна безпека — це міждисциплінарна наука, яка має забезпечувати безпечне функціонування в інформаційному просторі як для всього людства, так і для окремих держав та їхніх громадян. Злочинні посягання на інформацію, такі як викрадення, спотворення, пошкодження чи знищення даних, порушують її цілісність. Завдання інформаційного захисту полягає в

запобіганні таким порушенням, незалежно від того, чи мають вони навмисний чи ненавмисний характер.

Особливе значення має інформаційна безпека в правоохоронних органах, адже вона спрямована на захист цілісності даних, що циркулюють у цих установах. Особливу увагу приділяють державній таємниці, перелік якої визначено у "Зводі відомостей, що становлять державну таємницю", затвердженому наказом Голови Служби безпеки України № 52 від 1 березня 2001 року.

Крім того, конфіденційна інформація в автоматизованих системах, каналах зв’язку та робочих приміщеннях правоохоронних органів також потребує надійного захисту. Ще одним викликом для правоохоронних органів є протидія дезінформації, яка може негативно впливати на прийняття рішень та порушувати громадський порядок.

Комплексний підхід до криптографічного захисту та інформаційної безпеки є важливим інструментом у забезпеченні національної безпеки та ефективного функціонування ключових державних структур.

1.10 Постанова задачі

Цілі: створення ефективної системи захисту інформації для корпоративної мережі контакт-центру «НОВА ПОШТА» із застосуванням сучасних методів шифрування, таких як криптографічний алгоритм Twofish, та інструментів моніторингу загроз.

Об’єкт: аналіз стану інформаційної безпеки та забезпечення комплексного захисту даних в офісі контакт-центру «НОВА ПОШТА».

Предмет: структура, засоби та механізми захисту інформації в офісі контакт-центру «НОВА ПОШТА».

На основі проведеного аналізу проблеми сформульовано ключові завдання та критерії для виконання комплексного аналізу.

Основні завдання проекту:

1. Провести оцінку поточного стану систем захисту інформації в офісі.
2. Виконати аналіз існуючої мережевої інфраструктури підприємства та її вразливостей.
3. Оцінити стан програмного забезпечення, яке використовується в підприємстві, з акцентом на безпеку.
4. Розробити рекомендації щодо вдосконалення засобів захисту інформації, включаючи апаратні та програмні компоненти.
5. Реалізувати систему інформаційного захисту, яка включатиме механізм передачі даних та повідомлень із застосуванням криптографічного алгоритму Twofish. Розробка здійснюватиметься на основі мови програмування C#.

Цей підхід дозволить забезпечити конфіденційність, цілісність та доступність інформації, а також знизити ризики, пов’язані з можливими кібератаками на мережу та системи контакт-центру.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ЙОГО ВДОСКОНАЛЕННЮ

2.1 Загальні відомості про підприємство

Рисунок 2.1 – Історія створення компанії

Компанія «Нова Пошта» розпочала свою діяльність у лютому 2001 року, коли друзі В'ячеслав Климов і Володимир Поперешнюк вирішили заснувати власну справу. Їм було по 25 років, і вибір ніші підказав кондитерський бізнес Володимира, який потребував швидкої доставки товарів. Так виникла ідея запропонувати українцям послугу експрес-доставки (рис. 2.1).

Стартовий капітал компанії становив 7000 доларів, а перша команда налічувала 7 осіб. Основними засновниками стали Климов і Поперешнюк, а Інна Поперешнюк долучилася як міноритарний партнер.

Це стало початком історії компанії, яка згодом створила в Україні ринок швидкої доставки [9].

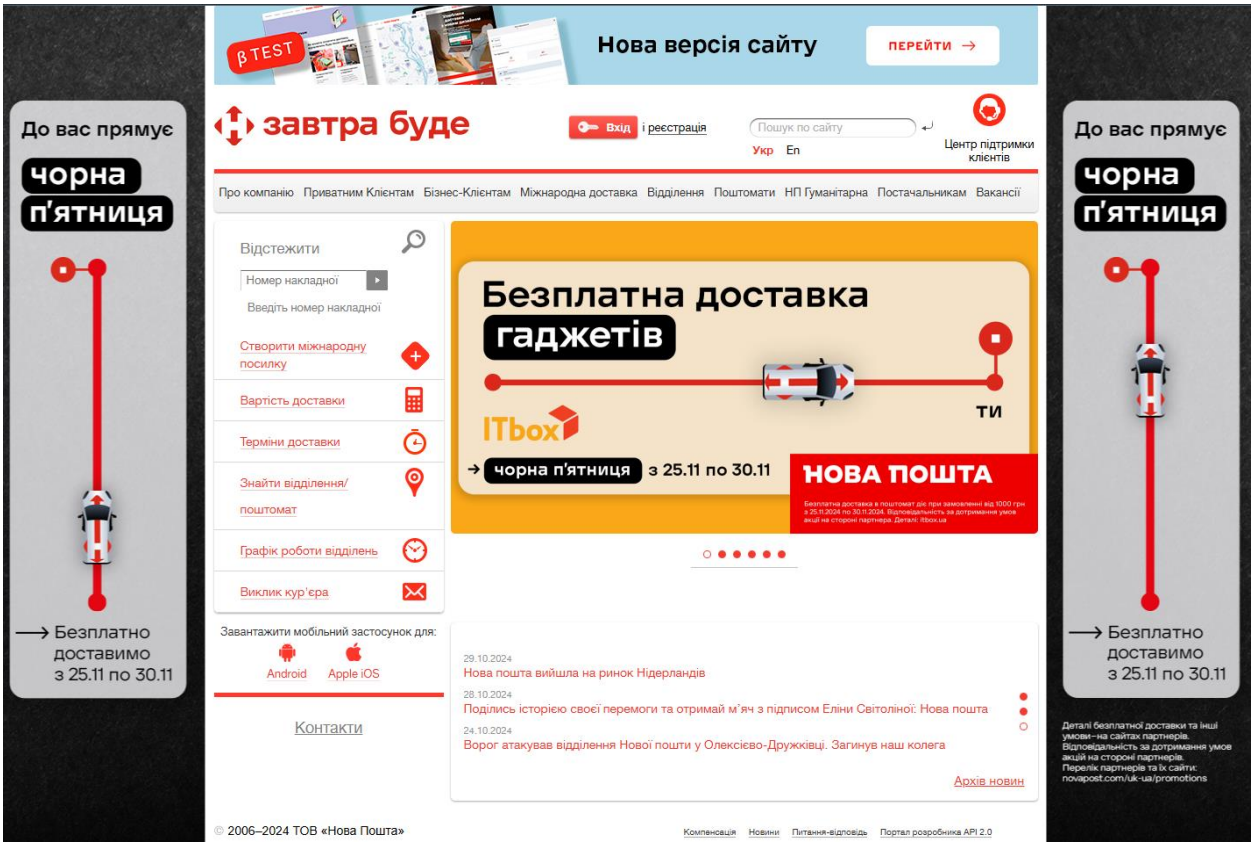

Рисунок 2.2 – Офіційний сайт «Нової пошти»

Рисунок 2.3 – Логотип компанії «Нова пошта»

Рисунок 2.4 – Офіс контакт центру «Нової пошти»

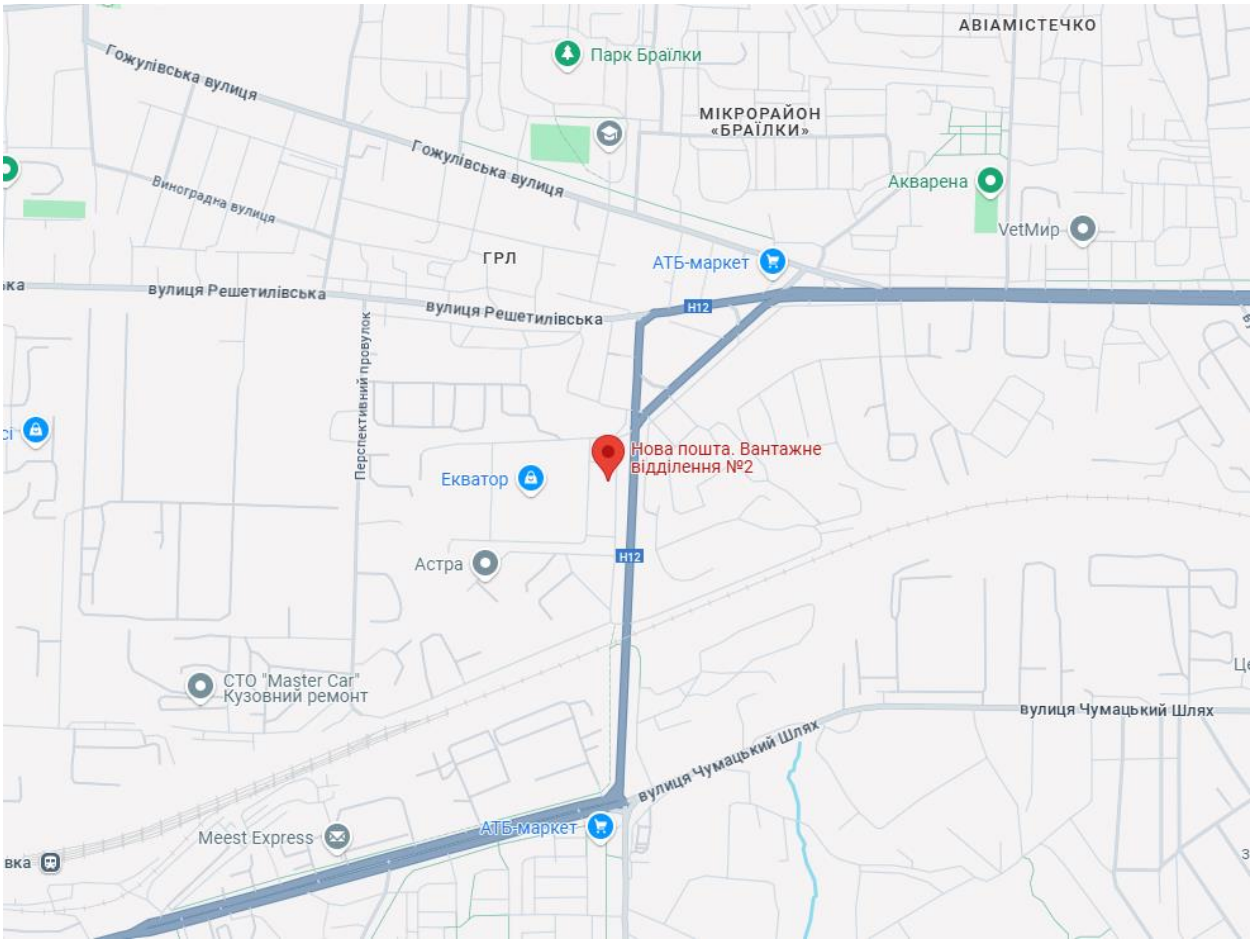

Рисунок 2.5 – Карта (1) розміщення офісу контакт центру «Нової пошти»

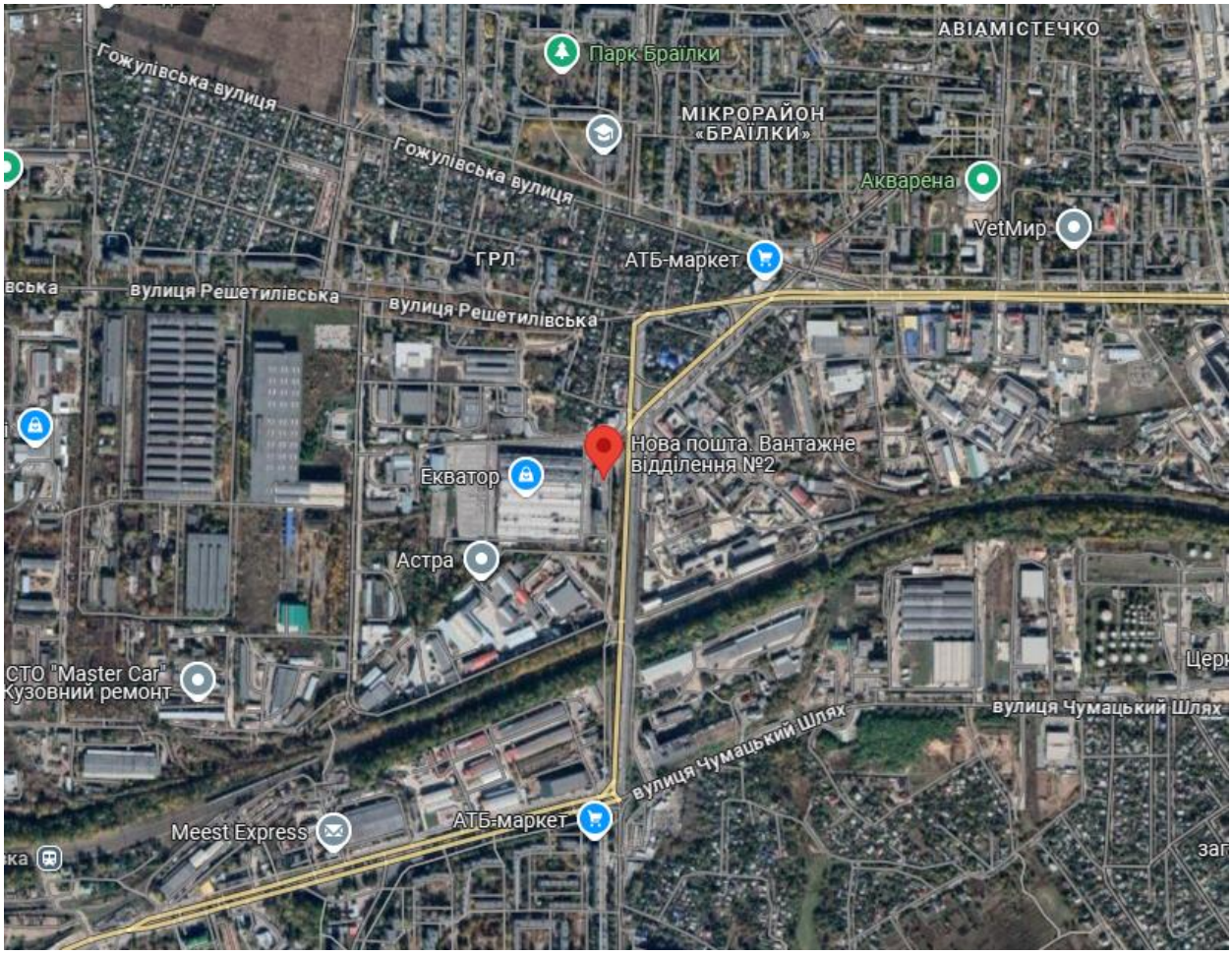

Рисунок 2.6 – Карта (2) розміщення офісу контакт центру «Нової пошти»

Контакт-центр «Нової Пошти» є важливою частиною клієнтського обслуговування та забезпечення високої якості надання послуг. Його завдання полягає у забезпеченні швидкої та ефективної комунікації між компанією та клієнтами, а також підтримці високого рівня задоволеності користувачів. Цей підрозділ працює через різноманітні канали зв’язку, включаючи телефонні дзвінки, електронну пошту, онлайн-чати, соціальні мережі та мобільний додаток. Такий багатоканальний підхід допомагає забезпечити оперативний зв’язок із клієнтами та розв'язання будь-яких питань, що виникають у процесі користування послугами компанії.

Контакт-центр виконує кілька важливих функцій для забезпечення якісного обслуговування клієнтів:

1. *Консультації щодо послуг компанії.* Це один із найважливіших напрямків діяльності контакт-центру. Працівники надають консультації щодо широкого спектру послуг, які пропонує «Нова Пошта».

2. *Обробка запитів і скарг.* У роботі контакт-центру вагоме місце займає обробка скарг та вирішення проблемних ситуацій. Оператори контакт-центру здійснюють координацію з відділом логістики та іншими підрозділами, щоб оперативно розв'язати проблему клієнта. Додатково, збираються відгуки про послуги компанії, щоб аналізувати типові проблеми та допомагати керівництву у вдосконаленні процесів.

3. *Підтримка користувачів онлайн-сервісів.* Це включає допомогу в реєстрації, оформленні заявок на доставку, користуванні трекінговою системою для відстеження посилок та отриманні інформації про статус відправлень. Працівники контакт-центру консультують користувачів з питань функціональності онлайн-платформ, інформують про нові можливості та, за потреби, надають інструкції з їх використання.

4. *Продажі та промоція нових послуг.* Контакт-центр також виконує функцію інформування клієнтів про нові послуги та акції, які пропонує компанія. Наприклад, оператори можуть пропонувати клієнтам скористатися додатковими послугами, такими як пакування відправлень, страхування вантажу чи доставка за адресою. Така діяльність допомагає розширити користування послугами та покращує загальний клієнтський досвід.

5. *Оперативна допомога.* Оператори контакт-центру мають можливість швидко реагувати на запити та забезпечувати оперативне внесення змін, щоб відповідати потребам клієнтів. Це особливо актуально для бізнес-клієнтів, які мають термінові відправлення або специфічні вимоги до доставки.

Контакт-центр працює через декілька каналів комунікації:

1. *Телефонні дзвінки.* Це найпоширеніший спосіб зв'язку з контакт-центром. Телефонні лінії надають змогу клієнтам швидко зв'язатися з оператором, особливо у випадках, що потребують оперативної допомоги.

2. *Електронна пошта.* Клієнти, які мають нетермінові питання, можуть звертатися через електронну пошту. Це зручний спосіб подання скарг або запитів на додаткову інформацію.

3. *Чат на сайті та в мобільному додатку.* Онлайн-чат у мобільному додатку «Нової Пошти» та на її офіційному сайті дозволяє клієнтам отримати консультацію в реальному часі. Це зручно для молодших клієнтів, які звикли користуватися месенджерами та онлайн-комунікацією.

4. *Соціальні мережі.* Контакт-центр також відповідає на повідомлення, які надходять через сторінки компанії в соціальних мережах. Це дозволяє компанії бути ближче до клієнтів і швидко відповідати на загальні питання або відгуки.

Контакт-центр «Нової Пошти» є важливою складовою клієнтського обслуговування і забезпечує багато переваг для клієнтів:

1. *Зручність і доступність.* Клієнти можуть звертатися за допомогою через різноманітні канали, що робить процес комунікації простішим і зручнішим для всіх.

2. *Оперативність.* Контакт-центр працює за принципом оперативного реагування на звернення клієнтів, що дозволяє швидко вирішувати більшість питань та проблем.

3. *Індивідуальний підхід.* Оператори надають індивідуальні консультації та допомогу відповідно до потреб клієнта, що підвищує рівень задоволеності та лояльності.

4. *Поліпшення репутації.* Завдяки якісній роботі контакт-центру компанія отримує позитивні відгуки та репутацію відповідального та надійного партнера.

Контакт-центр «Нової Пошти» відіграє важливу роль у підвищенні якості обслуговування клієнтів та зміцненні позитивного іміджу компанії. Завдяки професійній підтримці та мультиканальній взаємодії, компанія забезпечує високу лояльність клієнтів та розвиває тривалі партнерські відносини.

2.2 Структура компанії

Структуру компанії створено за допомогою убудованого в MS Word інструменту SmartArt. Цей інструмент дозволяє швидко та зручно створювати візуальні схеми, які відображають організаційну структуру. Завдяки SmartArt можна легко додавати, видаляти або змінювати елементи, що дозволяє оперативно коригувати схему відповідно до потреб компанії.

Використання цього інструменту забезпечує чітке представлення ієрархічної структури організації, включаючи різні відділи, підрозділи та ролі. Крім того, SmartArt дозволяє наочно показати взаємозв’язки між елементами, що сприяє кращому розумінню процесів управління і координації в компанії.

Це рішення є ефективним для презентацій, звітів та внутрішніх документів, оскільки створює професійний вигляд і спрощує сприйняття інформації (рис. 2.9).

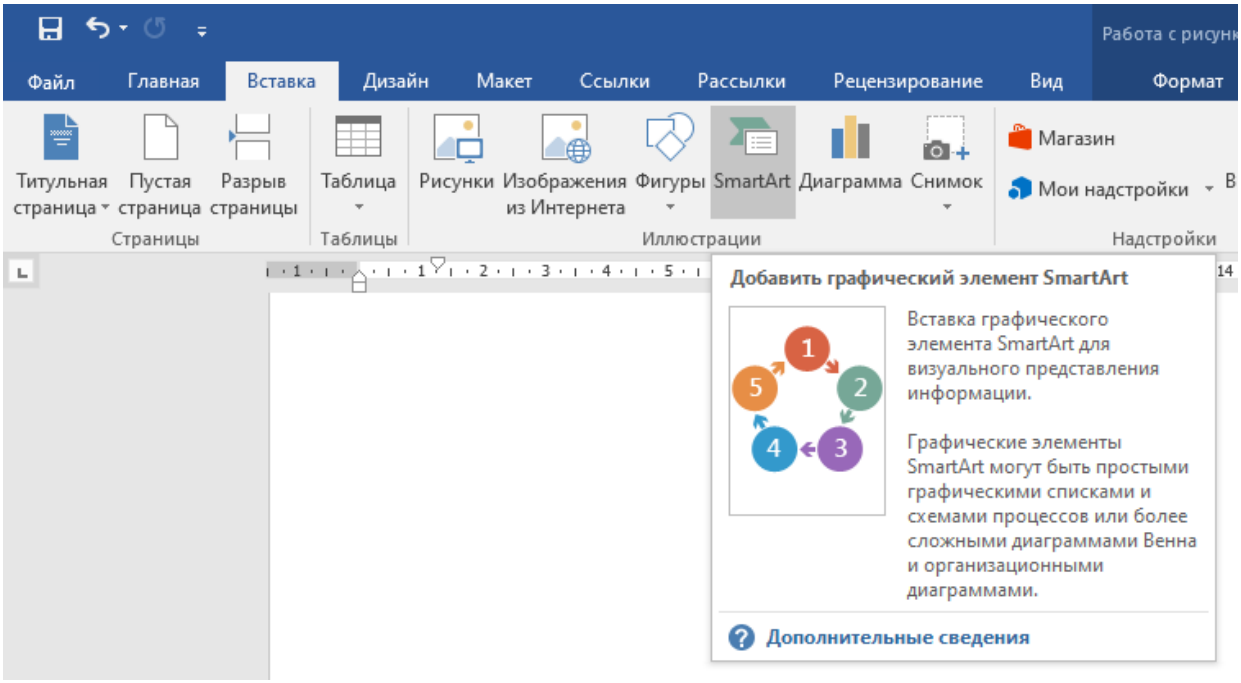

Рисунок 2.7 – Вибір SmartArt в MS Word

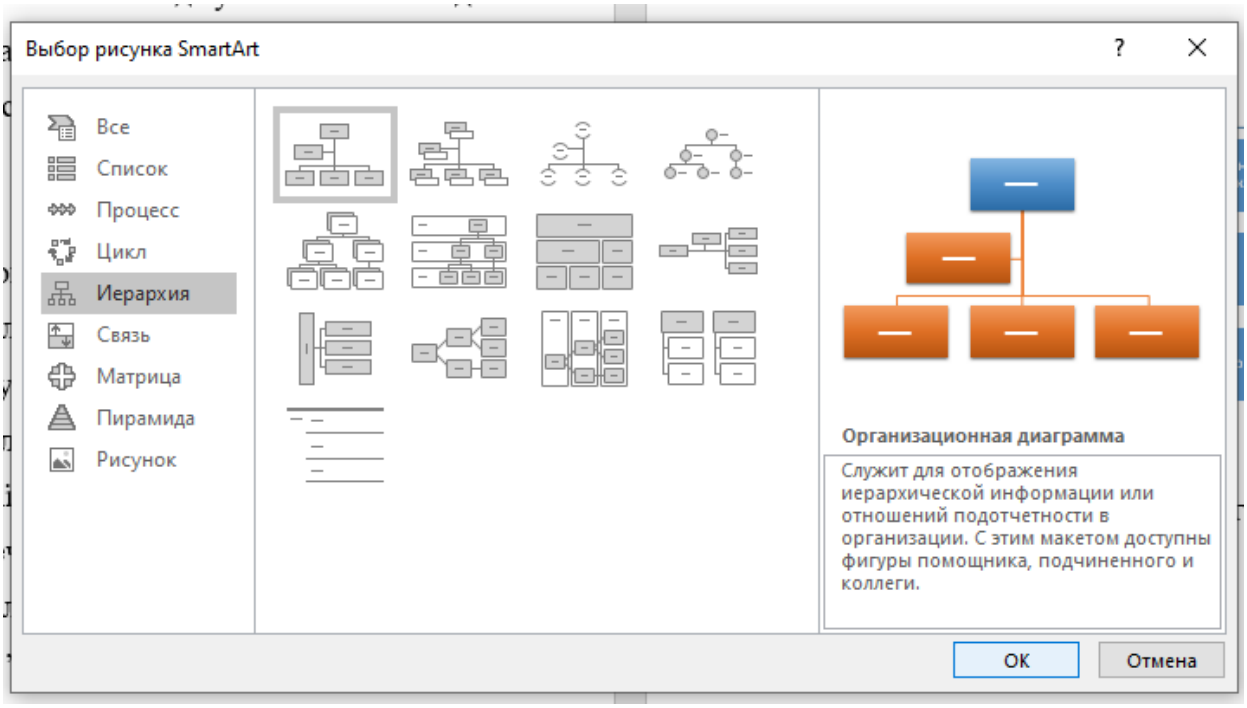

Рисунок 2.8 – Вибір макету в SmartArt

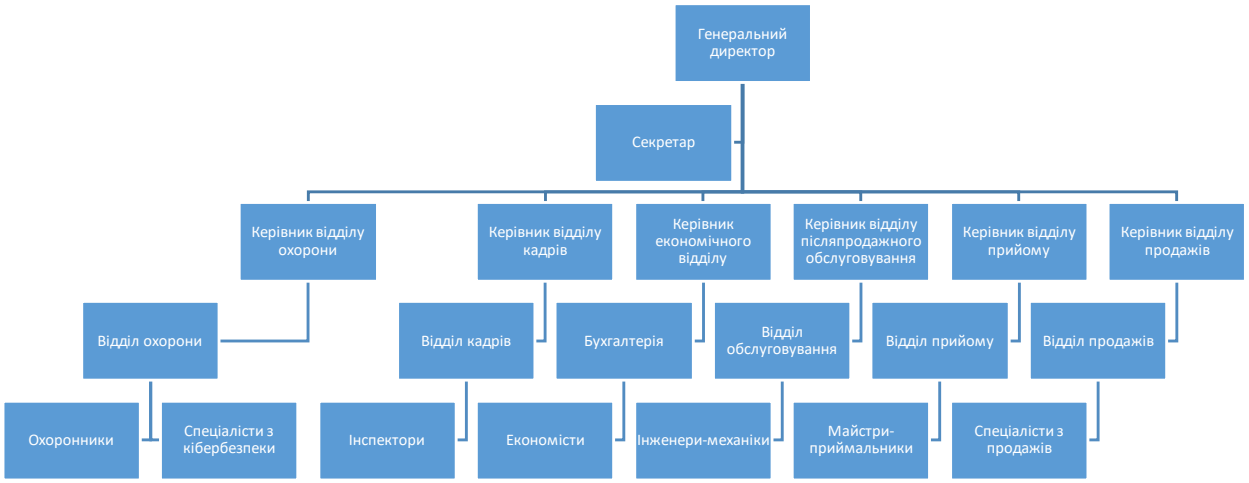

Рисунок 2.9 – Організаційна структура «Нової пошти»

Таблиця 2.1 Кількість та види техніки в кожному відділі

Посада	**Техніка**	**К-сть**
Генеральний директор	Комп’ютер Принтер	1 1
Секретар	Комп’ютер Принтер	1 1
Керівник відділу охорони	Комп’ютер	1
Охоронники	Комп’ютер	3
Спеціалісти з кібербезпеки	Комп’ютер Сервер	3 1
Керівник відділу кадрів	Комп’ютер	1
Інспектори відділу кадрів	Комп’ютер	3
Керівник економічного відділу	Комп’ютер Принтер	1 1
Економісти	Комп’ютер	5
Керівник відділу обслуговування	Комп’ютер	1
Інженери-механіки	Комп’ютер	4
Керівник відділу прийому	Комп’ютер	1
Майстри-приймальники	Комп’ютер	3
Керівник відділу продажів	Комп’ютер	1
Спеціалісти з продажів	Комп’ютер	6
	Всього	39

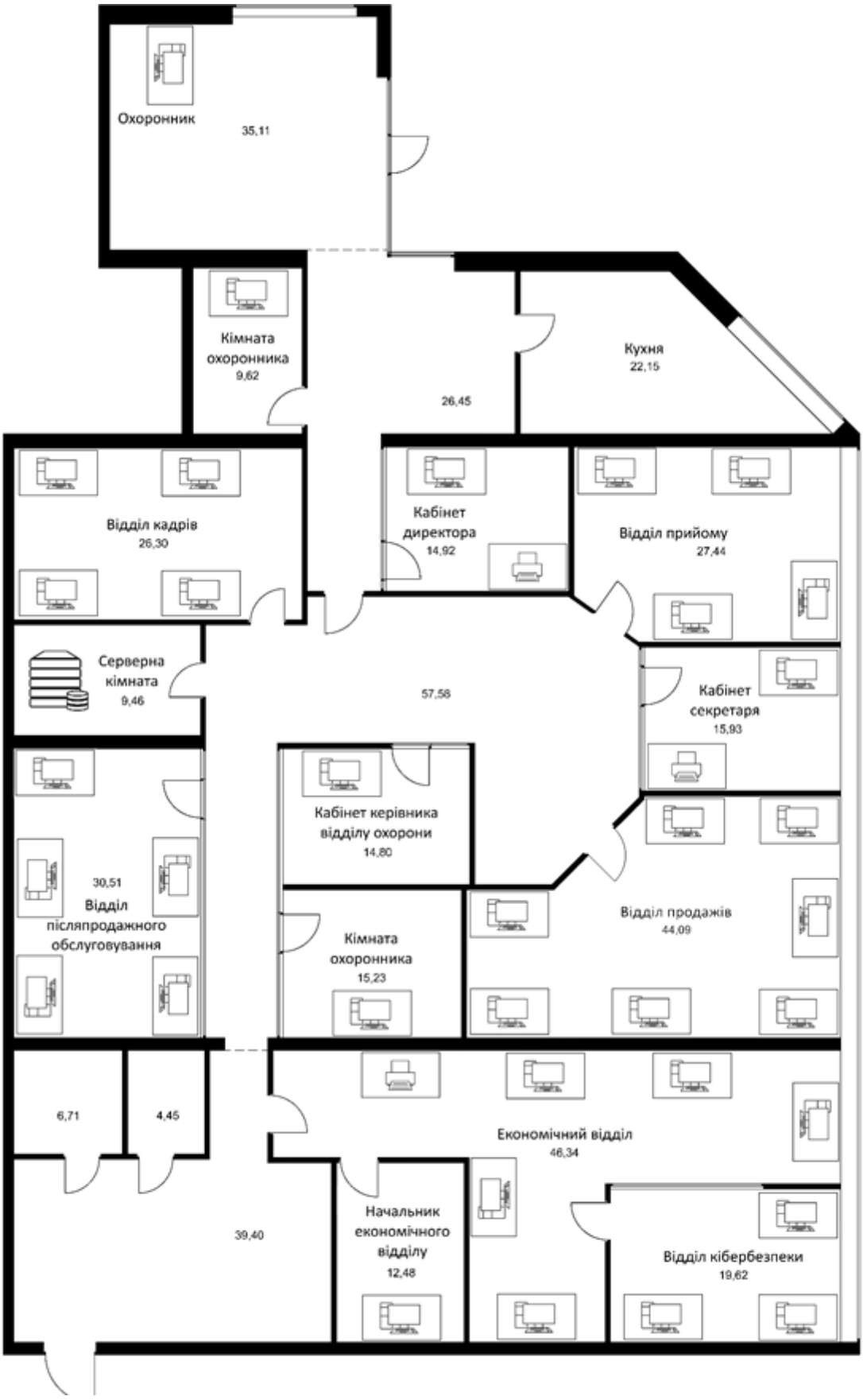

Рисунок 2.10 – Розміщення комп’ютерної техніки в офісі

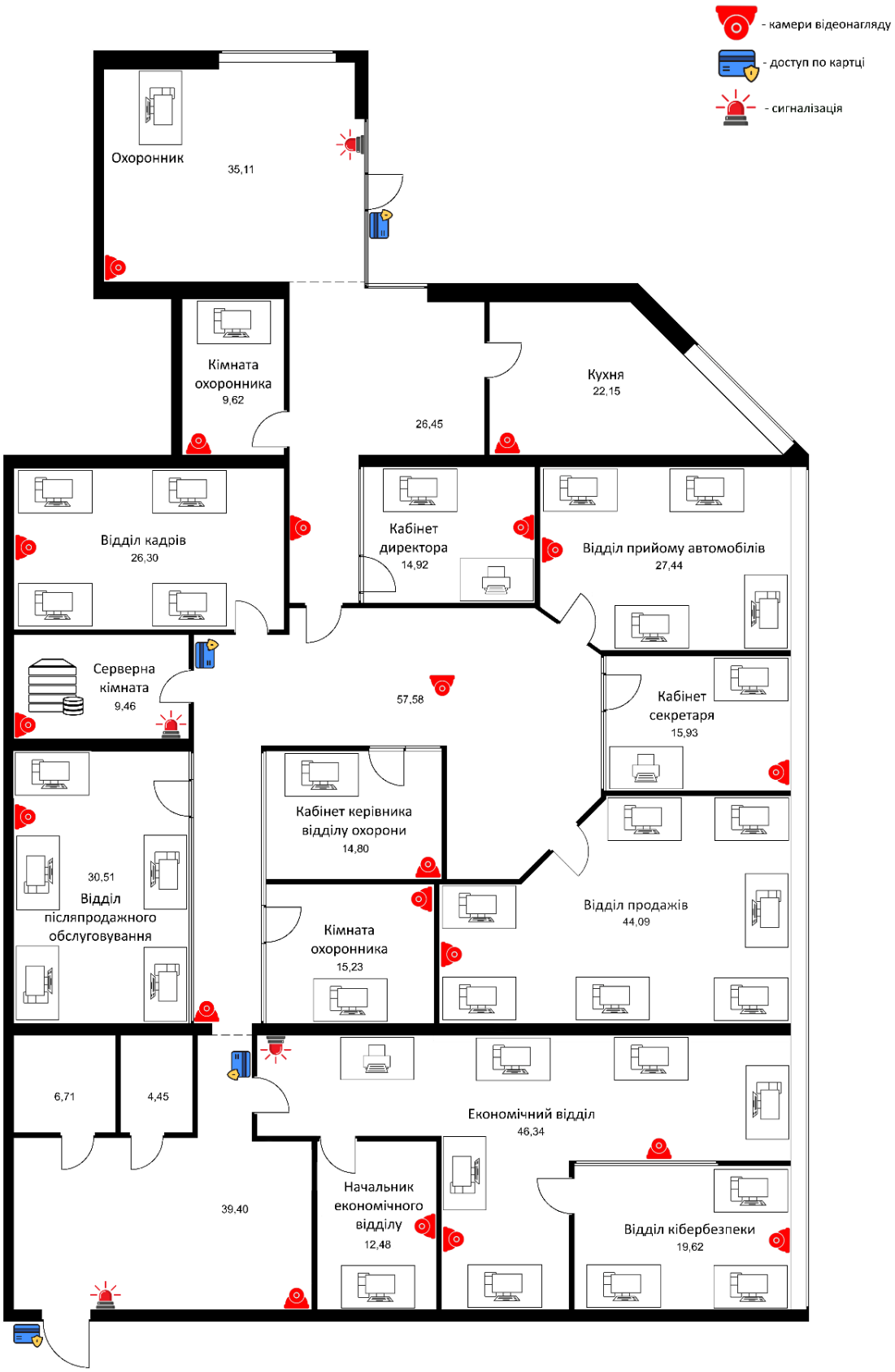

Рисунок 2.11 – План будівлі та розміщення засобів технічного та апаратного захисту

Таблиця 2.2 Назва кімнат та їх розміри

Назва кімнати	Розміри ($м^2$)
Охоронник	35.11
Кімната охоронника №1	9.62
Кімната охоронника №2	15.23
Кухня	22.15
Відділ кадрів	26.30
Серверна кімната	9.46
Відділ післяпродажного обслуговування	30.51
Кабінет директора	14.92
Кабінет керівника відділу охорони	30.51
Відділ прийому	27.44
Кабінет секретаря	15.93
Відділ продажів	44.09
Економічний відділ	46.34
Начальник економічного відділу	12.48
Відділ кібербезпеки	19.62
Прохідна зона (коридор 1)	26.45
Прохідна зона (коридор 2)	57.58
Прохідна зона (коридор 3)	39.40
Інша кімната	6.71
Інша кімната	4.45

2.3 Організація засобів захисту інформації на підприємстві

Для управління засобами захисту інформації на підприємстві призначається відповідальна особа — керівник охоронного відділу. Основними його завданнями є:

1. розробка і впровадження системи розмежування доступу, включаючи фізичний захист території, приміщень та технічного обладнання;

2. забезпечення інформаційної безпеки від витоків через технічні канали, наприклад, через електромагнітні випромінювання;

3. проведення технічних заходів із впровадження інноваційних рішень для захисту інформації, таких як впровадження кібербезпекових політик і моніторинг потенційних загроз.

2.4 Особливості реалізації системи розмежування доступу

Система розмежування доступу покликана гарантувати, що кожен користувач має доступ лише до тієї інформації, яка входить у сферу його повноважень. Це реалізується завдяки використанню диспетчера доступу, який аналізує запити користувачів у реальному часі.

Диспетчер взаємодіє із базою повноважень, де зберігаються дані про об’єкти та суб’єкти доступу. Процес прийняття рішень базується на декількох рівнях перевірок, серед яких:

4. розробка верифікація повноважень користувача;

5. забезпечення перевірка рівня чутливості інформації (наприклад, «Конфіденційно» чи «Секретно»);

6. реєстрація подій у системі з можливістю подальшого аудиту.

Адаптивні системи доступу з алгоритмами машинного навчання динамічно налаштовують рівні доступу залежно від поведінки користувача чи контексту [10].

2.5 Засоби охорони об’єкта

Для захисту об’єкта, на якому обробляється конфіденційна інформація, використовується багаторівнева система безпеки, яка охоплює:

1. *Фізичні бар’єри:* встановлення металевих дверей, решіток на вікнах та замків із електронними ключами.
2. *Системи моніторингу:* використання камер відеоспостереження та датчиків руху.
3. *Системи ідентифікації:* застосування карт доступу, біометричних систем (відбитків пальців, розпізнавання обличчя).

Додатково можна використовувати спеціалізовані програмні рішення для моніторингу внутрішніх мереж. Такі інструменти можуть аналізувати поведінку користувачів і виявляти аномалії, які можуть свідчити про спроби несанкціонованого доступу [11].

2.6 Технічні заходи

До технічних заходів із захисту інформації належить впровадження активних і пасивних методів:

Пасивні заходи:

- екранування технічного обладнання;
- встановлення звукоізоляції та фільтрів для зниження електромагнітного випромінювання;
- стабілізація джерел живлення для уникнення збоїв у роботі техніки.

Активні заходи:

- генерація електромагнітних завад для ускладнення перехоплення сигналів;
- регулярне сканування приміщень на наявність прихованих пристроїв для прослуховування.

Окрім цього, доцільно впроваджувати системи багатофакторної автентифікації для критично важливих вузлів, які можуть вимагати комбінацію кількох методів доступу: пароля, біометрії та фізичного ключа [12].

2.7 Розмежування доступу та модель Белла-ЛаПадули

Для гарантування інформаційної безпеки на підприємстві ключовим є впровадження ефективних моделей доступу, які забезпечують контроль над використанням даних. Однією з таких моделей є модель Белла-ЛаПадули. Її основна концепція полягає в мандатному керуванні доступом, що ґрунтується на встановленні ієрархічних рівнів доступу до даних і визначенні обмежень для їх передачі між суб’єктами системи.

Модель Белла-ЛаПадули працює за принципом "no read up, no write down":

1) *"No read up"* — суб’єкт із нижчим рівнем доступу не має права читати інформацію, призначену для суб’єктів із вищим рівнем допуску. Це запобігає витоку секретних даних.

2) *"No write down"* — суб’єкт із вищим рівнем доступу не може записувати дані на рівні з нижчими правами, щоб уникнути випадкового або навмисного зниження рівня захисту інформації.

Ця модель є надзвичайно корисною для підприємств із чіткою ієрархією управління та класифікацією даних, наприклад:

- у військових структурах для розмежування стратегічних і тактичних даних;
- у державних установах, де існують різні рівні секретності;
- у фінансових організаціях для захисту банківської таємниці.

У сучасних умовах динамічних даних рекомендується рольова модель доступу (RBAC), яка гнучко налаштовує доступ відповідно до завдань працівників.

Наприклад, у великій IT-компанії програмісти мають доступ лише до частини коду, а адміністративний персонал — до фінансових документів. [13].

Окрім моделей доступу, сучасні системи захисту інформації передбачають інтеграцію додаткових технологій і заходів:

1) *Криптографія:* Шифрування захищає дані під час передачі або збереження, наприклад, за допомогою TLS/SSL для безпечного обміну в Інтернеті.

2) *Штучний інтелект (ШІ):* ШІ аналізує поведінку користувачів і виявляє підозрілі дії, як-от раптовий доступ до великих обсягів даних.

3) *Аудит інформаційних систем:* Регулярні перевірки допомагають виявляти вразливості та впроваджувати оновлення.

Для підприємств, що працюють із великими обсягами конфіденційних даних, важливо створювати резервні копії та розробляти план відновлення у разі кібератак або технічних збоїв.

Отже, модель Белла-ЛаПадули в поєднанні з сучасними підходами до інформаційної безпеки допомагає підприємствам не лише забезпечувати конфіденційність і цілісність даних, а й адаптувати захисні системи до нових викликів цифрової епохи.

Таблиця 2.3 Матриця доступу

Види інформації / Відділи	Загальна інформація	Особиста інформація	Фінансова інформація	Економічна інформація	Технічна інформація	Правова інформація
Генеральний директор	+	+	+	+	+	+
Секретар	+	-	-	-	-	+
Керівник відділу охорони	+	+	-	-	-	+
Відділ охорони	+	-	-	-	-	-
Охоронник	+	-	-	-	-	-
Спеціаліст із кібербезпеки	+	+	-	-	-	+
Керівник відділу кадрів	+	+	-	-	-	+
Відділ кадрів	+	+	-	-	-	+
Інспектор з відділу кадрів	+	+	-	-	-	+
Керівник економічного відділу	+	-	-	+	-	+
Бухгалтерія	+	-	-	+	-	-
Економіст	+	-	-	+	-	-
Керівник відділу обслуговування	+	-	-	-	+	-
Відділ обслуговування	+	-	-	-	+	-
Інженер-механік	+	-	-	-	+	-
Керівник відділу прийому	+	-	-	-	+	-
Відділ прийому	+	-	-	-	+	-
Мастер-приймальник	+	-	-	-	+	-
Керівник відділу продажів	+	-	+	-	-	-
Відділ продажів	+	-	+	-	-	-
Спеціаліст з продажів	+	-	+	-	-	-
Рівень секретності інформації	Н	Т	ДСК	ДСК	ДСК	ДСК

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

Таблиця 2.4 Мандатна модель доступу

Види інформації / Відділи	Загальна інформація	Особиста інформація	Фінансова інформація	Економічна інформація	Технічна інформація	Правова інформація
Генеральний директор	П	Ч	Ч	Ч	Ч	П
Секретар	П	Ч	Н	Н	Н	Ч
Керівник відділу охорони	Ч	ЧД	Н	Н	Н	П
Відділ охорони	Ч	Ч	Н	Н	Н	Н
Охоронник	Ч	Ч	Н	Н	Н	Н
Спеціаліст із кібербезпеки	Ч	ЧД	Н	Н	Н	Ч
Керівник відділу кадрів	Ч	П	Н	Н	Н	Ч
Відділ кадрів	Ч	П	Н	Н	Н	Ч
Інспектор з відділу кадрів	Ч	П	Н	Н	Н	Ч
Керівник економічного відділу	Ч	Н	Н	П	Н	Ч
Бухгалтерія	Ч	Н	Н	П	Н	Н
Економіст	Ч	Н	Н	П	Н	Н
Керівник відділу обслуговування	Ч	Н	Н	Н	П	Н
Відділ обслуговування	Ч	Н	Н	Н	П	Н
Інженер-механік	Ч	Н	Н	Н	П	Н
Керівник відділу прийому	Ч	Н	Н	Н	П	Н
Відділ прийому	Ч	Н	Н	Н	П	Н
Мастер-приймальник	Ч	Н	Н	Н	П	Н
Керівник відділу продажів	Ч	Н	Н	П	Н	Н
Відділ продажів	Ч	Н	Н	П	Н	Н
Спеціаліст з продажів	Ч	Н	Н	П	Н	Н

Ч – читання;
ЧД – частковий доступ;
П – повний доступ;
Н – немає доступу;

2.8 Механізми аудиту і протоколювання. Облікові записи

Протоколювання — це систематичний процес збору, накопичення та збереження даних про події, що відбуваються в межах інформаційної системи. Це важливий компонент забезпечення інформаційної безпеки, який дозволяє створювати детальний журнал роботи системи. Завдяки цьому механізму можна аналізувати активність користувачів, адміністраторів, а також поведінку самої системи.

Події, які реєструються в системах протоколювання, можна умовно поділити на три основні категорії:

1) *Зовнішні події.* Вони викликані діями або впливом інших сервісів чи систем. Наприклад, це може бути запит від сторонньої системи на обмін даними або авторизація зовнішнього користувача.

2) *Внутрішні події.* Генеруються самою системою або її компонентами. Це можуть бути автоматичні оновлення, виконання запланованих завдань або обробка запитів користувачів.

3) *Клієнтські події.* Спричинені діями користувачів або адміністраторів системи. Наприклад, це входи в систему, зміна налаштувань або запити на виконання операцій.

Аудит інформаційної безпеки — це структурований процес оцінки поточного стану системи захисту даних організації. Його мета полягає у визначенні відповідності рівня безпеки встановленим стандартам, критеріям та вимогам.

Аудит дозволяє отримати об'єктивну картину захищеності системи та знайти слабкі місця для їх подальшого усунення.

Основні завдання аудиту та протоколювання:

1) *Підзвітність дій користувачів і адміністраторів.* Реєстрація всіх дій у системі створює прозоре середовище, що дисциплінує користувачів та адміністраторів. У разі підозр у неправомірних діях можна детально перевірити активність конкретного користувача, включно з його запитами та навіть натисканням клавіш. Такий підхід сприяє розслідуванню інцидентів, захисту цілісності даних і відновленню інформації після помилкових або зловмисних змін.

2) *Реконструкція подій.* Завдяки детальному журналу подій можна проаналізувати послідовність дій, які призвели до інциденту, виявити вразливості в системі, оцінити завдану шкоду і розробити план для усунення наслідків.

3) *Виявлення порушень.* Протоколювання дозволяє виявляти несанкціоновані дії навіть після їх завершення. Це важливо для аналізу вже здійснених порушень і створення механізмів їх запобігання в майбутньому.

4) *Покращення системи.* Аналіз даних протоколювання допомагає ідентифікувати "вузькі місця" системи, які можуть впливати на її продуктивність або доступність. Завдяки цьому можна оптимізувати конфігурацію системи, забезпечуючи її стабільну роботу.

Обліковий запис є основним механізмом, що забезпечує ідентифікацію користувачів в інформаційній системі. Він включає набір даних, які дозволяють визначити права доступу користувача до певних ресурсів та налаштувань.

Для входу в систему зазвичай потрібні:

a) Логін (ідентифікатор користувача).

b) Пароль. Це один із ключових елементів, що забезпечує аутентифікацію. Для підвищення безпеки паролі зазвичай зберігаються у зашифрованому або хешованому вигляді.

Окрім базових даних, обліковий запис може містити:

a) *Особисті дані користувача.* Наприклад, ім’я, прізвище, контактну інформацію.

b) *Запитання для відновлення доступу.* Це можуть бути секретні запитання з відповідями, відомими лише користувачеві.

c) *Додаткові параметри безпеки.* Наприклад, криптографічні ключі, апаратні токени, або біометричні дані.

Для посилення захисту системи часто використовуються додаткові механізми аутентифікації:

a) *Одноразові паролі.* Генеруються для одноразового використання і мінімізують ризик крадіжки пароля.

b) *Криптографічні ключі.* Вони можуть зберігатися на зовнішніх носіях або спеціалізованих апаратних пристроях.

c) *Біометричні дані.* Використовують унікальні характеристики користувача, наприклад відбитки пальців або розпізнавання обличчя.

Сучасні облікові записи інтегрують різноманітні засоби захисту, щоб запобігти несанкціонованому доступу. Проте ефективність цього залежить не лише від технічних заходів, а й від відповідальності самих користувачів, які повинні дотримуватись правил створення та зберігання паролів.

Сучасні системи протоколювання можуть бути інтегровані з аналітичними інструментами на базі штучного інтелекту. Це дозволяє не лише виявляти підозрілі події, але й прогнозувати потенційні загрози. Наприклад, автоматичне виявлення аномальної активності користувачів або зовнішніх підключень може допомогти запобігти кібератакам.

Таким чином, ефективне протоколювання, аудит та використання надійних облікових записів є основою для забезпечення комплексної інформаційної безпеки. Це поєднання технологій, процесів та правил дозволяє забезпечити

конфіденційність, цілісність і доступність даних у будь-якій інформаційній системі [14].

Для кожного користувача визначено окремі облікові записи (табл. 2.5).

Таблиця 2.5 Приклад облікових записів користувачів

Посада	**Логін**	**Пароль**
Сервер	server_1428	Novagorsaker
Генеральний директор	gendir_ceo	Gendirceo1000
Секретар	secr3tary	Secr3tary1001
Керівник відділу охорони	ohorsec_ker	Ohorsec2000
Охоронник – комп. №1	ohorsec1	Ohorsec2001
Спеціаліст з кібербезпеки – комп. №1	kiberbepzsec1	Ohorsec2004
Спеціаліст з кібербезпеки – комп. №2	kiberbezpsec2	Ohorsec2005
Спеціаліст з кібербезпеки – комп. №3	kiberbezpsec3	Ohorsec2006
Керівник відділу кадрів	kadryhr_ker	Kadryhr3000
Інспектор відділу кадрів – комп. №1	kadryhr1	Kadryhr3001
Керівник економічного відділу	econ3con_ker	Econ3con4000
Економіст – комп. №1	econ3con1	Econ3con4001
Керівник відділу післяпродажного обслуговування	prodservice_ker	ServiceProd5000
Інженер-механік – комп. №1	prodservice1	ServiceProd5001
Керівник відділу прийому авто	pryjcar_ker	Pryjcar6000
Майстер-приймальник – комп. №1	pryjcar1	Pryjcar6001
Керівник відділу продажів	prodsales_ker	Prodsales7000
Спеціаліст з продажів – комп. №1	prodsales1	Prodsales7001

Для кожного користувача можна створити окремий обліковий запис через налаштування Windows. Для цього потрібно перейти в меню «Облікові записи», вибрати «Варіанти входу» та налаштувати «Пароль» (рис 2.12).

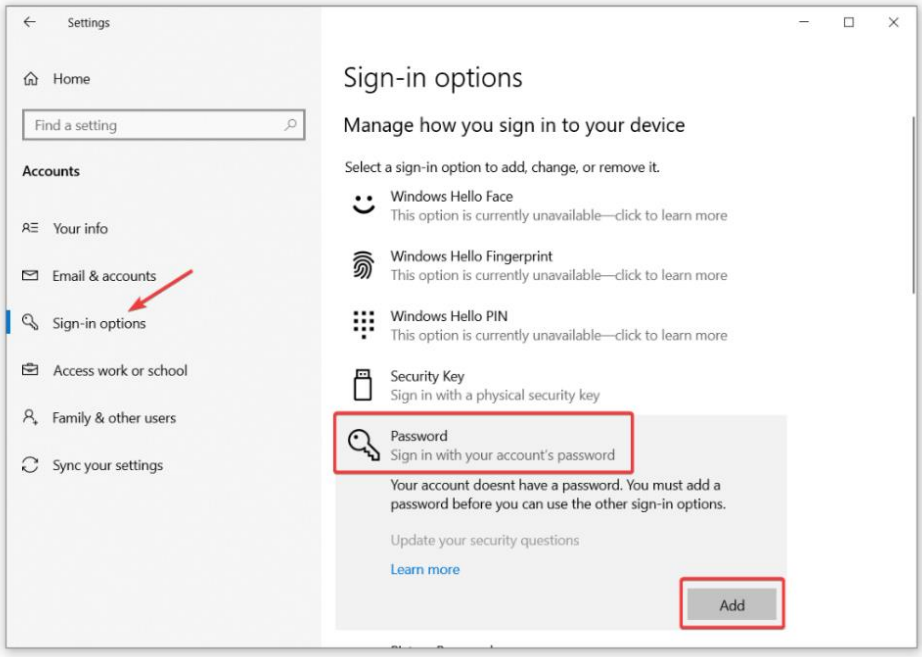

Рисунок 2.12 – Додавання паролю

До папки компанії призначено дозвіл на доступ за допомогою команд «Властивості» - «Безпека» - «Змінити» (рис. 2.13).

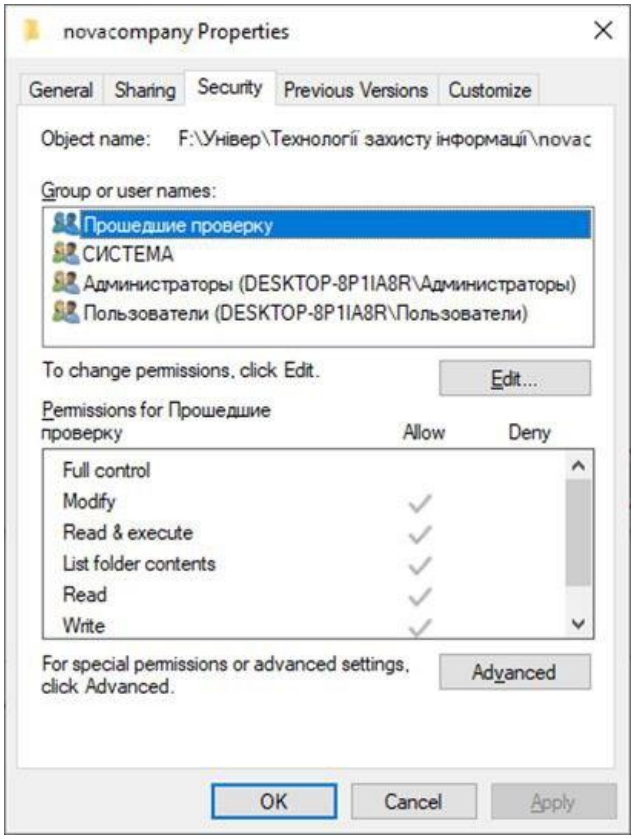

Рисунок 2.13 – Вікно «Властивості»

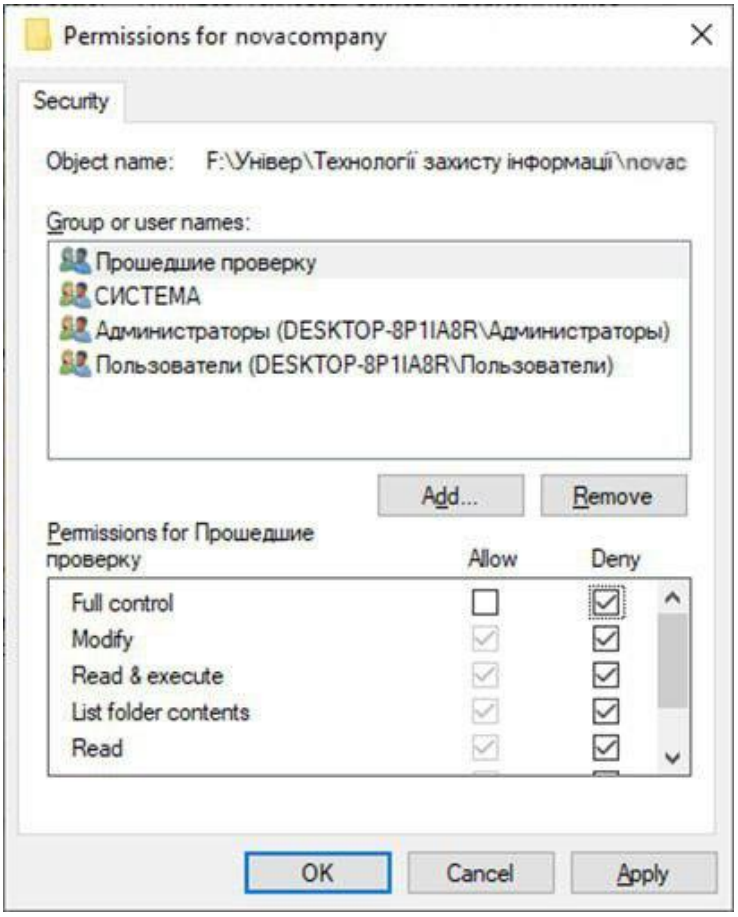

Рисунок 2.14 – Вікно налаштування доступу до папки

2.9 Захист на рівні реєстру

Реєстр Windows — це важливий компонент операційної системи, який функціонує як база даних для зберігання інформації про конфігурацію, налаштування програмного забезпечення, драйверів та самої ОС. Його структура представлена у вигляді дерева, що забезпечує зручність у зберіганні та організації даних.

Основні особливості:

1. Деревоподібна структура дозволяє легко орієнтуватися серед безлічі параметрів та розділів.

2. Доступ до редактора реєстру здійснюється за допомогою вбудованої утиліти RegEdit. Вона надає можливість ручного редагування налаштувань. Щоб

її запустити, потрібно відкрити меню «Пуск», вибрати «Виконати» та ввести команду *regedit*.

Заходи захисту реєстру:

1. Обмеження прав доступу. Для забезпечення безпеки слід надавати доступ до редагування реєстру лише адміністраторам. Це можна зробити через налаштування політик безпеки Windows.
2. Регулярне резервне копіювання. Перш ніж вносити зміни до реєстру, слід створювати резервну копію, щоб у разі помилок можна було відновити його початковий стан.
3. Використання антивірусного програмного забезпечення. Зловмисні програми часто змінюють критичні параметри реєстру. Антивірусний захист допомагає запобігти цьому.
4. Моніторинг змін у реєстрі. Використання спеціалізованих утиліт для моніторингу змін допомагає своєчасно виявляти небажані модифікації.
5. Шифрування реєстру. Шифрування ключів реєстру може додатково захистити конфіденційну інформацію від несанкціонованого доступу.

Потенційні ризики:

- неправильне редагування реєстру може спричинити нестабільну роботу ОС або навіть її відмову;
- відсутність обмежень доступу створює ризик втручання з боку зловмисників.

Для автоматизації роботи з реєстром можна використовувати сценарії PowerShell чи файли *.reg*, що спрощують внесення змін. Проте ці інструменти також вимагають обережності, щоб уникнути помилкових змін.

Захист реєстру — це важлива складова загальної стратегії інформаційної безпеки. Забезпечення належного захисту допомагає уникнути багатьох проблем, пов'язаних із порушенням роботи операційної системи чи втручанням у конфіденційну інформацію (рис. 2.15).

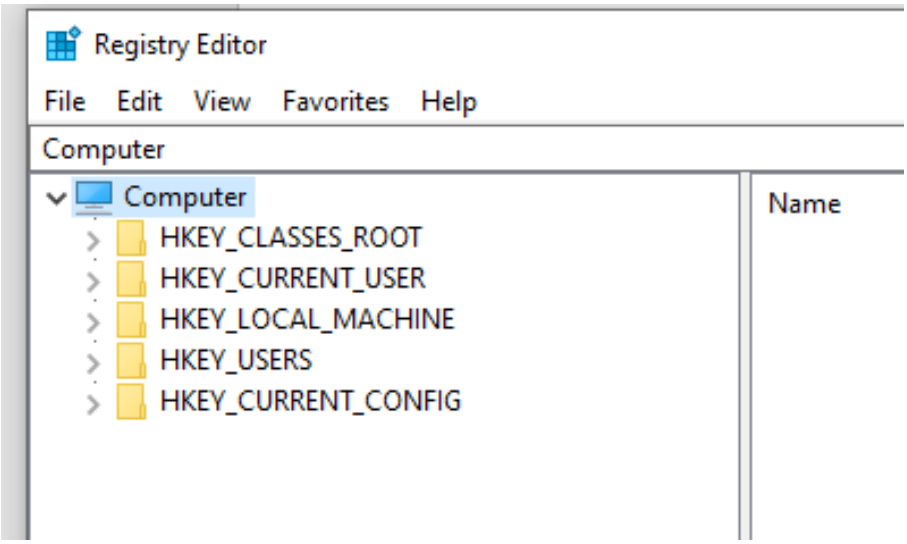

Рисунок 2.15 – Вікно редактора реєстру.

Реєстр Windows має чітку ієрархічну структуру, що дозволяє організовувати дані в розділи, які виконують різні функції. Він складається з п'яти основних розділів, кожен із яких має своє призначення:

1) HKEY_CLASSES_ROOT
   a) Цей розділ містить дані, які потрібні для підтримки технології OLE (Object Linking and Embedding), а також інформацію про асоціації файлів і налаштування користувацького інтерфейсу.
   b) Зокрема, тут зберігаються відомості про те, які програми пов'язані з конкретними типами файлів.
2) HKEY_CURRENT_USER
   a) У цьому розділі розташовані налаштування поточного користувача, який увійшов у систему.
   b) Зберігаються параметри персоналізації: колірні схеми, вибір шпалер, параметри програм тощо.

3) HKEY_LOCAL_MACHINE
   a) Один із ключових розділів реєстру, де зберігається інформація, специфічна для конкретного комп'ютера.
   b) Включає дані про конфігурацію обладнання, драйвери, параметри програмного забезпечення та загальні системні налаштування.
4) HKEY_USERS
   a) Містить налаштування для всіх користувачів, які зареєстровані на комп'ютері.
   b) У кожного користувача є своя окрема гілка, яка зберігає його індивідуальні параметри.
5) HKEY_CURRENT_CONFIG.
   a) Цей розділ зберігає дані про поточну апаратну конфігурацію пристроїв.
   b) При старті системи Windows копіює відповідну гілку з HKEY_USERS у HKEY_CURRENT_USER, а після завершення роботи зберігає зміни назад.

Нових користувачів можна створити через "Панель управління" у розділі "Користувачі". У цьому інтерфейсі можна налаштовувати облікові записи, встановлювати паролі та обмежувати доступ до певних функцій системи.

Додатково про використання:

1. Реєстр є ключовим елементом функціонування операційної системи. Будь-які зміни повинні виконуватися обережно, оскільки помилки можуть призвести до некоректної роботи програм або навіть до збою всієї системи.
2. Для автоматизації роботи з реєстром часто використовуються .reg файли, які дозволяють швидко імпортувати або експортувати певні параметри.

Вивчення структури реєстру та його компонентів є важливим кроком для розуміння принципів функціонування Windows і налаштування системної безпеки.

Створювати користувачів можна в "Панель управління" – "Користувачі".

2.10 Програмні методи захисту

Комп'ютерний вірус — це малий шкідливий код, розроблений кваліфікованим програмістом, який має здатність до самостійного відтворення та виконання руйнівних операцій на комп'ютерних пристроях. Станом на сьогодні існує понад 50 тисяч різновидів комп’ютерних вірусів, які продовжують активно розвиватися.

Історія виникнення комп’ютерних вірусів тісно пов’язана з ідеєю створення програм, які здатні до самовідтворення. Більшість фахівців вважають, що перші віруси з’явилися у 1986 році. Одним із перших задокументованих вірусів є "Brain", розроблений пакистанським програмістом на прізвище Алві. У США цей вірус вразив понад 18 тисяч комп’ютерів. Спочатку створення вірусів мало дослідницький характер, але з часом такі програми почали використовувати для завдання шкоди, перетворюючись на інструмент хакерів та кримінальних груп [15].

Комп’ютерні віруси діють виключно програмним шляхом. Їх механізм дії полягає у зараженні файлів шляхом приєднання до них або проникнення всередину. Такий файл вважається "зараженим", і вірус активується лише після його завантаження або запуску. Деякі віруси після активації стають резидентними, залишаючись у пам’яті комп’ютера, та можуть заражати інші файли й програми. Інші віруси здатні завдавати миттєвої шкоди, наприклад, видалення файлів або форматування жорсткого диска.

Дія вірусів може проявлятися у різний спосіб, зокрема:

- створення візуальних ефектів, які заважають роботі;
- пошкодження або видалення файлів;
- повна втрата інформації на комп’ютері.

Сучасні віруси найчастіше заражають виконувані файли з розширеннями *.EXE* та *.COM*. Однак із розвитком технологій значного поширення набули віруси, що розповсюджуються через електронну пошту, та інші типи мережевих атак.

Для запобігання зараженню комп’ютерними вірусами важливо дотримуватись таких правил:

1) Використання антивірусного програмного забезпечення. Регулярні сканування системи допоможуть виявляти й видаляти шкідливе ПЗ.

2) Оновлення операційної системи та програм. Багато вірусів використовують вразливості в застарілих версіях програмного забезпечення.

3) Обережність із файлами. Не слід відкривати файли чи посилання від невідомих відправників.

4) Резервне копіювання. Регулярне збереження даних дозволить мінімізувати збитки у разі зараження.

У багатьох країнах створення та розповсюдження комп’ютерних вірусів прирівнюється до комп’ютерних злочинів, за які передбачена кримінальна відповідальність. Це є важливим кроком у боротьбі з кіберзагрозами.

Комп’ютерні віруси залишаються однією з головних проблем інформаційної безпеки. Хоча вони не мають прямого впливу на людей, вони можуть завдавати значних фінансових та інформаційних збитків, тому обізнаність користувачів і профілактичні заходи є ключовими у боротьбі з цією загрозою.

Основними джерелами вірусів є:

- заражені файли на носіях;
- комп'ютерні мережі, включаючи електронну пошту та Інтернет;
- жорсткий диск, заражений через працюючі програми;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

Ранні ознаки зараження комп'ютера вірусом можуть включати:

- зменшення вільної оперативної пам'яті;
- сповільнення роботи комп'ютера;
- зміни в файлах без видимих причин;
- помилки при завантаженні операційної системи.

Активна фаза вірусу може призвести до:

- зникнення файлів;
- форматування жорсткого диска;
- неможливості завантажити операційну систему.

Для захисту від вірусів необхідно:

- використовувати антивірусні програми для автоматичного сканування комп'ютера;
- оновлювати бази даних вірусів;
- створювати резервні копії важливих даних [16].

2.11 Антивірусні програми

Антивірусні програми — це програми, створені для пошуку, нейтралізації та видалення шкідливого програмного забезпечення, такого як віруси, троянські коні чи шпигунські програми. Вони забезпечують захист комп'ютерних систем від загроз, які можуть викликати збої в роботі або втрату важливих даних.

Основні види антивірусних програм:

1. *Сканери.* Ці програми виконують перевірку файлів та системних об'єктів на предмет зараження. Вони порівнюють код у файлах із сигнатурами, що містяться в базі відомих вірусів. Приклад: Kaspersky Antivirus, Windows Defender.

2. *Монітори.* Працюють у режимі реального часу, постійно стежачи за всіма процесами на комп'ютері. Вони можуть автоматично блокувати підозрілу активність, попереджаючи про потенційну загрозу. Приклад: Bitdefender Total Security, Avast.

3. *Ревізори.* Ці програми аналізують стан системи, фіксуючи зміни в ключових файлах чи налаштуваннях. При виявленні несанкціонованих змін вони сигналізують про можливе зараження. Приклад: Ad-Aware Antivirus, McAfee.

4. *Фільтри.* Використовуються для запобігання завантаженню чи виконанню підозрілих файлів. Фільтри перехоплюють шкідливий код до його активації. Приклад: Panda Security, Sophos.

5. *Вакцини.* Ці програми змінюють структуру файлів або налаштувань системи, щоб зробити їх нечутливими до зараження певними типами вірусів. Приклад: Immunet, Comodo Antivirus

Антивірусні програми повинні постійно оновлювати базу вірусів, щоб ефективно боротися з новими загрозами [17].

2.12 Популярні антивірусні програми

Malwarebytes for Business.

Malwarebytes for Business — ефективне антивірусне рішення для захисту від шкідливих програм, таких як програми-вимагачі, трояни та фішинг. Воно включає розширене виявлення загроз, захист у реальному часі, централізовану панель управління та хмарне адміністрування для зручності керування безпекою (рис. 2.16).

Переваги:

- ефективне виявлення й блокування загроз;
- захист у реальному часі;
- зручність керування через хмарну панель;
- низький вплив на продуктивність системи;
- простий інтерфейс з легким доступом до функцій і налаштувань.

Недоліки:

- висока вартість для малих бізнесів;
- обмежені функції у базовій версії;
- періодичні хибні спрацьовування;
- відсутність брандмауера, що потребує додаткового пз для мережевої безпеки.

Malwarebytes for Business підходить для компаній, які потребують потужного захисту від шкідливих програм, але варто враховувати як переваги, так і обмеження перед вибором цього продукту [18].

Рисунок 2.16 – Логотип антивірусу «Malwarebytes»

Bitdefender GravityZone Business Security.

GravityZone Business Security — це потужне антивірусне програмне забезпечення для бізнесу, яке здобуло популярність завдяки своїй здатності ефективно боротися з сучасними кіберзагрозами. Завдяки впровадженню алгоритмів машинного навчання, цей антивірус забезпечує постійний захист від нових і складних атак. ПЗ пропонує широкий спектр функцій, включаючи розширене виявлення загроз, захист даних і шифрування, а також захист від мережевих атак, що дозволяє контролювати потенційні загрози, що можуть виникати в мережі (рис. 2.17).

Переваги:

- використання машинного навчання для виявлення нових загроз;
- розширений захист даних та шифрування;
- захист від мережевих атак.

Недоліки:

- може бути складним для налаштування без досвіду;
- високі системні вимоги.

Bitdefender GravityZone Business Security ідеальний для компаній, що потребують сильного захисту завдяки машинному навчанню та мережевому захисту. Однак варто враховувати складність налаштування та вимоги до ресурсів [19].

Bitdefender®

Рисунок 2.17 – Логотип антивірусу «Bitdefender»

Symantec End-User Endpoint Security.

Symantec End-User Endpoint Security — це ефективне рішення для захисту кібербезпеки, яке розроблене для великих компаній і забезпечує надійний захист усіх пристроїв, зокрема мобільних.

Антивірус пропонує розширену систему виявлення загроз з використанням машинного навчання та експертного аналізу, а також моніторинг і усунення загроз у реальному часі. Завдяки комплексному захисту на всіх етапах кібер-атаки, Symantec гарантує високу безпеку для організаційних мереж і пристроїв (рис. 2.18).

Переваги:

- потужний захист для всіх типів пристроїв, включаючи мобільні;
- використання машинного навчання для виявлення загроз;
- реальний моніторинг і швидке усунення загроз.

Недоліки:

- високі вимоги до системних ресурсів;
- може бути складним у налаштуванні для невеликих компаній.

Symantec End-User Endpoint Security підходить для великих підприємств, які потребують комплексного захисту від кіберзагроз, але варто враховувати як переваги, так і можливі обмеження перед вибором цього продукту [20].

Рисунок 2.18 – Логотип антивірусу «Symantec»

Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint — це надійне корпоративне рішення для захисту від кіберзагроз, яке ідеально підходить для компаній, що використовують екосистему Microsoft. Він забезпечує комплексний захист кінцевих точок, ефективно протидіючи різноманітним кіберзагрозам завдяки передовим технологіям виявлення та реагування на інциденти безпеки (рис. 2.19).

Переваги:

- ідеально інтегрується з іншими продуктами microsoft;
- потужний захист від різноманітних кіберзагроз;
- можливість централізованого управління безпекою в рамках екосистеми.

Недоліки:

- підходить переважно для користувачів microsoft;
- може мати обмежені можливості для користувачів з іншими операційними системами.

Microsoft Defender for Endpoint — це відмінний вибір для компаній, що активно використовують продукти Microsoft, забезпечуючи надійний захист, але варто враховувати, що його переваги найкраще розкриваються в екосистемі Microsoft [21].

Рисунок 2.19 – Логотип антивірусу «Microsoft Defender»

CrowdStrike Falcon Endpoint Protection.

CrowdStrike Falcon Endpoint Protection — це хмарне рішення для захисту кінцевих точок, яке застосовує штучний інтелект для активного виявлення і блокування кіберзагроз. Платформа відома своєю гнучкістю та масштабованістю, що дозволяє задовольняти потреби великих організацій у високому рівні безпеки. Вона включає антивірус нового покоління та надає можливість керування пристроями і брандмауером, забезпечуючи детальний контроль за параметрами безпеки (рис. 2.20).

Переваги:

- використання штучного інтелекту для швидкого виявлення загроз;
- гнучкість та масштабованість для великих організацій;
- детальний контроль за параметрами безпеки, включаючи керування пристроями і брандмауером.

Недоліки:

- потребує постійного інтернет-з’єднання для хмарної роботи;
- може бути складним у налаштуванні для дрібних компаній без досвіду в управлінні безпекою.

CrowdStrike Falcon Endpoint Protection є потужним рішенням для організацій, які шукають масштабований і проактивний захист від кіберзагроз, але варто врахувати його вимоги до налаштувань і інфраструктури для ефективного використання [22].

Рисунок 2.20 – Логотип антивірусу «Microsoft Defender»

Avast Business.

Avast Business — це надійний інструмент для малих та середніх компаній, що забезпечує всебічний захист важливих даних. Програма включає набір засобів безпеки в зручному пакеті, зокрема повне знищення даних для безпечного видалення конфіденційної інформації, вбудований VPN, надійний брандмауер та захист від витоку особистих даних (рис. 2.21).

Переваги:

- комплексний захист для малого та середнього бізнесу;
- вбудований vpn для забезпечення безпечного з'єднання;
- повне знищення даних для безпечного видалення конфіденційної інформації.

Недоліки:

- обмежені можливості для великих організацій;
- потребує регулярного оновлення для підтримки високого рівня безпеки.

Avast Business є чудовим варіантом для малих та середніх підприємств, які шукають ефективне та доступне рішення для захисту своїх даних, але може не задовольняти вимоги великих компаній у плані масштабованості [23].

Рисунок 2.21 – Логотип антивірусу «Microsoft Defender»

Для забезпечення захисту підприємства було вибрано антивірус Bitdefender GravityZone Business Security через його високу ефективність у виявленні загроз, здатність до масштабування для підтримки розвитку компанії, надійний захист і шифрування даних, а також зручність у процесі впровадження та управління.

Таблиця 2.6 Порівняння даних антивірусів

Характеристика	Malwarebytes	Bitdefender	Symantec	Microsoft Defender	CrowdStrike Falcon	Avast Business
Тип захисту	+	+	+	+	+	+
Маштабованість	+	+	+	+	+	+
Легкість налаштування	+	-	-	+	+	+
Підтримка хмарного керування	+	+	+	+	+	+
Захист від шкідливих програм	+	+	+	+	+	+
Розширена функціональність (шифрування тощо)	-	+	+	-	+	+
Інтеграція з іншими системами	+	-	+	+	+	+

2.13 Характеристики апаратного та технічного забезпечення

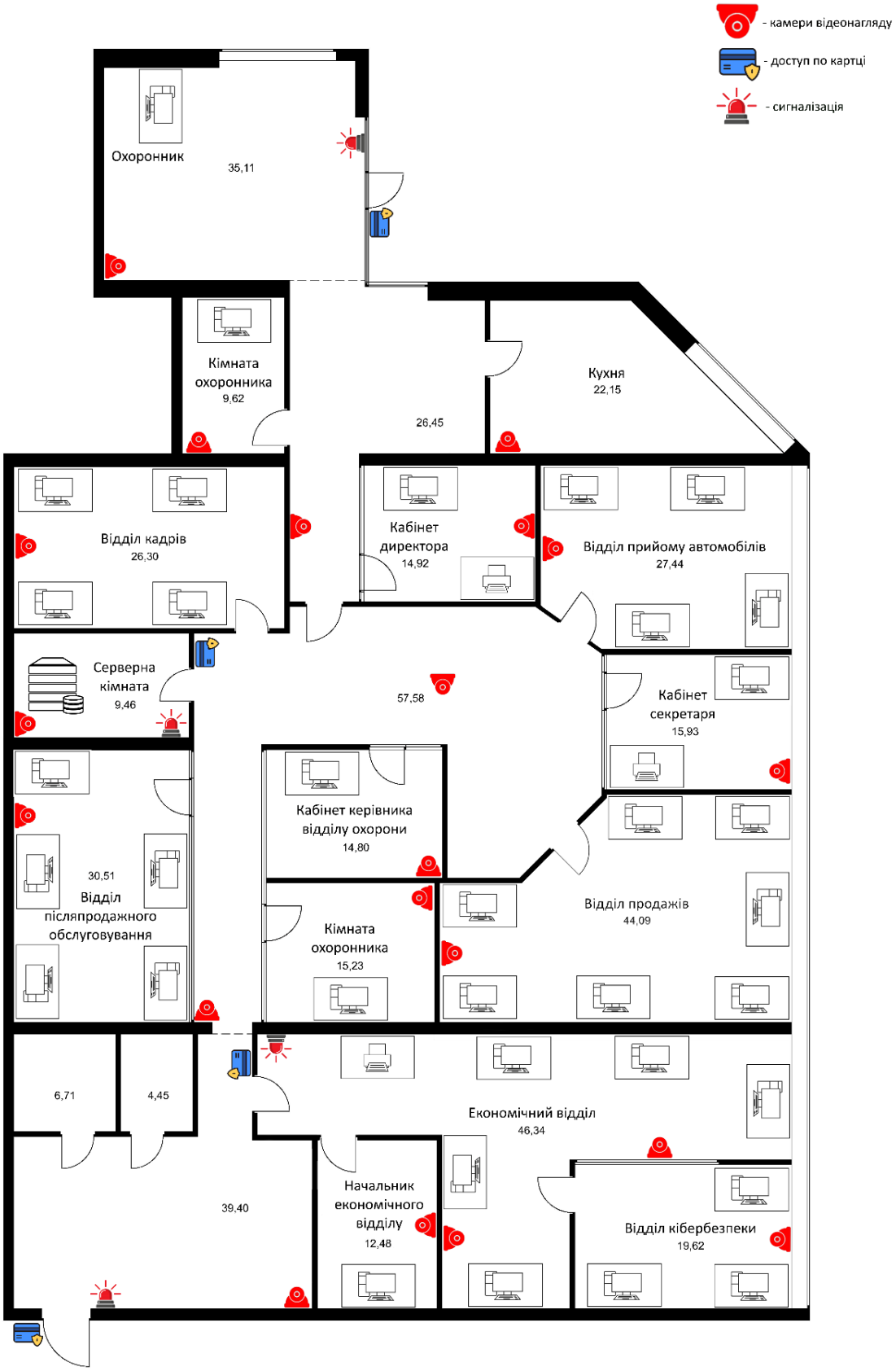

Рисунок 2.22 – Розміщення апаратного та технічного забезпечення.

Таблиця 2.7. Характеристики апаратного та технічного забезпечення

Найменування	Характеристика
IP-камера TP-LINK Tapo C200	Інфрачервона підсвітка: до 9 м Роздільна здатність відео: 1920x1080 Розмір матриці: 1/2.9" Тип: дротова
Автономний комплект СКД для офісу CoVi Security Access-1	Тип контролера: автономний Тип встановлення: внутрішня Тип підключення: дротове Кількість точок проходу/дверей: 1 Інтерфейси зв'язку: Dallas Touch Memory Обсяг пам'яті: 1364 ідентифікаторів Приєднання додаткового зчитувача: 1 Струм споживання, мА: 20
Сигналізація Security Alarm System GSM A30	Центральний модуль GSM30A Бездротовий датчик руху Бездротовий датчик відкриття на двері/вікно Брелок дистанційного керування Блок живлення Провідна сирена

2.14 Програмне забезпечення для захисту інформації

Таблиця 2.8. Вартість програмного забезпечення для захисту мережі

Найменування	Кількість	Вартість усього, грн
Антивірус Bitdefender GravityZone Business Security для 35 комп'ютерів та 1 сервера – річна підписка	1	31 077
	Всього	31 077

2.15 Технічне обладнання

Таблиця 2.9. Вартість технічного обладнання для захисту підприємства

Найменування	Кількість	Вартість за 1 шт, грн	Вартість усього, грн
Автономний комплект СКД для офісу CoVi Security Access-1	4	2 395	9 580
Сигналізація Security Alarm System GSM A30	4	2 498	9 992
		Всього	19 572

2.16 Загальна вартість

Таблиця 2.10. Вартість систем захисту

Складова	**Вартість, грн**
Програмне забезпечення для захисту мережі	31 077
Технічне обладнання	19 572
Загальна вартість	50649

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМИ ДЛЯ ШИФРУВАННЯ ІНФОРМАЦІЇ

3.1 Опис технологій та мови програмування для реалізації програми

Для обміну внутрішніми повідомленнями між підрозділами компанії було розроблено настільний додаток для операційної системи Windows. Програма побудована на основі платформи Windows Presentation Foundation (WPF) з використанням мови програмування C# (рис 3.1, рис. 3.2).

Мова C# була обрана для реалізації проєкту через такі переваги:

1) Зручність розробки: C# є сучасною, об'єктно-орієнтованою мовою програмування, що надає широкий спектр можливостей для створення настільних додатків.

2) Сумісність із Windows: C# у поєднанні з WPF є ідеальним рішенням для розробки програм під операційну систему Windows.

3) Швидкість виконання: Завдяки компіляції в проміжний байт-код (MSIL), програми на C# працюють швидко та ефективно.

4) Великий вибір інструментів: Оточення розробки Visual Studio пропонує потужні інструменти для ефективного створення, налагодження та тестування програм.

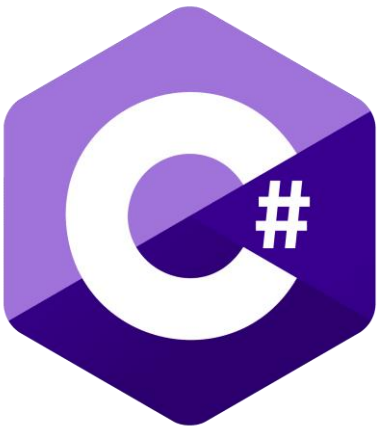

Рисунок 3.1 – Об'єктно-орієнтована мова програмування C#.

Windows Presentation Foundation (WPF): WPF є сучасною технологією для створення настільних додатків, яка дозволяє розробляти зручні та інтуїтивно зрозумілі користувацькі інтерфейси (UI). Основні переваги WPF:

1. Гнучкість дизайну: Використання XAML для відокремлення логіки від представлення дозволяє створювати привабливі та функціональні інтерфейси.
2. Масштабованість: WPF підтримує векторну графіку, що забезпечує високу якість відображення на різних моніторах та роздільній здатності екрана.
3. Зручна інтеграція: Легко інтегрується з мовою C# для обробки даних і реалізації логіки програми.

Рисунок 3.2 – Windows Presentation Foundation (WPF).

Додаток було спроєктовано за модульною архітектурою, що дозволяє легко масштабувати і вдосконалювати програму в майбутньому.

Основні компоненти додатку:

a) Інтерфейс користувача (UI): Побудований за допомогою XAML, надає зручний доступ до функцій програми, таких як шифрування, дешифрування та авторизація.

b) Обробка даних: Реалізована мовою C#, відповідає за логіку програми, включно з операціями шифрування/дешифрування повідомлень.

c) Система авторизації: Забезпечує розмежування доступу до повідомлень залежно від ролі користувача в компанії.

Використання C# та WPF забезпечило швидку та ефективну розробку надійного настільного додатка для внутрішнього обміну повідомленнями. Обрана технологія дозволяє легко підтримувати програму, розширювати функціонал і забезпечувати високий рівень безпеки інформації.

3.2 Криптологічний захист інформації

Розвиток комп'ютерної безпеки на початкових етапах був тісно пов’язаний із криптографією. Основними вимогами до захисту інформації є її доступність та цілісність. Це означає, що користувач повинен мати можливість отримати необхідний набір послуг у будь-який час, при цьому система безпеки гарантує коректну роботу. Будь-який файл або ресурс системи має бути доступним за умови дотримання прав доступу. Якщо ресурс недоступний, то він втрачає свою цінність. Ще одне завдання захисту — збереження незмінності даних під час їх передачі чи зберігання, що забезпечує умова цілісності.

Шифр є спорідненим із кодом і являє собою набір криптографічних алгоритмів, які перетворюють відкриті дані у зашифровані, а також здійснюють зворотні перетворення. Ключ є важливим елементом будь-якого шифру, оскільки він визначає конкретне перетворення з можливого набору криптографічного алгоритму. У сучасній криптографії дотримуються принципу Керкгоффса, згідно з яким секретність алгоритму полягає саме у ключі, а не в деталях його роботи.

Шифри поділяють на два основні типи: ті, які теоретично неможливо дешифрувати, і ті, які неможливо дешифрувати практично. За типом ключів шифри поділяють на симетричні та асиметричні. У симетричних шифрах один і той самий ключ використовується для шифрування і розшифрування, а в асиметричних — ключі різні. Симетричні шифри бувають блоковими і потоковими.

До найдавніших криптографічних методів належать перестановочні та підстановочні шифри. Через їх низьку криптостійкість вони нині

використовуються рідко. Серед сучасних шифрів, які відповідають високим стандартам безпеки, можна виділити *AES* і *Twofish* [24].

У сучасній літературі шифри поділяють на симетричні та асиметричні, блочні та потокові.

Шифри використовуються для забезпечення секретності листування між дипломатичними представниками (послами, аташе тощо) та їхніми урядами, а також у військовій сфері для передачі наказів, розпоряджень і донесень. Процес шифрування полягає у заміні фраз, слів, складів або окремих літер на комбінації цифр чи інших символів, використовуючи попередньо визначену систему, яка слугує ключем для дешифрування тексту. Іноді застосовується подвійне шифрування, що потребує використання двох ключів для розшифрування.

Однак навіть найскладніші шифри не гарантують повної секретності, оскільки до них можна підібрати ключ, використовуючи методи аналізу, наприклад, дослідження повторюваних символів.

Процеси шифрування та дешифрування у сучасних інформаційних системах можуть уповільнювати передачу даних і знижувати їхню доступність. Це створює незручності для користувачів, які не можуть оперативно отримати захищені дані. Тому у системах безпеки пріоритетним завданням є забезпечення доступності та цілісності інформації, а вже потім її конфіденційності..

Twofish - це симетричний блоковий шифр із розміром блоків 128 біт і ключем змінної довжини: 128, 192 або 256 біт. Алгоритм оптимізований для 32-розрядних процесорів, має відкритий код і доступний для безкоштовного використання. Побудований на основі Blowfish, він включає вдосконалення для заміни застарілого DES (рис. 3.3).

Twofish використовує один ключ для шифрування та дешифрування даних. Однією з особливостей алгоритму є залежні від ключа S-блоки (блоки підстановки), які приховують взаємозв’язок між ключем та зашифрованим текстом, забезпечуючи високу стійкість шифру [25].

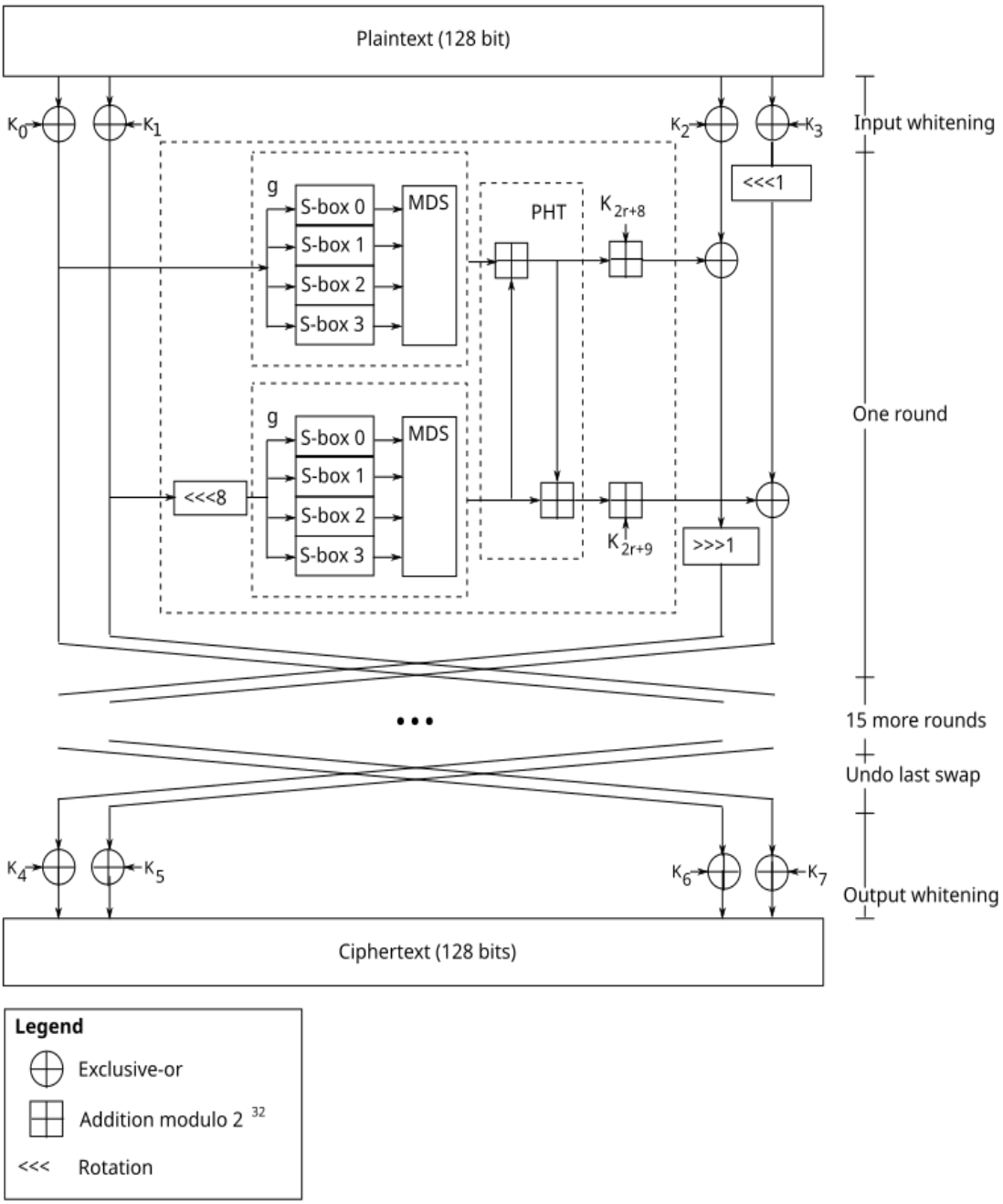

Рисунок 3.3 – Алгоритм шифру Twofish

Twofish складається з наступних ключових елементів:

1. *Мережа Фейстеля.* Основний механізм перетворення, що забезпечує перестановку даних за допомогою F-функції, широко використовується в багатьох блокових шифрах.

2. *S-блоки.* Нелінійні табличні операції підстановки. Twofish застосовує чотири попередньо обчислені S-блоки розміром 8×8 біт, залежні від ключа, які додають алгоритму стійкості.

3. *MDS-матриці.* Матриці з максимальною відстанню, які є важливим компонентом кодів з виправленням помилок. У Twofish використовується єдина 4×4 MDS-матриця над полем Галуа для ефективного змішування даних.

4. *Псевдоперетворення Адамара (PHT).* Проста, швидка для виконання операція змішування. У Twofish застосовується 32-розрядне PHT, яке об'єднує виходи двох паралельних 32-розрядних функцій g.

5. *Відбілювання.* Для підвищення безпеки шифру Twofish використовує операцію XOR з підключами перед першим і після останнього раунду мережі Фейстеля.

6. Ключовий розклад. Механізм, що перетворює біти основного ключа на круглі ключі для використання в шифруванні. У Twofish реалізовано складний процес генерації цих ключів, що додає алгоритму криптостійкості.

Процес шифрування в Twofish виконується через такі етапи:

1) Обробка даних функцією F. На кожному раунді два 32-розрядні слова подаються як вхід функції F.

2) Розбиття на байти. Кожне слово розбивається на чотири байти, які передаються через чотири S-блоки. Ці S-блоки залежать від ключа та мають 8-бітний ввід і вивід.

3) Поєднання через MDS-матрицю. MDS-матриця об’єднує чотири вихідні байти в єдине 32-розрядне слово, додаючи змішування для підвищення стійкості шифру.

4) Змішування через PHT. Два 32-розрядних слова об’єднуються за допомогою псевдоперетворення Адамара (PHT), що забезпечує додаткове змішування даних.

5) Додавання підключів і XOR. Отримані 32-розрядні слова додаються до двох кругових підключів, після чого застосовується операція XOR із правою половиною даних, підготовлюючи їх для наступного раунду.

Дослідження Twofish із зменшеним числом раундів показало, що алгоритм має значний запас стійкості. Серед фіналістів конкурсу AES він продемонстрував найвищу криптостійкість. Однак незвичайна структура та відносна складність викликали певні сумніви щодо її реальної якості.

Критика стосувалася розділення ключа на дві частини для формування раундових підключів. Криптографи Фаузан Мірза та Шон Мерфі припустили, що це може дозволити організувати атаку за принципом «розділяй і володарюй», розділивши завдання на дві простіші. Проте практичної реалізації такої атаки досягти не вдалося.

Станом на 2008 рік найефективнішою спробою криптоаналізу Twofish залишалася усічена диференціальна атака, запропонована Шіхо Моріаї та Їчун Ліза Їнь у 2000 році. Вони теоретично встановили, що для її реалізації потрібно 2^{51} підібраних текстів. Однак ця атака залишалася лише теоретичною, і жодних реальних загроз не виявлено. Сам творець алгоритму Брюс Шнайєр у своєму блозі заявив, що подібну атаку неможливо реалізувати на практиці.

3.3 Представлення роботи додатку

Для обміну внутрішніми повідомленнями між підрозділами компанії розроблено настільний додаток для Windows, побудований на платформі WPF із використанням мови програмування C#. Додаток створено з урахуванням потреб у зручності та безпеці, тому підтримує дві мови інтерфейсу — англійську та українську. Користувач може вибрати бажану мову на етапі авторизації, що робить систему доступною для працівників із різних регіонів.

Однією з ключових функцій програми є забезпечення шифрування та дешифрування повідомлень із використанням сучасного та надійного алгоритму TwoFish, що гарантує високий рівень захисту даних під час їх передачі.

Архітектура додатка була розроблена з акцентом на гнучкість і довговічність, використовуючи принципи Dependency Injection (ін'єкції залежностей). Цей підхід дозволяє розробникам легко замінювати певні компоненти системи, такі як база даних або алгоритм шифрування, без потреби суттєво переписувати код програми. Завдяки цьому зміни або розширення функціоналу можуть бути впроваджені швидко, із мінімальним ризиком виникнення помилок.

Такий підхід забезпечує програмі стійкість до змін, підвищує її адаптивність до нових вимог та спрощує тестування. Розділення залежностей і модульна структура коду роблять програму зручною в обслуговуванні, полегшуючи не лише впровадження оновлень, але й інтеграцію з іншими системами або сервісами в майбутньому.

Таким чином, додаток поєднує в собі безпеку, функціональність і можливість масштабування, що робить його універсальним рішенням для внутрішньої корпоративної комунікації.

```
public void ConfigureServices(ServiceCollection services)
    {
        services.AddSingleton<IDatabaseService, InMemoryDatabaseService>();
        services.AddSingleton<IEncryptor, TwofishEncryptor>();
    }
```

Рисунок 3.4 – Dependency Injection в коді програми

Логіни, паролі та відділ кожного працівника зберігаються у вбудованій базі даних, яка реалізована через список користувачів. Кожен користувач також має індивідуальний ідентифікатор (ID).

```
private readonly IEnumerable<User> _users = new List<User>() {
    new User(1, "gendir_ceo", "Gendriceo1000", "CEO"),
    new User(2, "secr3tary", "Secr3tary1001", "Secretary"),
    new User(3, "ohorsec_ker", "Ohorsec2000", "HEAD of the Security Dept."),
    new User(4, "ohorsec1", "Ohorsec2001", "Security Dept."),
    new User(5, "ohorsec2", "Ohorsec2002", "Security Dept."),
    new User(6, "ohorsec3", "Ohorsec2003", "Security Dept."),
    new User(7, "kiberbepsec1", "Ohorsec2004", "Security Dept."),
    new User(8, "kiberbepsec2", "Ohorsec2005", "Security Dept."),
    new User(9, "kiberbepsec2", "Ohorsec2006", "Security Dept."),
    new User(10, "kadryhr_ker", "Kadryhr3000", "HEAD of the HR Dept."),
    new User(11, "kadryhr1", "Kadryhr3001", "HR Dept."),
    new User(12, "kadryhr2", "Kadryhr3002", "HR Dept."),
    new User(13, "kadryhr3", "Kadryhr3003", "HR Dept."),
    new User(14, "econ3con_ker", "Econ3con4000", "HEAD of the Economics Dept."),
    new User(15, "econ3con1", "Econ3con1001", "Economics Dept.")
};
```

Рисунок 3.5 – Вбудована база даних користувачів

На стартовому екрані користувач може вибрати мову інтерфейсу та виконати авторизацію. У разі невдалої авторизації буде виведено повідомлення про помилку. Для кожної мови інтерфейсу повідомлення про помилки також переведені, щоб користувачі могли зрозуміти їх зміст.

На зображеннях нижче показано вигляд вікна авторизації програми з обраною англійською та українською мовами. У обох випадках для авторизації потрібно ввести логін і пароль, після чого натиснути кнопку "Sign In" (для англійської мови) або "Увійти" (для української). Якщо логін або пароль введені неправильно, відобразиться повідомлення про помилку: "Incorrect Login or Password" для англійської мови або "Неправильний логін або пароль" для української (рис. 3.6, рис 3.7).

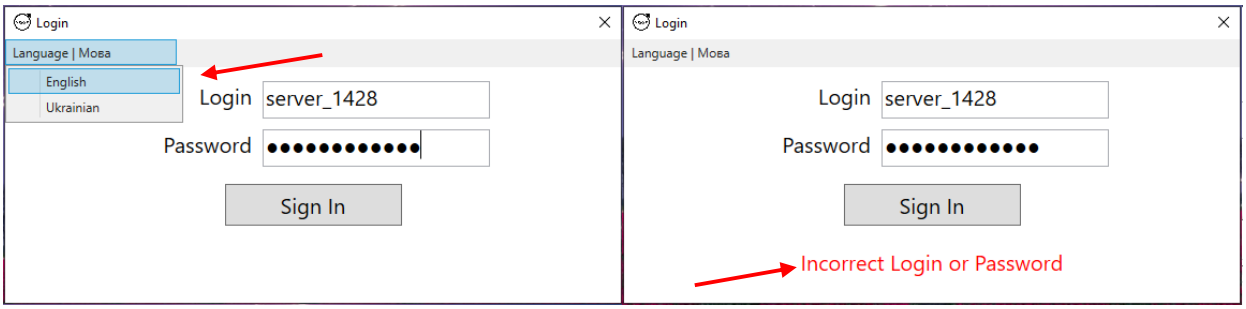

Рисунок 3.6 – Вікно авторизації та невдалої авторизації (Англ.)

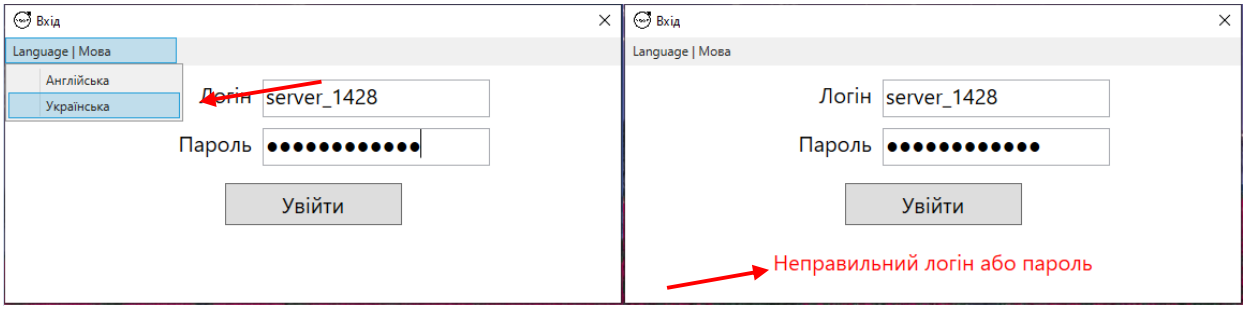

Рисунок 3.7 – Вікно авторизації та невдалої авторизації (Укр.)

Для прикладу здійснено авторизацію в акаунт одного з фахівців кібербезпеки. Після успішної авторизації користувача в акаунт одного з фахівців з кібербезпеки, з'являється вікно, в якому він може вибрати дію: зашифрувати або розшифрувати інформацію, а також вийти з акаунту і повернутися до вікна авторизації. У верхній частині цього вікна відображаються дані поточного користувача, зокрема його логін та відділ, до якого він належить (рис. 3.8).

Логін: kiberbepzsec1.

Пароль: Ohorsec2004.

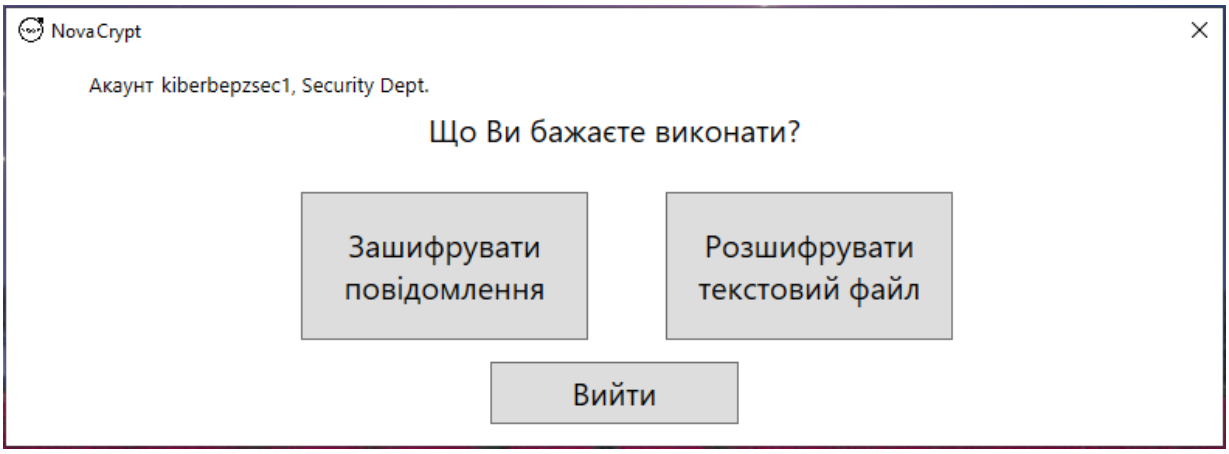

Рисунок 3.8 – Головне вікно програми

При виборі опції «Зашифрувати повідомлення» користувачу відкривається вікно, в якому він може ввести текст повідомлення та вибрати одержувача. Для здійснення шифрування необхідно ввести пароль, що є однаковим для всіх

користувачів компанії - *novaplt1307*. Цей самий пароль використовується для дешифрування інформації.

У списку отримувачів відображається перелік відділів компанії. Голови відділів позначені як «HEAD of» (з англ. «голова», «начальник») перед назвою відповідного відділу. Якщо вибрано одержувача «All» (з англ. «всі»), повідомлення стане доступним для працівників будь-якого відділу, оскільки воно буде загальним.

Текст повідомлення вводиться в правій частині вікна програми. Після натискання кнопки «Відправити» на екрані з'явиться або текст помилки, або повідомлення «ОК», що підтверджує успішне відправлення.

Наприклад, якщо повідомлення відправляється директору компанії (CEO), у директорії компанії створюється папка «CEO», у яку додається зашифроване повідомлення. Якщо така папка вже існує, файл буде додано до неї (рис. 3.9).

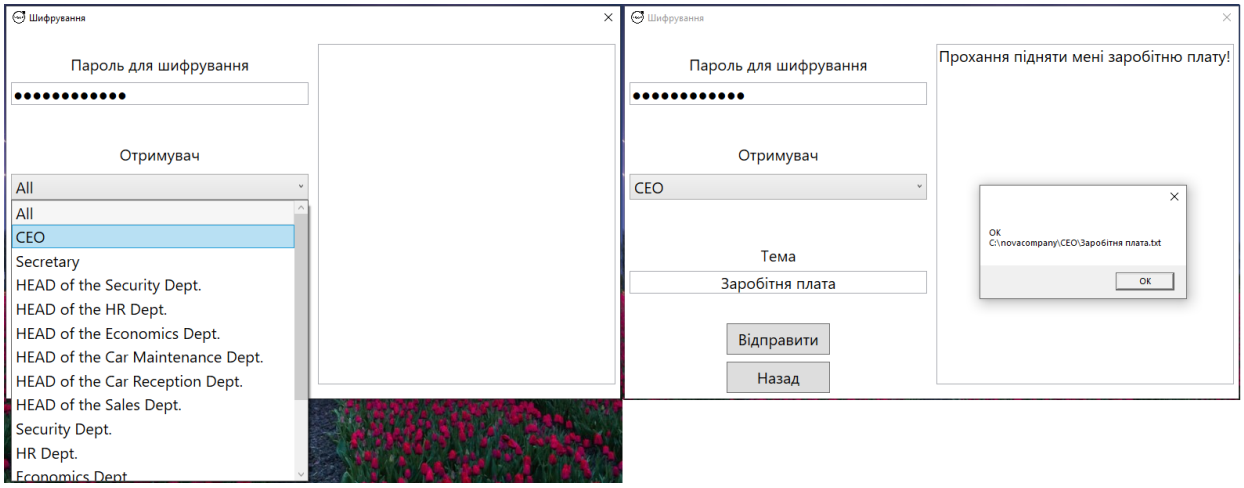

Рисунок 3.9 – Вигляд вікна шифрування

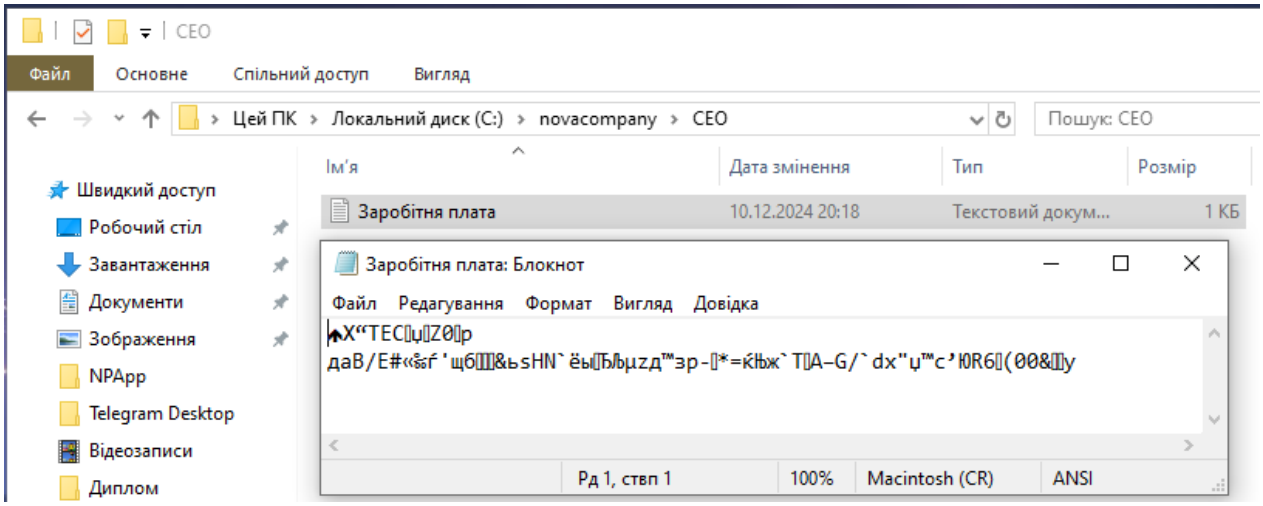

Рисунок 3.10 – Зашифроване повідомлення

Тільки директор компанії має доступ до розшифровки цього повідомлення в розшифрованому вигляді, оскільки він є єдиним користувачем з правами для цього. Для демонстрації техніки розмежування доступу в додатку можна спробувати розшифрувати повідомлення, надіслане директору, увійшовши до акаунту фахівця з кібербезпеки.

Однак спроба розшифрувати це повідомлення з акаунту інспектора відділу кадрів завершиться помилкою, оскільки цей користувач не має необхідних прав для доступу до вмісту повідомлення, відправленого директору. Це підтверджує правильність налаштування механізму доступу та демонструє, як розмежування прав доступу забезпечує безпеку інформації в системі.

Для дешифрування повідомлення користувачеві потрібно ввести пароль *novaplt1307* та натиснути кнопку «Відкрити файл». Після цього програма автоматично відкриє директорію підприємства, де зберігаються зашифровані повідомлення.

Директор компанії, маючи відповідні права доступу, зможе відкрити потрібне зашифроване повідомлення. Це дозволяє ефективно контролювати доступ до конфіденційної інформації та забезпечує її безпеку, оскільки тільки авторизовані користувачі з правильним паролем можуть отримати доступ до розшифрованого вмісту.

Для перевірки безпеки даних здійснимо вхід під іншим логіном і паролем працівника, якому не було надано доступ до перегляду цього файлу (рис. 3.11).

Логін: kadryhr1.

Пароль: Kadryhr3001.

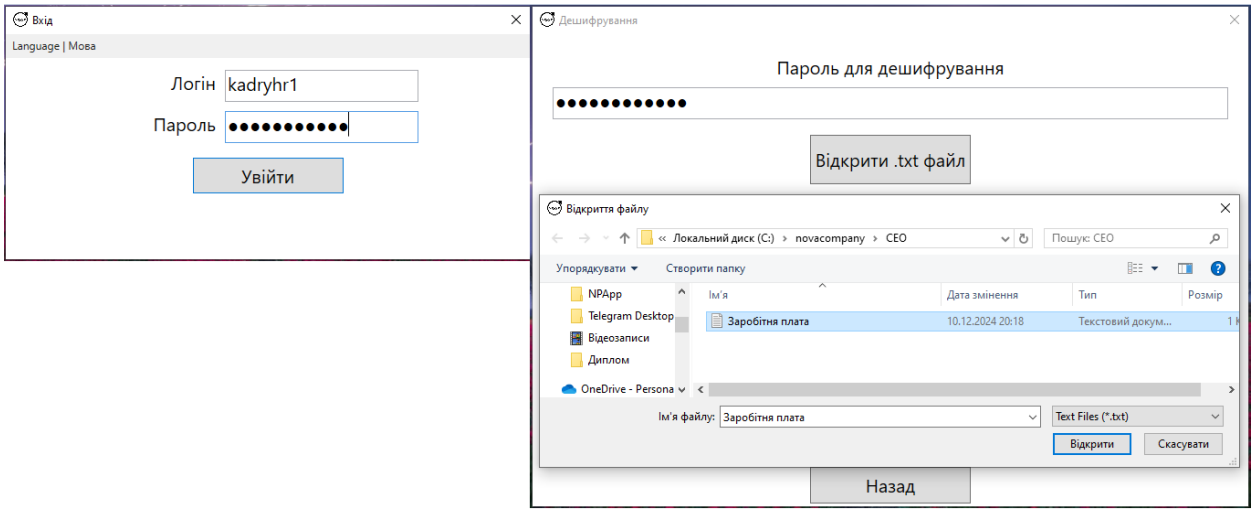

Рисунок 3.11 – Відкриття файлу для шифрування

В даному випадку буде виведено вікно «Доступ заблоковано», оскільки інспектор відділу кадрів не має доступу до повідомлень, які були відправлені генеральному директору (рис. 3.12).

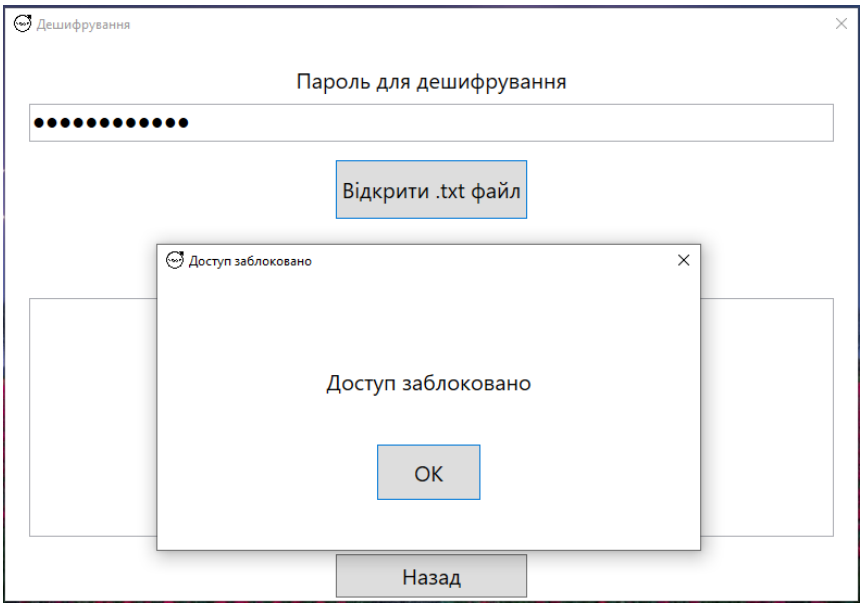

Рисунок 3.12 – Блокування доступу

Проте з акаунта генерального директора дане повідомлення доступне (рис. 3.13, рис. 3.14).

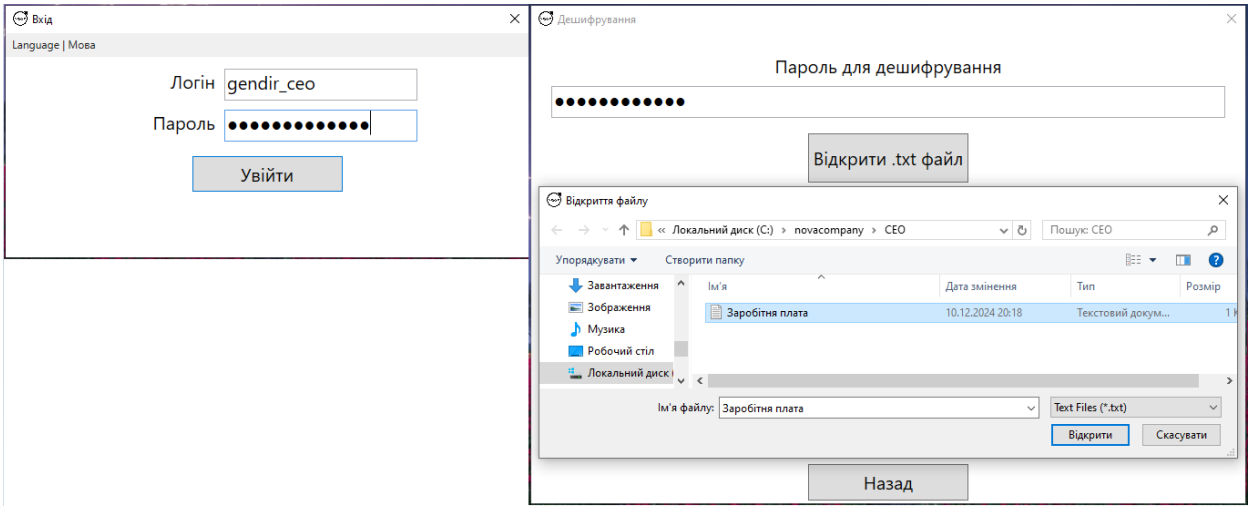

Рисунок 3.13 – Розшифроване повідомлення.

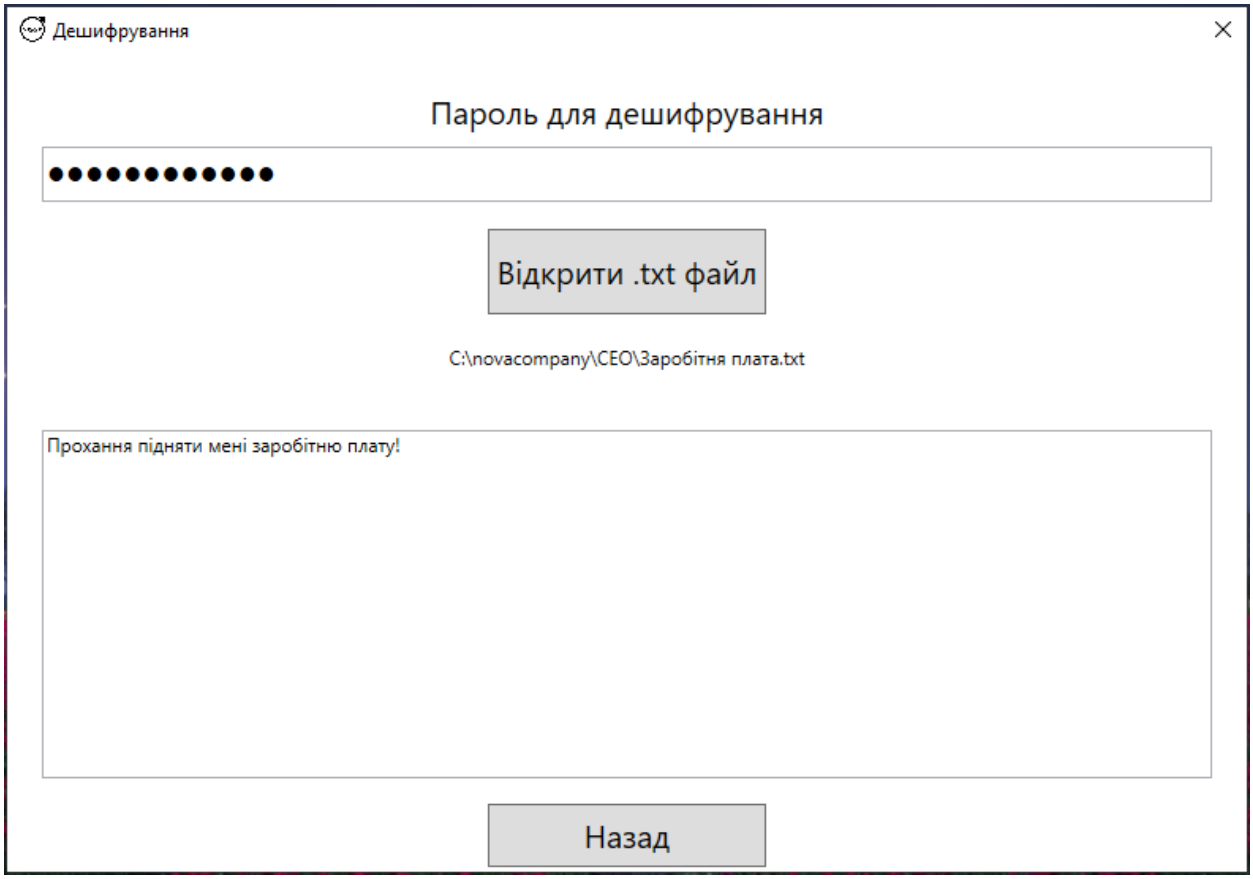

Рисунок 3.14 – Розшифроване повідомлення.

Слід зазначити, що працівники одного підрозділу не можуть отримати доступ до повідомлень іншого підрозділу, навіть генеральний директор.

Голова підрозділу має доступ до повідомлень, які були надіслані його підрозділу, а також до повідомлень, адресованих йому особисто. Звичайний працівник підрозділу може переглядати лише ті повідомлення, що призначені виключно його підрозділу, але не голові підрозділу. Загальні повідомлення доступні для всіх працівників.

3.4 Перспективи розвитку програми

Розроблений настільний додаток для обміну внутрішніми повідомленнями між підрозділами компанії на базі платформи WPF та мови програмування C# є важливим кроком для покращення внутрішньої комунікації. Проте, існує низка перспектив для його подальшого розвитку та вдосконалення.

Розширення функціональних можливостей:

1) Додавання шифрування різного рівня складності: Замість єдиного пароля для всіх користувачів можна інтегрувати індивідуальні ключі шифрування або двофакторну аутентифікацію для підвищення рівня захисту даних.

2) Розробка системи сповіщень: Додаток може бути доповнено функцією миттєвих сповіщень про нові повідомлення, що підвищить ефективність обміну інформацією.

3) Архівування та пошук повідомлень: Реалізація можливості зберігання старих повідомлень у зашифрованому форматі та створення пошукового механізму для швидкого доступу до потрібної інформації.

Подальший розвиток програми може включати адаптацію для інших операційних систем, таких як Linux або macOS, а також створення мобільної

версії для платформ Android та iOS. Це дозволить користувачам отримувати доступ до програми з різних пристроїв, незалежно від їх операційної системи.

Інтеграція з корпоративними сервісами:

a) Підключення до корпоративних систем управління проектами (наприклад, Jira, Trello чи Microsoft Teams) для централізованого обміну повідомленнями та завданнями.

b) Інтеграція з базами даних компанії, що дозволить автоматизувати створення звітів або обмін важливими документами.

Впровадження технологій штучного інтелекту:

Для підвищення зручності та ефективності роботи можна додати:

a) Автоматичний аналіз та категоризацію повідомлень, що дозволить визначати їх пріоритетність.

b) Інтелектуальних помічників, які будуть допомагати користувачам формувати повідомлення або вчасно реагувати на них.

У разі зростання компанії програма може бути масштабована для підтримки великої кількості підрозділів та користувачів одночасно, з урахуванням підвищених вимог до продуктивності та безпеки.

Таким чином, подальший розвиток додатка дозволить підвищити його функціональність, зробити його більш гнучким, безпечним та зручним для використання в умовах зростаючих вимог сучасного бізнесу.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи була розроблена система захисту інформації для корпоративної мережі контакт-центру «Нової пошти», що базується на сучасних методах шифрування та моніторингу загроз. Відповідно до плану будівлі було встановлено:

- 20 камер відеоспостереження;
- 4 системи контролю доступу за допомогою карток;
- 4 комплекти сигналізації;
- 1 річну підписку на антивірус Bitdefender GravityZone Business Security для 35 комп'ютерів та 1 сервера;
- розроблено програму для шифрування та дешифрування внутрішніх повідомлень компанії на платформі WPF.

Загальна вартість проекту мережі становить 50 649 грн (1 235,78 доларів США).

Таким чином, реалізація та впровадження цих комплексних заходів забезпечують надійний захист інформації для офісу контакт-центру «Нової пошти».

В результаті виконання кваліфікаційної роботи була створена ефективна система захисту інформації для офісу контакт-центру «Нової пошти», що включає в себе як апаратні, так і програмні рішення для забезпечення конфіденційності та цілісності даних. Запровадження відеоспостереження, систем контролю доступу, сигналізації та антивірусного програмного забезпечення гарантує фізичний захист корпоративної мережі, а використання сучасних методів шифрування для обміну внутрішніми повідомленнями забезпечує надійний захист інформації в цифровому вигляді.

Однією з ключових переваг розробленої системи є її гнучкість та адаптивність до змін. Інтеграція інструментів шифрування та моніторингу загроз

дозволяє компанії швидко реагувати на потенційні ризики, що виникають у процесі роботи. Крім того, завдяки використанню платформи WPF для розробки програмного забезпечення для шифрування, система відрізняється високою швидкістю роботи та зручним інтерфейсом, що сприяє безпеці без додаткового навантаження на користувачів.

Впровадження таких комплексних заходів не лише підвищує рівень захисту корпоративної інформації, але й формує культуру кібербезпеки в компанії, що є важливою умовою для подальшого розвитку та стабільної роботи організації. Враховуючи сучасні виклики у сфері кіберзагроз, така система захисту є важливою інвестицією в безпеку та майбутній розвиток «Нової пошти», що дозволяє ефективно реагувати на змінні умови зовнішнього середовища.

ВИКОРИСТАНІ ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Поняття, сутність, значення захисту інформації. URL: https://esu.com.ua/article-15872 (дата звернення: 02.09.2024).

2. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 07.09.2024).

3. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.09.2024).

4. Закон України «Про Національну програму інформатизації». URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 17.09.2024).

5. Закон України «Про захист інформації в автоматизованих системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 22.09.2024).

6. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 28.09.2024).

7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/nd-tz-1.1-002-99.html (дата звернення: 02.10.2024).

8. Закон України «Основи законодавства України про охорону здоров'я». URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 07.10.2024).

9. Історія компанії «Нова Пошта». URL: https://novaposhta.ua/istoriya_kompanii (дата звернення: 12.10.2024).

10. Особливості реалізації системи розмежування доступу. URL: https://studfile.net/preview/9094212/page:82/ (дата звернення: 17.10.2024).

11. Засоби охорони об'єкта. URL: https://sg-ukraine.com.ua/technical-security-systems/ (дата звернення: 22.10.2024).

12. Технічні заходи. URL: https://studies.in.ua/bjd-zaporojec/1211-173-osnovn-tehnchn-ta-organzacyn-zahodi-schodo-proflaktiki-virobnichogo-travmatizmu-ta-profesynoyi-zahvoryuvanost.html (дата звернення: 27.10.2024).

13. Розмежування доступу та модель Белла-ЛаПадули. URL: https://studfile.net/preview/5470392/page:5/ (дата звернення: 01.11.2024).

14. Додаткові можливості протоколювання. URL: https://www.prostir.ua/?kb=protokolyujemo-pravylno-abo-yak-pidhotuvaty-meeting-minutes (дата звернення: 06.11.2024).

15. Комп'ютерні віруси. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/kompyuternyy-virus/?srsltid=AfmBOoowMyiSdSNfsT_9jdfcP71Gt93otoUzwXbqbDre0vBCTR6PGG1s (дата звернення: 11.11.2024).

16. Джерела вірусів. URL: https://studfile.net/preview/7357935/page:7/ (дата звернення: 16.11.2024).

17. Антивірусні програми. URL: https://2ip.ua/ua/blog/antivirus (дата звернення: 21.11.2024).

18. Malwarebytes for Business. URL: https://www.malwarebytes.com/ (дата звернення: 26.11.2024).

19. Bitdefender GravityZone Business Security. URL: https://bitdefender.ua/for-business/business-security/ (дата звернення: 01.12.2024).

20. Symantec End-User Endpoint Security. URL: https://www.broadcom.com/products/cybersecurity/endpoint/end-user (дата звернення: 03.12.2024).

21. Microsoft Defender for Endpoint. URL: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint (дата звернення: 05.12.2024).

22. CrowdStrike Falcon Endpoint Protection. URL: https://www.crowdstrike.com/en-us/products/ (дата звернення: 07.12.2024).

23. Avast Business. URL: https://www.avast.ua/business#pc (дата звернення: 09.12.2024).

24. Криптологічний захист інформації. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/12447/1/75%20%D0%A2.1-456-458.pdf (дата звернення: 11.12.2024).

25. Twofish. URL: https://studfile.net/preview/2807205/page:23/ (дата звернення: 15.12.2024).