Нaцioнaльний унiвepcитeт «Пoлтaвcькa пoлiтeхнiкa iмeнi Юpiя Кoндpaтюкa»

(пoвнe нaймeнувaння вищoгo нaвчaльнoгo зaклaду)

Нaвчaльнo нaукoвий iнcтитут iнфopмaцiйних тeхнoлoгiй тa poбoтoтeхнiки

(пoвнa нaзвa інституту)

Кaфeдpa кoмп’ютepних тa iнфopмaцiйних тeхнoлoгiй i cиcтeм

(пoвнa нaзвa кaфeдpи)

**Пoяcнювaльнa зaпиcкa**

**дo диплoмнoгo пpoєкту (poбoти)**

магістра

(piвeнь вищої освіти)

нa тeму

«Захист інформації на підприємстві з використанням

криптографічного алгоритму шифрування даних»

Викoнaв: cтудeнт 6 куpcу, гpупи 602– ТН

cпeцiaльнocтi

122 Кoмп’ютepнi нaуки

(шифp i нaзвa спеціальності)

Литвиненко О.С.

(пpiзвищe тa iнiцiaли)

Кepiвник Білоусько Т.М.

(пpiзвищe тa iнiцiaли)

Peцeнзeнт Очерідник О.В.

(пpiзвищe тa iнiцiaли)

Пoлтaвa – 2023 poку

**МIНICТEPCТВO OCВIТИ I НAУКИ УКPAЇНИ**

**НAЦIOНAЛЬНИЙ УНIВEPCИТEТ**

**«ПOЛТAВCЬКA ПOЛIТEХНIКA IМEНI ЮPIЯ КOНДPAТЮКA»**

**НAВЧAЛЬНO НAУКOВИЙ IНCТИТУТ IНФOPМAЦIЙНИХ ТEХНOЛOГIЙ ТA POБOТOТEХНIКИ**

**КAФEДPA КOМП’ЮТEPНИХ ТA IНФOPМAЦIЙНИХ ТEХНOЛOГIЙ I CИCТEМ**

**КВAЛIФIКAЦIЙНA POБOТA МАГІСТРА**

**cпeцiaльнicть 122 «Кoмп’ютepнi нaуки»**

**нa тeму**

**«Захист інформації на підприємстві з використанням криптографічного алгоритму шифрування даних»**

**Cтудeнта гpупи 602– ТН Литвиненко Олександра Сергійовича**

Кepiвник poбoти

кaндидaт економічних нaук,

дoцeнт Білоусько Т.М.

Консультант

кaндидaт тeхнiчних нaук,

дoцeнт Гoлoвкo Г.В.

Зaвiдувaч кaфeдpи

кaндидaт фізико-математичних нaук,

Двірна О.А.

Полтава – 2023

**PEФEPAТ**

Кваліфікаційна робота магістра: 79 с., 34 малюнка, 1 додаток, 13 джерел.

**Об’єкт дослідження:** організація захисту інформації на підприємстві, реалізація криптографічного алгоритму шифрування даних.

**Мета роботи:** аналіз рівня інформаційної безпеки на підприємстві, рекомендації щодо його покращення та розробка програмного забезпечення для безпечної роботи з файлами.

**Методи:** комплексна організація захисту інформації на підприємстві, створення та впровадження програмного додатку безпечної передачі даних шляхом їх шифрування та забезпечення розмежування доступу між користувачами.

**Ключові слова:** інформаційна безпека, захист інформації, розмежування доступу, криптографічний захист, локальна комп’ютерна мережа.

**ANNOTATION**

Qualification work of master’s degree: 79 p., 34 pictures, 1 application, 13 sources.

**Object of study:** organisation of information security at the enterprise, implementation of a cryptographic data encryption algorithm.

**The goal of the work:** analysis of the level of information security at the enterprise, recommendations for its improvement and development of software for secure file management.

**Methods:** comprehensive organisation of information protection at the enterprise, creation and implementation of a software application for secure data transmission by encrypting them and ensuring access separation between users.

**Keywords:** information security, information protection, access control, cryptographic protection, local computer network.

**ЗМІСТ**

[ПEPEЛIК УМOВНИХ ПOЗНAЧEНЬ, CИМВOЛIВ, CКOPOЧEНЬ I ТEPМIНIВ 6](#_Toc154138850)

[ВCТУП 7](#_Toc154138851)

[POЗДIЛ 1 АНАЛІТИЧНИЙ ОГЛЯД 9](#_Toc154138852)

[1.1 Опис предметної області 9](#_Toc154138853)

[1.2 Сутність та задачі комплексної системи захисту інформації 14](#_Toc154138854)

[1.3 Поняття комплексної системи захисту інформації 15](#_Toc154138855)

[1.4 Призначення комплексної системи захисту інформації 18](#_Toc154138856)

[1.5 Розробка політики безпеки 20](#_Toc154138857)

[1.6 Методи захисту інформації 24](#_Toc154138858)

[1.7 Шифрування інформації 28](#_Toc154138859)

[1.8 Формування вимог до програмного продукту 29](#_Toc154138860)

[1.8.1 Функціональні вимоги 30](#_Toc154138861)

[1.8.2 Нефункціональні вимоги 30](#_Toc154138862)

[POЗДIЛ 2 ОРГАНІЗАЦІЯ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМТСВІ 31](#_Toc154138863)

[2.1. Історія підприємства 31](#_Toc154138864)

[2.2. Опис діяльності 32](#_Toc154138865)

[2.3. Організаційна структура 34](#_Toc154138866)

[2.4. Варіанти інженерно-технічних заходів захисту інформації 37](#_Toc154138867)

[2.5. Опис наявних засобів захисту інформації 41](#_Toc154138868)

[2.6. Рекомендації щодо покращення рівня захисту інформації 45](#_Toc154138869)

[2.7. Антивірусний захист 50](#_Toc154138870)

[2.8. Організація підрозділу захисту інформації 52](#_Toc154138871)

[2.9. Розмежування доступу 54](#_Toc154138872)

[2.10. Ідентифікація та облікові записи 58](#_Toc154138873)

[POЗДIЛ 3 ПРАКТИЧНА ЧАСТИНА РОЗРОБКА ІНФОРМАЦІЙНОГО ЗАХИСТУ 61](#_Toc154138874)

[3.1 Криптологія та її складові 61](#_Toc154138875)

[3.2 Опис алгоритму шифрування RC4 та принцип його роботи 62](#_Toc154138876)

[3.3 Опис програми та блок-схема алгоритму її виконання 63](#_Toc154138877)

[ВИCНOВКИ 72](#_Toc154138878)

[CПИCOК ВИКOPИCТAНИХ ДЖEPEЛ 73](#_Toc154138879)

[ДОДАТОК А ВИХІДНИЙ КОД ПРОГРАМИ 75](#_Toc154138880)

# 

# **ПEPEЛIК УМOВНИХ ПOЗНAЧEНЬ, CИМВOЛIВ, CКOPOЧEНЬ I ТEPМIНIВ**

**ЗІ** – захист інформації;

**СІБ** – система інформаційної безпеки;

**ІзОД** – інформація з обмеженим доступом;

**СЗІ** – система захисту інформації;

**ІС** – інформаційна система;

**КС** – комп’ютерна система;

**ПЗІ** – підрозділ захисту інформації;

**НСД** – несанкціонований доступ;

**СКС** – структурована кабельна система.

# **ВCТУП**

Інформація була цінним ресурсом у всі часи. Її цінність можна визначити не лише кількістю затраченого на її отримання часу, а й безпосередньо прибутком, який можна отримати при її реалізації.

Інформаційна безпека являє собою вміння особового складу підприємства гарантувати захист інформаційних ресурсів та потоків від небезпеки несанкціонованого доступу до них.

За наслідками негативного впливу на загальні властивості інформації (конфіденційність, цілісність, доступність) виділяють дестабілізуючі чинники техногенного, антропогенного, природного характеру.

Нині зростання суспільства можна охарактеризувати негативною динамікою не тільки зумисних посягань на роботу інформаційних систем чи мереж, а й правопорушень, вчинених з використанням сучасних технологій, найновішої техніки.

У цей час перед приватними підприємствами питання створення умов захисту комерційної таємниці стоїть особливо гостро. При нинішній економічній конкуренції розповсюдженими стали наступні протизаконні процедури, як крадіжка комерційної інформації, прослуховування, вилучення інформації з технічних каналів зв’язку через комп’ютерні мережі тощо. Витік даних з обмеженім доступом може завдати значних збитків власнику компанії. Інформація, не призначена для загального доступу, використовується злочинцями або конкурентними компаніями для досягнення своїх корисливих цілей, і в інтересах підприємства запобігти виникненню таких ситуацій. Обізнаність у питанні можливих небезпек, причин та умов скоєння таких правопорушень дасть змогу працівникам підрозділів служб безпеки підприємств у межах своєї компетенції реалізовувати наміри, що будуть перешкоджати незаконним посяганням на інформаційні ресурси та потоки господарюючого суб’єкта.

Однак не всі керівники розуміють критичну необхідність у забезпеченні належного рівня інформаційної безпеки. А ті, хто розуміють, не завжди вдало організовують процес захисту інформації. Перш за все треба розуміти, що організація захисту інформації на підприємстві передбачає не лише впровадження деяких технічних та програмних засобів, а саме комплексний підхід до оптимізації всієї системи, а не покращення показників окремих її елементів. Для того. щоб забезпечити усунення недоліків у сфері підприємництва, можна вдатися до проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства, а також її ресурсного забезпечення. Планування захисту інформації на підприємстві необхідно в першу чергу для:

* недопущення втрати, розкрадання, видозміни, підробки, несанкціонованого копіювання або блокування інформації;
* попередження погрозам, загрозам безпеці осіб та безпосередньо підприємству;
* запобігання іншим формам протизаконного проникнення в інформаційний простір підприємства, підтримка законного режиму документованої інформації як об'єкту власності;
* охорона конституційних прав громадян на недопущення розповсюдження особистої таємниці і забезпечення конфіденційності персональних даних, наявних в інформаційних системах;
* зберігання конфіденційності документованої інформації відповідно до законодавства.

Тобто, нині існує дуже багато варіантів підтримання безпеки інформації, але не всі вони являються дійсно ефективними, оскільки лише комплексний підхід може забезпечувати підтримку максимальної ефективності захисту інформації, тому що системний підхід забезпечує потрібні елементи захисту й встановлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових та всеохоплення захисту, забезпечує її надійність.

# **POЗДIЛ 1 АНАЛІТИЧНИЙ ОГЛЯД**

## **Опис предметної області**

Ефективне функціонування підприємства чи організації неможливе без управління ресурсами, що використовуються для досягнення мети. Говорячи про поняття ресурсів, зараз в управлінській літературі панує ідея що воно вміщує в себе не тільки людей, сировину чи капітал, а також й інформацію. Ціллю направленої діяльності підприємства є встановлення необхідних ресурсів і трансформування їх у корисну продукцію [1].

З одного боку природні ресурси, а з іншого інформація для суспільства у будь-який час були лімітованими. Потреба у інформації у декілька разів перевищує перспективу її задовольнити. Для того, щоб вдовольнити запити підприємства у інформації, має бути створена найкраща структура з формулюванням вимог, що висуваються для підтримання інформаційної безпеки на високому рівні [1].

Інформація становить собою об’єкт цивільних прав, що входить до складу нематеріальних благ. Відповідно до статті 178 Цивільного кодексу України, інформація може вільно переходити за правонаступництвом або у спадок чи відчужуватися, якщо вона не була прибрана з цивільного обороту чи не була обмежена в ньому або являється неодмінною частиною фізичної чи юридичної особи [1].

Найсуттєвішими, з практичного погляду, характеристиками інформації є:

* корисність інформації, яка визначається можливістю досягнення мети, яку ставить перед собою отримувач інформації;
* правдивість, яка визначається відповідністю отриманої інформації об'єктивній реальності навколишнього світу;
* актуальність як міра відповідності цінності та правдивості інформації поточному часу (певному часовому періоду);
* хронологічні характеристики, які визначають здатність даних передавати динаміку зміни ситуації (динамічність);
* оперативність як властивість даних, що вказує на те, що час їхнього збору та обробки відповідає динаміці зміни ситуації;
* ідентичність як характеристика даних, що визначає їхню відповідність стану об'єкта [2].

Встановлення складу інформації, яка потребує захисту, є першим етапом у розробці системи безпеки. Від точності цього процесу залежить ефективність функціонування розробленої системи. Загальний підхід полягає у тому, що під захистом перебуває вся інформація з обмеженим доступом (ІзОД), включаючи державну таємницю (секретну інформацію), комерційну таємницю, що визначається її власником, та частину відкритої інформації. У цьому контексті ІзОД повинна бути захищена від можливого витоку та втрат, тоді як відкрита інформація має бути захищена лише від можливих втрат [3].

Часто висловлюється погляд, що будь-яка відкрита інформація не повинна підлягати захисту. Захист відкритої (публічної) інформації завжди існував і виконувався через реєстрацію носіїв інформації, відстеження їх руху та місцезнаходження, а також створення безпечних умов для зберігання. При цьому важливо враховувати, що відкритість інформації не зменшує її цінності, і цінна інформація вимагає захисту від втрати. Забезпечення цього захисту не повинно спрямовуватися на обмеження загальної доступності інформації. Існує принцип, згідно з яким відмова від доступу до інформації не припускається, але при цьому доступ повинен здійснюватися з дотриманням встановлених вимог з її збереження та використання [3].

Інформація – це властивість взаємодії повідомлення з користувачем. На Рисунку 1.1 наведено класифікацію інформації за порядком доступу [3].

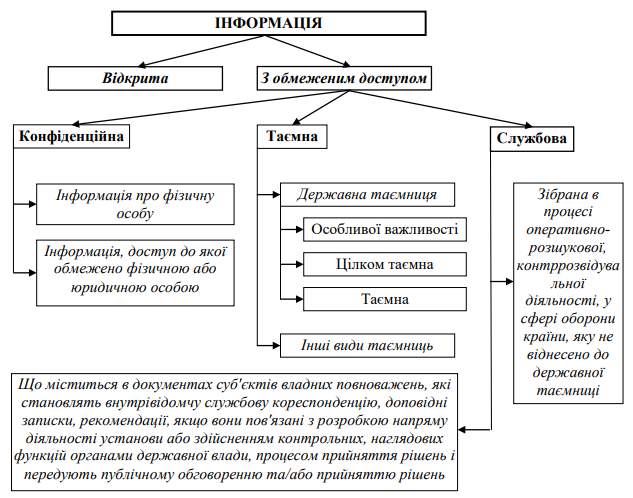


Рисунок 1.1- Класифікація інформації за порядком доступу

Публічна інформація - це інформація, яка була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством. Ця інформація може бути відображена та задокументована за допомогою різних засобів та на різних носіях. Також до публічної інформації відноситься інформація, яка знаходиться у володінні суб'єктів владних повноважень та інших розпорядників публічної інформації, визначених законом України "Про доступ до публічної інформації" [3].

Інформація з обмеженим доступом поділяється на:

* конфіденційну;
* таємну;
* службову [3].

Конфіденційна інформація – це та, до якої доступ обмежений фізичною або юридичною особою, за винятком суб'єктів владних повноважень. Ця інформація може розповсюджуватися суб'єктами владних повноважень за їхнім бажанням відповідно до умов, передбачених ними [3].

Таємна інформація - це інформація, до якої обмежено доступ, а розголошення якої може призвести до шкоди особі, суспільству або державі. Таємною вважається інформація, яка включає в себе державну, професійну, банківську таємницю, а також таємницю розслідування та інші види таємниць, передбачені законом [3].

До службової інформації може належати інформація, яка міститься в документах суб'єктів владних повноважень, що складають внутрівідомчу службову кореспонденцію. Сюди входять доповідні записки, рекомендації та інші матеріали, якщо вони пов'язані з розробкою напряму діяльності установи або виконанням контрольних наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень [3].

Інформаційна безпека - це стан інформації, за якого забезпечується збереження визначеними політиками безпеки властивостей інформації. Основні складові інформаційної безпеки включають **конфіденційність**, **цілісність** та **доступність** [3].

**Конфіденційність** інформації полягає в її властивості залишатися невідомою для широкого загалу, мати характер секретності та бути чисто особистою [3].

**Цілісність** інформації виявляється у тому, що неавторизований користувач чи процес не може здійснити зміни в ній. Цілісність інформації забезпечується, коли фіксуються чіткі правила для її зміни та вилучення [3].

Можливість використання інформаційного ресурсу визначається його **доступністю**, що означає, що користувач чи процес з належними повноваженнями може користуватися цим ресурсом відповідно до встановлених політикою безпеки правил [3].

Основними причинами порушення безпеки інформації є:

* **несанкціонований доступ**: незаконне отримання доступу до інформації, порушуючи встановлені в інформаційній системі правила розмежування доступу;
* **витік інформації**: результат дій порушника, через які інформація стає відомою (доступною) суб'єктам, які не мають права доступу до неї;
* **втрата інформації**: дія, внаслідок якої інформація в комп'ютерній системі припиняє існування для осіб, які мають право власності на неї в повному або обмеженому обсязі;
* **підробка інформації**: умисні дії, що призводять до спотворення інформації, яка повинна оброблятися або зберігатися в комп'ютерній системі;
* **блокування інформації**: дії, що призводять до припинення доступу до інформації;
* п**орушення роботи комп'ютерної системи**: дії або обставини, які призводять до спотворення процесу обробки інформації [2].

Причини виникнення вказаних випадків включають:

* **збої обладнання**: включають у себе неполадки в кабельних системах, переривання електроживлення, збої на серверах, робочих станціях, мережних картах, дискових системах та інше;
* **некоректна робота** програмного забезпечення: охоплює втрату або зміну даних у разі помилок у програмному забезпеченні, втрату даних внаслідок зараження системи комп'ютерними вірусами та інше;
* **навмисні дії сторонніх осіб**: включають несанкціоноване копіювання, знищення, підробку або блокування інформації, спричинення витоку інформації та інші атаки;
* **помилки обслуговуючого персоналу та користувачів**: охоплюють випадкове знищення або зміну даних, некоректне використання програмного та апаратного забезпечення, що призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або зміну даних, порушення інтересів інших законних користувачів та інше;
* **навмисні дії обслуговуючого персоналу та користувачів**: включають у себе усе вище сказане, а також ознайомлення сторонніх осіб із конфіденційною інформацією. Важливо відзначити, що порушенням безпеки можуть вважатися і дії, які не призводять безпосередньо до втрати або витоку інформації, але передбачають втручання в роботу системи [2].

Для нормального функціонування компанії важливо мати доступ до наступної інформації:

* фінансовий стан компанії;
* конкурентоспроможність її продукції;
* кількість та рівень кваліфікації працівників [1].

Набір різноманітної інформації для прийняття рішень в сфері підприємництва можна визначити як інформаційне забезпечення підприємства. Це включає вхідну та вихідну інформацію. З точки зору захисту інформаційних ресурсів, особливо важливою є вихідна інформація [1].

Найдоступнішою для підприємця є інформацію про стан фірми, оскільки вона формується за його участі. У випадку фірми, яка вже діє або лише створюється, є деякі відмінності в обсязі, джерелах отримання та складі такої інформації. З огляду вже наявної інформації може бути створений деякий інформаційний масив за плановою і звітною інформацією, такою як місячні, квартальні, річні звіти фірми, прогнози розвитку фірми, бухгалтерські звіти тощо [1].

## **Сутність та задачі комплексної системи захисту інформації**

Є погляд, що проблеми захисту інформації обмежуються лише інформацією, яку обробляє комп'ютер. Це, можливо, пов'язано з тим, що комп'ютер, особливо особистий, вважається центром зберігання інформації. Однак об'єкт інформатизації, на який спрямовані заходи з захисту інформації, може виглядати більш широким поняттям, ніж просто особистий комп'ютер [3].

У реальному житті всі ці окремі "об'єкти інформатизації" знаходяться в межах одного підприємства і утворюють єдиний комплекс компонентів, які мають спільні цілі, завдання, структурні зв'язки, технологію інформаційного обміну та інші взаємозв'язки [3].

Сучасне підприємство представляє собою значну кількість різноманітних компонентів, які об'єднані в складну систему для досягнення визначених цілей. Протягом функціонування підприємства ці компоненти можуть зазнавати модифікацій. Різноманітність і складність впливу внутрішніх та зовнішніх факторів, які часто не можуть бути однозначно оцінені в кількісному виразі, призводять до того, що ця складна система може набувати нових якостей, які не є характерними для її окремих компонентів [3].

Типовою особливістю таких систем є наявність людей в кожній з їх компонентів і фізичне віддалення людини від об'єкта її діяльності. Це пояснюється тим, що безліч компонентів, що складають об'єкт інформатизації, можна інтегрувати в сукупність трьох груп систем: люди, технічні системи та приміщення, в яких вони розташовані, і програмне забезпечення, що виступає інтелектуальним посередником між людиною і технікою. Ця трійця утворює соціотехнічну систему. Таке розуміння соціотехнічної системи є досить поширеним і може застосовуватися до багатьох об'єктів. В нашому випадку область дослідження обмежується аналізом безпеки систем, які призначені для обробки вхідної інформації та видачі результату [3].

## **Поняття комплексної системи захисту інформації**

Основний напрямок пошуку нових методів захисту інформації не обмежується лише створенням відповідних механізмів; він передбачає реалізацію систематичного процесу, який охоплює всі етапи життєвого циклу інформаційних систем. Цей процес включає комплексне використання всіх доступних засобів захисту. При цьому всі інструменти, методи і заходи, що використовуються для захисту інформації, оптимально поєднуються в єдиний цілісний механізм. Цей механізм спрямований на захист не лише від зловмисників, а й від некваліфікованих або недостатньо підготовлених користувачів і персоналу, а також від позаштатних технічних ситуацій [3].

Однією з ключових проблем впровадження систем захисту є балансування між двома аспектами:

* забезпечення надійного захисту ідентифікації у системі інформації, включаючи уникнення випадкового і навмисного доступу сторонніх осіб до інформації, ефективне розмежування доступу до пристроїв і ресурсів системи для всіх користувачів, адміністрації та обслуговувального персоналу;
* забезпечення того, щоб системи захисту не викликали помітних незручностей для користувачів під час роботи з ресурсами системи [3].

Розв'язання проблеми забезпечення необхідного рівня захисту інформації є вкрай складним завданням. Це передбачає не лише впровадження певних наукових та науково-технічних заходів та використання спеціалізованих засобів і методів, але і створення цілісної системи організаційно-технологічних заходів, а також використання комплексу спеціальних засобів і методів в галузі ЗІ [3].

При створенні систем інформаційної безпеки в інформаційних системах увага в першу чергу приділяється принципам безперервного розвитку системи та системному (комплексному) підходу. На підставі теоретичних аналізів та результатів практичних досліджень у галузі захисту інформації розроблено системно-концептуальний підхід [3].

У рамках системно-концептуального підходу системність розглядається з кількох аспектів:

* цільова системність визначає захищеність інформації як ключовий аспект загального поняття якості інформації;
* просторова системність передбачає взаємодію всіх компонентів підприємства для вирішення всіх питань щодо захисту;
* тимчасова системність визначає безперервність робіт з захисту інформації, які виконуються відповідно до заздалегідь розроблених планів;
* організаційна системність підкреслює необхідність єдності в організації всіх аспектів робіт з захисту інформації та їх управління [3].

Підхід є концептуальним у тому сенсі, що він передбачає створення єдиної концепції, яка включає в себе повний набір науково обґрунтованих поглядів, положень і рішень. Ця концепція є необхідною і достатньою для оптимальної організації та забезпечення надійного захисту інформації. Крім того, концептуальний підхід передбачає цілеспрямовану організацію всіх робіт з ЗІ [3].

Комплексний (системний) підхід до побудови будь-якої системи передбачає вивчення об'єкта впроваджуваної системи, оцінку загроз безпеки цього об'єкта, аналіз доступних засобів, оцінку економічної доцільності, дослідження самої системи, її властивостей та принципів роботи, а також можливість внесення змін для підвищення ефективності. Цей підхід враховує всі внутрішні та зовнішні фактори, а також дозволяє організувати процес від початку до кінця, забезпечуючи повну координацію всіх етапів [3].

Комплексний (системний) підхід орієнтується на розгляд проекту як цілісної системи, а не окремих її складових частин. Його метою є оптимізація всієї системи в комплексі, замість поліпшення лише окремих її елементів. Це обумовлено тим, що покращення одних параметрів може призвести до погіршення інших, і тому важливо забезпечити баланс між протиріччями вимог і характеристик системи [3].

Підхід до створення системи безпеки, заснований на системних принципах, означає досягнення найкращого поєднання взаємопов'язаних характеристик, таких як організаційні, програмні, апаратні, фізичні та інші, які мають підтверджену ефективність у практиці створення схожих систем захисту, і використовуються на всіх стадіях технологічного циклу обробки інформації [1].

Постійний розвиток системи є фундаментальною засадою для комп'ютерних інформаційних систем і залишається важливим принципом для системи інформаційної безпеки. Способи захисту інформації в галузі інформаційних технологій постійно збагачуються і, отже, забезпечення безпеки інформаційних систем вимагає постійного зусиль і не може бути вирішено одноразово. Цей процес продовжується невпинно і включає в себе наступні аспекти:

* розроблення і реалізація найбільш раціональних методів, прийомів і стратегій для вдосконалення системи інформаційної безпеки (СІБ);
* постійний моніторинг і контроль;
* виявлення слабких точок і недоліків у СІБ;
* встановлення потенційних шляхів витоку інформації;
* розробка нових способів запобігання несанкціонованому доступу [1].

## **Призначення комплексної системи захисту інформації**

Основною метою створення системи захисту інформації є забезпечення надійності ЗІ. Система ЗІ представляє собою організовану сукупність об'єктів і суб'єктів ЗІ, методів і засобів захисту, а також проведених захисних заходів [3].

Таким чином, компоненти ЗІ, з одного боку, входять в систему як її складова частина, а з іншого боку, самостійно організовують систему, забезпечуючи виконання захисних заходів [3].

У зв'язку з тим, що систему можна визначити як сукупність взаємопов'язаних елементів, завданням системи захисту інформації є інтеграція всіх компонентів в єдину структуру, де кожен компонент, виконуючи свою функцію, сприяє виконанню завдань інших компонентів і логічно взаємодіє з ними [3].

Забезпечення надійності системи захисту означає, що рівень цієї надійності не може бути зниженим в разі виникнення в системі збоїв, відмов, навмисних атак з боку зломлювачів або ненавмисних помилок з боку користувачів та обслуговуючого персоналу [1].

Рівень надійності захисту інформації прямо залежить від системності. Якщо окремі компоненти технології захисту не узгоджені між собою, існує збільшений ризик виникнення "проколів" в системі захисту [3].

По-перше, потреба у комплексних рішеннях полягає у єднанні локальних систем захисту інформації в єдину цілісну структуру, де вони мають працювати як взаємопов'язані компоненти. Локальні системи захисту можуть включати різні види захисту інформації, такі як правовий, організаційний та інженерно-технічний [3].

По-друге, необхідність комплексних рішень обумовлена метою самої системи. Система повинна логічно і технологічно об'єднати всі компоненти захисту. Проте, в її області дії можуть виникнути питання щодо повноти цих компонентів, оскільки вона не охоплює всі можливі фактори, що впливають на якість захисту. Наприклад, система може включати певні об'єкти захисту, але чи охоплені всі вони - це вже виходить за межі системи [3].

Таким чином, якість і надійність захисту залежать не лише від видів складових системи, але й від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Другим призначенням комплексності є забезпечення повноти всіх компонентів системи захисту, що базується на аналізі таких факторів і обставин [3].

Так, при розробці систем захисту інформації важливо враховувати всі параметри уразливості інформації, потенційно можливі загрози її безпеці та охоплювати всі необхідні об'єкти захисту. Також важливо використовувати всі можливі види, методи і засоби захисту, а також мати достатні кадрові ресурси для ефективної реалізації заходів з захисту [3].

По-третє, при комплексному підході до захисту інформації важливо захищати всі носії інформації, у всіх місцях її збирання, зберігання, передачі і використання, незалежно від умов та режимів функціонування систем обробки інформації. Такий підхід дозволяє забезпечити безпеку інформації в широкому спектрі ситуацій та в усіх етапах її обробки [3].

Диференційований підхід до захисту інформації передбачає врахування різних аспектів, таких як види таємниць, ступінь конфіденційності, технічні характеристики систем зберігання та обробки даних, умови виявлення вразливостей, а також методи та канали несанкціонованого доступу. Комплексність підходу передбачає, що ці варіабельні аспекти не вилучаються, але, навпаки, враховуються для ефективного забезпечення безпеки інформації [3].

Таким чином, важливість комплексного підходу до захисту інформації визначається наступним:

* об'єднанням локальних систем захисту;
* забезпеченням повноти всіх компонентів системи захисту;
* забезпеченням всебічного захисту інформації [3].

Забезпечення контролю над функціонуванням системи захисту включає в себе створення засобів і методів для відстеження та контролю над працездатністю захисних механізмів [1].

Забезпечення економічної доцільності використання системи захисту означає, що вартість розробки та експлуатації системи інформаційної безпеки (СІБ) має перевищувати можливі збитки, які ІС і ІТ можуть понести в результаті реалізації загроз [1].

## **Розробка політики безпеки**

Перш ніж вносити конкретні пропозиції щодо організації системи захисту інформації, необхідно розробити політику безпеки. Політика безпеки представляє собою набір законів, правил і практичних рекомендацій, які формують управління, захист і розподіл критичної інформації в системі. Вона охоплює всі аспекти обробки інформації та визначає поведінку системи в різних ситуаціях. Реалізація політики безпеки включає організаційні заходи та програмно-технічні засоби, які визначають архітектуру системи захисту, а також використання засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, враховуючи конкретну технологію обробки інформації, використовувані програмні і технічні засоби, розташування організації і інші фактори [3].

Політика безпеки ґрунтується на механізмі керування доступом, який визначає правила доступу суб'єктів системи до об'єктів системи [3]. Управління доступом є методом захисту інформації, що регулює доступ до всіх ресурсів інформаційних систем і технологій [1].

Розмежування і зниження повноважень щодо доступу до оброблюваної інформації і процедур оброблення полягає у встановленні обмежень для користувачів і співробітників інформаційної системи (ІС), щоб надавати їм лише необхідні повноваження для виконання своїх службових обов'язків [1].

Забезпечення повноцінного контролю і реєстрації спроб несанкціонованого доступу передбачає необхідність точного визначення ідентифікації кожного користувача і фіксацію його дій з метою можливого подальшого розслідування. Крім того, будь-яка операція з обробки інформації в інформаційних технологіях не може здійснюватися без попередньої реєстрації цієї операції[1].

Існує набір вимог, спрямованих на управління інформаційними потоками в системі. Важливо зауважити, що заходи безпеки, спрямовані на впровадження будь-якого з названих методів управління доступом, лише надають можливості для надійного контролю за доступом інформаційними потоками [3].

В основі вибіркової політики безпеки лежить вибіркове керування доступом, що передбачає:

* ідентифікацію всіх суб'єктів і об'єктів системи;
* визначення прав доступу суб'єкта до об'єкта системи на підставі певного правила (властивість вибірковості) [3].

Для характеризації властивостей вибіркового керування доступом застосовується матрична модель системи, відома як матриця доступу або матриця контролю доступу. Ця модель представляє собою прямокутну матрицю, де кожному об'єкту системи відповідає рядок, а кожному суб'єкту — стовпець. У кожній комірці матриці зазначається тип дозволеного доступу суб'єкта до об'єкта, який зазвичай включає "доступ на читання", "доступ на запис", "доступ на виконання" та інші [3].

Матриця доступу визначає і контролює різноманітні об'єкти та типи доступу суб'єкта, які можуть змінюватися згідно з правилами, що існують у даній системі. Вона включає в себе завдання визначення та модифікації цих правил [3].

Рішення щодо доступу суб'єкта до об'єкта визначається відповідно до типу доступу, вказаного у відповідній клітинці матриці доступу. Зазвичай вибіркове управління доступом реалізує принцип "що не дозволено, то заборонено", що передбачає явний дозвіл на доступ суб'єкта до об'єкта. Матриця доступу представляє собою найбільш простий підхід до моделювання системи доступу [3].

Управління доступом включає такі функції захисту:

* визначення користувачів, персоналу і ресурсів системи шляхом присвоєння кожному об'єкту персонального ідентифікатора;
* визначення достовірності об'єкта або суб'єкта на підставі пред'явленого ідентифікатора;
* перевірка повноважень, що включає в себе перевірку відповідності дня тижня, часу доби запитуваних ресурсів і процедур в межах встановленого регламенту;
* надання дозволів та створення умов для роботи в межах встановленого регламенту;
* реєстрація доступу до конфіденційних ресурсів;
* реагування на спроби несанкціонованих дій, включаючи сигналізацію, відключення, затримку робіт і відмову у запиті [1].

Вибіркова політика безпеки широко використовується в комерційному секторі, оскільки її реалізація відповідає вимогам комерційних організацій щодо розмежування доступу та підзвітності. Крім того, ця політика має прийнятну вартість і невеликі накладні витрати [3].

Основу повноважної політики безпеки становить система повноважень управління доступом, враховуючи такі аспекти:

* всі суб'єкти і об'єкти системи повинні бути чітко ідентифіковані;
* кожному об'єкту системи привласнюється мітка критичності, що визначає цінність, яка зберігається в ньому;
* кожному суб'єкту системи присвоюється рівень прозорості, який визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ [3].

Коли всі мітки в системі мають однакові значення, вважають що вони належать до одного рівня безпеки. Система міток організована за ієрархічною структурою, де рівень критичності визначає важливість об'єкта чи суб'єкта. Це дозволяє реалізувати ієрархічний потік інформації в системі, наприклад, від рядових виконавців до керівництва. Об'єкти та суб'єкти з вищими значеннями міток критичності є найбільш захищеними в системі [3].

У кожного суб'єкта, окрім рівня прозорості, є поточне значення рівня безпеки, яке може змінюватися від певного мінімального значення до рівня прозорості, визначеного для нього [3].

Основна мета повноважної політики безпеки полягає у регулюванні доступу суб'єктів системи до об'єктів з різним рівнем критичності та у запобіганні витоку інформації від верхніх рівнів посадової ієрархії до нижніх. Вона також має завдання блокувати можливі спроби проникнення з нижніх рівнів в верхні. При цьому повноважна політика безпеки функціонує в рамках виборчої політики, дотримуючись її вимог та ієрархічно упорядкованого характеру (відповідно до рівнів безпеки) [3].

## **Методи захисту інформації**

Всі заходи, спрямовані на протидію комп’ютерним злочинам та забезпечення безпеки інформації, можна розділити на такі групи:

* правові;
* організаційно-адміністративні;
* інженерно-технічні [2].

Правові методи передбачають розроблення комплексу нормативно-правових актів і положень, які регламентують відносини в сфері інформації в суспільстві. Вони також включають в себе створення керівних і нормативно-методичних документів, спрямованих на гарантування інформаційної безпеки [1].

Законодавче забезпечення захисту інформації включає в себе ряд законів та підзаконних актів, які охоплюють різні галузі права, такі як кримінальне, цивільне, адміністративне та інші [4].

В Україні правові механізми захисту різних видів інформації закріплені в таких нормативних актах, як:

* + 1. Конституція України від 28.06.1996.
    2. Цивільний кодекс України від 16.01.2003.
    3. Кримінальний кодекс України від 05.04.2001.
    4. Кримінальний процесуальний кодекс України від 13.04.2012.
    5. Кодекс адміністративного судочинства від 06.07.2005.
    6. Закон України «Про захист персональних даних» від 01.06.2010.
    7. Закон України «Про оперативно-розшукову діяльність» від 18.02.1992.
    8. Закон України «Про Національну поліцію» від 02.07.2015.
    9. Закон України «Про інформацію» від 02.10.1992.
    10. Закон України «Про державну таємницю» від 21.01.1994.
    11. Закон України «Про національну безпеку України» від 21.06.2018.
    12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994.
    13. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017.
    14. Доктрина інформаційної безпеки, затверджена Указом Президента України від 25.02.2017 № 47/2017.
    15. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373.
    16. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету Міністрів України від 19.10.2016 № 736.
    17. Інші нормативно-правові акти, що містять окремі питання захисту інформації [4].

На Рисунку 1.2 зображено складові правового забезпечення безпеки інформації.

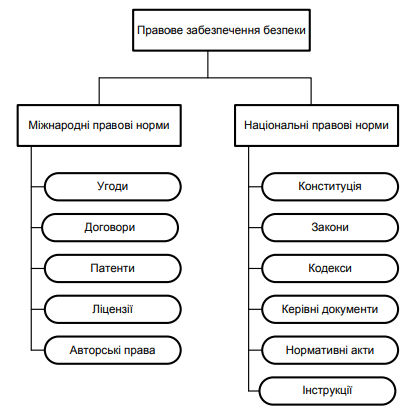
****

Рисунок 1.2 - Правове забезпечення безпеки інформації

Крім нормативних актів на рівні законів і підзаконних нормативів, внутрішнє правове забезпечення системи захисту інформації включає також внутрішні нормативно-організаційні документи, такі як накази та розпорядження, інструкції, зокрема посадові, положення, договори, пам'ятки, протоколи і інші [4].

Останніми роками в Україні спостерігається наростання зацікавленості у вирішенні проблем правової боротьби з комп'ютерними злочинами. Вітчизняне законодавство також зазнало змін, орієнтованих на протидію комп'ютерній злочинності [2].

Інженерно-технічні методи представляють собою набір засобів, які включають в себе:

* заходи для запобігання витоку інформації;
* механізми для усунення можливості несанкціонованого доступу до інформації;
* заходи для запобігання впливам, які можуть призвести до знищення або руйнування інформації, а також до збоїв або відмов у функціонуванні інформаційних засобів;
* системи для виявлення вмонтованих пристроїв або апаратних модифікацій;
* заходи для запобігання перехопленню інформації за допомогою технічних засобів;
* використання криптографічних засобів захисту інформації під час передачі через канали зв'язку [1].

На Рисунку 1.3 наведено складові інженерно-технічного забезпечення безпеки.

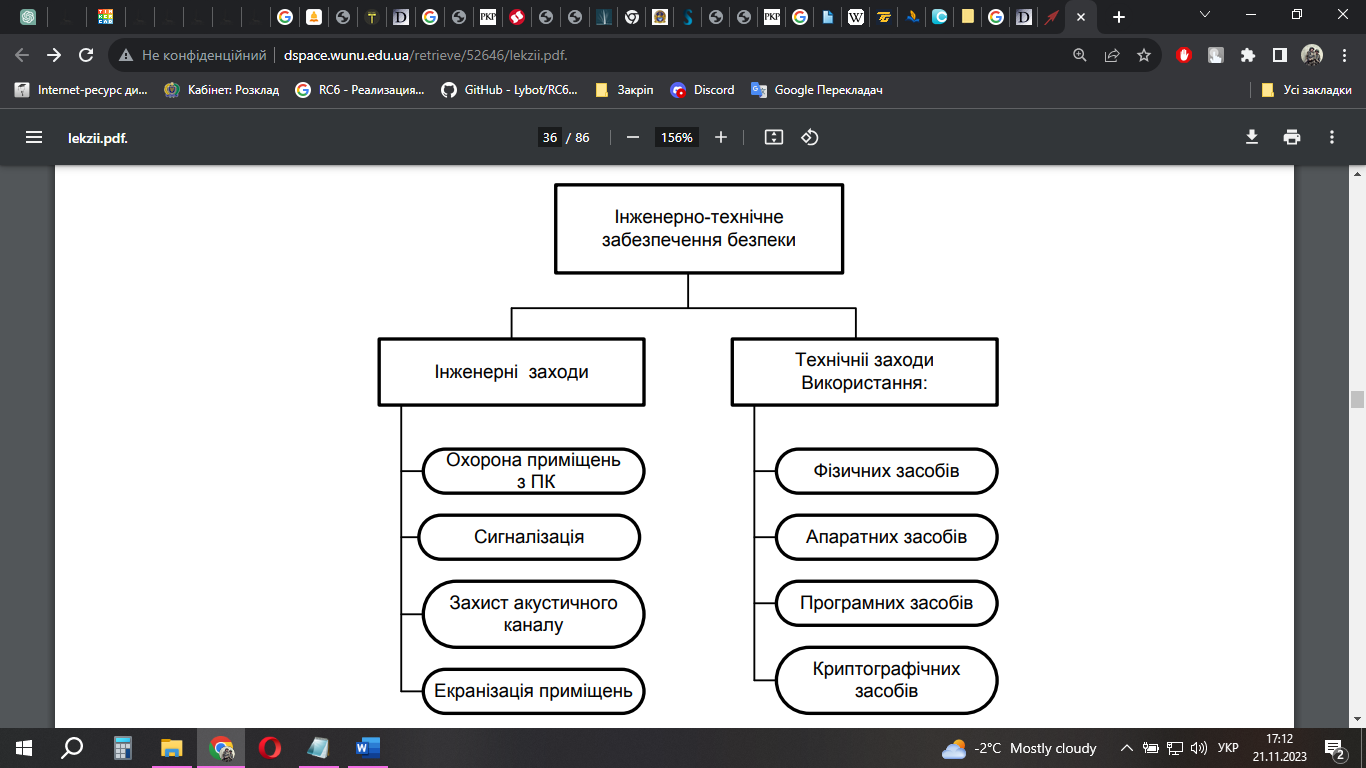


Рисунок 1.3 – Основні інженерно-технічні заходи захисту інформації

Організаційні заходи включають розробку концепції інформаційної безпеки та також враховують наступні аспекти:

* підготовка посадових інструкцій для користувачів та обслуговувального персоналу;
* створення правил адміністрування компонентів інформаційної системи, включаючи облік, зберігання, розмноження, та знищення носіїв інформації, а також ідентифікацію користувачів;
* розробка планів дій у випадку виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, відмови засобів захисту або виникнення надзвичайної ситуації;
* проведення навчань користувачів щодо правил інформаційної безпеки [3].

При необхідності може бути введена служба інформаційної безпеки, створений режимно-пропускний відділ, а також проведена реорганізація системи діловодства та зберігання документів в рамках організаційних заходів [3].

На Рисунку 1.4 зображено організаційно-адміністративні заходи захисту інформації.

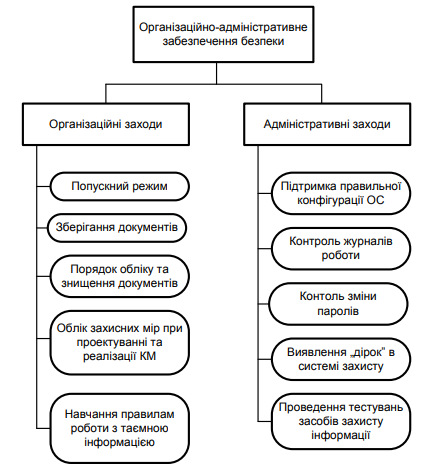
****

Рисунок 1.4 - Організаційно-адміністративні заходи захисту інформації

Запобігання інформаційним загрозам вимагає уваги до мотивації, економічних стимулів і психологічної підтримки персоналу, який забезпечує інформаційну безпеку [1].

## **Шифрування інформації**

Шифрування є ключовим методом криптографічного захисту інформації, призначеним для забезпечення її конфіденційності [5].

Процес шифрування інформації полягає в перетворенні відкритих даних у зашифровану форму і навпаки. Перша частина цього процесу називається шифруванням, а друга – розшифруванням. Алгоритми шифрування можна поділити на дві основні категорії: алгоритми симетричного шифрування та алгоритми асиметричного шифрування [5].

Симетричне шифрування використовує один і той самий ключ для обох операцій – шифрування та розшифрування. Однак ключ для розшифрування може легко отримати з ключа для шифрування і навпаки. Симетричне шифрування існує у двох формах – блоковому та потоковому. В разі блокового шифрування інформація розбивається на блоки з певною фіксованою довжиною та обробляється послідовно. Ці блоки можуть бути шифровані незалежно один від одного або в залежності від значення або результату шифрування попереднього блоку. Алгоритми потокового шифрування діють на дані на рівні окремих бітів або символів, і тому в певних класифікаціях це також описується як шифрування блоків з фіксованою довжиною [5].

У випадку асиметричного шифрування використовуються два ключі: відкритий для шифрування даних та секретний для розшифрування. Ці ключі взаємозв'язані таким чином, що можна отримати відкритий ключ з секретного, але навпаки це практично неможливо зробити за обмеженого часу і ресурсів. На Рисунку 1.5 показано принцип дії асиметричного шифрування. На першому етапі користувач 2 шифрує повідомлення за допомогою відкритого ключа, отриманого від користувача 1. На другому етапі користувач 1 розшифровує зашифроване повідомлення за допомогою свого секретного ключа [5].

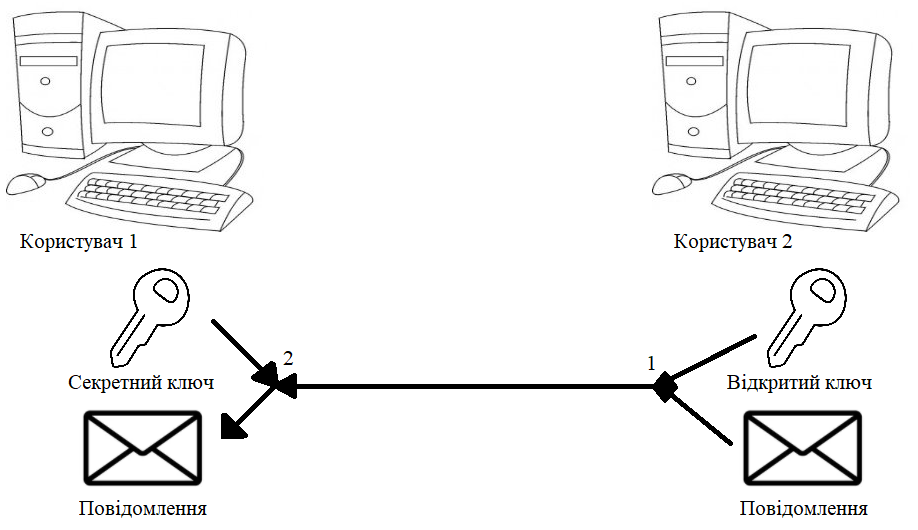


Рисунок 1.5 – Принцип дії асиметричного шифрування

## **Формування вимог до програмного продукту**

Метою цієї роботи є розробка програмного продукту, призначеного для шифрування та розшифрування файлів, а також для проведення тестування з метою виявлення можливих вразливостей та помилок. Крім того, в рамках цього проекту передбачено реалізацію системи авторизації з метою забезпечення конфіденційності інформації на підприємстві. Ідентифікація, доступ та розподіл рівнів доступу до даних забезпечується використанням FTP-сервера FileZilla Server.

## **Функціональні вимоги.** Функціональними вимогами до програмного продукту є:

* можливість шифрувати та розшифровувати файли за допомогою секретного ключа;
* наявність модулю авторизації для запобігання несанкціонованого доступу до інформації;
* можливість збереження файлів у встановлених для кожного зареєстрованого користувача директоріях;
* можливість завантаження, збереження та видалення файлів з серверу;
* зміна рівнів доступу для зареєстрованих користувачів.

## **Нефункціональні вимоги.** Нефункціональними вимогами до програмного продукту є:

* апаратні та програмні вимоги - процесор Pentium 4 або кращий з тактовою частотою ЦП від 1,3 ГГц та підтримкою SSE3, 512 Мб RAM та 350 Мб на жорсткому диску;
* вимоги безпеки – програмний продукт має забезпечувати високий рівень конфіденційності інформації завдяки використанню криптографічного алгоритму шифрування даних, доступ до інформації має бути обмежений числом людей, які мають дозвіл на опрацювання даної інформації;
* вимоги продуктивності – програмний продукт має бути оптимізований для роботи з обмеженими апаратними ресурсами, робота з шифруванням та розшифруванням інформації не має займати дуже багато часу.

# **POЗДIЛ 2 ОРГАНІЗАЦІЯ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМТСВІ**

# **Історія підприємства**

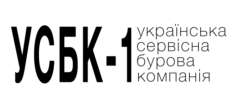


Рисунок 2.1 – Логотип компанії

Приватне підприємство «Українська сервісна бурова компанія-1» було засноване в 2009 році. З травня 2009 року по серпень 2012 року компанія здійснювала поставки нафтогазового обладнання, а з вересня 2012 року розпочала новий вид діяльності, а саме капітальний ремонт і буріння нафтогазових свердловин [6].

Першим досвідом була свердловина Карайкозовского нафтового, газового та газоконденсатного родовища №21, на якій проводився плановий капітальний ремонт свердловини в 2012 р для ТОВ “Еско-Північ” [6].

Свою діяльність як сервісна компанія УСБК-1 почала з використанням орендованої мобільної бурової установки Salzgitter EA-620 виробництва Німеччини. МБУ ЕА-620 з дизельним приводом призначена для виконання повного обсягу технологічних операцій при бурінні, освоєнні і ремонті нафтових і газових свердловин [6].

Після цього компанія придбала мобільну бурову установку ZJ-30 (Китай) вантажопідйомністю 160 т. За 5 років діяльності компанія розширювалася і тепер має в наявності 5 мобільних бурових установок, готових до виконання робіт. У 2016 році компанія придбала мобільну бурову установку ZJ40 вантажопідйомністю вже 225 т [6].

Наймасштабнішим проектом у виконанні УСБК-1 було буріння похило-спрямованої свердловини глибиною 3380 м (свердловина Васищевського газоконденсатного родовища №5) в 2014-2015 роках [6].

На Рисунку 2.1 наведено логотип підприємства. На Рисунку 2.2 зображено карту розташування свердловин, на яких підприємством виконувалися ремонті роботи.

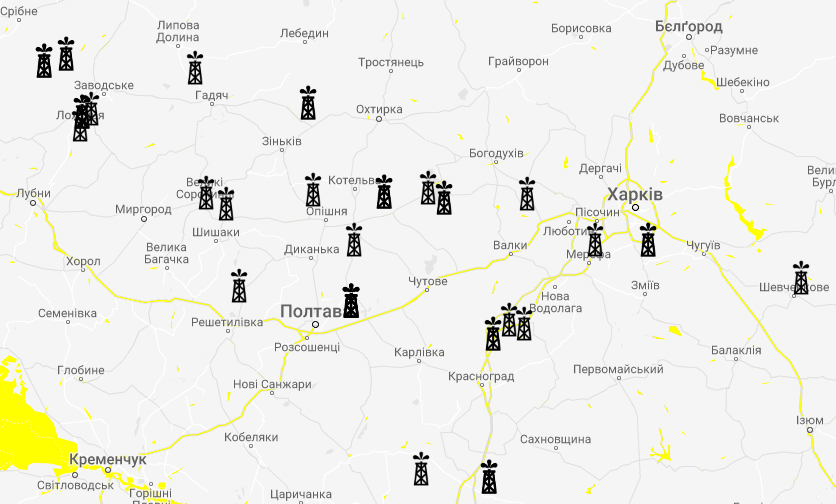


Рисунок 2.2 – Карта свердловин, на яких виконувалися ремонті роботи

# **Опис діяльності**

У 2023 році підприємство здійснює діяльність за такими напрямами:

* надання допоміжних послуг у сфері добування нафти та природного разу, а саме капітальний/підземний ремонт свердловин, спорудження/будівництво свердловин, їх ліквідація, сервісні послуги по інженерному супроводу гвинтових вибійних двигунів;
* оптова торгівля машинами та устаткуванням для добувної промисловості та будівництва;
* надання в оренду інших машин, устаткування та товарів, а саме оренда гвинтових вибійних двигунів, бурильних труб, аварійного та ловильного обладнання та іншого обладнання для нафтогазовидобувної галузі;
* ремонт та технічне обслуговування машин і устаткування промислового призначення, а саме ремонт бурильних труб, бурильних установок, гвинтових вибійних двигунів та іншого обладнання для нафтогазовидобувної галузі;
* будівництво трубопроводів, а саме будівництво артезіанської свердловини, буріння та кріплення водних свердловин, капітальний ремонт артезіанських свердловин [7].

Для здійснення виробничої діяльності підприємство має наступні виробничі потужності:

* мобільна бурова установка ZJ-40 (виробництво КНР);
* мобільна бурова установка ZJ-30 (виробництво КНР);
* парк гвинтових вибійних двигунів та гідравлічних ударних механізмів зворотної дії;
* насоси різної потужності;
* очисні системи, противикидне обладнання, енергетичне обладнання тощо;
* вахтові містечка;
* автомобільний та спеціалізований транспорт (насосні агрегати, трактори, автоцистерни, бульдозери, тягачі, оперативний та вахтовий транспорт);
* бурильний інструмент;
* ловильний та аварійний інструмент;
* база виробничого обслуговування [7].

Крім того, на основі довготривалих договорів оренди додатково використовуються:

* мобільна бурова установка ZJ-30 (виробництво КНР, 2 одиниці);
* мобільна бурова установка ZJ-20 (виробництво КНР);
* агрегат для ремонту та освоєння свердловин АОРС-80(2 одиниці);
* буровий верстат 1БА15В [7].

Для здійснення підприємницької діяльності підприємство має наступні дозвільні документи:

* дозволи на експлуатацію машин, механізмів, устаткування підвищеної небезпеки;
* дозволи виконувати роботи підвищеної небезпеки [7].

Основним видом діяльності підприємства є капітальний ремонт свердловин, який здійснюється бригадами капітального ремонту свердловин (КРС) з використанням мобільних бурових установок та іншого супутнього обладнання. Нині працює 7 таких бригад, одна з них виконує роботи з будівництва, капітального ремонту та ліквідації артезіанських/водних свердловин [7].

Для забезпечення виконання робіт була створена база виробничого обслуговування та будівельно-монтажна дільниця [7].

База виробничого обслуговування має в своєму складі укомплектовані у відповідно до вимог основного виробництва наступні підрозділи:

* дільниця по ремонту та обслуговуванню противикидного обладнання;
* дільниця по ремонту та обслуговуванню бурового обладнання;
* автотранспортний цех;
* трубо-інструментальний майданчик;
* дільниця по ремонту труб і вибійних двигунів;
* енергоцех [7].

# **Організаційна структура**

Організаційна структура підприємства є гнучкою та змінюється для досягнення максимального фінансово-економічного результату. Відобразимо її за допомогою редактора діаграм з пакету Microsoft Office – Microsoft Visio Professional 2019. Відображення наведено на Рисунку 2.3.

Зазначимо, що база виробничого обслуговування та її підструктури як прокатно-ремонтний цех бурового обладнання, автотранспортний цех, трубно-інструментальний майданчик, дільниця по ремонту труб і відбійних двигунів, енергоцех, склад та будівельно-монтажна дільниця знаходяться поза межами офісу в іншому місці, як і бригади КРС. Тому на плані офісного центру вони не відображатимуться.

У офісі працює 45 осіб, включаючи директора, його секретаря у приймальному приміщенні, заступника директора з питань безпеки, головного інженера, головного інженера з будівництва, заступника головного інженера, головного енергетика, заступника директора з виробництва, технологічний відділ з двох фахівців, начальника технологічного відділу, начальника бази виробничого обслуговування, головного механіка, заступника директора з охорони праці, начальника відділу охорони праці, відділ охорони праці з двох фахівців, виробничо-технічний відділ з двох фахівців, начальника будівельно-монтажної дільниці, начальника відділу матеріально-технічного постачання, відділ матеріально-технічного постачання з двох фахівців, головного економіста, начальника відділу кадрів, відділ кадрів з трьох фахівців, економіста, начальника юридичного відділу, юридичний відділ з двох фахівців, співробітника відділу безпеки, що відповідає за відеоспостереження, охоронця на пункті охорони, фахівця для підтримання працездатності мережі, відділ безпеки з двох фахівців, начальника відділу безпеки, головного бухгалтера, бухгалтерії з трьох фахівців, начальника відділу тендерних закупівель та конкурсних торгів, менеджера з зовнішньоекономічної діяльності та відділу тендерних закупівель та конкурсних торгів, що складається з двох фахівців.

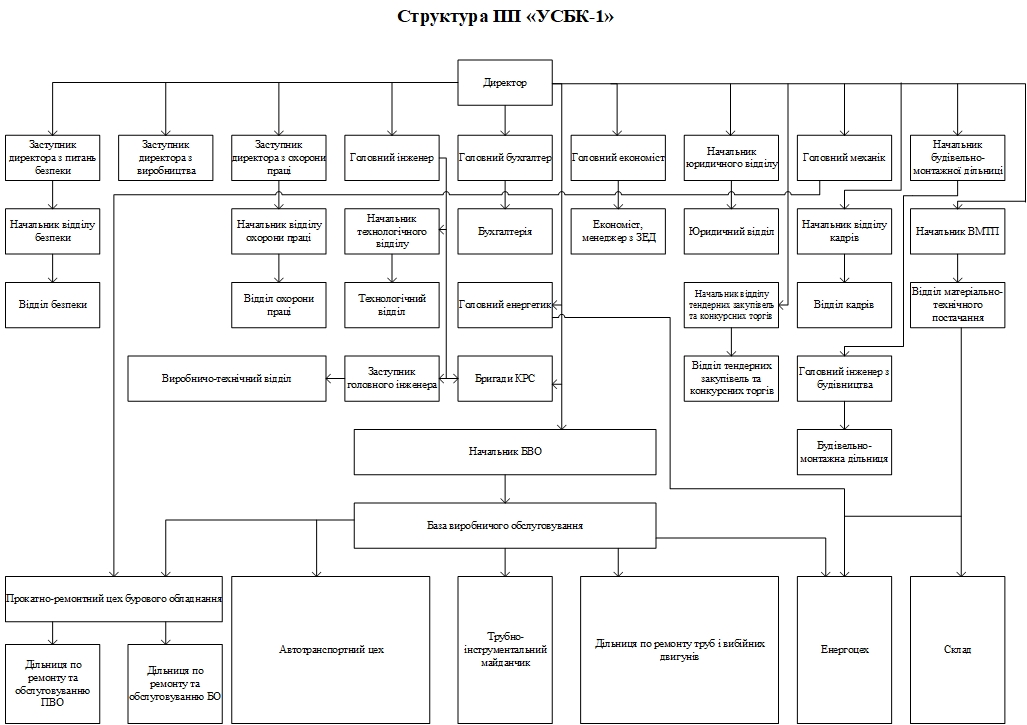


Рисунок 2.3 – Організаційна структура підприємства

# **Варіанти інженерно-технічних заходів захисту інформації**

Відділ безпеки підприємства є самостійним структурним підрозділом, призначеним для вирішення завдань прямого забезпечення захисту життєво-важливих інтересів підприємства в умовах комерційного та підприємницького ризику та конкурентної боротьби [1].

Головною метою функціонування відділу безпеки є запобігання ризикам, таким як розголошення, проникнення інформації та несанкціонований доступ до конфіденційної інформації; втратам фінансових і матеріально-технічних ресурсів, а також знищенню майна та цінностей; порушенням роботи технічних засобів, включаючи системи інформатизації [1].

Розглянемо більш детально аспект захисту інформації, а саме зосередимо увагу на інженерно-технічних заходах.

Інженерно-технічні заходи забезпечення безпеки інформації включають в себе різноманітні механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, які призначені для унеможливлення несанкціонованого доступу, викрадення інформації, а також запобігання втратам у результаті різних негативних впливів, таких як порушення роботоздатності компонентів ІС, природні катастрофи, саботаж, диверсії і т. д [2].

До цієї групи належать:

1. Засоби захисту кабельної системи: Дослідження свідчать, що більше половини відмов в локальних обчислювальних мережах виникають через несправності кабельних систем. Ефективним способом запобігання таким ситуаціям є побудова структурованої кабельної системи (СКС). В рамках СКС використовуються однакові кабелі для передавання даних в інформаційні системи, сигналів від датчиків пожежної безпеки, відеоінформації від охоронних систем і локальної телефонної мережі. Поняття "структурованість" передбачає розділення кабельної системи будинку на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС рекомендується дотримуватися міжнародних стандартів.
2. Засоби захисту системи електроживлення. Вони грають важливу роль у запобіганні втрат інформації внаслідок тимчасових вимкнень електроенергії або стрибків напруги в електромережі. Встановлення джерел безперебійного живлення є найбільш надійним способом. Різноманітні технічні та експлуатаційні характеристики дозволяють вибрати відповідний засіб, який відповідає конкретним вимогам. У випадках, коли роботоздатність інформаційних систем вимагає підвищених стандартів, можна використовувати аварійні електрогенератори або резервні лінії електроживлення, підключені до різних підстанцій.
3. Засоби архівації та дублювання інформації. Вони виявляються доречними в умовах великих обсягів даних. Рекомендується встановлення спеціалізованого сервера для ефективної архівації інформації. Якщо архівна інформація є важливою, розглядається можливість зберігання її в спеціально обладнаному приміщенні, яке забезпечується системами безпеки. З метою захисту від пожежі або стихійних лих рекомендується створення дублікатів найцінніших архівів та їх зберігання в іншому будинку, можливо, в іншому районі або навіть в іншому місті.
4. Засоби захисту від відпливу інформації, яка може виникати внаслідок фізичних полів, створених технічними засобами, включають в себе засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування за допомогою широкосмугових генераторів шумів і інші технічні заходи [2].

До цієї самої категорії можна віднести матеріали, які забезпечують безпеку зберігання та транспортування носіїв інформації, а також захищають їх від незаконного копіювання. Головним чином це спеціальні тонкоплівкові матеріали зі змінною кольоровою гамою або голографічні мітки, які наносяться на документи та об'єкти, включаючи елементи комп'ютерної техніки. Ці матеріали дозволяють ідентифікувати автентичність об'єкта та контролювати доступ до нього [2].

Як вже було висловлено, зазвичай заходи технічного захисту використовуються спільно з програмними заходами [2].

Програмні засоби захисту виконують завдання ідентифікації та аутентифікації користувачів, управління доступом до ресурсів відповідно до їх повноважень, реєстрацію подій в інформаційній системі, застосування криптографічних методів для захисту інформації, а також запобігання впливу комп'ютерних вірусів та інших загроз [2].

Фізичні засоби захисту представляють собою різноманітні пристрої, пристосування, конструкції та апарати, які спроектовані для утруднення руху потенційних зловмисників [8].

До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні, а також інші пристрої, які призначені для запобігання несанкціонованому доступу (входу, виходу), передачі (вивезення) засобів і матеріалів та інших можливих форм злочинної діяльності [8].

Ці засоби використовуються для вирішення різних завдань:

* захист території підприємства та проведення спостереження за нею;
* охорона будівель, внутрішніх приміщень та контроль над ними;
* захист устаткування, продукції, фінансів та інформації;
* забезпечення контрольованого доступу до будівель та приміщень [8].

До засобів фізичного захисту входять:

1. Природні і штучні бар'єри, призначені для запобігання незаконному проникненню на територію об'єкта. Однак основний захисний фактор зазвичай лежить на штучних бар'єрах, таких як паркани та інші види огороджень. Практика свідчить, що огородження складної конфігурації можуть значно затримати зловмисника на тривалий час. На сьогодні існує значний вибір таких засобів, від простих сітчастих до складних комбінованих огороджень, які в певній мірі відлякують потенційного порушника.
2. Особливі конструкції, такі як периметри, проходи, віконні і дверні плетіння, а також оснащення приміщень, сейфів, сховищ тощо є обов'язковими для будь-яких організацій і підприємств з точки зору безпеки. Ці конструкції мають витримувати будь-які фізичні впливи, зокрема механічні деформації, руйнування свердлінням, термічне і механічне різання, вибухи та інші методи, які можуть бути використані зловмисниками. Крім того, вони повинні запобігати несанкціонованому доступу, такому як підробка ключів чи вгадування коду. Замки виступають одним з основних технічних засобів захисту проходів, приміщень, сейфів і сховищ. Вони можуть бути простими (з ключами), кодовими (включаючи в себе ті, що працюють зі затримкою часу на відкривання) або оснащеними програмними пристроями, які відкривають двері і сейфи тільки у певні години.
3. Зони безпеки на об'єкті повинні бути розташовані послідовно, починаючи від паркана навколо території об'єкта і закінчуючи сховищами цінностей. Такий ланцюг перешкод або рубежів створює послідовні зони, які зловмисникові доведеться подолати. Складніше і більш надійно перешкода на шляху зловмисника вимагатиме більше часу для подолання кожної зони, і це збільшує ймовірність виявлення порушника, оскільки в кожній зоні розташовані засоби виявлення, такі як охоронні пости, охоронна сигналізація і відеоспостереження. У випадку виявлення порушення буде подано сигнал тривоги [8].

Всі фізичні засоби захисту об'єктів розділяються на три основні категорії:

* засоби попередження (наприклад, грати та посилені двері);
* засоби виявлення (такі як сигналізація та охоронне телебачення);
* системи ліквідації загроз (включаючи засоби пожежогасіння) [8].

# **Опис наявних засобів захисту інформації**

Опишемо інженерно-технічні заходи захисту, присутні на підприємстві.

Приміщення, в якому знаходиться офіс підприємства, розташований за адресою вулиця Зигіна, будинок 29. На Рисунку 2.4 зображено мапу з відміткою місця знаходження.



Рисунок 2.4 – Місце знаходження офісного приміщення

Підприємство орендує перші два поверхи, і як можна побачити на Рисунку 2.5, перший та цокольний поверхи будівлі обладнані гратами на вікнах. Всі двері всередині приміщення обладнані замками для захисту від доступу всередину кабінетів сторонніх осіб, що зображено на Рисунку 2.6.

Як бачимо на Рисунку 2.7, на першому поверсі приміщення знаходиться охоронний пункт, який забезпечує ідентифікацію осіб, які потрапляють всередину. Також для забезпечення пожежної безпеки у охоронця знаходиться вогнегасник. У кімнаті з відчиненими дверями знаходиться пункт відеоспостереження, в якому на моніторах транслюється запис з камер. Камери знаходяться у коридорах і відповідно на кожному поверсі є дві камери.

Говорячи про програмні заходи захисту, на персональних комп’ютерах не встановлені паролі для доступу до операційної системи, але деякі програмні продукти обладнані обліковим записом, та для їх запуску необхідно ввести пароль. Також для захисту від комп’ютерних вірусів встановлено антивірусний захист.



Рисунок 2.5 – Зовнішній вигляд будівлі



Рисунок 2.6 – Двері обладнані замками



Рисунок 2.7 – Перший поверх офісного приміщення

На Рисунках 2.8 та 2.9 зображено план першого та другого поверхів офісного центру, на яких функціонують структурні підрозділи підприємства. Він містить кабінети і кімнати, в яких є робочі місця, їх підписи, сходи та загальні розміри будівлі. На плані також відображено елементи наявного захисту, такі як грати на вікнах першого поверху та камери відеоспостереження. Рекомендовані елементи, які пропонуються до встановлення, зображені червоним кольором. Планування виконано за допомогою редактора діаграм з пакету Microsoft Office – Microsoft Visio Professional 2019.

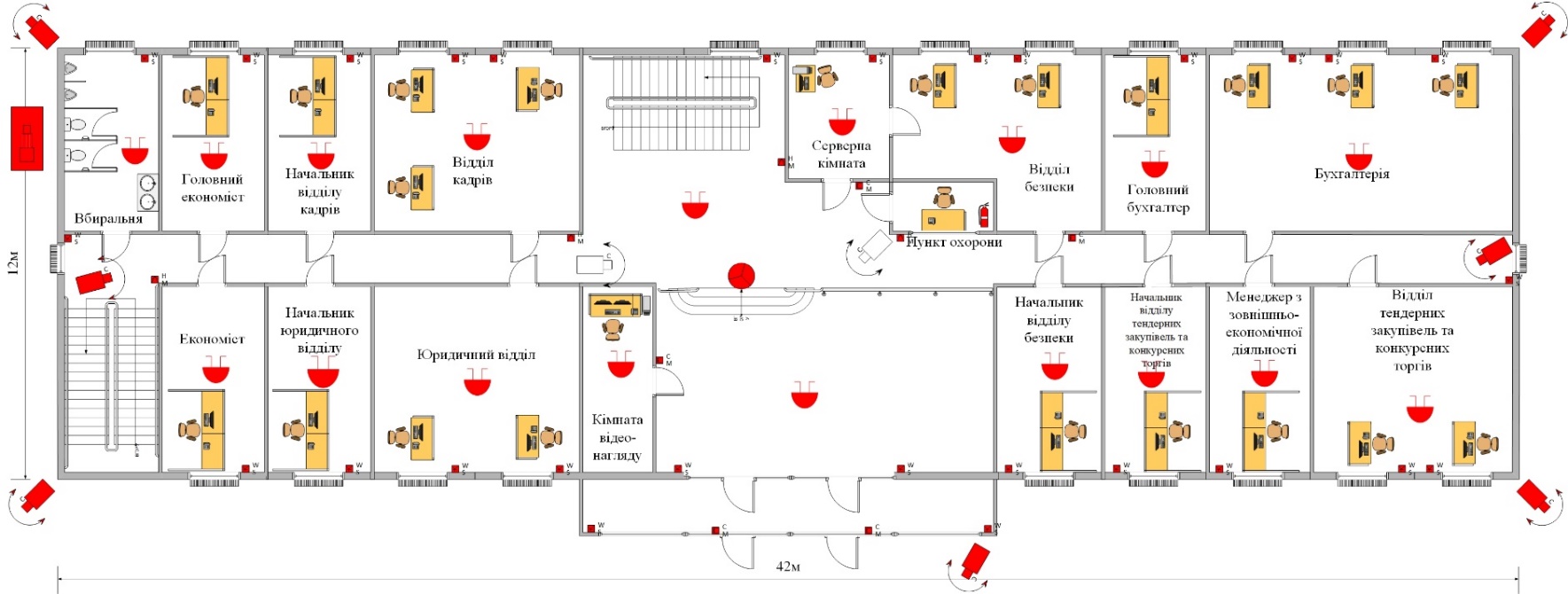


Рисунок 2.8 – План першого поверху офісного центру

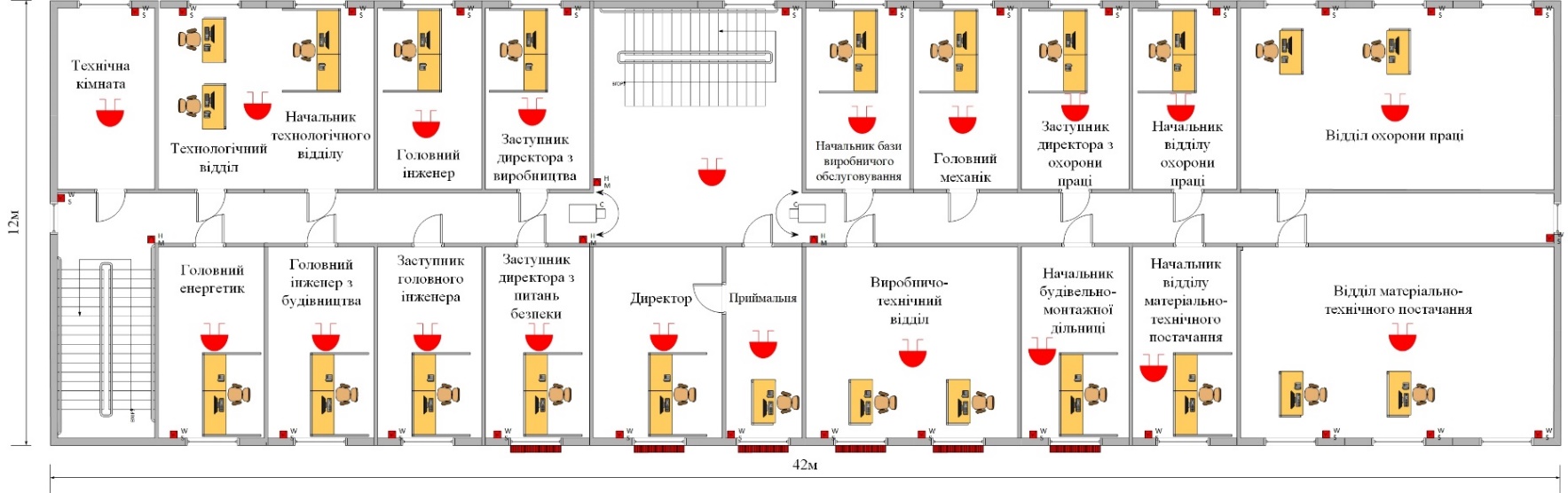


Рисунок 2.9 – План другого поверху офісного центру

# **Рекомендації щодо покращення рівня захисту інформації**

Опишемо процес покращення рівня захисту інформації шляхом рекомендацій щодо певних так званих етапів захисту.

Першим етапом буде захист прилеглої до підприємства території. Як можна побачити на Рисунку 2.10, будівля ніяким чином не обмежена від доступу на її прилеглу територію сторонніх осіб. Але встановлення огорожі буде означати необхідність додаткового встановлення зовнішнього пропускного пункту з турнікетом, що збільшить фінансові витрати на покращення рівня захисту. Тому пропонується встановити камери спостереження ззовні будівлі безпосередньо біля входу та на кутах будівлі, щоб контролювати ситуацію навколо по всьому периметру.



Рисунок 2.10 – Вигляд прилеглої території

Наступним етапом буде забезпечення достатнього рівня безпеки в межах офісного центру. Почнемо з пропозиції додаткового встановлення камер на першому поверсі біля бокових вікон, щоб покращити контроль над переміщенням осіб у віддалених областях будівлі. Також пропонується встановити грати на другому поверсі над входом на шість вікон, оскільки зловмисники можуть потрапити всередину через дах входу. Варто зазначити, що вікна, які знаходяться в зоні небезпеки є вікнами кабінетів директора, приймальної кімнати, заступника директора з питань безпеки та виробничо-технічного відділу, тому в них може зберігатися важлива інформація, що потребує захисту.

Також рекомендовано встановити охоронну сигналізацію з акустичними, магнітоконтактними оповіщувачами та датчиками руху, що будуть реагувати на звуки, несанкціоноване відчинення дверей та знаходження в приміщенні сторонніх осіб в час, коли сигналізацію активовано. У разі виявлення порушення система буде надсилати сповіщення та за допомогою звукових сигналів повідомляти про наявність порушника.

Небезпеку можуть становити не лише люди, а й стихійні лиха, тому наступною рекомендацією буде встановлення системи автоматичного пожежогасіння. Її основними завданнями є:

* виявлення та припинення займання;
* запобігання подальшому розповсюдженню пожежі;
* захист людей і матеріальних цінностей від небезпеки пожежі.

Наступним кроком є встановлення турнікету на першому поверсі. Працівники будуть забезпечені картками, які містять інформацію про них, і під час проходження через турнікет буде відбуватися фіксація, хто і коли відвідував будівлю. Це рішення унеможливить несанкціонований доступ сторонніх осіб і підвищить загальний рівень безпеки. З цього кроку випливає наступний – підвищити рівень безпеки охоронної кімнати. Оскільки вхід до кімнати відеоспостереження знаходиться одразу біля входу в приміщення, пропонується перенести його за турнікет. Також розглядається варіант заміни дверей кімнати відеоспостереження та серверної кімнати на міцніші, щоб забезпечити належний рівень безпеки даних приміщень.

Беручи до уваги військово-політичну ситуацію, що склалася навколо нашої країни, пропонується забезпечити офіс підприємства безперебійними джерелами живлення та генератором, що дозволить продовжити роботу навіть у випадку аварійних відключень електроенергії.

Тепер поговоримо про забезпечення захисту інформаційної системи.

Зловмисні загрози є одним з основних видів потенційних небезпек для цілісності, конфіденційності та працездатності інформаційної системи (ІС). Ці загрози виникають внаслідок умисного планування заздалегідь, спрямованого на завдання шкоди [2].

Ці загрози можна поділити на дві основні групи:

* загрози, при яких реалізація вимагає постійної участі людини (зловмисника);
* загрози, при яких реалізацію забезпечують відповідні комп'ютерні програми без безпосередньої участі людини [2].

Перелік основних методів захисту інформації в ІС поданий на Рисунку 2.11.

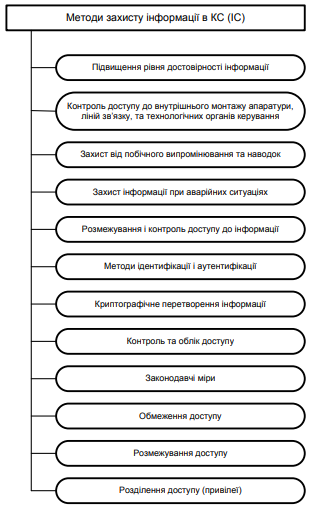


Рисунок 2.11 - Методи захисту інформації в ІС

Завдання захисту від загроз кожного з цих типів однакові і включають в себе наступне:

* перешкоджання несанкціонованому доступу до ресурсів комп'ютерних систем;
* перешкоджання несанкціонованого використання комп'ютерних ресурсів у випадку незаконного доступу до них;
* своєчасне виявлення факту несанкціонованих дій і усунення їх причин та наслідків [2].

Способи вирішення зазначених завдань захисту від несанкціонованих дій людей і комп'ютерних програм значно відрізняються один від одного. Основні функції системи захисту полягають у перешкоджанні несанкціонованому доступу людей до ресурсів ІС шляхом ідентифікації та підтвердження достовірності користувачів при вході в ІС, а також у розмежуванні їх доступу до комп'ютерних ресурсів [2].

Також важливою є функція правильного завершення сеансу роботи користувачів, яка запобігає можливості реалізації загрози, коли зловмисник намагається маскуватися під зареєстрованого користувача ІС [2].

Захист від дослідження і копіювання інформації передбачає використання криптографічних методів для шифрування даних, щоб забезпечити їх конфіденційність. Крім того, необхідно передбачити ефективне знищення залишкової інформації та аварійне знищення даних [2].

Захист програм від копіювання має на меті унеможливити використання несанкціоновано-скопійованої програми на іншому комп’ютері. Захист програм від дослідження спрямований на захист алгоритмічних та інших деталей реалізації програми від дослідження [2].

Система захисту для кожного користувача повинна включати наступні етапи доступу до інформаційної системи:

* ідентифікація;
* перевірка достовірності (аутентифікація);
* визначення повноважень для подальшого контролю та розмежування доступу до комп’ютерних ресурсів [2].

Важливо виконувати ці етапи і при підключенні до ІС пристроїв, таких як віддалені робочі станції і термінали [2].

Наступним кроком буде забезпечення захисту інформації в персональних комп’ютерах.

У вирішенні питань загальної організації захисту для персональних комп'ютерів можна використовувати такі підходи:

* фізична ізоляція, наприклад, розміщення ПК в окремій кімнаті, яка закривається на ключ. Тут внутрішній захист має визначальне значення;
* розпізнавання (аутентифікація) користувачів та компонентів інформації;
* розмежування доступу до елементів інформації;
* криптографічний захист інформації, яка зберігається на носіях;
* криптографічний захист інформації в процесі її опрацювання;
* реєстрація всіх звернень до інформації, що захищається [2].

Захист інформації вимагає уваги та дбайливості від самих користувачів. Важливо враховувати, що більшість користувачів не є фахівцями у сфері захисту інформації і, в багатьох випадках, мають обмежені навички вирішення конкретних завдань [2].

Фізична цілісність інформації в ПК залежить від цілісності самого пристрою, стану дисків та пристроїв флеш-пам'яті, а також від цілісності інформації на накопичувачах, таких як диски, флеш-пам'ять та оперативна пам'ять. У широкому спектрі загроз цілісності інформації в ПК важливо враховувати ризики, пов'язані з низьким рівнем кваліфікації великої кількості власників ПК. Особливу небезпеку становить можливість втрати або спотворення даних на жорсткому диску (HDD), на якому користувачі можуть зберігати значні обсяги інформації [2].

Однією з небезпечних форм несанкціонованої модифікації інформації в особистих комп'ютерах є дія шкідливих програм, які можуть спричиняти руйнування або навіть знищення програм або обсягів інформації (даних). Це стає особливо актуальним у зв'язку з практикою обміну пристроями флеш-пам'яті серед користувачів ПК [2].

Основні модулі і блоки, в яких можуть міститися дані, що потребують захисту, включають наступне:

* системні плати особистих комп'ютерів;
* зовнішні пристрої зберігання даних;
* внутрішні жорсткі диски ПК;
* монітори;
* друкуючі пристрої;
* канали зв'язку [2].

# **Антивірусний захист**

Захист від комп'ютерних вірусів та інших програмних атак є самостійним аспектом забезпечення безпеки обробки інформації в ПК, комп'ютерних і інформаційних системах [2]. Оскільки йде мова про небезпеку великих збитків, у якості системи захисту пропонується обрати Cisco Secure Endpoint.

Cisco Secure Endpoint – це комплексний і вдосконалений механізм захисту кінцевих точок, який слугує важливим компонентом загальної стратегії кібербезпеки організації. Проактивний підхід, реагування на загрози в режимі реального часу та можливості інтеграції інших систем безпеки Cisco роблять його надійним вибором для організацій, яким потрібен комплексний захист кінцевих точок в умовах постійно мінливого ландшафту загроз.

Термін "кінцева точка" у сфері інформаційних технологій вказує на кінцевий пристрій, який може бути підключений до комп'ютерної мережі. З погляду кібербезпеки, кінцеві точки представляють потенційні точки вразливості, оскільки можуть бути предметом кібератак або несанкціонованого доступу. Таким чином, захист кінцевих точок визнається важливою складовою стратегії інформаційної безпеки [9].

Cisco Secure Endpoint – система, яка захищає ваш бізнес до, під час та після атаки, що робить її найбільш надійною формою захисту від шкідливих програм. Система використовує глобальний аналіз загроз для посилення захисту мережі ще до того, як відбудеться проникнення. Під час злому мережі вона ідентифікує та блокує атаку, використовуючи потужну комбінацію інтелекту, сигнатур файлів та розширеного аналізу шкідливих програм. Після того, як зловмисник проникне у вашу мережу, Cisco Secure Endpoint надаватиме чітке уявлення про походження шкідливого ПЗ, його метод і точку входу, де він знаходиться, та його поточну траєкторію. Ця комбінація захисту на певний момент часу дозволяє досить швидко виявляти, обмежувати та усувати загрозу для захисту вашого бізнесу від незворотних збитків [9]. На Рисунку 2.12 наведено структуру архітектури Cisco Secure.

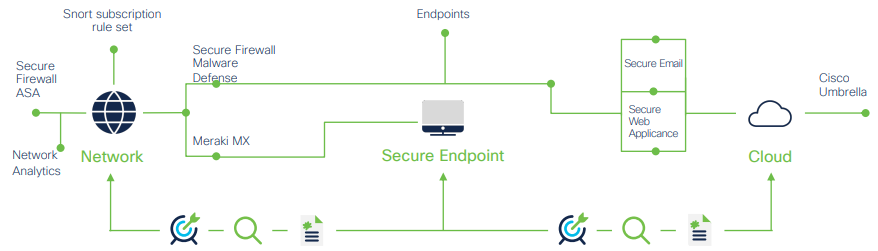


Рисунок 2.12 – Архітектура Cisco Secure

Використання Cisco Secure Endpoint надає вашому бізнесу доступ до широкого набору функцій безпеки, у тому числі:

* фільтрування файлів, які порушують політику безпеки, та які отримуються з Інтернету, електронної пошти тощо;
* розпізнавання, блокування та аналіз шкідливих файлів;
* виявлення шкідливих програм та виявлення потенційно зламаних пристроїв;
* відстеження поширення шкідливих програм та комунікацій;
* зниження загроз повторного зараження [9].

# **Організація підрозділу захисту інформації**

Беручи до уваги всі рекомендації щодо покращення рівня захисту інформації на підприємстві, також пропонується на основі наявного відділу безпеки організувати підрозділ захисту інформації (ПЗІ).

Створення підрозділу захисту інформації (ПЗІ) має на меті організаційне забезпечення управління комплексною системою захисту інформації на підприємстві та здійснення контролю за її ефективністю [3].

ПЗІ відповідає за виконання завдань, пов'язаних із визначенням вимог до захисту інформації в автоматизованій інформаційній системі підприємства під час її проектування, розроблення і модернізації. Також, ПЗІ здійснює контроль за ефективністю комплексної системи захисту інформації під час експлуатації, обслуговування, підтримки працездатності та ведення моніторингу стану захищеності інформації в інформаційній системі [3].

Підрозділ захисту інформації буде складатися з керівника ПЗІ та двох спеціалістів програмно-апаратного та інженерно-технічного захисту інформації.

Підрозділ захисту інформації (ПЗІ) виконує такі завдання:

* вчасне виявлення загроз інформації, що захищається, та аналіз причин і умов їхнього виникнення і реалізації;
* виявлення та максимальне перекриття потенційно можливих каналів і методів несанкціонованого доступу до інформації;
* розробка механізмів оперативного реагування на загрози, залучення різноманітних засобів і методів, таких як юридичні, економічні, організаційні, соціально-психологічні, інженерно-технічні для виявлення й нейтралізації джерел загроз безпеки компанії;
* організація спеціального діловодства, що має за мету запобігання несанкціонованому одержанню конфіденційної інформації [10].

Функції ПЗІ під час експлуатації КСЗІ підприємства включають:

* організацію процесу керування КСЗІ;
* розслідування випадків порушення політики безпеки, а також аналіз небезпечних та непередбачених подій, включаючи визначення причин, що призвели до них, супровід бази даних щодо цих подій;
* прийняття заходів у випадку виявлення спроб несанкціонованого доступу до ресурсів ІС, порушення правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
* забезпечення контролю за цілісністю засобів захисту інформації та оперативне реагування на їх вихід з ладу або порушення режимів функціонування;
* організація управління доступом до ресурсів КС (розподіл необхідних реквізитів захисту інформації, таких як паролі, привілеї, ключі і т. д. між користувачами);
* організація та проведення заходів з модернізації, тестування та оперативного відновлення функціонування КСЗІ після збоїв, відмов або аварій;
* проведення аналітичного оцінювання поточного стану безпеки інформації в КС (прогнозування нових загроз, їх врахування в моделі загроз, визначення необхідності коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз тощо);
* контроль за виконанням персоналом і користувачами КС вимог та інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації. Крім того, контроль за забезпеченням режиму обмеження доступу у разі обробки в КС інформації, що становить державну таємницю, а також контроль за забезпеченням охорони і порядку зберігання носіїв інформації, які містять відомості, що підлягають захисту [3].

# **Розмежування доступу**

Для розмежування доступу на підприємстві використаємо модель Бела-ЛаПадули та дискреційну модель Харрісона-Руззо-Ульмана. За змістом поділимо інформацію на:

1. Публічну інформацію, її визначення було наведено вище.
2. Адміністративну або ділову інформацію різного змісту.
3. Клієнтську інформацію, що містить персональні дані клієнтів, історію взаємодії, деталі замовлень, контактну інформація та інше.
4. Економічну інформацію, що містить дані техніко-економічного планування і прогнозування, обліку та економічного аналізу діяльності підприємства.
5. Фінансову інформацію, що містить бухгалтерські звіти, фінансові показники, бюджети, рахунки, податкову звітність та інше.
6. Виробничу інформацію, яка містить дані оперативно-виробничого планування, обліку та контролю роботи підприємств і їх підрозділів.
7. Правову інформацію, що містить договори, правові документи, ліцензії, юридичні зобов'язання та інші юридичні матеріали.
8. Технічну інформацію, що містить дані про інформаційну систему, включаючи бази даних, програми, паролі, архітектуру мережі та інше [11].

Використаємо ці види інформації як множину об’єктів для моделі, а посади та відділи як множину суб’єктів. Відобразимо модель у Таблиці 2.1.

Таблиця 2.1 – Модель Бела-ЛаПадули

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Види інформації | Публічна інформація | Адміністративна інформація | Клієнтська інформація | Економічна інформація | Фінансова інформація | Виробнича інформація | Правова інформація | Технічна інформація |
| Посади та відділи |
| Директор | + | + | + | + | + | + | + | + |
| Секретар | + | + | - | - | - | - | - | - |

Продовження таблиці 2.1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Види інформації | Публічна інформація | Адміністративна інформація | Клієнтська інформація | Економічна інформація | Фінансова інформація | Виробнича інформація | Правова інформація | Технічна інформація |
| Посади та відділи |
| Головний інженер | + | - | - | - | + | + | + | - |
| Головний інженер з будівництва | + | - | - | - | + | + | + | - |
| Головний енергетик | + | - | - | - | + | + | + | - |
| Головний механік | + | - | - | - | + | + | + | - |
| Головний економіст | + | - | - | + | + | - | - | - |
| Заступник директора з питань безпеки | + | + | + | - | - | - | + | + |
| Заступник головного інженера | + | - | - | - | + | + | + | - |
| Заступник директора з виробництва | + | - | - | - | + | + | + | - |
| Заступник директора з охорони праці | + | - | - | - | - | + | + | - |
| Начальник технологічного відділу | + | - | - | - | - | + | + | - |
| Технологічний відділ | + | - | - | - | - | + | - | - |
| Виробничо-технічний відділ | + | - | - | - | - | + | - | - |
| Начальник бази виробничого обслуговування | + | - | - | - | - | + | + | - |
| Начальник відділу охорони праці | + | - | - | - | - | + | + | - |
| Відділ охорони праці | + | - | - | - | - | + | + | - |
| Начальник відділу матеріально-технічного постачання | + | - | - | - | + | + | + | - |
| Відділ матеріально-технічного постачання | + | - | - | - | + | + | - | - |
| Начальник будівельно-монтажної дільниці | + | - | - | - | - | + | - | - |
| Начальник відділу кадрів | + | + | - | - | + | - | + | - |

Продовження таблиці 2.1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Види інформації | Публічна інформація | Адміністративна інформація | Клієнтська інформація | Економічна інформація | Фінансова інформація | Виробнича інформація | Правова інформація | Технічна інформація |
| Посади та відділи |
| Відділ кадрів | + | + | - | - | + | - | + | - |
| Економіст | + | - | + | + | + | - | + | - |
| Начальник юридичного відділу | + | - | + | - | - | - | + | - |
| Юридичний відділ | + | - | + | - | - | - | + | - |
| Начальник відділу безпеки | + | + | + | - | - | - | + | + |
| Відділ безпеки | + | + | + | - | - | - | + | + |
| Головний бухгалтер | + | + | + | - | + | + | + | - |
| Бухгалтерія | + | + | + | - | + | + | + | - |
| Начальник відділу тендерних закупівель та конкурсних торгів | + | - | + | - | + | + | + | - |
| Відділ тендерних закупівель та конкурсних торгів | + | - | + | - | + | + | + | - |
| Менеджер з зовнішньоекономічної діяльності | + | - | + | + | - | - | + | - |

Тепер побудуємо модель Харрісона-Руззо-Ульмана. Множина суб’єктів і об’єктів буде такою самою, як і для моделі Бела-ЛаПадули. Встановимо перелік рівнів доступу наступним чином:

* читання;
* запис;
* редагування;
* повний доступ;
* відсутність доступу.

Скоротимо рівні доступу до Ч, З, Р, П та Н для зручного відображення в клітинках таблиці. Результат зображено у Таблиці 2.2.

Таблиця 2.2 – Модель Харрісона-Руззо-Ульмана

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Види інформації | Публічна інформація | Адміністративна інформація | Клієнтська інформація | Економічна інформація | Фінансова інформація | Виробнича інформація | Правова інформація | Технічна інформація |
| Посади та відділи |
| Директор | П | П | П | П | П | Ч | П | Ч |
| Секретар | Ч | Ч | Н | Н | Н | Н | Н | Н |
| Головний інженер | Ч | Ч | Н | Н | Ч | П | Ч | Н |
| Головний інженер з будівництва | Ч | Ч | Н | Н | Ч | П | Ч | Н |
| Головний енергетик | Ч | Н | Н | Н | Ч | П | Ч | Н |
| Головний механік | Ч | Ч | Н | Н | Ч | П | Ч | Н |
| Головний економіст | Ч | Н | Ч | П | Ч/Р | Ч | Н | Н |
| Заступник директора з питань безпеки | П | Ч | Ч | Н | Н | Ч | П | П |
| Заступник головного інженера | Ч | Ч | Н | Н | Ч | П | Ч | Н |
| Заступник директора з виробництва | Ч | Ч | Н | Н | Ч | П | Н | Н |
| Заступник директора з охорони праці | П | Н | Н | Н | Н | Ч | Ч/З | Н |
| Начальник технологічного відділу | Ч | Н | Н | Н | Н | П | Ч | Н |
| Технологічний відділ | Ч | Н | Н | Н | Н | П | Ч | Н |
| Виробничо-технічний відділ | Ч | Н | Н | Н | Н | П | Ч | Н |
| Начальник бази виробничого обслуговування | Ч | Ч | Н | Н | Н | П | Н | Н |
| Начальник відділу охорони праці | П | Н | Н | Н | Н | Ч | Ч/З | Н |
| Відділ охорони праці | П | Н | Н | Н | Н | Ч | Ч/З | Н |
| Начальник відділу матеріально-технічного постачання | Ч | Н | Ч | Ч | Ч/З | П | Ч | Н |
| Відділ матеріально-технічного постачання | Ч | Н | Ч/Р | Ч | Ч/З | П | Ч | Н |
| Начальник будівельно-монтажної дільниці | Ч | Ч | Н | Н | Н | П | Н | Н |

Продовження таблиці 2.2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Види інформації | Публічна інформація | Адміністративна інформація | Клієнтська інформація | Економічна інформація | Фінансова інформація | Виробнича інформація | Правова інформація | Технічна інформація |
| Посади та відділи |
| Начальник відділу кадрів | Ч | П | Ч | Н | Ч/З | Н | Н | Н |
| Відділ кадрів | Ч | П | Ч | Н | Ч/З | Н | Н | Н |
| Економіст | Ч | Н | Ч | П | Ч | Ч | Н | Н |
| Начальник юридичного відділу | Ч | Ч | Ч | Н | Ч | Ч | П | Н |
| Юридичний відділ | Ч | Ч | Ч | Н | Ч | Ч | П | Н |
| Начальник відділу безпеки | П | Ч | Ч/Р | Н | Н | Н | П | П |
| Відділ безпеки | П | Ч/Р | Ч/Р | Н | Н | Н | П | П |
| Головний бухгалтер | Ч | Ч | П | Ч | П | Ч | Н | Н |
| Бухгалтерія | Ч | Ч | П | Ч | П | Ч | Н | Н |
| Начальник відділу тендерних закупівель та конкурсних торгів | Ч | Н | Ч/Р | Н | Ч/З | Ч/Р | Ч | Н |
| Відділ тендерних закупівель та конкурсних торгів | Ч | Н | Ч/Р | Н | Ч/З | Ч/Р | Ч | Н |
| Менеджер з зовнішньоекономічної діяльності | П | Н | Ч/Р | Ч | Ч | Н | Н | Н |

# **Ідентифікація та облікові записи**

Ідентифікація необхідна для присвоєння унікального ідентифікатора користувача КС, який використовується для виконання подальших захисних функцій. Процес встановлення достовірності (аутентифікація) полягає в перевірці особи користувача, який намагається отримати доступ до системи. Для надійного розпізнавання можуть використовуватися методи, які базуються на використанні технічних засобів для визначення унікальних характеристик людини, таких як голос, відбитки пальців, структура зіниці ока та інші [2].

Забезпечимо ідентифікацію користувачів інформаційної системи шляхом створення облікових записів для всіх осіб, що працюють в ній. У Таблиці 2.3 наведено посаду, логін та пароль для облікових записів зареєстрованих користувачів.

Таблиця 2.3 – Облікові записи

|  |  |  |
| --- | --- | --- |
| Посада | Логін | Пароль |
| Директор | director | r9E7aLp2 |
| Секретар | secretary | x5jQp4Zu8 |
| Головний інженер | chiefE | c2vM1aWq7 |
| Головний інженер з будівництва | chiefCE | k6o3Bv8Jg |
| Головний енергетик | chiefEE | p1gR9sLw2 |
| Головний механік | chiefM | u4q9Yw7Zp |
| Головний економіст | chiefEC | a8o2W5gNc |
| Заступник директора з питань безпеки | deputydirector4sec | z3q7Hl9Pb |
| Заступник головного інженера | deputychiefE | h2U4m8aTn |
| Заступник директора з виробництва | deputyderectorofP | w3q7Vp6Rt |
| Заступник директора з охорони праці | deputyderectorofDP | b6r2C9w0J |
| Начальник технологічного відділу | headofTTD | f7g1D8s4L |
| Технологічний відділ | techDep1  techDep2 | c3k5R9p2J  l2w7G3r1V |
| Виробничо-технічний відділ | protechDep1  protechDep2 | n8B4m7Tl9  s6D1v7Qr9 |
| Начальник бази виробничого обслуговування | headofPSB | a9z3X8j7W |
| Начальник відділу охорони праці | headofTLPD | g1H7j2Cp4 |
| Відділ охорони праці | depofLP1  depofLP2 | p5L9n8V4r  q7O3z2Yu8 |
| Начальник відділу матеріально-технічного постачання | headofTLD | o5I9r2Yl6 |
| Відділ матеріально-технічного постачання | depofMaTS1  depofMaTS2 | t2q9S3k7v  e7U8m4Op2 |

Продовження Таблиці 2.3

|  |  |  |
| --- | --- | --- |
| Посада | Логін | Пароль |
| Начальник будівельно-монтажної дільниці | headofTCaID | j9T6r7D2x |
| Начальник відділу кадрів | headofHR | i1N8w4X6o |
| Відділ кадрів | humanRD1  humanRD2 | p3Q2f9H7r  c6v4Z7h9m  r7T4s2J5l |
| Економіст | economist | m8B9Y1q6n |
| Начальник юридичного відділу | headofLD | n5G1p7F3q |
| Юридичний відділ | legalD1 legalD2 | v4J6k8P9x  t2R8e4D7s |
| Начальник відділу безпеки | headofSD | d7C5o2N8v |
| Відділ безпеки | SD1  SD2  SD3  SD4 | q4H9r2E1t  o1X7w4V8u  z6H1g7N3p  g3L7f1H2j |
| Головний бухгалтер | chiefAccountant | f9Q4W7n2x |
| Бухгалтерія | accounting1  accounting2  accounting3 | w2T8v6L1u  b7Z2m1X5v  s9T4x2H8p |
| Начальник відділу тендерних закупівель та конкурсних торгів | headofTDoTPaCB | x6B2j8W9s |
| Відділ тендерних закупівель та конкурсних торгів | pedoTPaCB1  pedoTPaCB2 | a1C9p4L7m  j3P7k9D4s |
| Менеджер з зовнішньоекономічної діяльності | managerofFEA | h8N4r2M6o |

Підбиваючи підсумки даного розділу, можна зазначити що було проаналізовано наявні заходи захисту інформації на підприємстві та запропоновано ряд покращень організаційно-адміністративних та інженерно-технічних заходів, що мають посприяти загальному рівню безпеки. Окремо виділимо заходи з розмежування доступу, які були запроваджені шляхом побудови моделі Бела-ЛаПадули та дискреційної моделі і забезпечення ідентифікації користувачів шляхом створення облікових записів.

# **POЗДIЛ 3 ПРАКТИЧНА ЧАСТИНА РОЗРОБКА ІНФОРМАЦІЙНОГО ЗАХИСТУ**

## **Криптологія та її складові**

Криптологія - наука, що вивчає методи побудови та аналізу систем захисту інформаційних ресурсів, що ґрунтуються на математичних перетвореннях даних та використанні секретних параметрів. Криптологія об'єднує два взаємозалежні напрями: криптографію, що включає в себе розробку захисних систем, та криптоаналіз, що займається аналізом та розкриттям цих систем [12].

Криптографія - це галузь криптології, яка досліджує основні закономірності, методи, системи та засоби забезпечення конфіденційності, цілісності, дійсності, доступності та спостережливості інформації та ресурсів. Вона базується на використанні криптографічних перетворень [12].

Криптоаналіз - це галузь криптології, яка вивчає основні закономірності, протиріччя, методи та засоби аналізу криптографічних систем. Вона базується на використанні вхідних та вихідних даних цих систем, включаючи частину ключових даних, з метою визначення спеціальних (ключових) даних і значущої інформації, які можуть бути використані для порушення конфіденційності, цілісності, справжності, доступності інформації та ресурсів і т. д. [12].

Кожне криптографічне перетворення визначається конкретним ключем (секретним параметром) та описується за допомогою криптографічного алгоритму. Криптографічний алгоритм представляє собою набір математичних правил і процедур, які регулюють різновиди перетворень, такі як шифрування, створення та перевірка цифрового підпису, обчислення хеш-значень, а також спеціальних криптографічних контрольних сум та інших операцій. Колекція криптографічних алгоритмів, використовуваних для шифрування, отримала назву "шифр" [12].

Криптографічний ключ – це конфіденційний та змінний компонент шифру, який використовується для шифрування конкретного повідомлення [12].

Шифрування даних – це комплексний процес, який включає в себе дві основні операції:

1. Шифрування: це перетворення відкритого тексту у вигляд, незрозумілий несанкціонованому користувачеві. Відкритий текст представляє собою початкове повідомлення, яке піддається шифруванню. Результатом цього процесу є шифротекст, також відомий як криптотекст чи криптограма.
2. Розшифрування: це обернений процес, спрямований на відновлення початкової інформації (відкритого тексту) з зашифрованого повідомлення за допомогою конкретних правил шифру та використаного ключа [12].

Криптостійкість - це властивість криптосистеми, яка полягає в опорі до атак, спрямованих на отримання секретного ключа або відкритого повідомлення. Рівень стійкості криптосистеми визначається її здатністю протистояти всім можливим атакам. Атака на криптосистему передбачає спробу порушення безпеки конкретної реалізації криптосистеми. В криптографії існує загальноприйняте правило, визначене голландським вченим Огюстом Керкхофом, яке стверджує, що стійкість зашифрованого повідомлення, в першу чергу, забезпечується секретним ключем. Це означає ймовірність того, що сам алгоритм шифрування, шифротекст або його певна частина є відомими зловмиснику та доступними для вивчення [12].

## **Опис алгоритму шифрування RC4 та принцип його роботи**

Rivest Cipher 4 (RC4) - це один із найпоширеніших алгоритмів шифрування, що застосовується в різних галузях, включаючи сферу інтернет-безпеки [13]. Основні переваги шифру – висока швидкість роботи та змінний розмір ключа.

Основний принцип роботи RC4 полягає в генерації псевдовипадкового потоку бітів, який потім використовується для шифрування даних. Ключ виступає як ініціатор цього потоку. Під час ініціалізації внутрішнього блоку даних, відомого як S-блок, ключ використовується для створення початкового стану.

Після ініціалізації S-блоку генерується псевдовипадковий потік бітів, відомий як «потік ключів». Кожен біт вхідних даних (відкритий текст) потім комбінується за допомогою операції XOR з відповідним бітом у потоці ключів. Цей процес повторюється для кожного байта вхідних даних, і отримуємо зашифрований текст.

Розшифрування відбувається аналогічним чином. Потік ключів, згенерований тим самим ключем, використовується для застосування операції XOR до кожного байта зашифрованого тексту. Це дозволяє відновити вхідні дані, що були зашифровані.

Шифр RC4, завдяки своїй простоті та швидкодії, став популярним у безлічі систем, включаючи застосування в безпровідних мережах та інших областях.

## **Опис програми та блок-схема алгоритму її виконання**

Опишемо програму, яка створена для реалізації криптографічного захисту інформації на підприємстві.

Програму написано за допомогою мови програмування C# в інтегрованому середовищі розробки Microsoft Visual Studio. Для керування обліковими записами та збереження та отримання доступу до визначеної інформації на сервері було використано FTP-сервер FileZilla Server. Програма виконує задачі шифрування, розшифрування за вказаним ключем, відображає перелік файлів, завантажених на сервер для авторизованого користувача, а також надає можливість завантаження файлів на сервер та з серверу, і видалення обраних файлів з серверу. Кожен користувач має свою директорію на сервері, до якої має доступ лише він. Без авторизації на сервері користувач не зможе отримати доступ до безпосередньо програми.

Представимо алгоритм виконання програми за допомогою блок-схеми, що зображена на Рисунку 3.1.

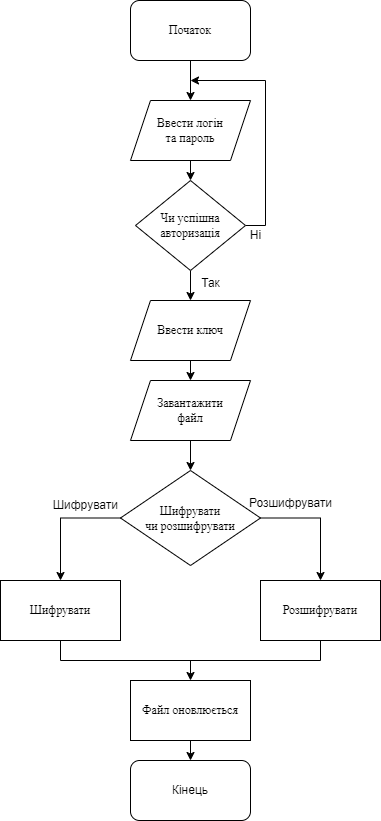


Рисунок 3.1 – Блок-схема алгоритму виконання програми

Тепер поетапно розглянемо процес роботи з програмою. Першим, що ми побачимо після запуску програми буде вікно авторизації. Не пройшовши авторизацію, користувач не зможе мати доступ до безпосередньо процесу шифрування і розшифрування. Вікно авторизації зображено на Рисунку 3.2.

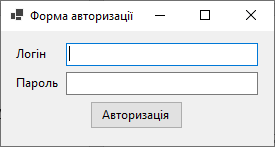


Рисунок 3.2 – Вікно авторизації

Дані зареєстрованих користувачів вносяться в конфігурацію серверу. Як бачимо на Рисунку 3.3, для кожного користувача вказаний логін, пароль, шлях до його директорії і тип доступу, яким він володіє. За бажанням можна додати опис та занести користувача в окремо створену групу.

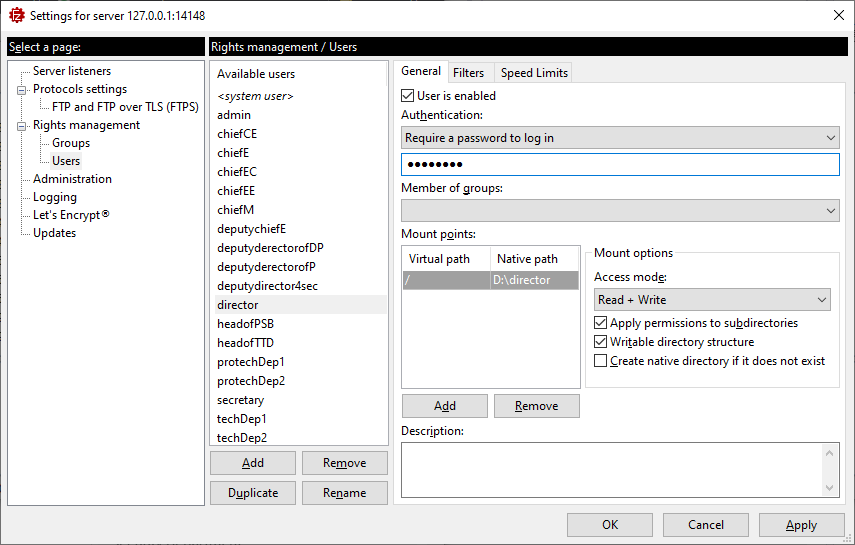


Рисунок 3.3 – Перелік доданих до конфігурації серверу користувачів

У разі успішної авторизації буде виведено відповідне повідомлення, яке зображено на Рисунку 3.4. Після цього користувач отримує доступ до основної частини програми з можливістю шифрувати, розшифровувати файли та додавати, видаляти чи завантажувати файли з серверу.

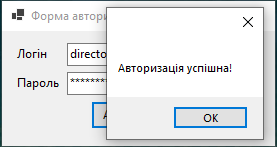


Рисунок 3.4 – Успішна авторизація

У серверній програмі буде відображено інформацію про те, що користувач з вказаним логіном авторизувався успішно і його сесія буде активною поки він не завершить роботу. Вікно серверної програми зображено на Рисунку 3.5.

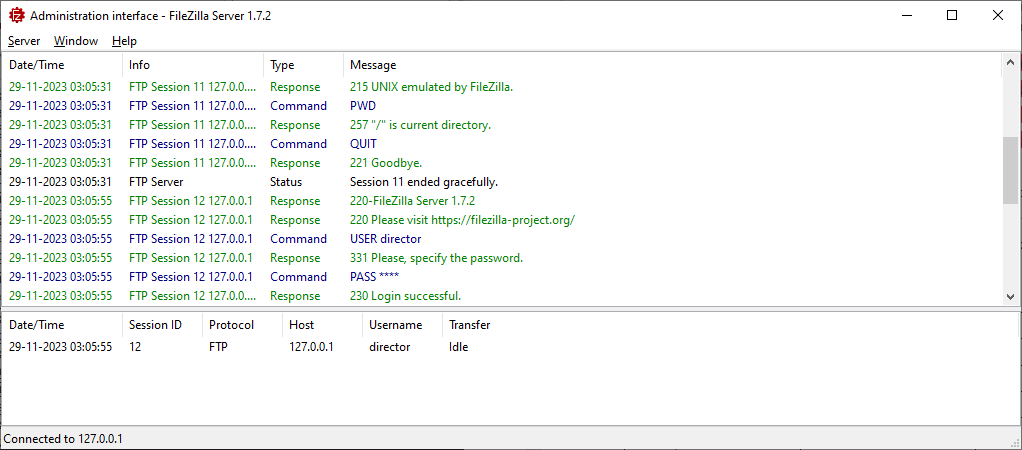


Рисунок 3.5 – Вікно FileZilla при авторизації користувача

На Рисунку 3.6 зображено інтерфейс основної частини програми.

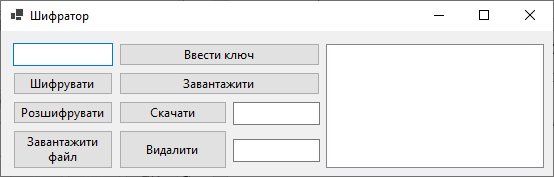


Рисунок 3.6 – Інтерфейс основної частини програми

Користувач, авторизований під своїм обліковим записом, має доступ лише до папки, визначеної для нього адміністратором. Для процесу шифрування необхідно ввести ключ, натиснути «Ввести ключ», натиснути «Завантажити файл» для завантаження файлу для шифрування та натиснути кнопку «Шифрувати». Файл буде зашифровано з використанням вказаного ключа. На Рисунку 3.7 зображено процес введення ключа та підтвердження успішності цієї дії.

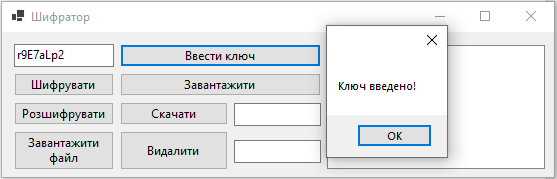


Рисунок 3.7 – Введення ключа

На Рисунках 3.8-3.9 наведено процес завантаження файлу на сервер та обрання його для виконання шифрування.

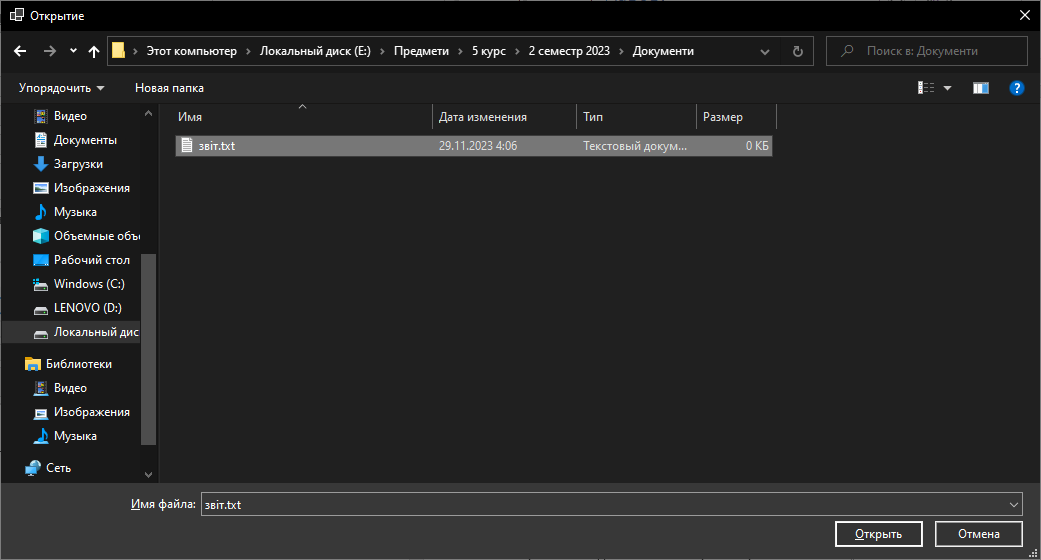


Рисунок 3.8 – Завантаження файлу на сервер

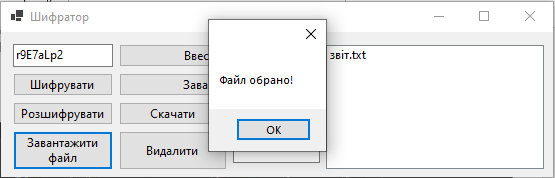


Рисунок 3.9 – Результат обрання файлу для шифрування

На Рисунку 3.10 наведено вміст файлу до процесу шифрування.

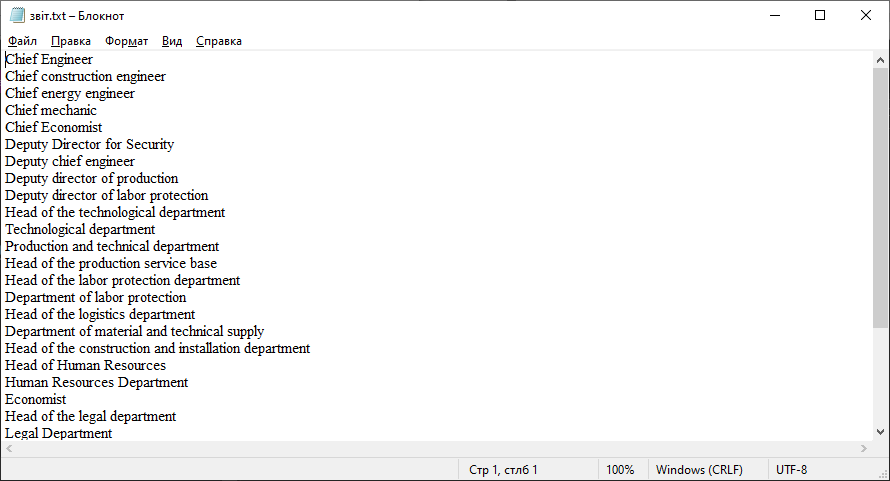


Рисунок 3.10 – Вміст файлу до процесу шифрування

Натискаємо на кнопку «Шифрувати», програма зашифровує файл і виводить відповідне повідомлення, що наведено на Рисунку 3.11.

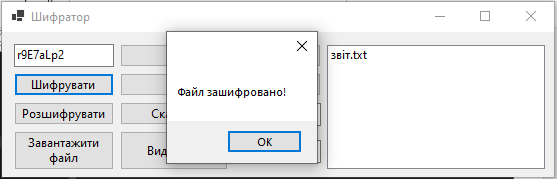


Рисунок 3.11 – Повідомлення про шифрування файлу

Переглянемо файл після шифрування, його нинішній вміст наведено на Рисунку 3.12. Як бачимо, інформація була зашифрована.

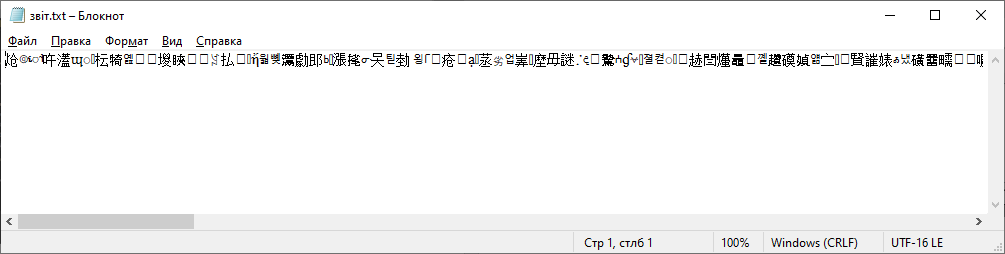


Рисунок 3.12 – Зашифрована інформація всередині файлу

Для розшифрування необхідно обрати файл та виконати операцію «Розшифрувати». Успішний результат розшифрування наведено на Рисунку 3.13.

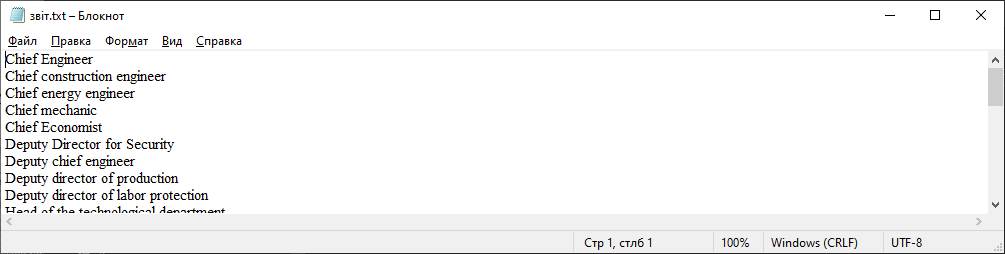


Рисунок 3.13 – Результат розшифрування файлу

Розглянемо додатковий функціонал програми, такий як завантаження файлів з серверу на комп’ютер та видалення файлів з серверу. Для завантаження файлів з серверу на комп’ютер необхідно ввести в текстове поле назву файлу та натиснути «Скачати». З’явиться діалогове вікно, яке зображено на Рисунку 3.14, де необхідно буде ввести назву для збереженого файлу та обрати місце збереження.

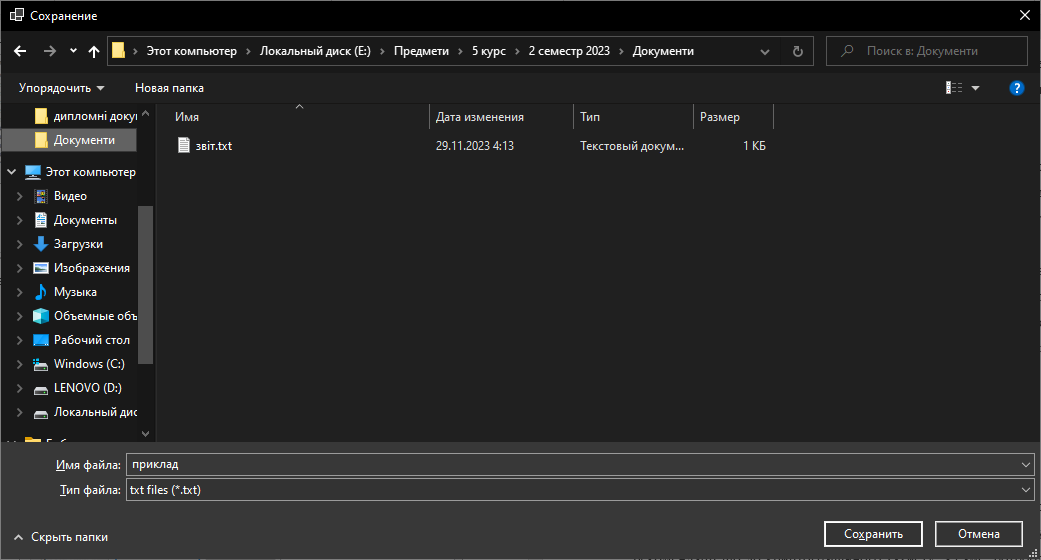


Рисунок 3.14 – Діалогове вікно збереження файлу

Як бачимо на Рисунку 3.15, в новому файлі міститься інформація з завантаженого на сервер файлу.

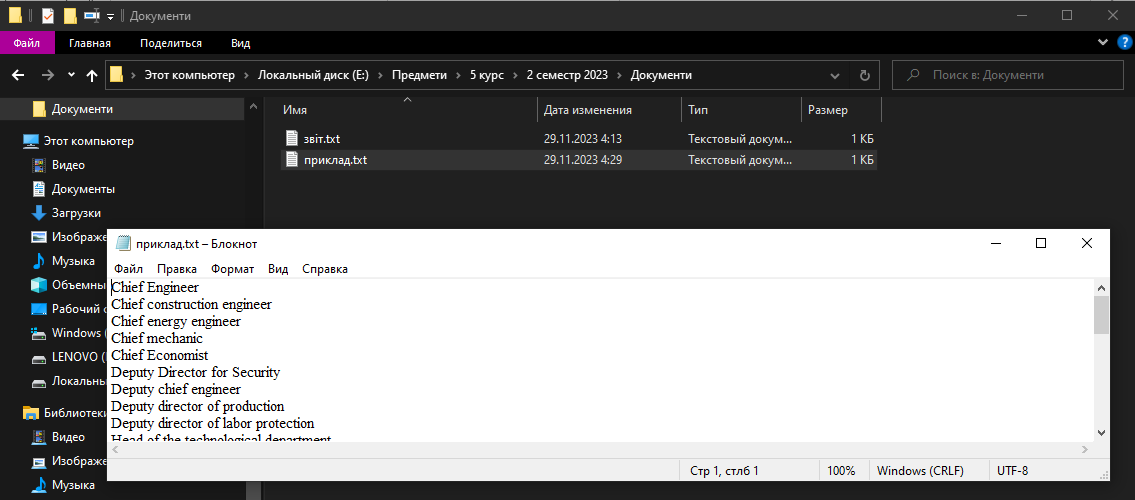


Рисунок 3.15 – Завантажений з серверу файл

Для видалення введемо назву файлу в текстове поле і натиснемо на кнопку «Видалити», як зображено на Рисунку 3.16.

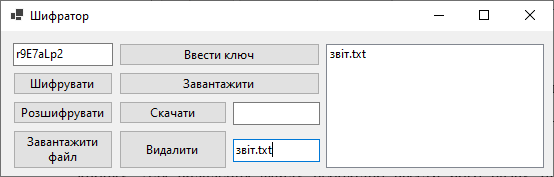


Рисунок 3.16 – Видалення файлу з серверу

Після натискання з серверу буде видалений вказаний файл, що зображено на Рисунку 3.17.

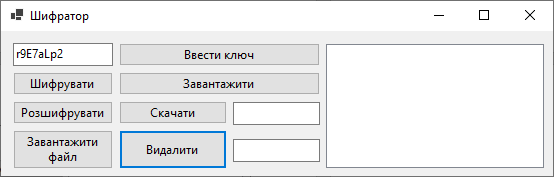


Рисунок 3.17 – Результат видалення

Як бачимо з опису функціоналу програми, вона відповідає вимогам, встановленим на етапі постановки задачі і разом з локальним сервером може бути впровадженою в інженерно-технічні заходи з забезпечення інформаційної безпеки на підприємстві.

# **ВИCНOВКИ**

В ході виконання магістерської кваліфікаційної роботи було проведено аналіз приватного підприємства «Українська сервісна бурова компанія-1», що включав в себе розгляд організаційної структури, особливостей підприємницької діяльності та планів офісного центру зі зосередженням уваги на інженерно-технічних засобах забезпечення інформаційної безпеки. Після проведення аналізу були описані запропоновані рекомендації щодо підвищення рівня захисту інформації та розроблено програмний продукт для організації криптографічного захисту інформації шляхом шифрування та розшифрування даних з функціями роботи з файлами.

Рекомендації щодо підвищення рівня захисту інформації включають в себе створення окремого підрозділу захисту інформації, встановлення додаткових відеокамер, грат на вікнах, турнікету, охоронної сигналізації з акустичними, магнітоконтактними оповіщувачами та датчиками руху і системи автоматичного пожежогасіння. Безпосередній захист персональних комп’ютерів передбачає організацію ідентифікації користувачів, які працюватимуть з даними та інформацією, антивірусний захист і організацію криптографічного захисту, реалізованого за допомогою потокового алгоритму шифрування даних RC4. Розмежування доступу та ідентифікація користувачів забезпечуються використанням локального серверу FileZilla.

Розробка програмного продукту здійснювалась за допомогою мови програмування C#, і створена програма містить такі функції, як шифрування та розшифрування файлів за вказаним ключем, завантаження файлів на сервер та з серверу, а також можливість видалення файлів з серверу. Кожен зареєстрований користувач має окрему директорію, в якій він працює з файлами, доступними йому. Додаток відповідає вимогам, встановленим на етапі постановки задачі, та готовий до використання.

# **CПИCOК ВИКOPИCТAНИХ ДЖEPEЛ**

1. Економічна безпека підприємств: підручник / Ортинський В.Л. та ін. Київ: Алерта, 2011, 704 с.
2. Карачка А.Ф. Технології захисту інформації: текст лекцій. Тернопіль: ТНЕУ, 2017. 86 с.
3. Комплексні системи захисту інформації: навч. посіб. /  
   Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Вінниця: ВНТУ, 2017. 120 с.
4. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. Харків: Панов, 2020. 162 с.
5. Панасенко С.П. Алгоритми шифрування. Спеціальний довідник. СПб.: БХВ-Петербург, 2009. 579 с.
6. Українська сервісна бурова компанія – 1. URL: <https://usdc-1.com.ua/uk/#main-office> (дата звернення: 16.11.2023).
7. Українська сервісна бурова компанія – 1. Політика та цілі компанії. URL: <https://usdc-1.com.ua/sertifikati-ta-litsenziyi/> (дата звернення: 19.11.2023).
8. Основи інформаційної безпеки. Поняття інженерно-технічного захисту. URL: <https://studfile.net/preview/6012701/page:38/> (дата звернення: 21.11.2023).
9. Cisco Secure Endpoint. URL: <https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html> (дата звернення: 23.11.2023).
10. Ахрамович В.М., Амелькін С.В. Cистема захисту інформації приватного підприємства. Організація служби захисту інформації приватного підприємства. *Сучасний захист інформації.* 2019. №1(37). С. 21-27.
11. Інформація та її види. URL: <https://studopedia.com.ua/1_282403_Informatsiya-ta-ii-vidi.html> (дата звернення: 25.11.2023).
12. Щур Н.О., Покотило О.А. Основи криптології: навч. посіб. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
13. Сафар’ян О. А., Дедиченко Д. В., Свистун Н. О., Найденова Ю. І.  
    Криптоаналіз і реалізація потокового шифру RC4. *Молодий вчений*. 2023. № 21 (468). С. 69-73.

# **ДОДАТОК А ВИХІДНИЙ КОД ПРОГРАМИ**

Код файлу Form1.cs

using System.Windows.Forms;

using FluentFTP;

using System.Net;

namespace rgr2023.\_1

{

public partial class Form1 : Form

{

RC4 ob = new RC4();

public class RC4

{

public byte[] text; //текст для шифрування/розшифрування

private byte[] S = new byte[256];

private int i = 0;

private int j = 0;

private void swap(byte[] array, int ind1, int ind2)

{

byte temp = array[ind1];

array[ind1] = array[ind2];

array[ind2] = temp;

}

//ініціалізація, алгоритм ключового розкладу

public void init(byte[] key)

{

for (i = 0; i < 256; i++)

{

S[i] = (byte)i;

}

j = 0;

for (i = 0; i < 256; i++)

{

j = (j + S[i] + key[i % key.Length]) % 256;

swap(S, i, j);

}

i = j = 0;

}

//генератор псевдовипадкової послідовності

public byte kword()

{

i = (i + 1) % 256;

j = (j + S[i]) % 256;

swap(S, i, j);

byte K = S[(S[i] + S[j]) % 256];

return K;

}

//функція шифрування/розшифрування

public byte[] code()

{

byte[] data = text.Take(text.Length).ToArray();

byte[] res = new byte[data.Length];

for (int i = 0; i < data.Length; i++)

{

res[i] = (byte)(data[i] ^ kword());

}

return res;

}

//бінарний запис в файл

public void WriteByteArrayToFile(Byte[] buffer, string fileName)

{

try

{

FileStream fs = new FileStream(fileName, FileMode.Create, FileAccess.ReadWrite);

BinaryWriter bw = new BinaryWriter(fs);

for (int i = 0; i < buffer.Length; i++)

bw.Write(buffer[i]);

bw.Close();

fs.Close();

}

catch (Exception ex)

{

Console.WriteLine(ex.Message);

}

}

//бінарне читання з файлу

public Byte[] ReadByteArrayFromFile(string fileName)

{

Byte[] buffer = null;

try

{

FileStream fs = new FileStream(fileName, FileMode.Open, FileAccess.Read);

BinaryReader br = new BinaryReader(fs);

long numBytes = new FileInfo(fileName).Length;

buffer = br.ReadBytes((int)numBytes);

br.Close();

fs.Close();

}

catch (Exception ex)

{

Console.WriteLine(ex.Message);

}

return buffer;

}

}

public Form1()

{

InitializeComponent();

client.Connect();

// Отримання списку файлів

FtpListItem[] files = client.GetListing();

// Виведення списку файлів в ListBox

foreach (FtpListItem file in files)

{

listBox1.Items.Add(file.Name);

}

}

public void refresh()

{

listBox1.Items.Clear();

FtpListItem[] files = client.GetListing();

// Виведення списку файлів в ListBox

foreach (FtpListItem file in files)

{

listBox1.Items.Add(file.Name);

}

}

public string infile, outfile, upld, upld1, dwnld, dwnld1;

byte[] bytekey;

FtpClient client = new FtpClient("127.0.0.1", Data.Login, Data.Password); // конструктор фтп-серверу після авторизації

private void button1\_Click(object sender, EventArgs e) // введення ключа

{

int key = 0;

string query = textBox1.Text;

int.TryParse(query, out key);

bytekey = BitConverter.GetBytes(key);

MessageBox.Show("Ключ введено!");

}

public void button2\_Click(object sender, EventArgs e)

{

if (openFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

infile = openFileDialog1.FileName; // файл на вході

outfile = infile;

MessageBox.Show("Файл обрано!");

}

public void button4\_Click(object sender, EventArgs e) // шифрування

{

ob.text = ob.ReadByteArrayFromFile(infile);

ob.init(bytekey);

ob.WriteByteArrayToFile(ob.code(), outfile);

MessageBox.Show("Файл зашифровано!");

}

private void button5\_Click(object sender, EventArgs e) // розшифрування

{

ob.text = ob.ReadByteArrayFromFile(infile);

ob.init(bytekey);

ob.WriteByteArrayToFile(ob.code(), outfile);

MessageBox.Show("Файл розшифровано!");

}

private void button3\_Click\_1(object sender, EventArgs e) // завантаження файлу на сервер

{

openFileDialog1.ShowDialog();

upld = openFileDialog1.FileName;

upld1 = Path.GetFileName(upld);

client.UploadFile(upld, "/" + upld1);

refresh();

}

private void button6\_Click(object sender, EventArgs e) // завантаження файлу з серверу

{

saveFileDialog1.Filter = "txt files (\*.txt)|\*.txt|All files (\*.\*)|\*.\*";

saveFileDialog1.ShowDialog();

dwnld1 = textBox2.Text;

dwnld = saveFileDialog1.FileName;

client.DownloadFile(dwnld, "/" + dwnld1);

textBox2.Text = null;

refresh();

}

private void button7\_Click(object sender, EventArgs e) // видалення файлу з серверу

{

client.DeleteFile(textBox3.Text);

textBox3.Text = null;

refresh();

}

}

}

Код файлу Form2.cs

using FluentFTP;

namespace rgr2023.\_1

{

public partial class Form2 : Form

{

public Form2()

{

InitializeComponent();

textBox2.UseSystemPasswordChar = false;

textBox2.PasswordChar = '\*';

}

private void button1\_Click(object sender, EventArgs e)

{

var client = new FtpClient("127.0.0.1", textBox1.Text, textBox2.Text);

client.Connect();

Data.Login = textBox1.Text;

Data.Password = textBox2.Text;

client.Disconnect();

MessageBox.Show("Авторизація успішна!");

Form1 form1 = new Form1();// Створюємо новий екземпляр форми

this.Hide();

form1.Show();// Викликаємо форму, використовуючи метод ShowDialog()

}

}

}