МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ФІЗИКИ ТА МАТЕМАТИКИ
КАФЕДРА ІНФОРМАТКИ, ПРОГРАМНОЇ ІНЖЕНЕРІЇ ТА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ

РОЗРОБЛЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Кваліфікаційна робота (проєкт)

на здобуття ступеня вищої освіти "магістр"

Виконав: здобувач 2 курсу 12-231М групи
Спеціальності 122 Компютерні науки
Освітньої програми Комп'ютерні науки
другого (магістерського) рівня освіти
Євдокимов Сергій Олександрович
Керівник: доктор педагогічних наук,
професор Шерман Михайло Ісаакович
Рецензент: кандидат педагогічних наук,
деканеса Гончаренко Тетяна Леонідівна

Херсон – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

CSS – Cascading Style Sheets

DLP – Data Leak Prevention

DNS – Domain Name System

DFD – Data Flow Diagrams

ESA – Evdokymov Serhii Olexandrovych

EMM – Enterprise Mobility Management

FTP – File Transfer Protoco

HTTP – HyperText Transfer Protocol

HTML – HyperText Markup Language

IDEF – Integrated Computer-Aided Manufacturing

IT – Informaition Technology

IM – Instant Messaging

LAN – Local Area Network

MDM – Mobile device management

MCM – Mobile Content Management

MAM – Mobile Application Management

MC – Microsoft Corporation

OS/ОС – Operation System

PHP – Hypertext Preprocessor

SLL – Secure Sockets Layer

SMB – Server Message Block

Win. NT – Windows New Technology

WBS – Work Breakdown Structure

WMI – Windows Management Instrumentation

АС – Автоматизована система

БД –База даних

ЗІ – Захист інформації

ЕОМ – Електроно Обчислювальна Машина

ОЗУ – Оперативно запам’ятовуючий пристрій

СЗІ – Система Захисту Інформації

СУБД – Система управління базами даних

КІ – Конфіденційна інформація

ІБ – Інформаційна безпека

ПЗ – Програмне забезпечення

ПБ – Політика безпеки

ПП – Програмний продукт

НС – Надзвичайний стан

ЗВО – Заклад вищої освіти

ПС – Програмне середовище

ШНМ – Штучні нейроні мережі

ШПЗ – Шкідливе програмне забезпечення

ICMP – Internet Control Message Protocol

ЕЦП – Електронно-цифровий підпис

RSA – Rivest, Shamir и Adleman

SSH – Secure Shell

WLAN – Wireless Local Area Network

VPN – Virtual Private Network

MAC – Media Access Control

DHCP – Dynamic Host Configuration Protocol

SLL –Small Lymphocytic Lymphom

EMM – Enterprise Mobility Management

WBS – Work Breakdown Structure

UML – Unified Modeling Language

ЦДПУ - Центральноукраїнський державний педагогічний університет

JPEG – Joint Photographic Experts Group

GIF – Raphics Interchange Format

ЗУ – Закон України

НПА – Нормативно-правовий акт

ВСТУП

Актуальність теми

Будь-яка державна та комерційна установа зацікавлена в збереженні інформації, яка може завдати йому шкоду, у випадку, якщо потрапить до рук зловмисників чи буде знищена. Для державних установ така інформація носить гриф "Таємно", для комерційних підприємств – "Комерційна таємниця" або "Цінна інформація". Інформація, яка потребує захисту, включаючи електроні документи, становить потенційний інтерес для зловмисника – це, як правило, важливі договори, списки клієнтів, бази даних бухгалтерських програм, паролі та ключі системи "клієнт-банк", канали зв'язку з підрозділами і т. д. Посітйно в ЗМІ повідомляють про витоки інформації в мережі Інтернет та Dark Net, при цьому зловмисників знаходять дуже рідко. А більшість установ приховують витоки електронної документації, щоб зберегти ділову репутацію. Одна з проблем, пов'язаних з критеріями оцінки безпеки систем, полягала в недостатньому розумінні механізмів роботи мережі. У звязку з вищевказаним, застосування нових методів щодо підвищення рівня захищеності систем захисту електронного документообігу ще дуже дового не втратить своєї актуальності.

Зв’язок роботи з науковими програмами, планами, темами

Дослідженням різних теоретичних і практичних аспектів проблем інформаційної безпеки, методам побудови захищених комп'ютерних систем присвячені численні роботи провідних вчених усього світу. Робота виконана відповідно до наукових праць українського дослідника Домарєва В.В. та його дисертаційних досліджень присвячених проблемам створення комплексних систем захисту інформації. Робота виконана спираючись на рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» затвердженої президентом України Володимиром Зеленським Указом від 26.08.2021 № 447/2021 року.

Мета і завдання дослідження

Метою кваліфікаційної роботи (проєкту) є розроблення засобів забезпечення інформаційної безпеки електронного документообігу і реалізація політики безпеки в локальній мережі. Для досягнення зазначеної мети необхідно виконати ряд завдань:

1. Вявлення ймовірних джерел загроз об'єктів атаки в мережі ЗВО;
2. Розлянути особливості побудови СЗІ;
3. Проаналізувати існуюче ПЗ аналогічного спрямування;
4. Розробити проект та реалізувати програмне забезпечення щодо захисту електронного докуметнообігу;

Об’єктом дослідження є електронний документообіг в локальній мережі, де використовується інформація, яку необхідно зберігати в таємниці і робити все, щоб вона була надійно захищена.

Предметом дослідження є комплексна система захисту електронного документообороту в локальній мережі установи.

Методи дослідження включають в себе криптографічні засоби та DLP-технології від несанкціонованог доступу та витоків електронного документообігу за межі локальної мережі установи.

Наукова новизна одержаних результатів визначається вдосконаленям вже існуючих моделей шифрування та методів забезпечення інформаційної безпеки електронного документообігу. В ході роботи проаналізовано алгортми роботи найвідоміших вірусів: «NotPetya», «Ransomware», «Gpcode» та ін. Також, розгянуто популярні програми СЗІ, такі як VeraCrypt (для шифрування), Symantec DLP, Kaspersky, Infowatch Traffic Monitor DLP та встановлено наступне, що кожний вищевказаний програний продукт має переваги та певні недоліки, що було враховано, при створенні комплексного підходу та поліпшення алгоритму для забезпечення програмного захисту.

Практичне значення одержаних результатів роботи полягає в розробці структурної програми для захищеності електроного документообігу. Одержані наукові результати є важливими для поліпшення захищеності документообігу в компютерних системах та мережах, щю циркулює в локальній мережі установи.

Результати роботи були апробовані на всеукраїнських наукових конференціях та опубліковані у наукових працях:

1. Всеукраїнська науково-практична конференція «Математичні, природничі та комп'ютерні науки, технології, навчання: науково-практичні рішення та підходи молодих науковців», 18 листопада 2021 року, ЦДПУ ім. В.Винниченка, м. Кропивницьк;

2. Міжнародна науково-практична конференція "Вектори розвитку науки та освіти в умовах глобалізації", 25 жовтня 2021 року, м. Полтава.

РОЗДІЛ 1
ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Характеристики каналів витоку інформації в електронній документації

На локальному рівні загроз комп'ютерної безпеки (наприклад приміщення, які вони займають установою, організацією, підприємством) виділяються канали витоків інформації (рис. 1.1), які є сукупністю джерел матеріальних носіїв, електронної інформації, середовищ поширення інформації про сигнали та інших засобів виділення з сигналів чи носіїв [1]. Об'єктивна присутність таких каналів витоку передбачає їх можливе використання зловмисниками шляхом несанкціонованого доступу до інформації, її спотворення, блокування доступу до неї та інших неправомірних маніпуляцій.

У зв'язку з актуальністю проблеми ЗІ необхідно визначити об'єкт захисту. В наукових працях Торокіна А.А. «Основи інженерно-технічної захисту інформації» разначається, що так як за допомогою матеріальних засобів можна захищати тільки матеріальний об'єкт, то об'єктами захисту є матеріальні носії інформації. Такий підхід видається конструктивним, особливо з урахуванням сучасних уявлень про інформацію і об'єктах інформатизації.

Канали витоку інформації – це шляхи та методи витоку інформації з інформаційної системи [2]. Велика частина витоків інформації, реалізованих в середині підприємства,що пов'язана з особистою користю і характеризується більш вузькою зоною інтересу і, отже, значно меншими обсягами викрадених даних [3]. Багато аналітичних джерел, наприклад: [2] підкреслюють, що у випадку зі внутрішніми навмисним порушеннями – обсяги вкрадених даних вище. На рис.1.1 показано, що більшість витоків проводяться через мережу підприємства. Існує кілька причин витоку важливої інформації, в основному це:

– слабка захищеність коштів авторизації (розкрадання паролів, смарт карт, фізичний доступ до незаблокованих робочих місць співробітників під час

відсутності персоналу); зловживання службовими повноваженнями (крадіжка резервних копій, копіювання інформації на зовнішні носії при праві доступу до інформації)[4-5] ;

– використання шпигунів, вірусів і троянів на комп'ютерах співробітників для їх персоналізації [6].

1.2 Види атак по локальной мережі

Необхідно вживати заходи щодо забезпечення захисту документообігу локальної мережі всередині установи постійно, але більшість адміністраторів не приділяють достатньо уваги в цьому питанні, тому і реалізовується велика кількість атак [7-8]. Проаналізувавши основні атаки за 2020 рік можна виділити наступні:

- ARP-атака

Коли в локальній мережі є кілька ЕОМ з одним IP-адресою, то користувач бачить повідомленням про те, що IP-адреса зайнята (використовується іншим комп'ютером). Windows про зайнятість IP-адреси дізнається за допомогою протоколу ARP. ARP-атака полягає в тому, що потенційний зловмисник може відправляти великою кількістю запитів до відмови ЕОМ в обслуговуванні під управлінням ОС Windows. Оскільки до кожного комп'ютеру будуть відправлені сотні запитів, в результаті користувачу буде складно постійно закривати спливаючі вікна та останній буде змушений, як мінімум перезавантажити комп'ютер.

- DoS та DDOS-атаки, в тому числі різні флуд-атаки

DoS атака – це атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких сумлінні користувачі системи не зможуть отримати доступ до надаваних системних ресурсів, або цей доступ

буде утруднений. А *DDoS-атаки* – атка, в якій багато шкідливих машини цілеспрямовані на один ресурс. Тому, атака розподіленого відмови в обслуговуванні (DDoS) набагато більш успішна в руйнуванні мети, ніж атака DoS Отже, існує два типи DoS/DDoS-атак, і найпоширеніша з них заснована на ідеї флуда, тобто завалення жертви величезною кількістю пакетів [7]. Флуд буває різним: ICMP-флуд, SYN-флуд, UDP-флуд і HTTP-флуд. Сучасні DoS-боти можуть використовувати всі ці види атак одночасно, тому слід заздалегідь поклопотатися про адекватний захист від кожної з нихПрирода DoS-атак може бути будь-який, однак, боротися з ними без брандмауера, який був би встановлений на кожній машині локальної мережі, неможливо. Один з видів DoS-атаки, який може з успіхом застосовуватися в локальній мережі - це ICMP-флуд. Ситуація досить поширена серед сучасних, наприклад, 4 жовтня 2021 року у користувачів по всьому світу почалися проблеми з Facebook і Instagram, що дало збитку компанії на суму 1,5 млрд. доларів.

- Заміна MAC-адреси

Як уже давно відомо, що у локальній мережі комп'ютери ідентифікуються не тільки за IP-адресою, а й по MAC-адресу, але деякі адміністратори до сих пір надають доступ по MAC-адресу до певних ресурсів, так як IP-адреси, в більшості випадків, динамічні і видаються DHCP. Такі рішення себе не виправдовують, тому що MAC-адрес дуже легко змінити. Та, на жаль, захиститися від зміни MAC-адреси за допомогою сучасних СЗІ не завжди ндається за можливе. Не кожна ситсема контролю мережевої активності перевіряє зміна MAC-адреси, оскільки прив'язаний до IP-адресами. Тут найбільш ефективне рішення – це використання комутатора, який надає можлоивість зробити прив'язку MAC-адреси до конкретного фізичного порту. Знайти недолік такої захищеності є досить складною річчю, та такий програмний продукт дороговартісний. Хоч, і є ПЗ протидії зі зміною MAC-адреси, але вони менш ефективні.

- Підміна IP-адреси

У мережах, де доступ до ресурсів обмежується по IP-адресами, зловмисник намагається змінити IP-адресу та отримати доступ до незахищаємого ресурсу. При використанні використанні комплексного підходу та СЗІ такий сценарій неможливий, оскільки немає прив'язки до IP-адресами навіть у самого брандмауера. Навіть якщо змінити IP-адресу комп'ютера, то він все одно не увійде до складу ІСПДн, до якої зловмисник намається проникнути.

- Routing-атаки

Даний вид атак заснований на відправку користувачу «підмінних» ICMP-пакетів. Суть цієї атаки в підміні адреси шлюзу те, що користувачу відправляють ICMP-пакет, який повідомляє про коротший маршрут. Але насправді: проходять пакети не через новий маршрутизатор, а через ЕОМ зловмисника. Існує і безліч інших атак в локальних мережах для того, щоб отримати необхідні документи, таприклад сніфери – аналізатори трафіку, та різні атаки з використанням DNS [Додаток Д]. Також, важливо використовувати комплексні програмні способи щодо захисту даних, встановлених на кожній робочій станції, що дозволяє підвищити захищеність мережі та для збереження електронної документації [4, 9].

1.3 Основи інформаційної безпеки в локальнівй мережі

«Захист інформації» – це особлива комбінація як технічних, так і програмних засобів для заходів щодо адміністрування системи відносно її цілісності, конфіденційності та досутпності, за умов впливу несанкціонованого [10]. Не варто вважати свою мережу «безпечною» на 100%,тому що «Ідеальна безпека» – недосяжний міф, який можна реалізувати, в накращому випадку, це

лише кілька професіоналів. Є один фактор, який унеможливлює подоланю на шляху до ідеальної безпеки – це людина.Тому, велика кількість існуючих інцидентів створюють різноманіттю нових методів для захисту. Також, взявши до прикладу, велику кількість публікацій від від компаній, які на професійному рівні займаються ЗІ в системах комп'ютерних мереж, вирішенню даному завданню надається досить велике значення [11-13]. Наявність великої кількості загроз викликають необхідність в забезпечені СЗІ, що включає: комплекс засобів, що проводяться для запобігання витоків електронних документів, а також для несанкціонованого доступу до інформації [10, стр. 13]. Програмні та технічні засоби щодо електронного документообігу в локальних мережах (з англ. Local Area Network, LAN), поєднані комп'ютерних систем на невеликій території, та включає специфічні особливості щодо інформації, яку можна легко та швидко копіювати та передавати по каналах зв'язку [11, стр. 28].

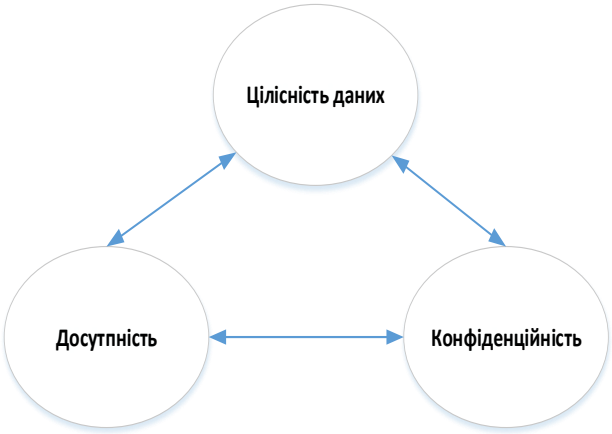

Рисунок 1.1 – Основні вимоги дозаходів безпеки електронного документообігу в локальної мережі

Цілісність даних. Одна із основних цілей безпеки – гарантовати, щоб дані не були змінені, підмінені або знищені. Цілісність даних повинна гарантувати як їх збереження в разі зловмисних дій з нею. Цілісність відноситься до однієї з найскладніших завдань мережевої безпеки [14].

Конфіденційність даних. Другою основною метою мережевої безпеки є

забезпечення конфіденційності даних. Не всі дані можна відносити до КІ. Існує досить велика кількість інформації, яка повинна бути доступна всім, але навіть забезпечити цілісность даних, особливо відкритих, що є пріоритетним завданням [15-16]. До конфіденційної інформації можна віднести наступні дані: особиста інформація користувачів, облікові записи, дані про кредитні картки, дані про розробки і різні внутрішні документи, бухгалтерська інформація та ін.

Доступність Даних. Третьою метою безпеки даних є їх доступність, якщо користувач не може працювати з інофрмацією через її недоступності. Ось приблизний список ресурсів, які зазвичай повинні бути «доступні» в локальній мережі: принтери, сервери, робочі станці, дані користувачів. Загрози і перешкоди, що стоять на шляху до безпеки мережі можна розділити на: технічні загрози та людський фактор [17].

1.4 Види загроз та засоби програмного захисту

Результати всебічного аналізу типів загроз та оцінки кожного об'єкта мережевої ІТ-інфраструктури є основою для розробки та впровадження політики безпеки. Виникає необхідність для створення складової професійної підготовки державних службовців з інформаційних технологій [18]. Вона буде включати в себе політику управління конфігураціями і оновленням, моніторинг і аудит систем, а також інші превентивні заходи операційних політик і процедур. Обов'язковою умовою є наявність тестової лабораторії зі зменшеням аналогів ІТ-середовищ. Накопичені знання і досвід, отримані при аналізі загроз і вразливостей систем, є, по суті, унікальну базу знань, що будуть фундаментом в побудові надійної і захищеної інфраструктури та подальшому навчанні персоналу [19-22]. Однак слід врахувати, що при зміні інфраструктури, додаванні нових об'єктів необхідно провести додаткову оцінку, аналіз та згодом модифікувати політику безпеки. Щоб зменшити можливість вторгнення процес електронного документообігу, необхідно

побудувати комплексні заходи захисту на всіх можливих рівнях. Така концепція інформаційної безпеки має на увазі, що є порушенням одного з рівнів захисту та не скомпрометує всю систему в цілому. Побудова та проектування кожного рівня безпеки повинні взяти до відома, що будь-який рівень може мати вразливості, що стане для зловмисника в нагоді. Крім того, кожен з рівнів має свої специфічні і найбільш ефективні методи захисту [23]. З переліку вендорів, які розроблені відомими технологій найбільш підходящих з технічних та економічних чинників досить мало, але можна обрати [24].

Традиційно вважається, що направлення з Інтернету є найбільш вразливим, однак загроза з інших напрямків не менш істотна. Важливо, щоб усі входи та виходи з мережі були надійно захищені. Безперервний контроль над процесом електронного додкументообігу локальної мережі, складової основи будь-якої мережі, для підтримки її в постійному працездатному стані [25].

Контроль – це головна стадія, яка виконується, в першу чергу, за управлінням мережею. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління та реалізують спеціалізованими засобами. Використання автономних засобів контролю забезпечує більше можливостей виявити проблемні частину програмного комплексу та налаштування документообігу в локальній мережі установи [26].

Для вирішення суперечністі між наявними освітньо-професійними потребами та існуючою практикою формування комп’ютерно-інформаційної компетентності державних службовців «Електронний документообіг та захист інформації» є досить важливою складовою по підвищенню компетеності для роботи з електронною та паперовою документацією [27]. Зокрема, необхідно забезпечити надійну автентифікацію користувачів у службі каталогів (єдиному центрі входу), хоч і аутентифікація на рівні сервера та сетевих робочих станцій значно знижує якість безпечної безпеки [28]. Сучасні вимоги передбачають наявність управління комунікаційною сетевою середовищем та розподіл на певні логічні сегменти (VLAN). Для

адміністрування віддалених пристроїв завжди потрібно використовувати підключення по захищеному протоколу (наприклад, SSH).

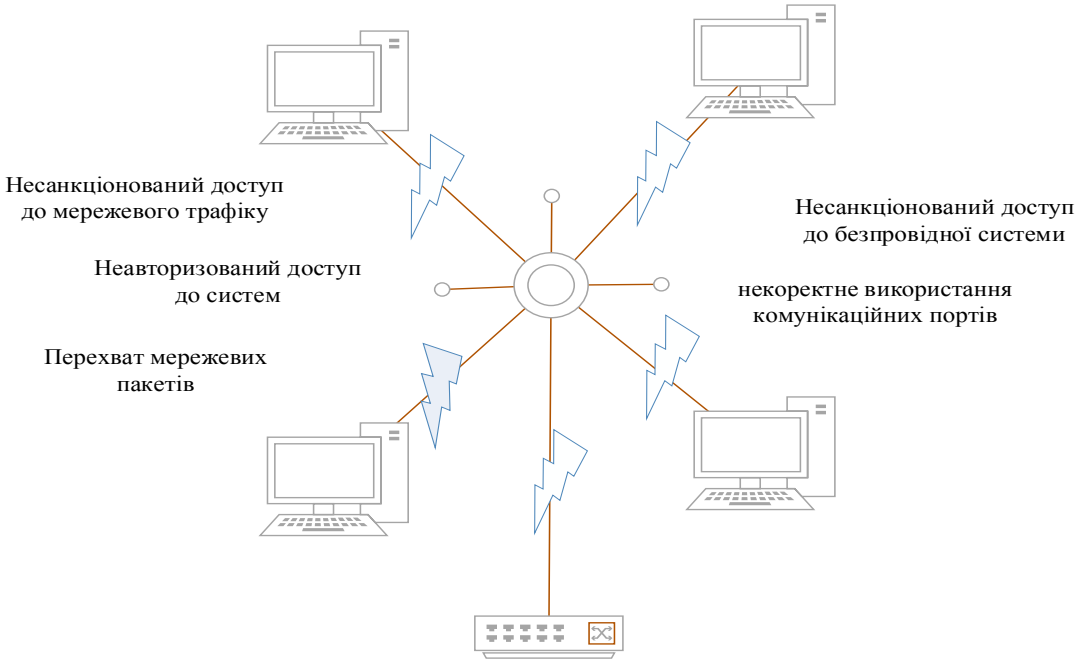

Рисунок 1.2 Загрози локальної мережі при звичайній роботі ЕОМ

Оскільки втрата інформації може відбуватися через суто технічні, об'єктивним і ненавмисним причин, під ці визначення підпадають також і заходи, пов'язані з підвищенням надійності сервера через відмови або збоїв в роботі вінчестерів, недоліків у програмному забезпеченні і т.д. Для забезпечення безпеки інформації та зменшення можливості витоку інформації використовуються наступні засоби та методи:

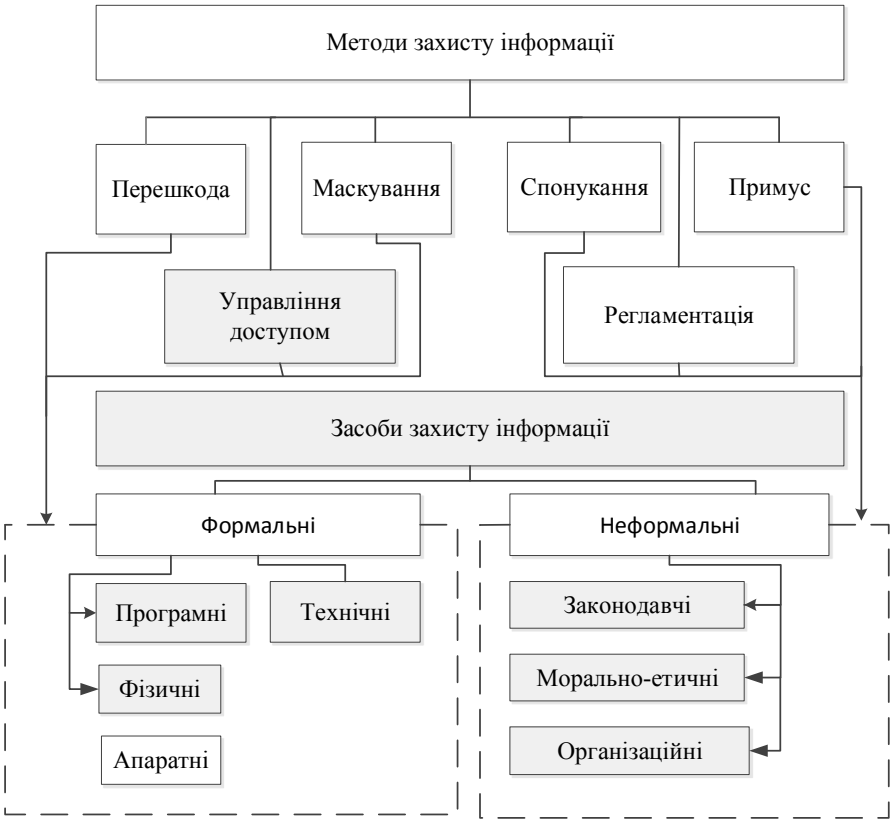

Рисунок 1.3 – Методи та засоби ЗІ в локальних мережах

За рівнем поширення та доступності на першому місці є ПЗ тому далі вони розглядаються більш докладно.

Серед ПЗ щодо захисту електронного докуметнообігу у мережах можна виділити наступні:

1) Архівація даних – програмні засоби, які здійснюють злиття в єдиний файл декількох файлів, але без втрат даних, та з можливістю достиь точного відновлення вихідних файлів.

2) Антивіруси – це розроблені програмні продукти для надійсного захисту даних від вірусів, в тому числі від ШПЗ.

3) Програми-шифрувальники – це програми, що включають в себе забезпечення заиссту електроних документів, та інших файлів від несанкціонованого доступу за допомогою алгоритмів шифрування та аутентифікації.

4) Програми зі встановленням автентичності – програмне забезпечення для перевірки належності відповідного доступу особи з наданими

ним ідентифікаторами входу та підтвердження його автентичності, також визначити його повноваження в системі та контролювання встановлених йому прав в процесі роботи в системі.

5) Засоби під управлінням доступу – це певні грошові затрати, які обмежують реєстрацію для входу до заданої території.

6) Протоколи та аудит – забезпечення збереженнята накопичення інформації про події, які є в інформаційній системі. Аудит забезпечує аналіз всього, що може відноситися до проблем безпеки, або все, що може привести до проблем захисту [8].

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби мережевих ОС [9]. З найбільш часто згадуваних слід зазначити DLP-систему, що дозволяє обмежити інформаційні потоки.

1.5 Компрометація та захист комп'ютерів в глобальній мережі

Навряд чи потрібно перераховувати всі переваги, які отримує сучасне підприємство, маючи доступ до глобальної мережі Internet, але як і багато інших нових технології має та негативні наслідки [8]. Наприклад, необмежений та безконтрольний доступ співробітників організації в глобальній мережі. У будь-якому випадку трафік контролюється провайдером. Але якщо одним каналом користується кілька людей, а то і весь штат співробітників, то може виникнути необхідність вважати трафік для кожного з них окремо. Комп'ютерні системи в мережі виконують завдання, які та визначають вимоги захисту. Мережеві хости можуть підвергати нападу, оскільки вони є публічно доступними. Зловмисники можуть розповсюджувати ШПЗ (віруси) для реалізації розповсюдженої атаки [10]. Встановлення на робочих станціях та серверах програмне забезпечення може мати недоліки на рівні програмного коду. Налаштування політики захисту рівня комп'ютера не повинні забезпечувати та контролювати централізовано, наприклад, за допомогою

групової політики (групової політики). Також, шифрування системи є ще одним з важливих елементів надійного захисту. Крім того, шифрування захищає від несанкціонованого доступу до інформації. Щоб запобігти несанкціонованому видалення, слід використовувати атрибути доступу.

1.6 Системи шифрування та їх можливості

На дисках комп'ютерів, на зовнішніх носіях та в пам'яті мобільних пристроїв зберігається досить значний обсяг даних. Це як незначна інформація, так і дуже дуже цінна, до якої можуть відноситись особисті фотографії, анкетні дані, номери банківських рахунків, медичні записи, інформація для доступу до різних сервісів, рахунки-фактури, результати роботи та інше.

Шифрування файлів, папок, передаваємих через мережу Інтернет даних, спрямована на збереження конфіденційності даних. Залежно від використовуваного методу (алгоритму), воно може бути менш або більш ефективним. Використання мережі Wi-Fi, використовувати інтернет-банкінгу або звичайна розмова по мобільному телефону – це дії, які вимагають шифрування. Воно має ту перевагу, що наші дані надійно захищені навіть в разі фізичної втрати телефону, ноутбука або флешки, а в результаті крадіжки або втрати.

Шифрування – це перш за все, перетворення інформації, що робить її недоступною для стороніх користувачів [29]. При цьому особи, які мають необхідні для входу дані для аутентифікації, можуть провести дешифрування і прочитати вихідну інформацію. Існує безліч способів шифрування та дешифрування, але більшість секретність даних заснована на тому, що ключ шифрування (пароль аутентифіакції) відомий тільки довіреним особам, та в більшості випадків не враховується можливість застосування на таємному алгоритмі, наприклад.

1.7 Аналіз існуючого ПЗ

Ознайомившись з кількома аналітичними матеріалами, які стосуються ринку інформаційної безпеки в Україні було з’ясовано наступне:

– незважаючи на загальну несприятливу ситуацію в країні (Військовий конфлікт «Війна на сході України», епідситуація щодо COVID-19, соціально-економічні проблеми та ін.) ринок інформаційної безпеки в Україні існує та розвивається [30]. Органом, який виступає регулятором в цій сфері і, відповідно, видає ліцензії є Державна служба спеціального зв'язку та захисту інформації в Україні.

– законодавча і нормативна база досить прозоро регламентує питання, що належать входять до державної і банківської таємниці. Однак, якщо розгляднути нормативно-правове поле України детальніше, то більшість нормативних актів, в тому числі прийнятих в кінці 90-х та на початку 2000х років, та досить повільно усередковуються серед сучасних загроз, та судова практика це підтверджує неодноразово [31].

Зокрема, сучасні системи «міжмережевого екрану» (з англ. Firewall, брандмауер – це технології програмних або програмно-апаратних пристроїв), спрямованих на запобігання витоку конфіденційної інформації за межі інформаційної системи підприємства. В даний час основними продавцями світового ринку відносно систем запобігання витоку даних є компанії, які широко відомі іншими своїми продуктами для забезпечення інформаційної безпеки в організаціях. Це, перш за все, Symantec, TrendMicro, InfoWatch, SmartLine Inc, Гарда Технологии, Zecurion, ESET, SearchInform, CoSoSys, Blue Coat, Check Point, Cisco (IronPort), Fidelis, McAfee, RSA, Verdasys, Symantec, Websense.. В загальному, обсяг світового ринку програмних рішень відносно СЗІ оцінюється на 400 млн доларів, що є зовсім не значною мірою в порівнянні з тим же ринком антивірусів. Проте, ринок ПЗ демонструє бурхливе зростання: ще в 2009 році він оцінювався трохи більше 200 млн. Ринок СЗІ знаходиться в

стадії розвитку, і є місце для появи нових вітчизняних компаній, які розроблятимуть нові рішення для усунення кіберінцидентів для інформаційної безпеки електронного документообігу та здатні до забезпечення належного захисту КІ та державної таємниці [1]. Виробники засобів криптографічного захисту інформації (СКЗІ) пропонують різні механізми для інтеграції кріптосредств в інформаційні системи. Існують рішення, які орієнтовані на підтримку систем з Web-інтерфейсом, мобільних серверних, програмних компонентів роботи з електронними документами в локальній мережі[32].

Розробка інформаційного суспільства взаємопов'язана з супроводженням інформаційних технологій в усі сфери суспільного життя [33-34]. Вони інтегруються в програмні продукти компанії Microsoft та в додатки Open Source, забезпечуючи підтримку різних прикладних протоколів та форматів ЕЦП. З урахуванням зростаючої кількості проектів із використанням електронного підпису та появи масових проектів для фізичних осіб, розробникам таких проектів потрібно добре орієнтуватися щодо розробниками рішеннь до електронного підпису, та щоб система була зручна в експлуатації, недорога відносно технічної підтримки. Таким чином, якщо ще декілька років назад головним фактором вибору СЗІ є відповідність вимогам регуляторів, то при сьогоднішній кількості необхідними чинниками є охоплення підтримуваних платформ, можливість інтеграції з прикладним програмним забезпеченням, підтримка мобільних користувачів, можливість інсталювання без прав системного адміністратора та ін .

Рисунок 1.4 – Ринок спеціалізованого ПЗ в Україні, стан на 2020 рік

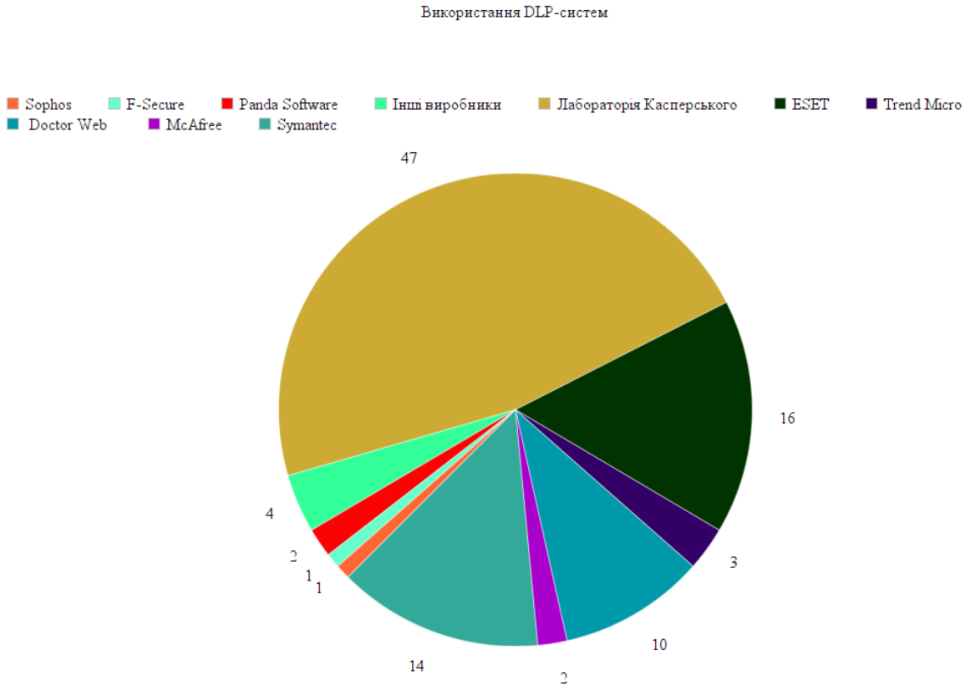

Рисунок 1.5 – Використання DLP-систем на сучасному ринку

В існуючих системах захисту інформації, механізми в певних каналах витоку інформації реалізовані на низькому рівні. У зв'язку з цим виникає ризик несанкціонованої передачі інформації, що захищається. Ринок програмного забезпечення досить різноманітний, є багато продуктів, які своєчасно

виявляють та запобігають витоку інформації. Але комплексних рішень, які забезпечили б активний захист, значно менше. У даній ситуації особливо важливим стає вибір тієї технології, яка зможе забезпечити захист від витоків з незначною кількістю помилкових спрацьовувань.

Зокрема, шифрування даних – це найнадійніший спосіб захисту конфіденційної інформації. Шифрування входить в п'ятірку найбільш затребуваних засобів безпеки. Технології шифрування забезпечують захист прав і свобод людини як особистості. В ході порівняльної характеристики серед сучасних програмних засобів шифруваннння були виділенні наступні: Zecurion Zdisk 7.1a, Secret Disk 4 та Zecurion Zdisk

Основною метою розробки продуктів ЗІ мати можливість сертифікації інформаційних систем в яких дані продукти будуть встановлені, на відповідність вимогам держкомісії. Така сертифікація є обов'язковою для інформаційних систем в яких обробляється держ. таємниця, що в основному забезпечує попит на програмні продукти з боку держ підприємств. Тому, набір функцій реалізованих визначався вимогами відповідних документівя, що в свою чергу спричинило той факт, що більша частина реалізованого в продуктах функціоналу, або дублює штатний функціонал Windows (очищення об'єктів після видалення, очищення ОЗП), або його неявно використовує (дескріцірнний контроль доступу). А розробники DallasLock пішли ще далі, реалізувавши мандатний контроль доступу своєї системи, через механізм дескріціонного контролю до ОС Windows та її фунціоналу, включаючи процеси та служби.

Практичне застосування подібних продуктів вкрай не зручно, наприклад DallasLock для установки вимагає переразбівкі жорсткого диска, яку до того ж треба виконувати за допомогою стороннього ПЗ. Дуже часто після проходження сертифікації ці системи віддалялися або відключалися.

1.8 Політика конфіденційності СЗІ для підприємства

Важливою концепцією в проектуванні і аналізі безпечних систем є модель безпеки, що реалізує прийняту в інформаційній системі політику безпеки [11]. Модель безпеки перетворює абстрактні мети політики в терміни інформаційних систем, точно описуючи структури даних, засоби і методи, необхідні для реалізації політики безпеки. Також слід звернути увагу на систему звітності та набори переднастроєних політик безпеки, які подаються DLP-рішенням, так як це допоможе уникнути деяких проблем і складнощів при впровадженні.

Політика конфіденційності – це важлива частина підприємства, що описує правила збору, зберігання і поширення КІ. Нерідко описується в документі «Положення про інформаційну політику». Під політикою безпеки розуміють сукупність документованих рішень, прийнятих керівництвом організації та спрямованих на захист інформації. Політика безпеки передбачає накреслення мети без конкретизації того, як вони повинні бути досягнуті.

Найбільш часто політики конфіденційності організації визначають інформацію, що становить комерційну таємницю у вигляді переліку, що затверджується генеральним директором підприємтсва чи установи [12]. Крім переліку інформації, керівник установи вказує список осіб, які здійснюють контроль за дотриманням у порядку встановленого при поводженні зі конфіденційною інфомрацією.

Типові види інформації, що містяться в переліку КІ:

- перелік конфіденційної документації;
- персональні дані співробітників;
- перелік ПІБ співробітників;
- електронні ключі.

Надалі, при використанні системи контролю та захисту електронного документовобігу, відповідальна особа за безпеку інформації в середині підприємства використовує даний перелік для задання необхідних правил та

шаблонів цих систем з використанням методів, розглянутих вище. Для цього виконується наступний набір дій:

1) задання шаблонів «персональні дані» (паспорт, ПІБ, телефон);
2) задання відбитків документації та інших конфіденційних файлів;
3) створення словників на базі конфіденційної документації;
4) задання таблиці замін;
5) задання системи політики та умови для спрацьовування.

1.9 Постановка задачі

Для створення системи захисту електронного документообігу в локальній мережі необхідно проаналізувати потоки інформації, які будуть циркулювати всередині неї [14]. Також бажано по можливості мінімізувати витрати на реалізацію даного проекту, але в той же час намагатися не нехтувати якістю використовуваних матеріалів і устаткування.

Мета кваліфікаційної роботи (проєкту) – це розробка системи захисту для електронного докумертообігу в локальній мережі підприємства та підготувати проект програмного засобу до впровадження. Завдання, які повинні вирішувати програмний продукт наступні:

- налаштування політики безпеки в локальній мережі;
- захист інформації від витоку шляхом контролю виведення даних на друк;
- блокувати спроби пересилання конфіденційних електронних документів;
- використання та відстеження електронних документів, генерація попереджувальних повідомлень при порушенні політики безпеки;
- запобігання витоків інформації шляхом контролю життєвого циклу конфіденційних відомостей електроного документообігу;
- моніторинг системних подій та виконувати дії певні в політиках інформаційної безпеки;
- аналізувати використовувані дані, на предмет їх конфіденційності і, за деяких умов;
- шифрування документів 2-го рівня секретності.

Тому – актуальним завданням є створення систем захисту електронних документів від несанкціонованої передачі та використання.

Для досягнення зазначеної мети необхідно виконати ряд завдань:

1) Проаналізувати предметну область та виділити список вимог.
2) Порівняння існуючого програмного забезпечення.
3) Визначитись з функціональністю розроблюваної системи.
4) Побудова структури інформаційної безпеки програмного продукту.
5) Обрати програмні засоби розробки.
6) Розробка програмного продукту.
7) Провести тестування в рамках розробленого комплексу системи.

РОЗДІЛ 2
РОЗРОБКА ПРОЕКТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Ескізний проект

2.1.1 Загальні принципи побудови СЗІ для LAN

Принцип роботи СЗІ полягає в аналізі всієї інформації: виходить, що входить і циркулюючої всередині компанії. СЗІ за допомогою алгоритмів аналізує, що це за інформація та у випадку, якщо вона критична – блокує передачу або повідомляє про це відповідального співробітника негайно. Доступ до каналів передачі блокується в залежності від рівня допуску користувача та рівня секретності інформації з якої ведеться робота. Для реалізації цього принципу зазначені продукти використовують механізм повноважного розмежування доступу [14]. Цей механізм зустрічається не дуже часто, тому зупинюся на ньому докладніше.

Функції систем контрюлю локальной мережі:

– контроль над переміщенням інформації як на рівні комунікацій із зовнішньою мережею, так і на рівні кінцевих пристроїв користувачів (рис. 1.5);

– сканування зберігаються файлів і баз даних для виявлення місць розташування конфіденційної інформації.

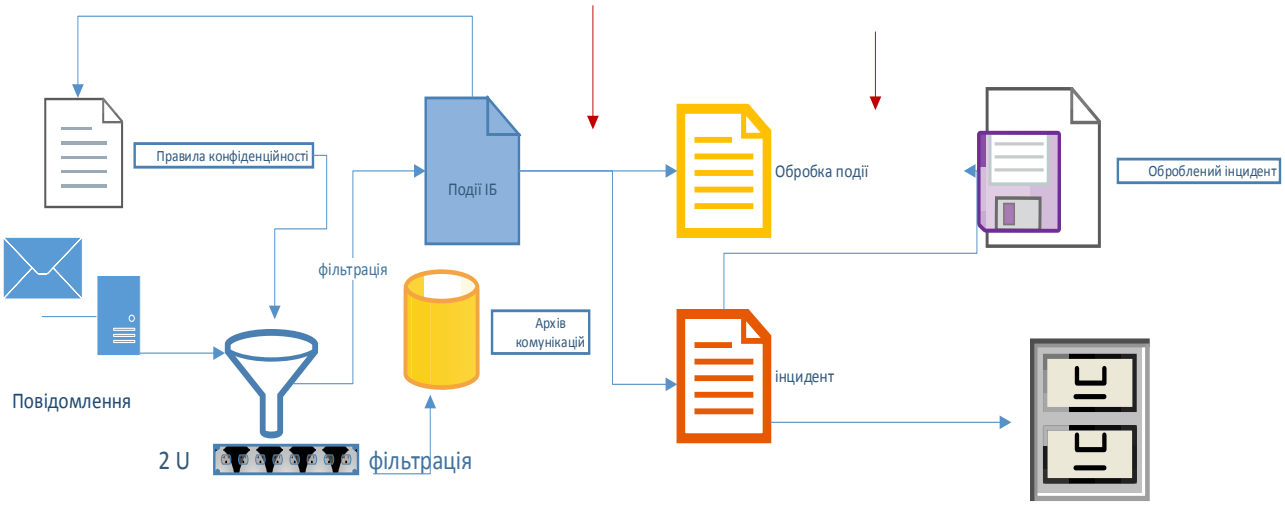

Рисунок 2.1 – Принцип роботи програмного продукту

Повноважний контроль доступу в порівнянні з дескріціонним, полягає в тому, що власник ресурсу не може послабити вимоги на доступ до цього ресурсу, а може лише посилювати їх в межах свого рівня та компетентності. Можливість послаблювати вимоги має можливість користувач наділений особливими правами, наприклад: адміністратор інформаційної безпеки.

При впровадженні на підприємстві рішення щодо супроводження електронного документообігу необхідно врахувати ряд нюансів, від яких залежить ефективність захисту: розшифровуваити SSL –обов'язковий елемент інсталяції DLP-шлюзу, але не всі DLP-системи вміють виконувати цю функцію, тому часто потрібно додаткове рішення для SSL-offload; опрацювання політик офлайн-режиму – DLP-агент повинен продовжувати працювати в режимі активного сканування також і поза офісної мережі; настройка політик не тільки за регулярними виразами, але також і за заданими зразками – фінгерпрінт (метадані файлу, хеші блоків тексту з імовірнісним аналізом і ін.); обмеження використання різних поштових агентів і web-браузерів, так як DLP-агенти розроблені не для всіх варіантів реалізації призначеного для користувача ПЗ; у випадку з мобільними пристроями бажано використання концепції EMM (Концепція Enterprise Mobility Management (EMM) включає в себе наступні компоненти: Mobile device management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM).) і забезпечення стандартизації мобільних пристроїв (наприклад, використання тільки пристроїв Samsung, так як дана платформа має глибоку інтеграцію з EMM-системами, відмова від використання мобільних платформ Windows).

2.1.2 Методи аналізу потоків даних для СЗІ

Завдання розбору потоків даних є виявлення секретної інформації, що впевнено можна назвати складною задачою [14]. Оскільки пошуки необхідних потоків даних ускладнений безліччю умов. Тому, на теперішню добу створено багато технологій для детектування зусиль передачі секретних цих. Будь-яка з їх виділяється від інших власним принципом роботи. Всі методи витоків можна

поділити на 2 групи. До першої - технології, які засновані на розборі конкретно самих слів переданих звісток або паперів (морфологічний і статистичний розбори, трафарети). За аналогічностьі з противірусною охороною їх можливо назвати проактивними. Іншу групу складають швидкі методи (Числові сліди і спритності). Вони призначають витоку за властивостями паперів або присутності в їх особливих спритність.

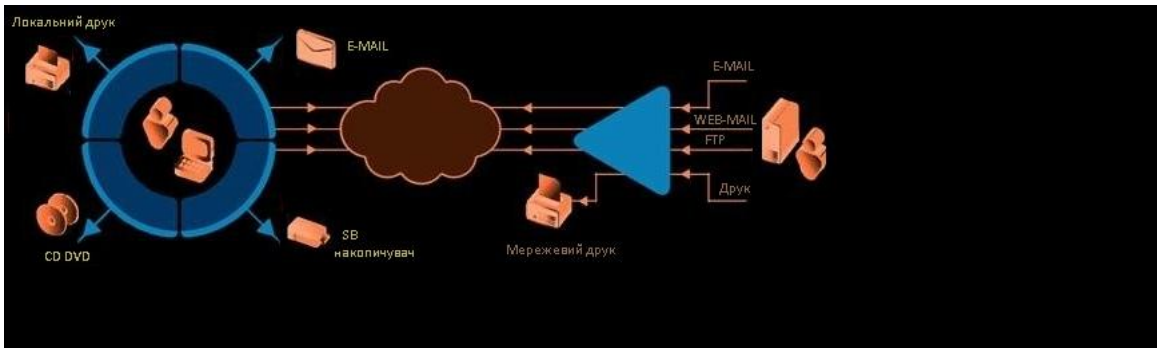

Рисунок 2.2 Інформаційні потоки, контрольовані за допомогою ПЗ

Основними модулями розробленого ПЗ є:

– перехоплювачі / контролери на різні канали передачі інформації;
– агентські програми, що встановлюються на кінцеві пристрої;
– центральний керуючий сервер.

На рис. 2.3 наведено приклад розміщення модулів СЗІ на пристроях інформаційної системи організації.

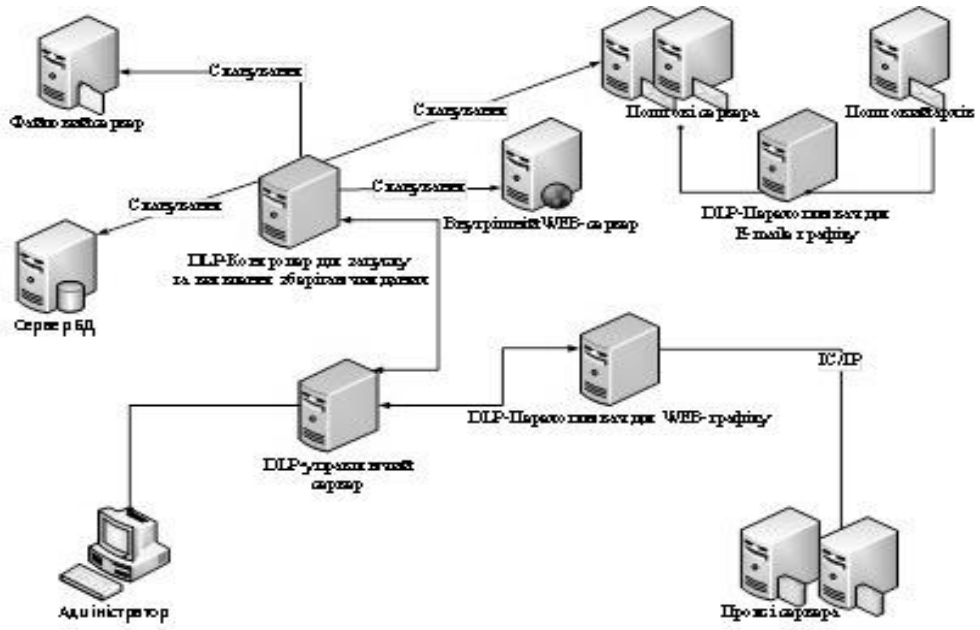

Рисунок 2.3 – Приклад розміщення модулів DLP-системи
на пристроях інформаційної системи організації

Перехоплювачі(сніфери) аналізують потоки інформації, яка може бути виведена за межі інформаційної системи організації, виявляють конфіденційні дані, класифікують інформацію і передають для обробки можливого інциденту на керуючий сервер. Перехоплювачі можуть, як копіювати вихідний трафік, так і перешкоджати його передачі за межі інформаційної системи організації. В останньому випадку потенційна витік може бути зупинена системою DLP.

Контролери для виявлення даних, що зберігаються запускають процеси виявленнях в мережевих ресурсах конфіденційної інформації [15]. Способи запуску виявлення можуть бути різними: від власне сканування від сервера контролера до запуску окремих програмних агентів на існуючі сервери або робочі станції. Контролери для операцій на робочих станціях розподіляють політики безпеки на кінцеві пристрої, аналізують результати діяльності співробітників з конфіденційною інформацією і передають дані можливого інциденту на керуючий сервер. Програми-агенти на кінцевих робочих місцях помічають конфіденційні дані в обробці та стежать за дотриманням таких правил, як збереження на змінний носій інформації, відправки, роздрукування, копіювання через буфер обміну. Керуючий сервер зіставляє надходять від

перехоплювачів і контролерів відомості і надає інтерфейс опрацювання інцидентів і побудови звітності. Сучасні рішення ЗСІ здатні детектувати не тільки цілі файли, але і їх фрагменти. При цьому можна навіть розрахувати ступінь відповідності. Такі рішення дозволяють створювати диференційовані правила, в яких описані різні дії для різних відсотків збігу [16]. Залежно від їх наявності система дозволяє або забороняє ті чи інші дії з файлами. Це дозволяє не тільки запобігти витоку конфіденційних документів, а й обмежити роботу з ними користувачів, що є безперечною перевагою даної технології.

2.1.3 Алгоритм роботи відділу ЗВО в конкретній ОС

В першу чергу документообіг будь-якої організації можна розділити на внутрішній і зовнішній залежно від його спрямованості. ористувачами внутрішніх документів є:

– співробітники;
– керівники.

Інші користувачі ззовні по необхідності або вимозі Закону, при цьому, як правило, їм або передаються копії, а не оригінали.

У внутрішніх документах присутні тільки підписи відповідальних осіб, багато хто навіть не вимагають друку. Внутрішнє листування може вестися і зовсім в безпаперовому форматі. Співробітник ідентифікується за логіном або адресою пошти (видаються при працевлаштуванні). Обсяги технічної роботи з документами іноді заміняють основний зміст діяльності організації [17]. Розгядаючи детальніше це питання, то в середині локальної мережі будь-якого ЗВО значна кількість електронного документообігу, поділяється за відділами, створюються та погоджується у загальному відділі: інформаційно-довідкові планові, звітні, та організаційні документи. Особливістю є створення на основі погодження індивідуальних особливостей структурт кожного вишу [18]. Саме тому, електронний документооіг перейшов до сучасних технологій та потребує досить серйозного захисту від такої кількості документації.

Згідно з аналізів за системою електрнного документообігу ВЗО функціонують п'ять загальних важливих документопотоків:

1) документи з контролем виконання;

2) підготовчі та узгоджені проекти документів.

3) службова кореспонденція;

4) нормативні документи установи(в);

5) організаційні документи навчального процесу;

Обмін даними між базовими автоматизованими системами в межах однієї локальної комп'ютерної мережі ЗВО забезпечується шляхом стандартного механізму обміну через "вхідні", "вихідні скриньки", реалізується у вигляді SQL - таблиць стандартної структури. Обмін даними між територіальними представництвами, де також встановлені базові автоматизовані системи, реалізується шляхом транспортної поштової служби корпоративної мережі ЗВО.

2.1.4 Функціональний аналіз проекту будови програмних компонентів для локальної мережі

Спираючись до аналізу предметної області, можна перейти до проектування та реалізації поставлених питань. На початкових етапах створення технології ЗІ від внутрішніх загроз і витоків необхідно зрозуміти, як працює локальна мережа організації, роботу якої збираються автоматизувати [19]. Для опису роботи підприємства необхідно побудувати модель Така модель повинна бути адекватна предметної області; отже, вона повинна містити в собі знання всіх учасників бізнес-процессоворганізації [20].

Побудуємо контекстну діаграму (DFD), що дозволить виявити сутності, які приймають участь у функціонуванні роботи програмного продукту, процеси, що в ній відбуваються, та інформацію, яка переходить від користувачів до програми й навпаки. Для виявлення секретної інформації пропонується метод збору та аналізу інформації, схема якого представлена на рис. 2.4

На підставі дослідження підприємства була побудована функціональна модель варіантів використання пакету програм адмінімтратором та користувачем представлена на рис. 2.4 та рис. 2.5 .

При формалізації предметної області «Пошук, моніторинг та захист конфіденційної інформації» були виявлені наступні об'єкти DFD:

Процеси:

1) Моніторинг;
2) Блокування;
3) Індексування КІ;
4) Формування звітів;

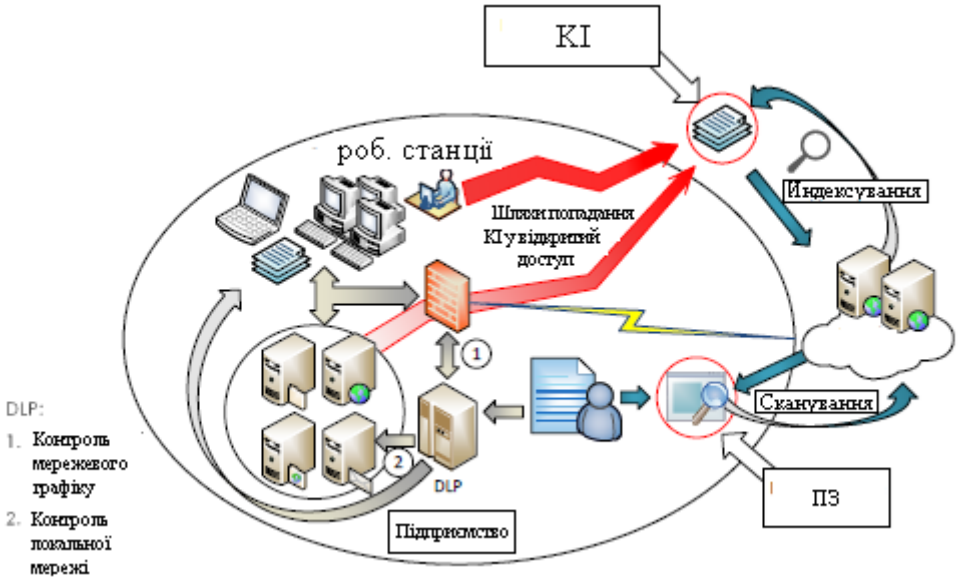

Рисунок 2.4 – Контекстна DFD діаграма процесу пошуку конфіденційної документації підприємства за допомогою DLP-системи

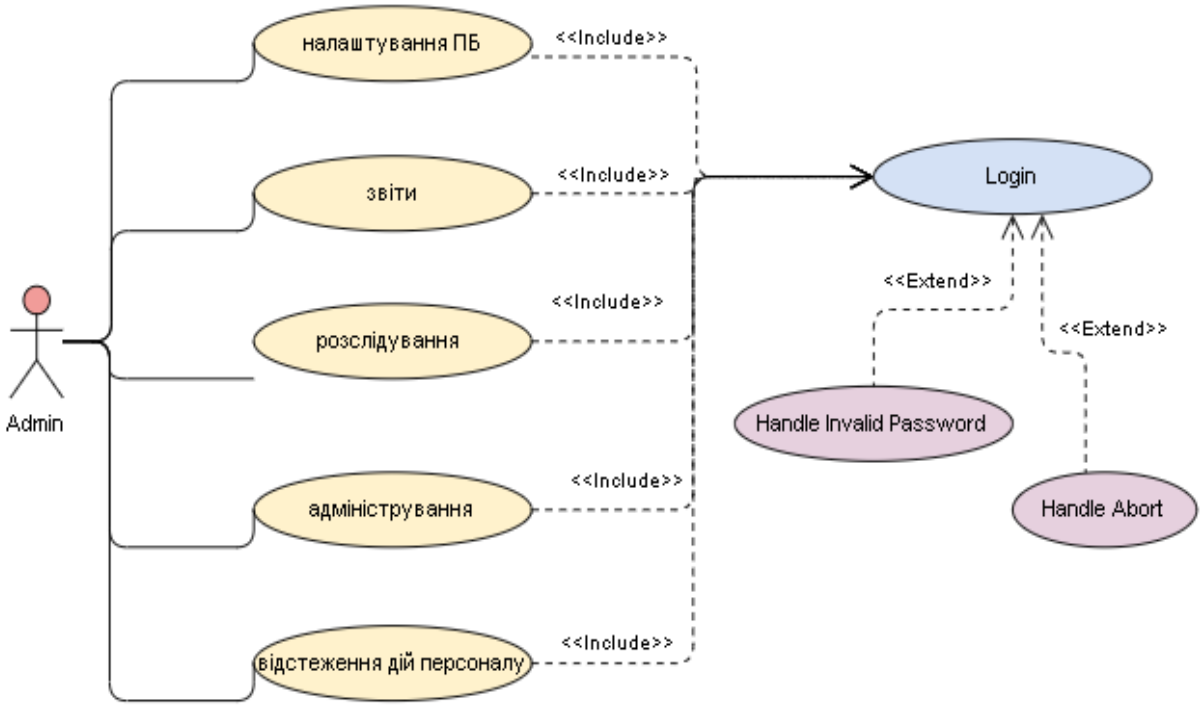

Рисунок 2.5 – Діаграма варіантів використання компонентів програми адмінімтратором

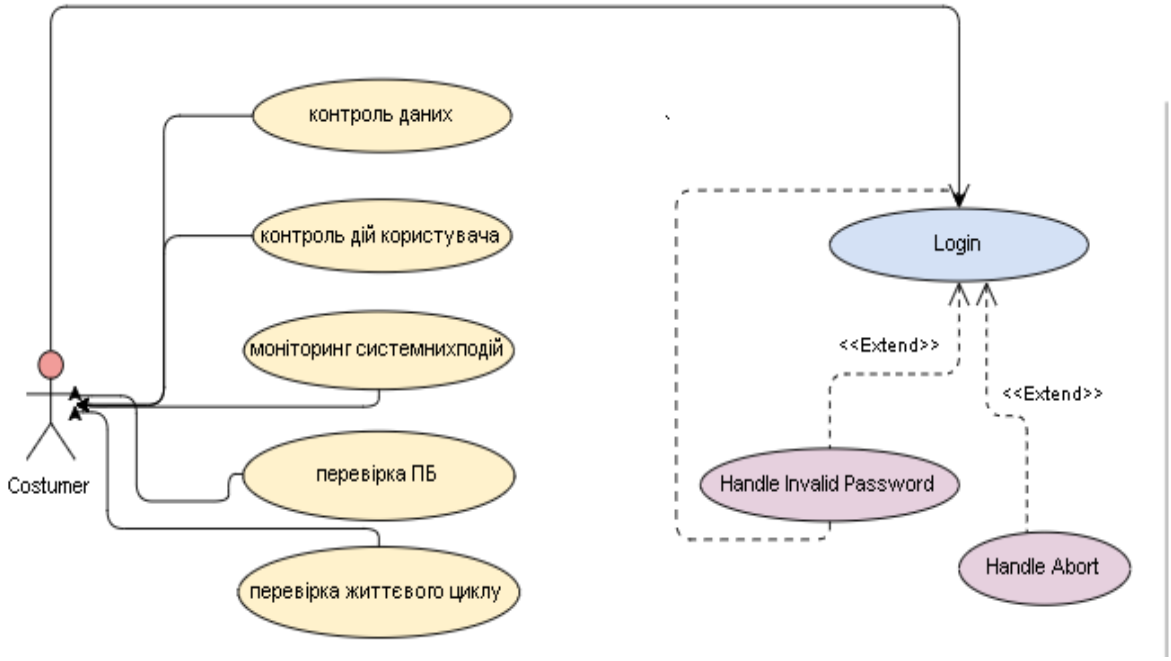

Рисунок 2.6 – Діаграма варіантів використання компонентів програми користувачем

2.1.5 Розробка структури даних

Структурна схема – це схема, яка визначає основні функціональні частини виробу, їх взаємозв'язки та призначення. Під функціональною частиною розуміють складову частину схеми: елемент, пристрій, функціональну групу, функціональну ланку.

Рисунок 2.7 – Загальна структурна схема DLP-системи

Структурна схема призначена для відображення загальної структури пристрою, тобто його основних блоків, вузлів, частин та головних зв'язків між ними. Із структурної схеми повинно бути зрозуміло, навіщо потрібний даний пристрій і як він працює в основних режимах роботи, як взаємодіють його частини. Позначення елементів структурної схеми можуть обиратись довільно, хоча загальноприйнятих правил виконання схем слід дотримуватись.

2.1.6 Діаграма станів програмного забезпечення

Діаграма станів DLP-системи описує можливі стану екземпляра класу «Моніторинг» і можливі послідовності його переходів з одного стану в інше (рис. 2.8)

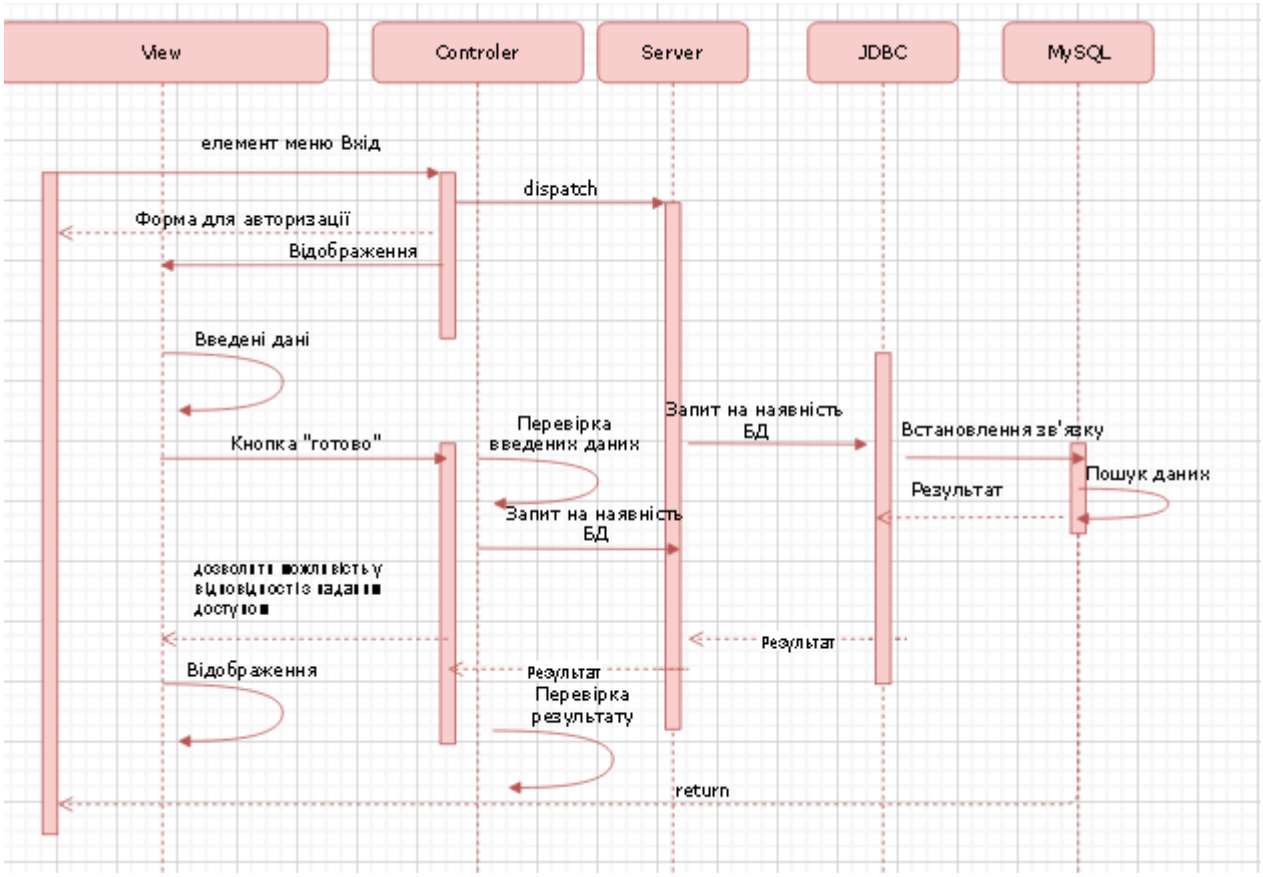

Рисунок 2.8 – UML-діаграма станів

2.2 Технічний проект

2.2.1 Декомпозиція моделі проекту програмного забезпечення

Структурна декомпозиція (дерево) розподілу ризиків по роботах проекту – структурна декомпозиція ймовірності ризикових подій з різних аспектів проекту (технічних, фінансових, організаційних і т. д.) При виконанні робіт проекту і оцінок їх впливу на результати виконання робіт і здійснення проекту в цілому. WBS визначає всі елементи проекту в рамках ієрархічної структури і вказує на їх відношення до кінцевого продукту проекту. Нижче на рис. 2.9 представлена структурна декомпозиція проекту розробки СЗІ з різними рівнями

деталізації робіт і цілей проекту, а також розподіл відповідальності між підрозділами організації в рамках структурної декомпозиції проекту.

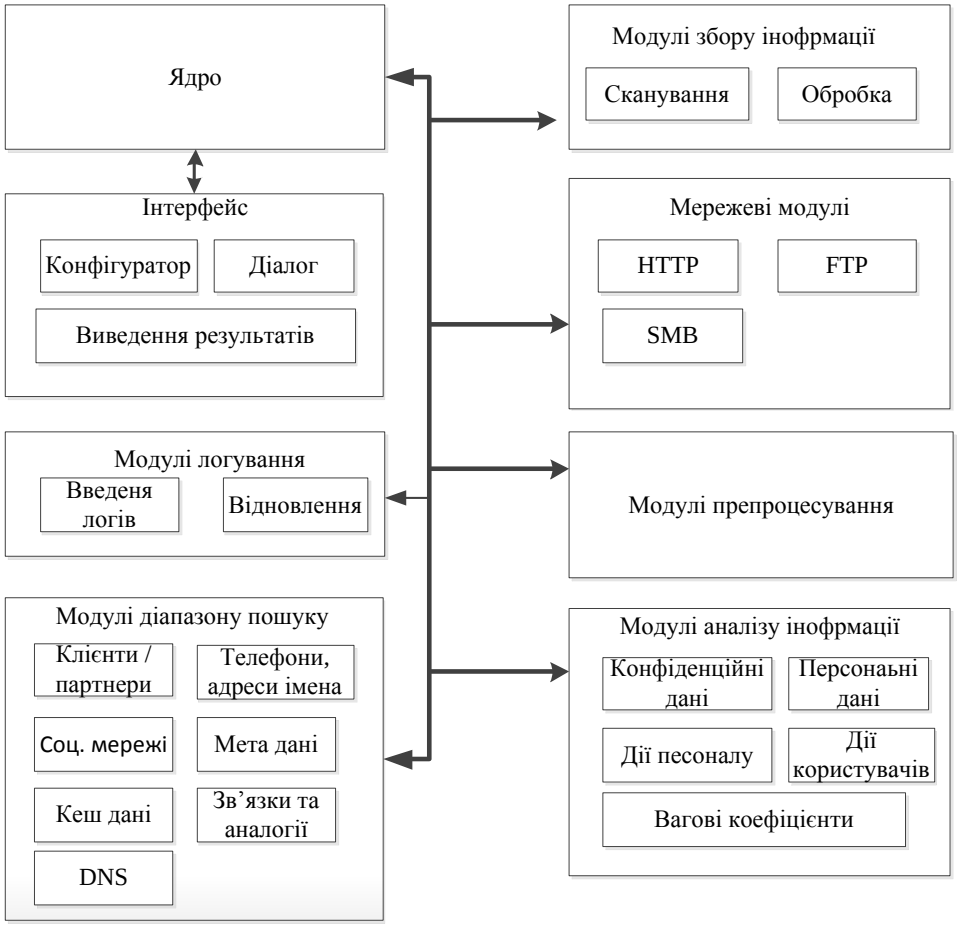

Рисунок 2.9 – Структурна декомпозиція проекту СЗІ

2.2.2 Деталізація потоків даних першого та другого рівня

При отримані на першому етапі контекстні діаграми відображається укрупнена модель бізнес процесів досліджуваної предметної області. Потоки даних, що входять до процесу і виходять з процесу контекстної діаграми переносяться на діаграму другого рівня. При цьому, вхідні потоки служать джерелом інформації для процесів деталізованої діаграми, а вихідні – результатом виконання процесів.

В результаті деталізації виходить діаграма першого рівня, отримана модель не в повній мірі докладно описує розглянуті бізнес процеси, необхідно проводити подальшу деталізацію шляхом побудови діаграм другого рівня. Тому, отриманий набір діаграм другого рівня, що описують процеси першого

рівня більш докладно. Так як наведена на рис. 2.10 діаграма потоків даних є укрупненою, а на рис.2.11 приведена DFD діаграма, що деталізує структуру СЗІ.

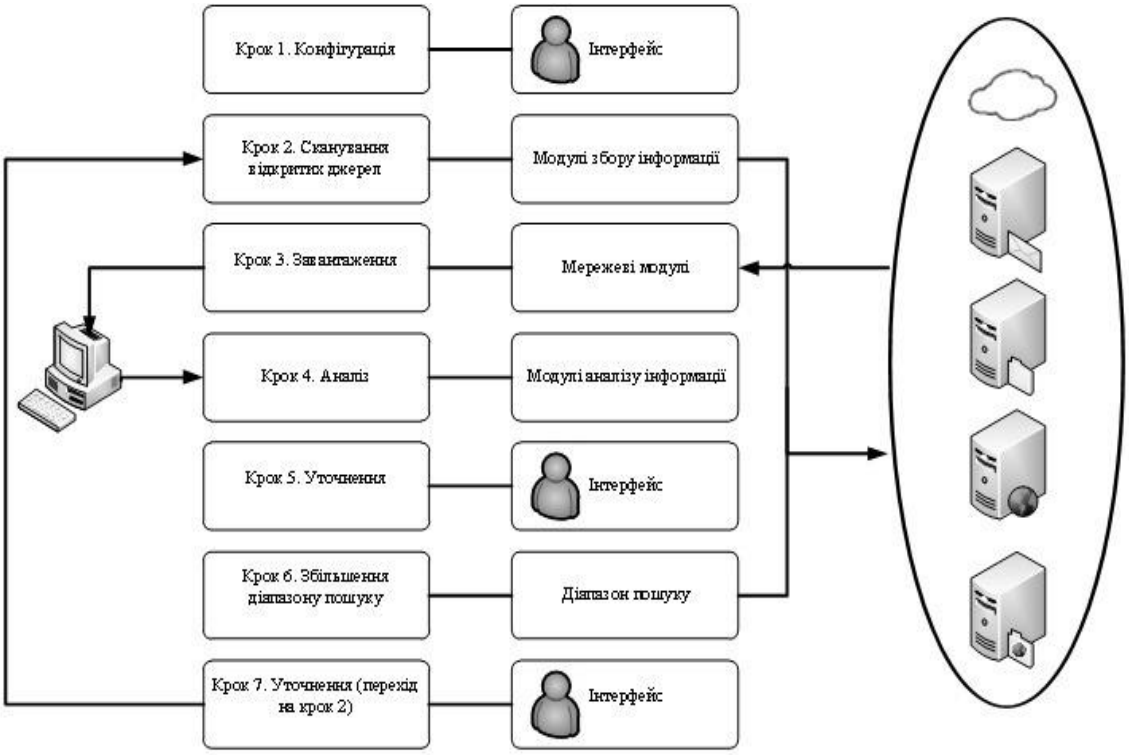

Рисунок 2.10 – DFD-Діаграма деталізації процесу пошуку конфіденційної документації підприємства за допомогою СЗІ

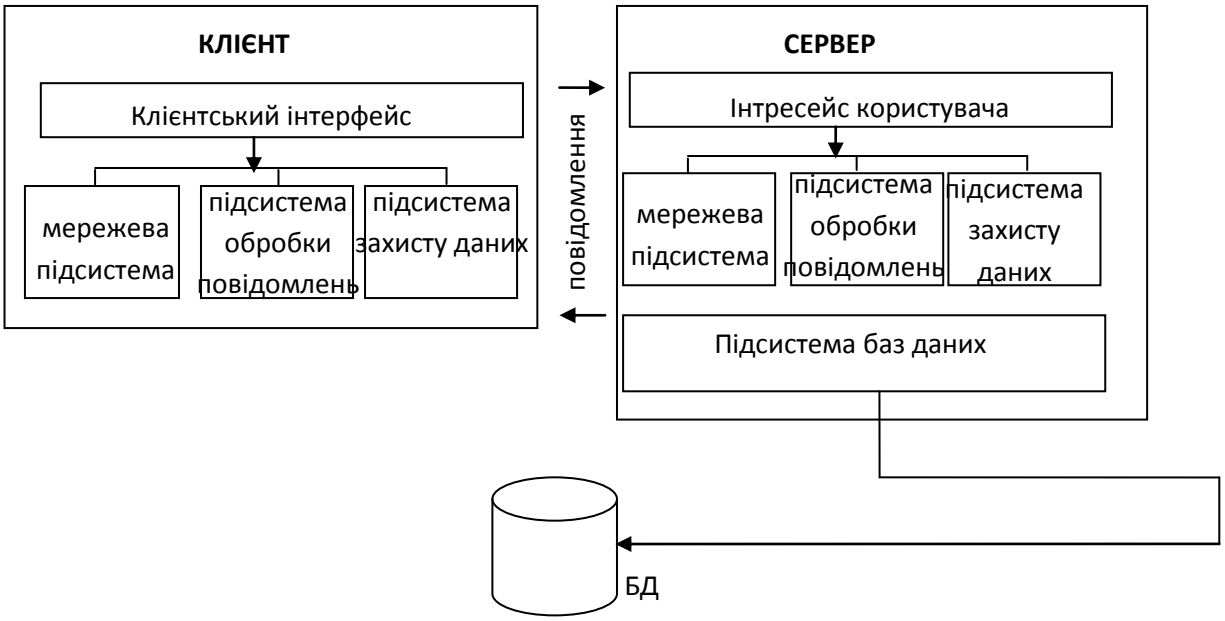

Рисунок 2.11 – Деталізація «Структура системи ПЗ»

2.2.3 Дослідження потоків даних процесів

Одним з найважливіших способів опису процесу є діаграми потоків даних. Діаграми потоків даних можна використовувати як доповнення до моделі IDEF0 для більш наочного відображення поточних операцій документообігу в корпоративних системах обробки інформації. Схема процесу в форматі DFD показана нижче (рис. 2.12).

Діаграми верхніх рівнів ієрархії (контекстні діаграми) визначають основні процеси або підсистеми з зовнішніми входами і виходами. Вони деталізуються за допомогою діаграм нижнього рівня. Така декомпозиція триває, створюючи багаторівневу ієрархію діаграм, до тих пір, поки не буде досягнутий рівень декомпозиції, на якому деталізувати процеси далі втрачає сенс.

Потоки даних:

- перелік конфіденційної документації;
- персональні дані співробітників та клієнтів;
- електронна документація;
- електронні ключі.
- держ.стардарти;
- політика безпеки;
- інтернет трафік;
- електроні паролі.

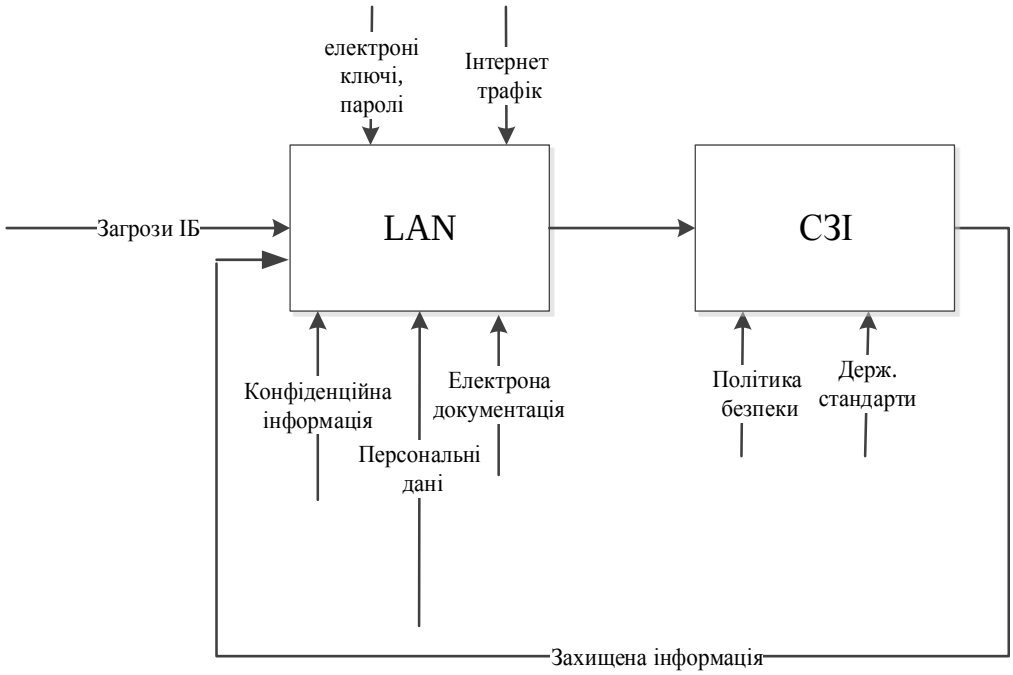

Рисунок 2.12 – Фукціональна діаграма потоків даних СЗІ для локальної мережі нульового рівня

2.2.4 Загальний опис модулів програмного забезпечення

Модулі – це невеликі програмні блоки, координовані ядром, що виконують різні вузькоспрямовані завдання. Діляться на типи, згідно виконуваної ними задачі:

- модулі збору інформації;
- модулі препроцессірованія;
- модулі розширення діапазону пошуку;
- модулі аналізу;
- модулі логірованія;
- мережеві модулі.

Вибір модульної архітектури забезпечує хорошу масштабованість і гнучкість. Число модулів не обмежена. Кожен тип модулів повинен мати свій строго обумовлений формат вхідних і вихідних параметрів:

1) Модулі збору інформації.

Основним завданням є сканування. Здійснюють запити у системі, отримуючи посилання на документи, працюють з документацією, зберігають сторінки.

2) Модулі розширення діапазону пошуку.

Основним завданням є збільшення границь для пошуку, отримавши нові данні для подальших стадій пошуку:

– зі зв'язків та аналогій;

– по користачам;

– мета дані (дата, відомості про файли, відомості про систему, відомості і користувачів, заголовках і т.д.);

– телефони, адреси, імена, їх зв'язку;

– DNS / whois / Shodan;

– використання кешованих версій сторінки і веб архіву даних інтернету;

–соціальні мережі (аналіз відомих профілів в соціальних мережах, телефонів, адрес, геопозіцій на фотографіях, викладених документів і зв'язків).

3) Модулі аналізу.

Основне завдання – аналіз викачаних документів на предмет відповідності заданим критеріям. Використовуються алгоритм 3 з ваговими коефіцієнтами. Значення коефіцієнтів підібрані експериментальним шляхом і забезпечують ефективне ранжирування результатів. Під час аналізу документа можна отримати додатковий інформацію, шляхом алгоритмами нейроних мереж, які є досить ефективні останім часом [5].

4) Модулі логувагування.

Основне завдання – ведення логів, що дозволяють аналізувати поведінку ПО, збирати інформацію про помилки. Додаткове завдання – забезпечення можливості відновлення системи після збоїв.

5) Мережеві модулі.

Основне завдання – завантаження документів для можливості локального аналізу через протоколи: HTTP, FTP, SMB.Програмні модулі також зображені на рис. 2.9 (стр. 39) відповідно декомпозиції моделі проекту ПЗ.

2.2.5 Специфікації програмних модулів

Специфікація програмного модуля складається з функціональної специфікації модуля, яка описує семантику функцій, які виконуються цим модулем по кожному з його входів, і синтаксичної специфікації його входів, що дозволяє побудувати на використовувану мову програмування синтаксично правильне звертання до нього. Функціональна специфікація модуля визначається тими ж принципами, що і функціональна специфікація програмної системи (рис. 2.13).

Рисунок 2.13 – Специфікація процесів системи

За данними клієнта системи, менеджера здійснюється пошук в базі користувачів, визначаючи його за категоріями. За визначеною категорією відповідно встановлюється повноваження, які будуть надаватись клієнту (користувачу) системи. Далі – здійснюється процедура доступу до системи, що

перевіряє відповідність ім'я, пароль, логін та додаткові дані, зазначні адміністратором системи, для доступу в систему чи відповідно до ЕОМ на якому вона встановлена. Для користувача формується набір деякиї дозволених дій, об'єднуючи інформацію на повноваження та рівні доступу до системи, чи дією з відповідною документацією. Тому, визначення рівня доступу до системи мє бути, як показано на рис. 2.14.

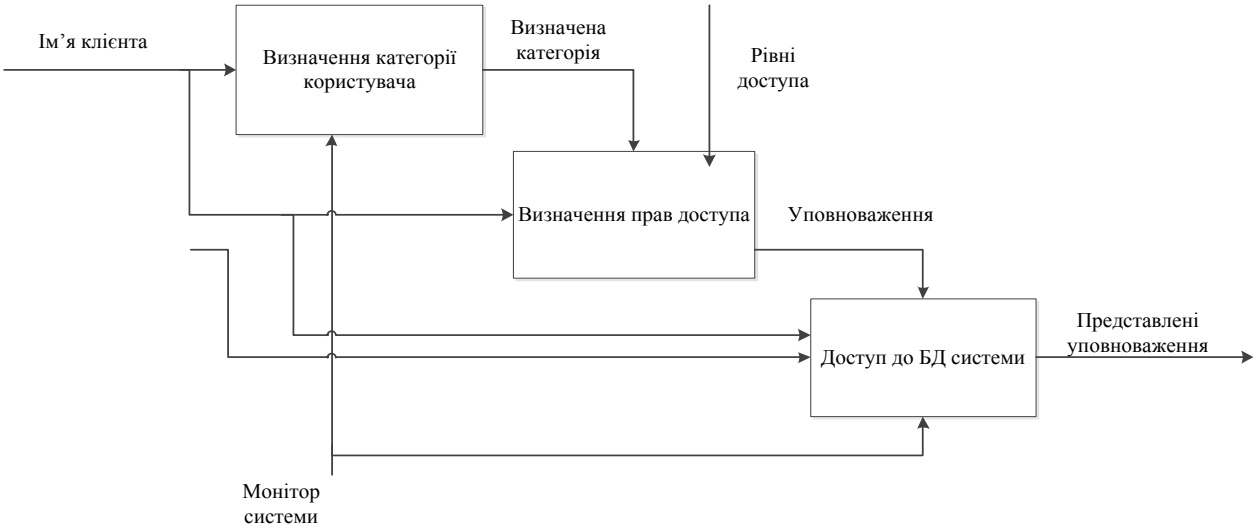

Рисунок 2.14 – Декомпозиція процесу
«Визначення рівня доступу до системи»

2.2.6 Розробка логічної моделі бази даних

Побудована діаграма класів (рис. 2.15) розбита на 3 пакета:

«Зовнішня модель» – містить зовнішні по відношенню до підсистеми класи;

«Об'єктна модель» – містить об'єктну модель, що додається розробляються плагіном «Побудова алгоритму»;

«Логіка» – містить основні керуючі класи, що реалізують бізнес-логіку побудови маршрутів.

Діаграма класів для реалізації приведена на рис. 2. 16

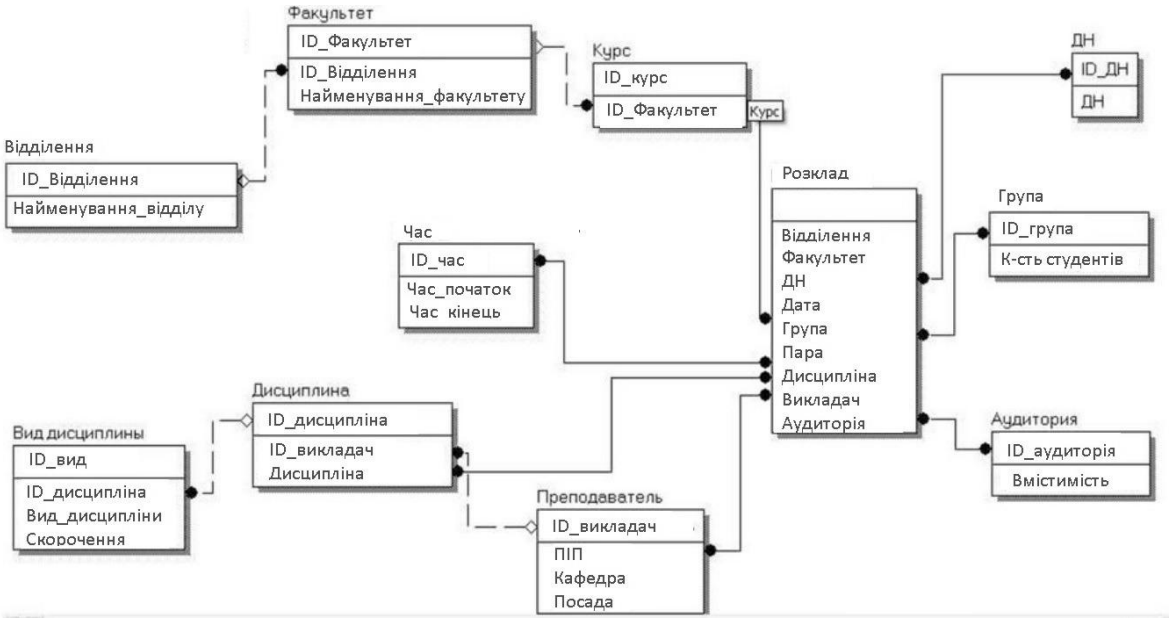

Рисунок 2.15 – «Діаграмма класів»

2.2.7 Нормалізація бази даних

Нормалізація призначена для приведення структури БД до виду, що забезпечує мінімальну логічну надмірність, та не має на меті зменшення або збільшення продуктивності роботи або ж зменшення або збільшення фізичного обсягу бази даних. Після того як закінчився процес щодо отримання доступу до системи (рис.2.16) міжекраний монітор здійснює аналіз на запит користувача, та вибравши підсистему, що обробляє запити. Так як, користувач системи буде розгядатати внутрішні алгоритми та його процесу роботи, автоматично буде обрана підсистема, без вибору користувача, тому декомпозиція звернення до підсистеми лише ускладнює модель. Надалі декомпозицією «Обробка запиту користувача» (рис. 2.17), для виконання підсистеми обробки запиту, здійснюється встановлення повноваження користувачів даної системи. Перед тим, як здійснюється пошук відповідей щодо запиту, відкривається БД (підключившись до неї). У загальному випадку БД перебуває на віддаленому сервері, тому в будь-яких момент може знадобитися встановлення з'єднання з нею. Визначимо послідовність робіт:

1. Відкриття БД.
2. Виконання запиту.

3. Генерація звітів.

Після того як відкрити БД потрібно вказати в системі: з'єднання з БД, після чого виконується запит та згенерується звіт для користувача системи (рис.2. 18).

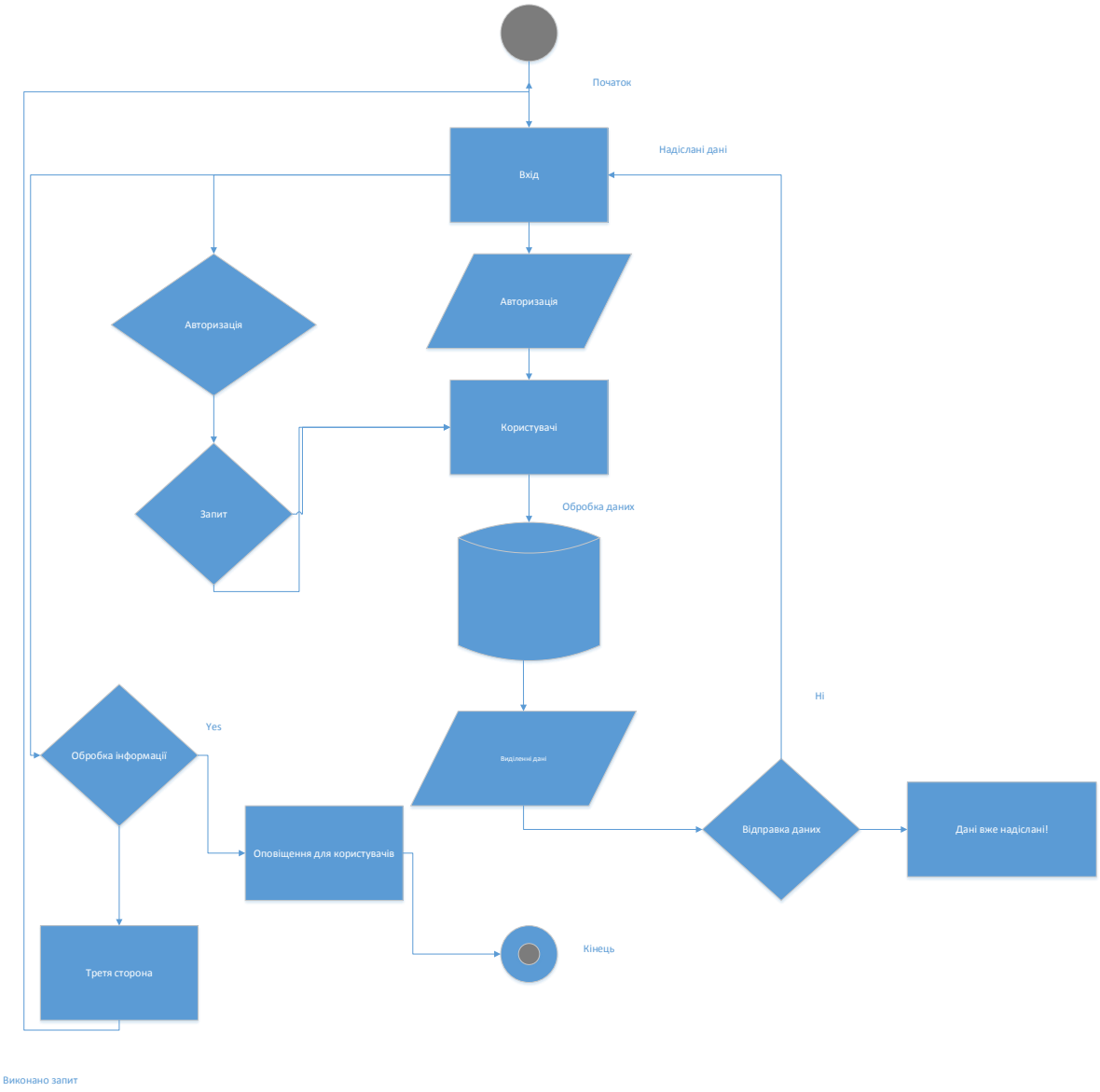

Рисунок 2.16 – Блок-схема процесу
«Входу в систему користувача та адміністратора»

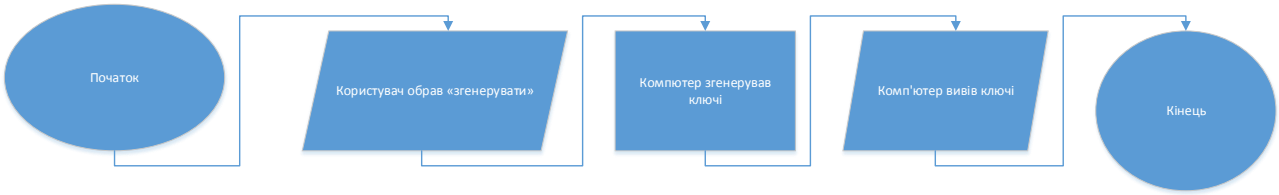

Рисунок 2.17 – Блок-схема процесу «Шифрування»

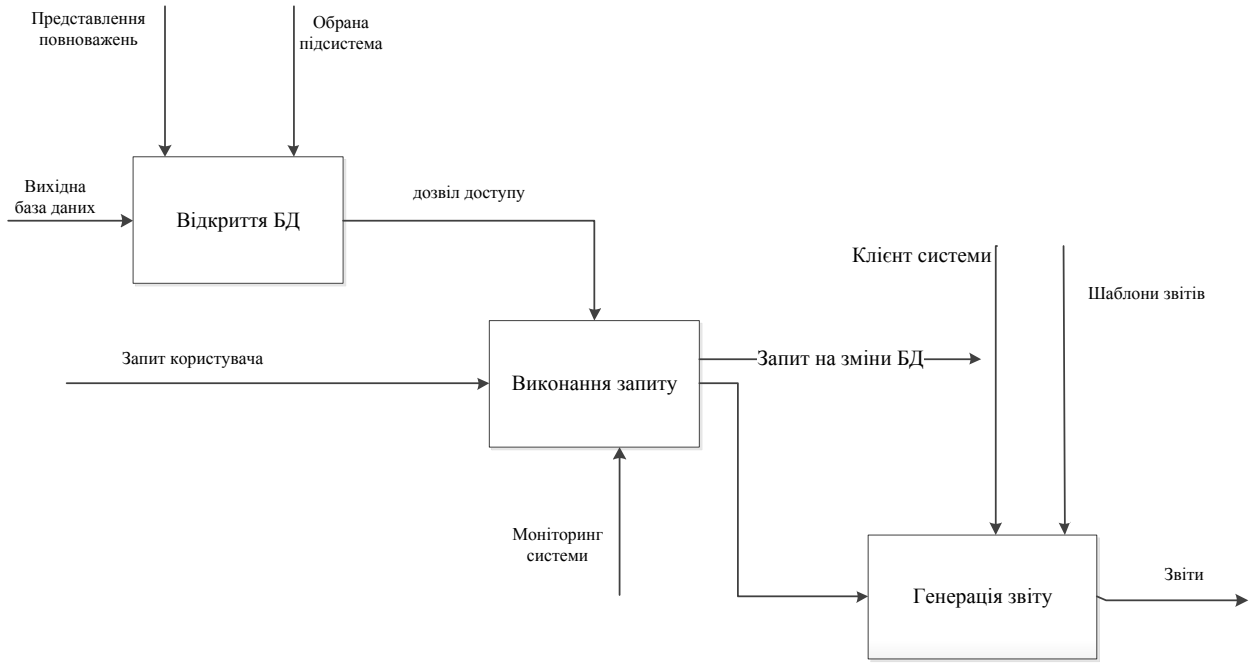

Рисунок 2.18 – Декомпозиція процесу «Обробка запиту користувача»

Потрібно зазначити, про те що до «Виконання запиту» (рис.2.16) підключється процеси роботи ще декількох різних підсистем.

Так, наприклад, у випадку, якщо до запиту включити тестування, то виконує підсистема професійних та психологічних перевірок. На протязі процесу при виконані запитів, при складанні експертних оцінок є необхідність зі зміною змісту БД. Тому, на діаграмі передбачено таку можливість.

Декомпозицію роботи «Виконання запиту» доцільно провести за допомогою діаграми DFD, так як методологія IDEFO розглядає систему як сукупність взаємопов'язаних робіт, що погано відображає процеси обробки інформації.

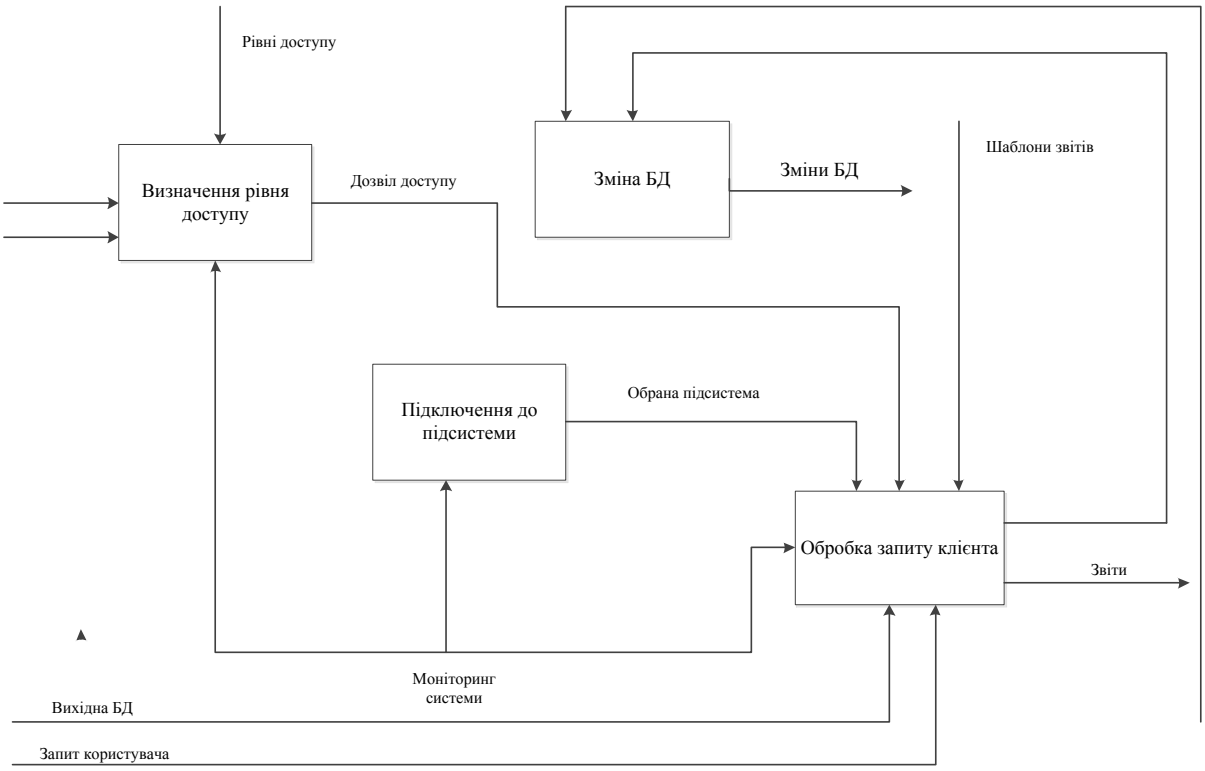

Рисунок 2.19 – Декомпозиция процесу «Виконання запиту»

Перейдемо до декомпозиції останнього блоку «Зміна БД». З точки зору клієнта, дані системи розташовуються в одній БД. Реально в системі присутні шість БД:

- БД співробітників;
- БД документації;
- БД ключів доступа;
- БД документації;
- БД доступа.

Відповідно до мети моделювання клієнту важливо розуміти, що надійшли дані не відразу оновлюються в системі, а проходять додатковий етап обробки і контролю. Алгоритм зміни можна сформулювати наступним чином:

1) Визначається БД, в якій буде змінюватися інформація;
2) Оператором формується набір даних та надається адміністратору;
3) Адміністратор здійснює контроль даних і вносить їх в БД.

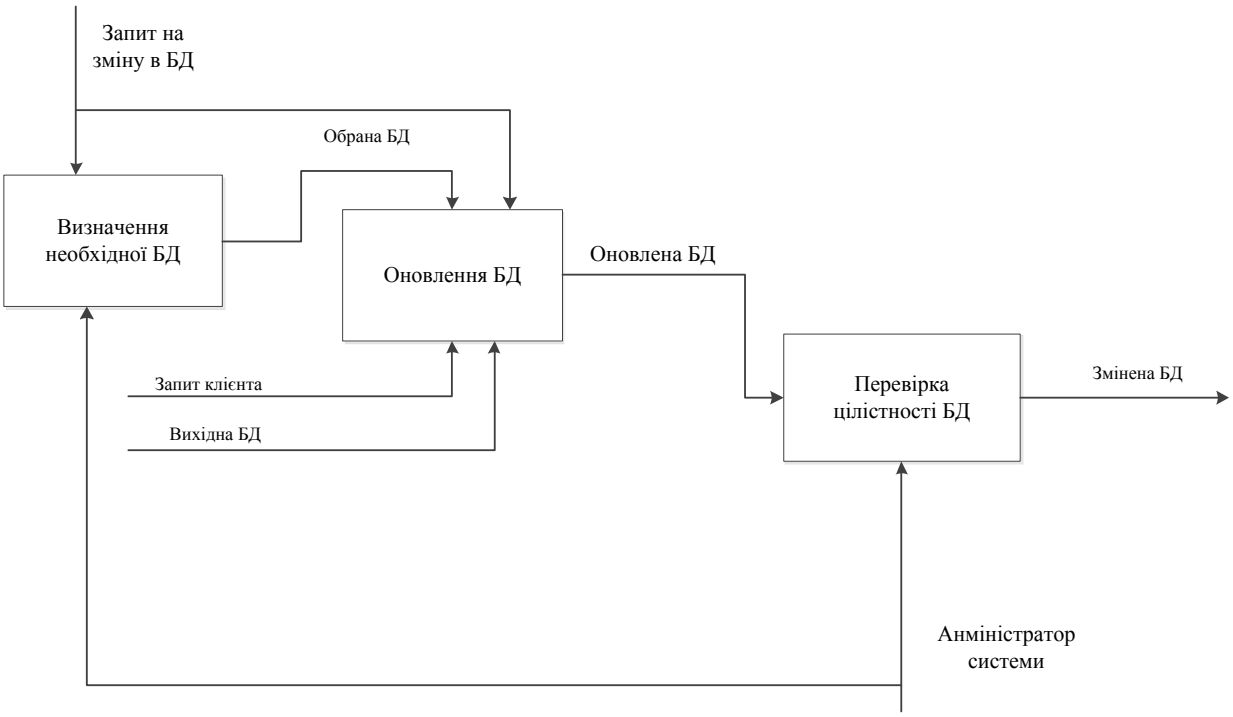

Рисунок 2.20 – Декомпозиція процесу «Зміни БД»

В ході подальшої побудови декомпозиції «Зміни БД» буде ускладнювати модель, пояснюючи, як здійснюється фізичне зміна БД в системі. При цьому користувач не отримає ніякої додаткової інформації про роботу системи служби зайнятості. Декомпозицію цієї роботи доцільно проводити в процесі проектування БД системи на етапі створення логічної моделі БД (об'єктно-орієнтований аналіз).

2.2.8. Програмний компонент шифрування данних на основі RSA

Наскільки б не була складною криптосистема, завжди знайдуться бажаючі її зламати [19]. Відомі кілька способів злому систем RSA. Найефективніший варіант - знаходження секретної компоненти, яка відповідала б використовуваному відкритого ключа. зловмисник в цьому випадку отримає повний доступ до даних зашифрованим відкритим ключем і отримає можливість підробляти підписи. У сучасному криптоанализе не існує ефективних способів вирішення такого завдання. Криптографічний алгоритм RSA був реалізований за допомогою інтегрованого пакета C# (об'єктно-

орієнтованого програмування), заснований на формах, які інтегровані з програмуванням для Windows та використовують компонентну технологію. Середовище візуального програмування C # сприяє компонентного підходу до створення додатків, і дозволяє, без особливих витрат часу, ємко і якісно "Зібрати" інтерфейс програми, для того, щоб більшу частину часу витрачати саме для реалізації складеного алгоритму. Компілятор в машинний код забезпечує високу продуктивність, яка є необхідною для побудови додатків. Цей компілятор в даний час є найшвидшим в світі. Він дозволяє легко розбирати і проводити швидкі перевірки готового програмного блоку, а також забезпечувати якість коду. Крім того, C # забезпечує ефективну і не витратну за часом розробку без необхідності писати вставки на C # або займатися написанням коду вручну (хоча це можливо).

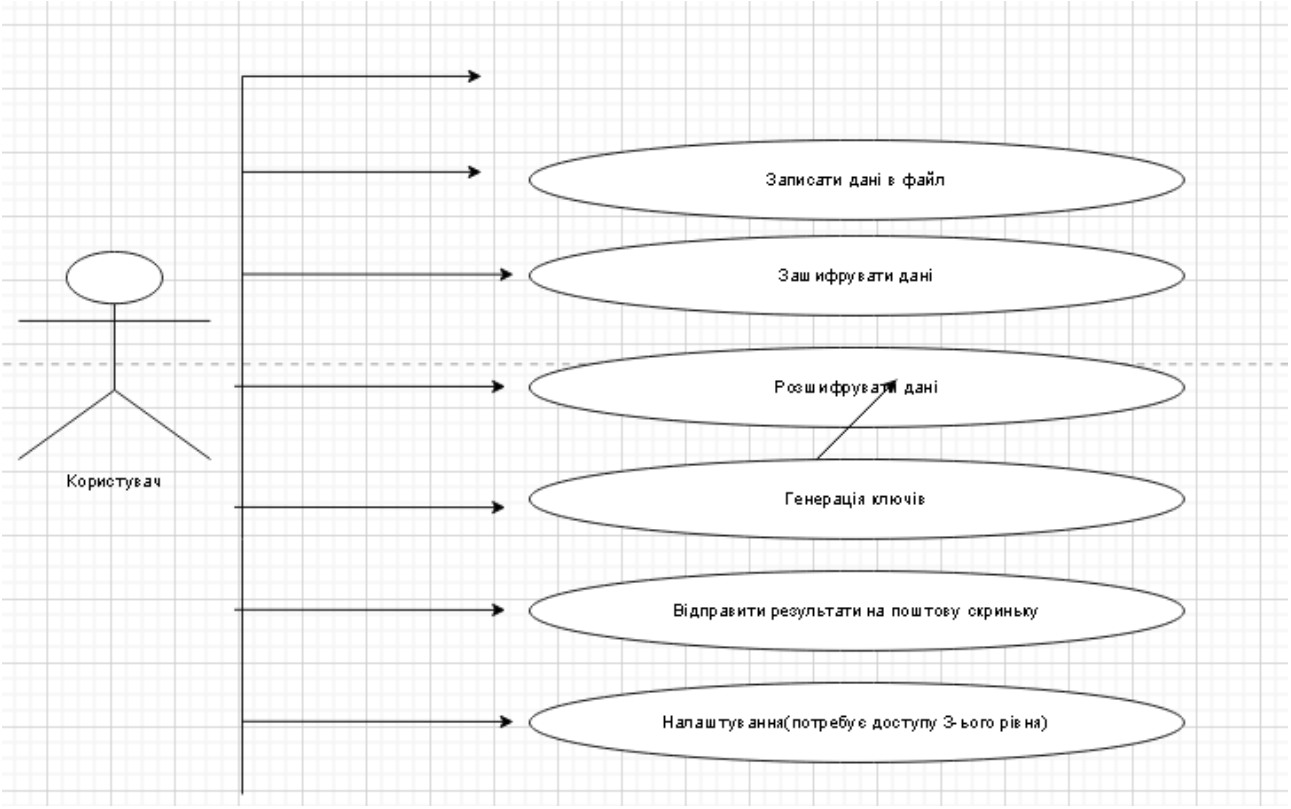

Рисунок 2.21 – Діаграмма варіантів використання

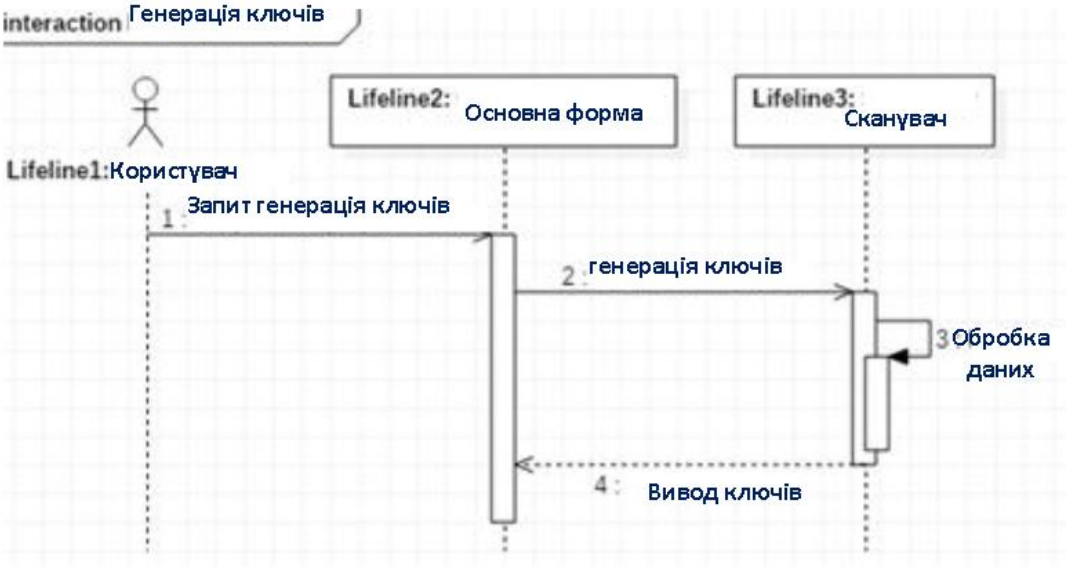

Рисунок 2.22 – Блок-схема «Генерація ключів»

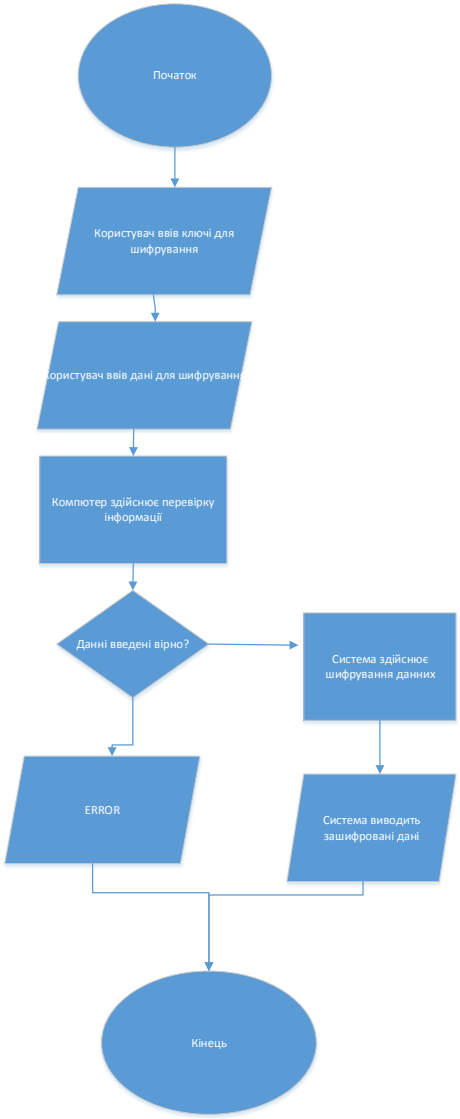

Рисунок 2.23 – Блок-схема «Шифування»

2.3 Робочий проект

2.3.1 Вибір засобів розв’язання поставленої задачі

Microsoft Visual Studio 2021 – універсальний набір утиліт, що надають інтегровану середовище для розробки додатків.

Windows Forms – інтерфейс програмування додатків, що відповідає за графічний інтерфейс користувача і є частиною Microsoft .NET Framework. Даний інтерфейс спрощує доступ до елементів інтерфейсу Microsoft Windows за рахунок створення обгортки для існуючого Win32 API в керованому коді [15].

MySQL для Visual Studio надає доступ до об'єктів і даних MySQL, не примушуючи розробників залишати Visual Studio.

2.3.2 Фізична модель бази даних

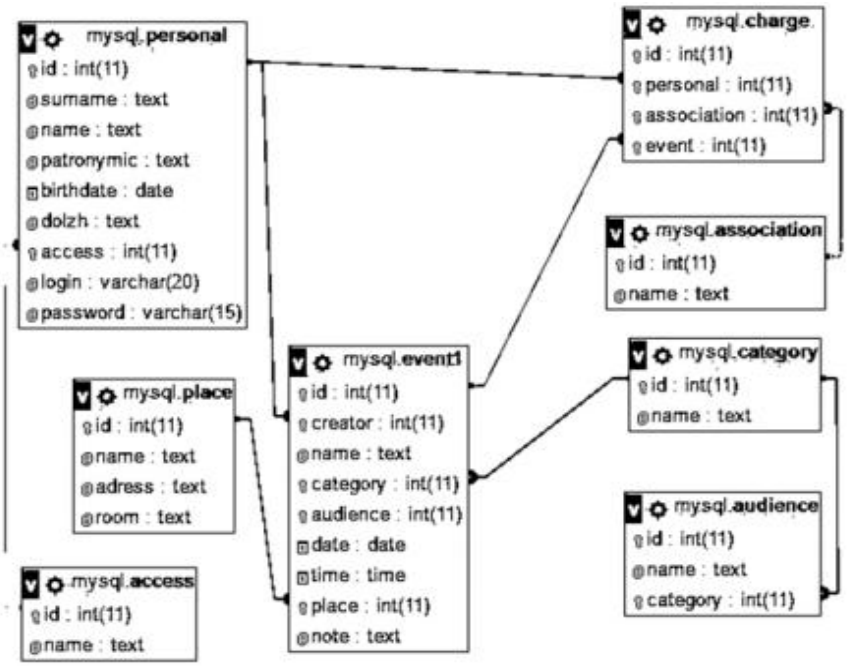

Рисунок 2.24 – Фізична модель бази даних

2.3.3 Реалізація інтерфейсу користувача

Після виявлення важливої інформації система запускає робочий процес відстеження подій для реєстрації та моніторингу даних, що піддаються ризику. Вона веде контрольний журнал подій і може сповіщати встановлене число осіб про настання якої-небудь події за допомогою автоматичної поштової розсилки. Події системи DLP так само можуть бути переправлені для спрощення процесів ідентифікації ризиків по всій інформаційній інфраструктурі за рахунок використання операційної консолі безпеки платформи.

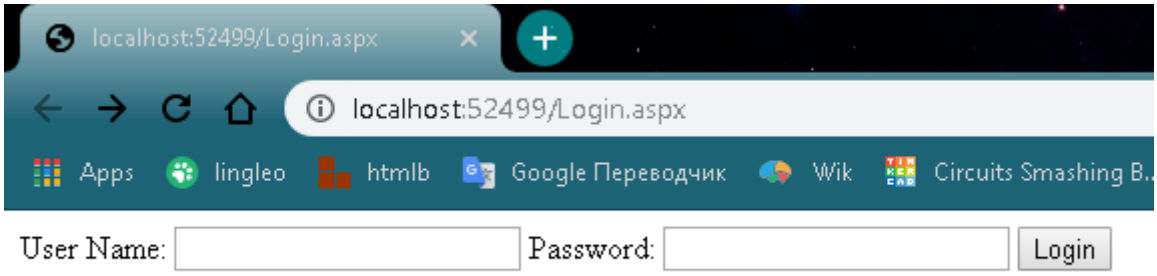

Рисунок 2.25 – Інтерфейс входу в систему адміністратора для моніторингу

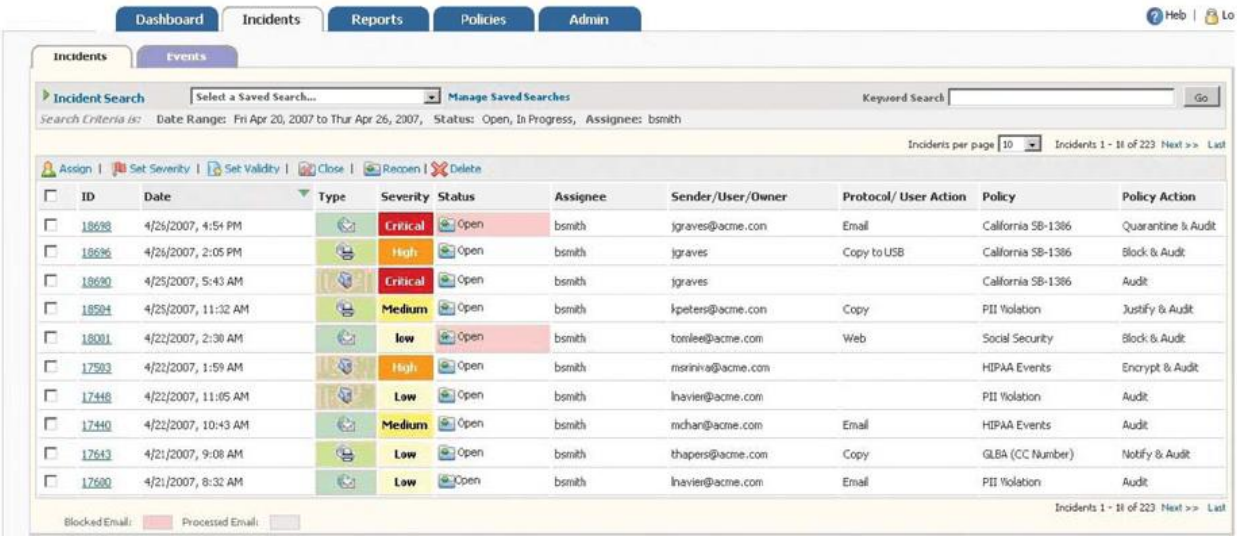

Рисунок 2.26 – Інтерфейс DLP-системи

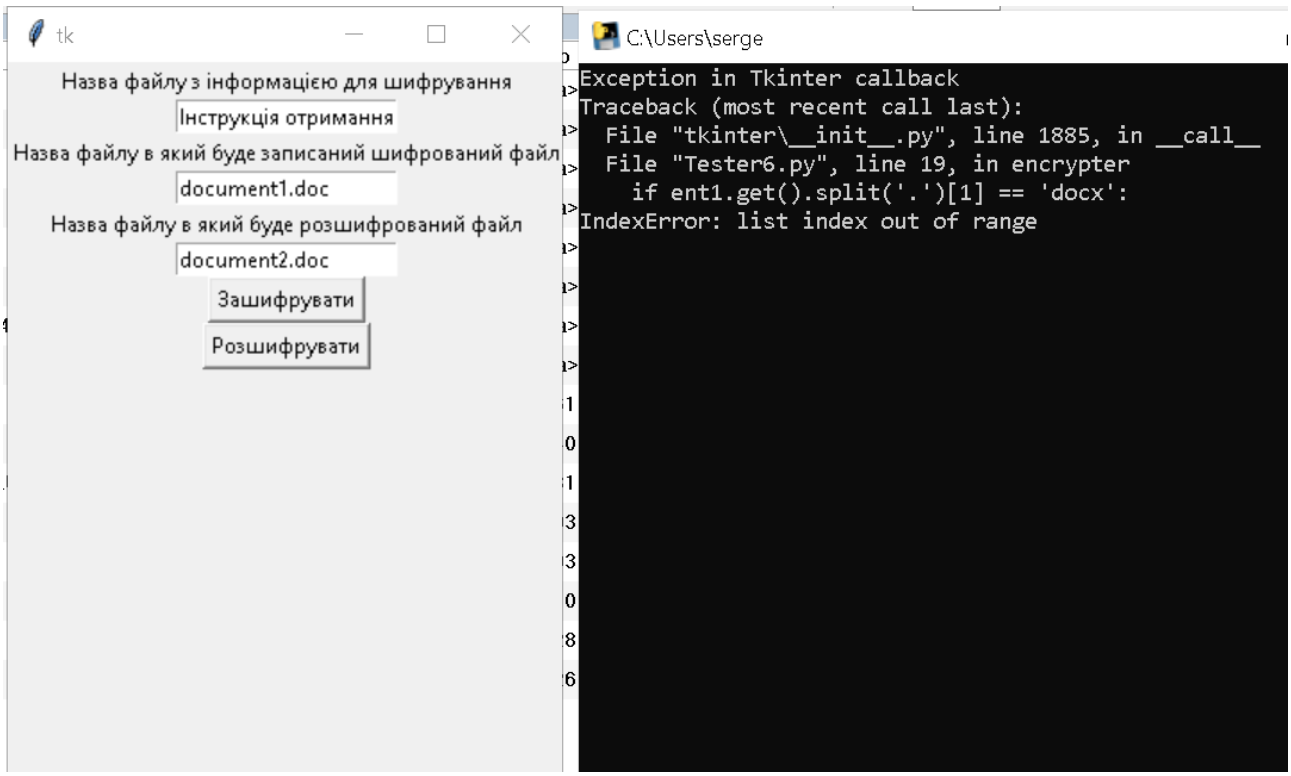

Рисунок 2.27 – Інтерфейс шифрувальника

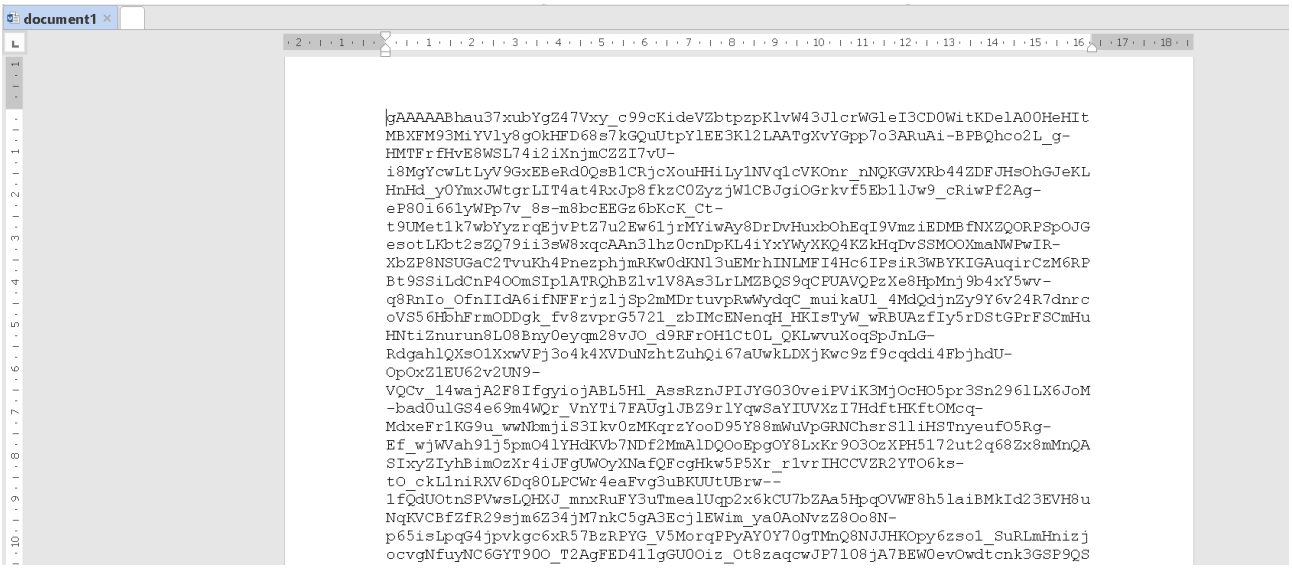

Рисунок 2.28 – Інтерфейс зашифрованого файлу

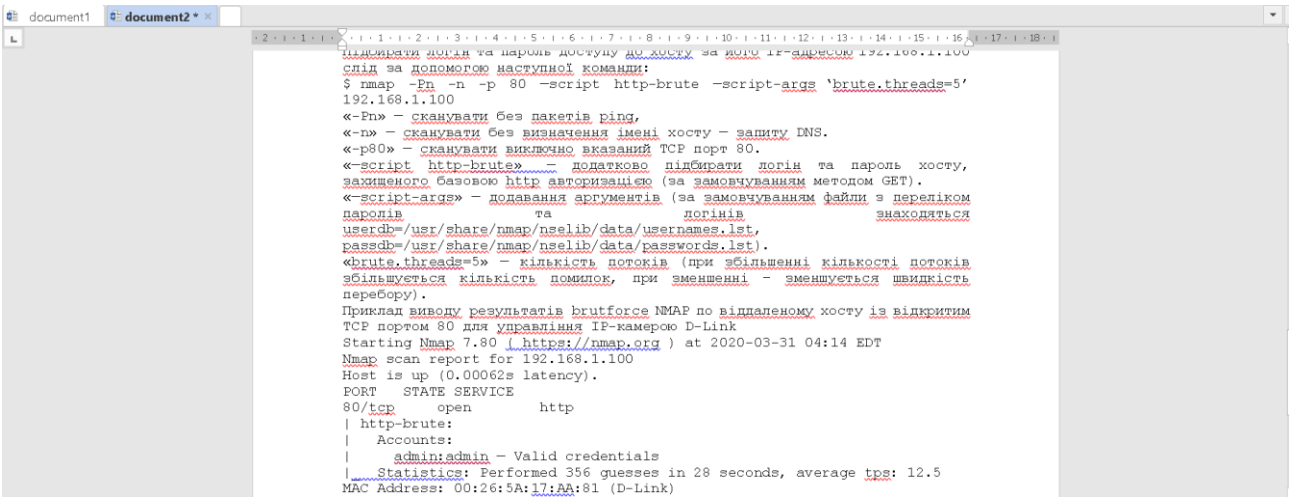

Рисунок 2.29 – Інтерфейс зашифрованого файлу

2.3.4 Кодування та тестування

Так як технологія WMI побудована на принципах методології обєктно-орієнтованого програмування, то усі дані в операційній системі показані як об'єкти, їх властивості та методи [38-39].

Блок обробки повідомлення WM_CHANGECBCHAIN може бути реалізований в такий спосіб. Вікно перегляду буфера обміну приймає повідомлення WM_CHANGECBCHAIN в той час, коли інше вікно віддаляється з ланцюжка вікон перегляду буфера. Іншими словами, це повідомлення має бути передано в наступне вікно в ланцюжку, за допомогою функції SendMessage, імпортованої з бібліотеки User32.dll. Реалізація цього блоку може мати такий вигляд:

[DllImport ("User32.dll", CharSet = CharSet.Auto)]

private static extern int SendMessage (IntPtr hwnd, int wMsg, IntPtr wParam, IntPtr lParam);

```
case WM_CHANGECBCHAIN:
{
if (wParam == m_nextClipboardViewer)
{
m_nextClipboardViewer = lParam;
}
else
{
SendMessage(m_nextClipboardViewer, msg, wParam, lParam);
}
```

```
        break;
        }
```

Обробка повідомлення WM_DRAWCLIPBOARD попереджає вікно перегляду буфера обміну про зміну вмісту буфера. При обробці даного повідомлення необхідно визначити тип операції буфера обміну і відпр вити повідомлення наступного вікна в ланцюжку вікон перегляду буфера.

Приведений приклад відміни процесу друку принтера, здійснюючи через виклик методу *Delete* для об'єкта з переліку діючих процесів. Для скасування роботи принтеру, приклад функції *CancelPrintJob* показаний далі:

```
public bool Cancel_PrintJOB(int PrintJobId1, string Print_Name)
{
   bool Action_Performed = false;
   string SearchQuer = "SELECT * FROM Win_PrintJOB";
   ManagementObjectSearcher PrintSearchJOB = new ManagementObjectSearcher(searchQuery);
   ManagementObjectCollection PrintJOB_Collect = PrintSearchJOB.Get();
   foreach (ManagementObject PrintJOB in PrintJOB_Collect)
   {
      string NAME_JOB = PrintJOB.Properties["Name"].Value.ToString();

      char[] ListARR = new char[] { ',' };
      string jobPrinterName = NAME_JOB.Split(ListARR)[0];
      int JOB_ID = Convert.ToInt32(NAME_JOB.Split(ListARR));
      string documentName = PrintJOB.Properties["Document"].Value.ToString();
      if (jobPrinterName == Print_Name)
      {
         PrintJOB.Delete();
         Action_Performed = true;
         break;
```

```
    }
}
return Action_Performed;
```

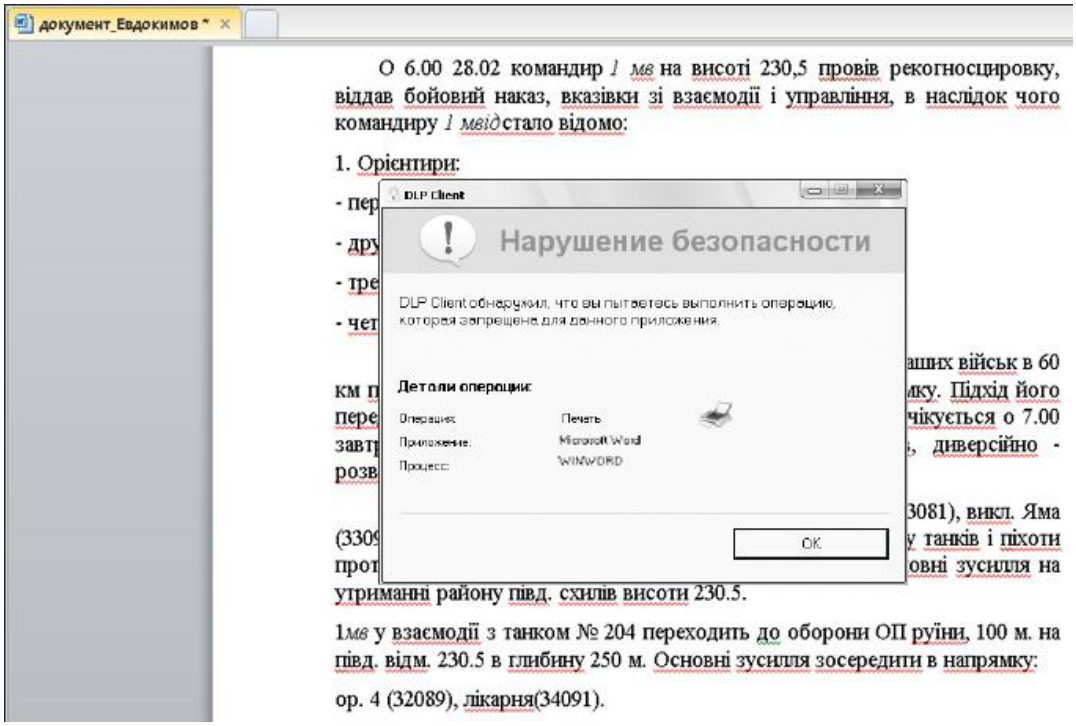

Рисунок 2.21 – Повідомлення про блокування файлу на друк

Для шифрування задних застосовуєтсья наступний код, написаний на мові Python на середовищі Microsoft Visual Studio 2021. Код програми:

```
import os
import shelve
from tkinter import *
import docx
root = Tk()
from cryptography.fernet import Fernet
root.geometry('310x500')

class Shyfr :
    def encrypter(self):
        # Зашифруємо файл та запишемо його
        f = Fernet(key)
        if ent1.get().split('.')[1] == 'docx':

            doc = docx.Document(ent1.get())
            ff = open(ent1.get().split('.')[0]+'.txt','w',encoding='utf-8')


            all_paras = doc.paragraphs
            text = ''
            for i in all_paras:
                text += i.text + '\n'
                text = (text)
            ff.write(text)
            ff.close()
            # Зашифровать дані
```

```
            with open(ent1.get().split('.')[0]+'.txt', 'rb') as file:
                file_data = file.read()
                encrypted_data = f.encrypt(file_data)
                # записати зашифрований файл
            with open(ent2.get(), 'wb') as file:
                file.write(encrypted_data)
            os.remove(ent1.get().split('.')[0]+'.txt')
        else :
            with open(ent1.get(), 'rb') as file:
                # прочитати всі дані файла
                file_data = file.read()
                print(file_data)
            # Зашифровать дані
            encrypted_data = f.encrypt(file_data)
            # записати зашифрований файл
            with open(ent2.get(), 'wb') as file:
                file.write(encrypted_data)


    def decrypter(self):
        # Розшифровуємо файл та записуємо його
        f = Fernet(key)
        with open(ent2.get(), 'rb') as file:
            # читати зашифровані дані
            encrypted_data = file.read()
        # расшифровать данные
        decrypted_data = f.decrypt(encrypted_data)
        # записати оригінальний файл
        with open(ent3.get(), 'wb') as file:
            file.write(decrypted_data)
def write_key():
    # Створюємо ключ та записуємо в файл
    key = Fernet.generate_key()
    with open('crypto.key', 'wb') as key_file:
        key_file.write(key)

def load_key():
    # Завантажуємо ключ 'crypto.key' з каталогу
    return open('crypto.key', 'rb').read()

key = load_key()
lbl1 = Label(text='Назва файлу з інформацією для шифрування')
lbl1.grid()
ent1 = Entry()
ent1.grid()
lbl2 = Label(text='Назва файлу в який буде записаний шифрований файл')
lbl2.grid()
ent2 = Entry(text='zashyfrovano')
ent2.grid()
lbl3 = Label(text = 'Назва файлу в який буде розшифрований файл')
lbl3.grid()
ent3 = Entry()
ent3.grid()
btn1 = Button(text='Зашифрувати', command=Shyfr().encrypter)
btn1.grid()
btn2 = Button(text='Розшифрувати', command=Shyfr().decrypter)
btn2.grid()
root.mainloop()

listt = Listbox(width=50)
listt.grid()
```

2.3.5 Випробування програмного забезпечення

На стадії тестувань було виконано перевірку програмного забезпечення, роботу алгоритму на певному наборі даних, враховуючи те, що для яких заздалегідь відомий результат, а також правило поведінки даних програм [55-58]. Тестування були проведені уже з програмами, що не мають помилок. Метою тестувань було наступне: отримання результатів по конкретним даним, а також контроль якості програми та переконатися в правильності та відповідності процесу роботи ПЗ.

Тестування включало перевірку всіх гілок програми і мінімальний набір прикладів. При тестуванні були такі всілякі ситуації, як незначні помилки програми-тестування, але вдалося домагатися певних результатів. Результати показали наступне: досить високий рівень роботи пакету програм на всіх її модулях. Тестування було проведене, використуовуючи компоратора файлів, генератора тестових даних, моніторингу, тестового моніторингу, програм-профіліровщиків. Трасування проведене через «STrace 1.1» та «VMProtect».

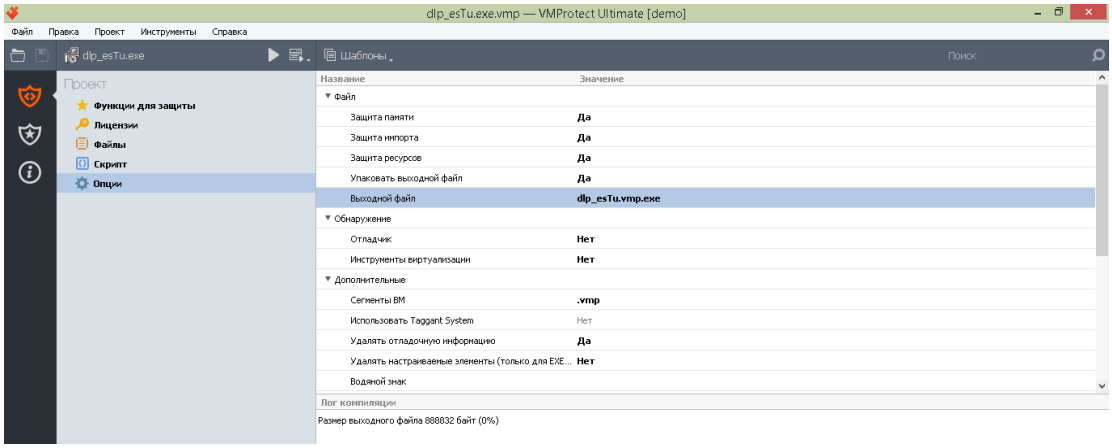

Рисунок 2.22 – Тестування

Рисунок 2.23 – Тестування

РОЗДІЛ 3
РЕЗУЛЬТАТИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В процесі виконання кваліфікаційної роботи (проєкту) було розроблено програмне забезпечення для підприємства будь-якої галузі, що ставить за мету захист локальної мережі від несанкціонованого доступу до конфіденційної інформації. Програмний продукт задовольняє усім заданим вимогам, що були поставлені у Технічному завданні (Додаток А).

Побудова системи ЗІ проводиться на основі обраної архітектури (рис. 2.9, стр. 39) програмного алгоритму розроблена клієнт-серверна система «ESA Security v. 0.9» [14], що поєднує в собі набір технологій запобігання витоку даних по локальних і мережевих каналах та програмний засіб для шифрування документів «ESA Shifr v. 0.8»

У серверних додатках формується політика безпеки, у якій визазначається назва файлу програми який виконується та його дії, що застосовані за виконанню процесів із буферу обміну. Клієнтські додатоки працють у фоновому режимі, та виконують потсійний моніторинг процесів у системі та мережі. У випадку появи певної події процесу(ів), інформація про нього передається з серверного додатку,на яке, згідно з політикам безпеки, приймає рішення відповідних дій по даній події.

Таким чином, що розробляється система виконує наступні функції:

– архівування повідомлень, що пересилаються для можливості розслідування інцидентів;

– запобігання передачі не тільки конфіденційної, а й іншої небажаної інформації;

– контроль як вихідного, так і вхідного трафіку;

– запобігання використанню працівниками службових –інформаційних

– ресурсів в особистих цілях;

– контроль завантаження каналів зв'язку, оптимізація трафіку в межах локальної мережі;

– оповіщення відповідальних осіб про порушення політик інформаційної безпеки.

Методика та програма випробуваня програмного продукту відображена в Додатку В.

Таким чином, аналіз відомих систем контролю даних в локальній мережі мають певні обмеження в їх застосуванні. З огляду на це, при проектуванні систем захисту конфіденційних даних в корпоративних мережах використовувати сучасну архітектуру СЗІ. На базі цієї архі-тектури та розробленого оригінального алгоритму створена нова програма «ESA Security v. 0.9» для виконання моніторингу системних подій Windows в додатках, визначених політиками інформаційної безпеки. Проведені експерименти показали високу ефективність (широке коло вирішуваних завдань і низька ресурсомісткість) даного підходу при вирішенні завдань обмеження несанкціонованого використання і модифікації даних. На прикладі додатка MS Word 2010, для якого в політиках безпеки визначено блокування операції копіювання даних в буфер обміну (рис.2.20).Розроблена СЗІ забезпечує максимально високу точність розпізнавання важливих даних: персональні дані, дані необхідної документації і дані про інтелектуальну власність. Поліпшення точності може досягатися за рахунок застосування нейронних мереж [23], які будуть вбудовані з поправками та особливості підприємства.

Інструкція користувача, для роботи з розробленою системою системою захисту інформації на основі СЗІ, наведена в Додатку В.

У подальшому є перспективи до поліпшення алгоритму за рахунок згорткових нейроних мереж, які можуть забезпечувати часткову стійкість до прогнозів, пошуків оптимізації, роботи асоціативної памяті й управління, а також гнучкі у використані серед інших ШНМ [5, стр. 3]

Також, розбений програмний засіб для шифрування даних, що йде в комплексі зі СЗІ є досить еферктивним, що покав себе на етапі тестування. програма здатна зашифровувати завантажуються користувачем файли, генеруючи відкриті та закрититі ключі на основі введених випадкових чисел, а

також може розшифровувати раніше зашифровані файли. Вхідні дані для шифрування файлів - два випадкових числа, а також файл, який попередньо повинен бути відкритий (або текст, введений в призначеному для цього текстовому полі). На основі введених користувачем чисел визначаються два найближчих до них простих числа.

РОЗДІЛ 4
ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗРАХУНОК ЕФЕКТИВНОСТІ ПЗ

1.1 Загальна характеристика

Сучасні обчислювальні засоби широко використовуються в повсякденній діяльності людини [24-25]. Сьогодні ЕОМ та засоби програмування дозволяють вирішувати багато найрізноманітнішіших завдань: починаючи зі поліпшення персоналу від монотонної ручної праці до складних технічних розрахунків, які не під силу виконати одній людині.

З розвитком нових технологій ріст у застосуванні обчислювальної техніки привели до широкого впровадження ЕОМ у вирішенні задач, що пов'язані з обробкою інформації, контролем та її аналізу. Сьогодні на основі засобів обчислювальної техніки розробляються і впроваджуються різні автоматизовані інформаційні системи (управління, проектування, технологічної підготовки виробництва). Успіх у розробці цих систем, їх роль в інтенсифікації розвитку народного господарства нашої країни багато в чому залежить від фахівців програмістів, які знають методику аналізу та проектування цих систем, можливості обчислювальної техніки, які володіють математичними методами, що використовуються при постановці та вирішенні задач.

Дана кваліфікаційна робота (проєкт) присвячена розробці засбів захисту електронного документообігу, з метою забезпечити захист інформації в локальної мережі підприємства будь-якої галузі.

Найбільш важливим моментом для розробника, з економічної точки зору, є процес формування вартості системи. Очевидно, що вона являє собою дуже специфічний товар з безліччю особливостей.

Розробка СЗІ вимагає одноразових витрат на його створення, придбання необхідних технічних засобів і поточних витрат на функціонування. Економія від функціонування СЗІ визначається враховуючи витрати на потреби його

експлуатації. Співвідношення цієї економії до витрат на створення програмного забезпечення характеризується економічною ефективністю капітальних вкладень. Економічні показники визначаються за діючими оптовими цінами, тарифами і ставкам заробітної плати на момент розрахунку.

4.2 Розрахунок витрат на створення та впровадження ПЗ

Витрати на розробку системи складаються з витрат на:

- заробітну платню розробника;
- амортизацію ЕОМ, на якій виконується розробка;
- експлуатацію цієї ЕОМ;
- засоби розробки;
- матеріали і комплектуючі.

Виходячи з того, що основна заробітна платня розробників з системою DLP складає 10000 грн./міс., вартість сучасної ПЕОМ складає 10000 грн. і вартість кіловат-години електроенергії складає 1,6194 грн., розрахуємо вартість розробки системи.

Розрахунок заробітної плати:

$$З_{зп}=ЗП_{роз} \cdot T_{роз} \qquad (4.1)$$

де $ЗП_{роз}$ – зарплатня розробника за місяць; $T_{роз}$ – тривалість розробки (дослідження, створення, налагодження і впровадження).

Для розробки даної системи необхідно 4 місяці (за експертною оцінкою часу на розробку аналогічних систем). Кількість розробників – 2 людини.

З цього випливає, що загальна сума витрат на заробітну платню складе:

$$З_{зп} = ЗП_{роз} \cdot T_{роз} = 10000 \cdot 4 \cdot 2 = 80000 \text{ (грн.)}$$

Витрати на амортизацію ЕОМ, на якій виконується розробка, розраховується за формулою:

$$З_{амор} = Ц_{варт} \cdot A \cdot T_{роз} \qquad (4.2)$$

Де $Ц_{варт}$ = 10000 грн. – балансова вартість ЕОМ; A = 60% – амортизація за рік; термін служби ЕОМ – 5 років; $T_{роз}$ = 0,33 року – час, необхідний для розробки системи.

$$З_{амор} = 10000 \cdot 0{,}6 \cdot 0{,}33 = 1980 \text{ (грн.)}$$

Витрати на експлуатацію ЕОМ, на якій виконується розробка, полягають в оплаті споживаної нею електричної енергії і розраховуються по формулі:

$$З_{Амор} = P_{EOM} \cdot T_{розр} \cdot N_{рд} \cdot N_{рч} \cdot E_{ел} \qquad (4.3)$$

де P_{EOM} = 0,4 квт./год. – потужність ЕОМ; $T_{розр}$ = 4 місяці – тривалість розробки; $N_{рд}$ = 22 дні – число робочих днів у місяці; $N_{рч}$ = 8 годин – число годин у робочому дні; $E_{ел}$ = 1,6194 грн. – вартість 1 кВт/год електроенергії.

$$З_{АМОР} = 0{,}4 \cdot 22 \cdot 8 \cdot 1{,}6194 = 12{,}64576 \text{ (грн.)}$$

Витрати на матеріали і комплектуючі вироби враховують витрати на папір для друкувальних пристроїв, на картридж і тонер для принтера, а також на непередбачені витрати. Розрахунок приведений у табл. 5.1 (ціни взяті відповідно до прайс-листів та договірних цін на даний вид матеріалів).

Табл. 4.1 – Розрахунок витрат на матеріали і комплектуючі вироби:

№ з/п	Найменування виробів	Вартість, грн.
1	Папір для принтера	100,00
2	Картридж та тонер для принтера	350,00
3	Література (доступ до Internet)	200,00
4	Непередбачені витрати	200,00
	Разом	850,00

Загальний кошторис витрат на створення системи, вищевказаного у таблиці 4.2. До витрат на впровадження системи відносяться витрати на придбання технічного забезпечення, вартість програмного забезпечення, вартість навчання кадрів, витрати на монтаж и настроювання мережі.

Оскільки параметри технічних засобів, які вже є, відповідають вимогам, то їх вартість при розрахунку витрат враховувати не будемо.

Таблиця 4.2 – Загальний кошторис витрат на створення системи:

№ з/п	Найменування витрат	Вартість, грн.
1	Заробітна платня основна	120 000,00
2	Заробітна плата додаткова (20% від п.1)	24 000,00
3	Відрахування на соціальне страхування (38% від пп. 1 та 2)	54720,00
4	Витрати на амортизацію ЕОМ	1 980,00
5	Витрати на експлуатацію ЕОМ	42914,00
6	Витрати на матеріали і комплектуючі вироби	850,00
7	Адміністративні витрати (50% від основної заробітної платні)	40 000,00
	Разом на створення системи	284464,00

Виходячи з вимог до програмного забезпечення, а також проаналізувавши цінову політику, можемо прийняти наступне (табл. 4.3).

Таблиця 4.3 – Перелік програмного забезпечення, необхідного для впровадження системи:

№	Найменування ПЗ	Кількість	Вартість, USD	Вартість, грн.
1	OS MC Windows 10	1	190	3135,00
2	PHP, MySQL, Python, C Sharp	безкоштовно		
3	Microsoft Visual Studio 2021			
4	OS Linux			
	Разом	3135,00		

Витрати на програмне забезпечення склали 3135 грн.

Згідно з досвідом створення аналогічних програм, приймаємо, що вартість підготовки кадрів дорівнює 600,00 грн. Витрати на супроводження інформаційної системи дорівнюватимуть 1% від вартості програми и становлять 313,50 грн.

Інвестиційні витрати на впровадження системи з урахуванням вартості навчання кадрів і витрати на супровід представлені в таблиці 4.4.

Таблиця 4.4 – Інвестиційні витрати на впровадження системи:

№	Найменування інвестицій	Вартість, грн.
1	Вартість програмного забезпечення	3135,00
2	Вартість підготовки кадрів	600,00
3	Супроводження системи	313,50
Разом на впровадження системи		4048,50

Разом загальна сума витрат на створення і впровадження системи складає 49 966,60 грн.

4.3 Розрахунок економічної ефективності розробки та впровадження ПЗ

Основним показником економічної ефективності функціонування системи захисту інформації є підвищення ефективності керування інформацією у вигляді зниження витрат на керування при одночасному збільшенні швидкості і якості одержання потрібного результату.

Економічна ефективність впровадження програмного засобу очікується за рахунок вивільнення робочого часу працівників та підвищення продуктивності праці. Крім того, не піддається прямій грошовій оцінці зменшення кількості помилкових та необережних рішень, підвищення оперативності керування, поліпшення організації роботи та своєчасне отримання необхідної інформації про пріоритетність варіантів рішень тощо.

Використання даної програми дозволяє вивільнити 0,5 роб. часу. Оскільки з системою працює один робітник, то умовно вивільниться 0,5 робітника.

Визначимо пряму економічну ефективність, ґрунтуючись на тому, що впровадження системи вивільнить 0,5 робітника.

Зарплата 0,5 робітника у рік складає $\Delta C = 5000 \cdot 12 \cdot 0,5 = 30000$ (грн.). Річний економічний ефект розраховується за формулою 4.4.

$$E_{рік} = \Delta C - Ц_{супр} - E_n \cdot k, \qquad (4.4)$$

де $Ц_{супр}$ – вартість супроводження системи; $E_п$ – нормативний коефіцієнт економічної ефективності капітальних вкладень у галузь – для обчислювальної

техніки приймається = 0,5; k – додаткові капітальні вкладення з урахуванням витрат на проектування, створення і функціонування системи.

$$E_{рік} = 30000 - 313{,}50 - 0{,}5 \cdot 49966{,}60 = 4703{,}20.$$

Строк окупності системи розраховується за формулою 5.5:

$$I = \frac{k}{\Delta C - Ц_{супр}}. \qquad (4.5)$$

$$I = \frac{49966{,}60}{30000 - 313{,}50} = 1{,}68 \text{ (року)}.$$

Тобто, система окупиться через 1,68 року, що приблизно дорівнює 20 місяцям.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Відповідно зі ст. 15 Закону України «Про охорону праці» кожен роботодавець повинен формувати у будь-якому структурному підрозділі також в трудовому ділянці вимога роботи у відповідності зі умовами нормативних актів, але крім того гарантувати виконання компетентиних співробітників, та у відповідності зі законодавством про охорону праці.

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров’я і працездатності людини в процесі праці [35]. Головний об’єкт охорони праці - це людина в процесі праці, виробниче середовище, організація праці на виробництві. Основна мета охорони праці - це створення здорових і безпечних умов праці.

5.1 Безпечна праця з комп’ютерною технікою

Сьогодні, комп'ютерною технікою користуютсья майже у всіх установах[36]. Використовуючи працівниками ЕОМ, при невиконанні інструкцій заходів безпеки, може спричинити негативні наслідки здоров'я організму, та призвести до НС, нещасних випадків на ЗВО [37]. Тому, для того, працівники уникнути такого, останні повинні постійно дотримуватись техніки безпеки при роботі з комп'ютером та затверженних інструкцій[35].

Персонал, який користується для своєї трудової діяльності ЕОМ, зазнає в певній мірі вплив наступних факторів негативного характеру, в тому числі електромагнітне та інфрачервоне випромінювання:

- шуми від працюючих комп'ютерів;
- ризик щодо ураження електричним струмом;
- можливе виникнення загоряння.

Тому, в будь-які установі може повинено бути передбачено за спеціальним (відповідним) документом, правила виконання з комп'ютерною

технікою на роботі.. Окремо положення щодо вказаних питань є скаладовою в інструкції щодо охорони праці для працівників в офісі.

Для офісних співробітників, які мінімум 50% свого робочого часу виділяють свого часу за комп'ютером, необхідно, щоб були передбачені спеціальні внутрішньозмінні перерви, тривалість і частота яких залежить від типу трудової функції Компанія повинна мати чітко встановлені перерви для інших працівників (за винятком обідів), як правило, 10–15 хвилин кожну годину або дві, залежно від складності роботи (п. 5.3, 5.8, 5.9, 5.10 Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98).. У будь-якому випадку роботодавець повинен надати такий графік роботи на підприємстві, щоб час безперебійної роботи з комп'ютером був не більше 4:00. Крім того, з метою збереження належного рівня здоров'я та професійної працездатності працівників, рекомендується на підприємстві забезпечити окреме приміщення для працівників для розслаблення та звільнення від нервово-емоційного стресу, що виникає при роботі з комп'ютером.

Дотримання правил роботи за комп'ютером дозволить знизити негативний вплив комп'ютера на здоров'я працівника. Однак найчастіше саме працівники нехтують цими правилами, і завдання роботодавця в даному випадку – постійно доводити до відома своїх співробітників інформацію про наслідки недотримання вищевикладених вимог і своїми розпорядженнями організовувати обов'язкові перерви в роботі.

5.2 Безпека людини в надзвичайних ситуаціях на підприємстві

Імовірність перетворення потенційної небезпеки в реальну залежить від взаємного розташування в просторі і часі людини і небезпечної зони [9]. При цьому можливі три основні варіанти:

- небезпека не збігається з місцезнаходженням людини;
- небезпека збігається в незначній мірі з місцезнаходженням людини;
- небезпека збігається з місцезнаходженням людини.

Якщо за критерій можливих негативних наслідків прийняти ризик, який визначається ймовірністю прояву небезпеки під час перебування людини в небезпечній зоні, то: в першому випадку ризик виключений повністю, так як людина не має контакту з небезпеками; у другому випадку ризик пошкодження здоров'я людини можливий тільки в разі збігу зони дії небезпек за місцем і за часом з місцем перебування людини, тому виключити або зменшити ризик можна, у випадку з постійним дотриманням Інструкціями та правила затвердженими зігдно роботи з ЕОМ.

5.3 Відповідні умови для праці та супроводження ЕОМ

Шум погіршує умови праці здійснюючи шкідливу дію на організм людини. Працюючі в умовах тривалої шумової дії випробовують дратівливість, головні болі, запаморочення, зниження пам'яті, підвищену стомлюваність, зниження апетиту, біль у вухах і т. д. Такі порушення в роботі ряду органів і систем організму людини можуть призвести до негативних наслідків. Під впливом шуму знижується концентрація уваги, порушуються фізіологічні функції, з'являється втома у зв'язку з підвищеними енергетичними витратами і нервово-психічним напруженням, погіршується мовна комутація. Все це знижує працездатність людини і його продуктивність, якість і безпеку праці [25].

Як вже було неодноразово відзначено, при роботі з персональним комп'ютером дуже важливу роль грає дотримання правильного режиму праці і відпочинку. В іншому випадку у персоналу наголошуються значна напруга зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в попереку, в області шиї і руках [26]. Підсумуючи, можна зробити наступний висновок. Створення сприятливих умов праці і правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці.

5.4 Вимоги в аварійних ситуаціях

Користувач зобов'язаний:

- у всіх випадках виявлення обриву проводів живлення, несправності заземлення та інших пошкоджень електрообладнання, появи запаху гару: негайно відключити живлення та повідомити про аварійну ситуацію керівнику

- у разі появи в очах різі, при погіршенні зору - неможливості сфокусувати погляд та появ болю, посилення серцебиття негайно покинути робоче місце, повідомити про це керівника, звернутися до лікаря;

РОЗДІЛ 6
ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ

Є необхідність в додатковому зазначенні праввих аспектів, та повторення такої теми, як легітимність впровадження систем для захисту від витоків інформації. Це дсоить добре, коли підприємтсво має замисли про збереження своїх інформаційних активів і впроваджує рішення [27]. Але якщо цього впровадженню не сприяє юридичне оформлення, частина функцій СЗІ просто «відвалюється». Компанія не зможе використовувати дані СЗІ в суді проти співробітника, винного в розголошенні КІ (а може і постраждати від позову самого –співробітника, наприклад). Ще один важливий момент, більшість регламентів і положень вимагає електронного підпису співробітника, який або виступає в якості однієї зі сторін угоди, або підтверджує ознайомлення зі змістом документу. Тому до роботи над юридичним оформленням СЗІ необхідно залучати HR-відділ і, юристів.

Впровадження СЗІ зачіпає важливі сторони роботи компанії. Для того щоб воно було в правовому полі, потрібно, по-перше, не виходити за рамки законодавства, по-друге, інтегрувати систему в інформаційну інфраструктуру компанії. Це означає, що легітимне використання СЗІ має спиратися на внутрішні документи і регламенти, такі як Положення про комерційну таємницю, Політика конфіденційності, Політика щодо персональних даних, кадрові документи та ін. Для того щоб можна було користуватися СЗІ-системою на законних підставах і мати право використовувати її дані при захисті своїх прав, відомості про неї повинні бути внесені в трудові договори і в правила внутрішнього трудового розпорядку. Якщо ж ви хочете максимально повно захиститися від інформаційних ризиків, вам допоможе чек-лист, до якого внесено всі необхідні заходи.

6.1 Дані СЗІ-системи як доказ

На підставі зібраних даних в програмному забезпеченні СЗІ про порушення роботи з електронною документацією, працівник несе відповідальность за порушення режиму комерційної таємниці чи інформаційній безпеці, порушення трудового розпорядку, порушення трудової дисципліни. Важливо, що в суворій відповідності Кодексу Законів про працю України зі ст. 148 «Застосування дисциплінарних стягнень та їх оскарження», якщо не дотримуватися процедури накладення дисциплінарних стягнень, співробітник може оскаржити такі дії в суді, до того ж відсудить гроші у роботодавця (втрачений дохід). У вимозі повинні бути вказані обставини справи, обставини виявлення інциденту і інша суттєва інформація. На підставі акта, звіту СЗІ-системи або система моніторингу і всіх інших документів видається наказ про дисциплінарне стягнення, яке може бути, в залежності від тяжкості порушення, трьох видів: звільнення, догана, попередження.

6.2 Перелік документів, що регулюють забезпечення інформаційної безпеки

Нижче наводиться список законодавчих актів, нормативно-правових актів (НПА) та нормативних актів щодо інформаційної безпеки (стосовно захисту інформації) в Україні, список не повний (до нього не входять НПА з обмеженим доступом та деякі НПА). Актуальні зміни на сайті Державної служби спеціального зв'язку та захисту інформації України: http://www.dstszi.gov.ua (Розділ нормативно-правова база).

Закони України:

- ЗУ «Про інформацію» від 02.10.1992 № 2657-XII
- ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

- ЗУ «Про державну таємницю» від 21.01.1994 № 3855-XII
- ЗУ «Про захист персональних даних» від 01.06.2010 № 2297-VI

Постанови КМУ:

Постановою Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373.

Постановою Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 року № 736.

За діючим Законодавством, особа яка порушує норми несе відповідальність за порушення вищевказаних несе кримінальну віповідальність зігдно ст. 361-365 КК України (Розділ XVI).

ВИСНОВКИ

Удосконалення процесу документообігу за допомогою впровадження електронної бази даних вже охопило низку державних структур, і стає все більш необхідним і у вищих навчальних закладах. Але оскільки процес переходу до електронного документообігу потребує значних капіталовкладень, тому дане дослідження має достатнє обґрунтування для спроби реалізації їх у майбутньому в роботі всіх підрозділів вищих навчальних закладів. Коли виникає необхідність забезпечити інформаційну безпеку компанії, керівництво, як правило, звертається до системних інтеграторів. Тому, проводиться комплексний аналіз та розробляють проект із захисту інформації. В остаточному підсумку це обертається купівлею дорогих програмних та апаратних засобів, таких як Cisco PIX, Checkpoint, Microsoft ISA. Такі великі комплексні проекти коштують більше 15 тис. доларів. Вимагають постійного супроводу та доцільні тільки для великих підприємств.

Все це ставить нові проблеми перед розробниками інформаційної інфраструктури. Деякі сучасні форми бізнесу повністю базуються на мережевих технологіях (електронна торгівля, IP-телефонія, мережеве провайдерство і т.д.) і з цієї причини особливо уразливі. Буде потрібно тут і міжнародне співробітництво в сфері законодавства і встановлення бар'єрів для мережевих терористів. Не є виключенням той факт, що з часом доводиться модифікувати інформацію з урахуванням вимог безпеки деякі протоколи програми.

Необхідно щоб система захисту інфомрації була комплексною – це апаратні і програмні засоби, такі як антивіруси. Апаратні брандмауери не мають можливості забезпечувати захист кожної робочої станції при вірусних атаках всередині мережі, тому не можуть виконувати розмежування, які виконуються відносно захисту персональних даних.

Організація ефективного захисту від витоків інформації вимагає комплексного підходу, який передбачає аналіз основних каналів витоку даних,

реалізацію постійного моніторингу нових загроз, а для масштабних і різноманітних загроз.

В перспективі, проведене дослідження надає можливості до створення швидкодіючих, компактних та енергонезалежних систем штучного інтелекту. При всьому цьому відзначимо, що СЗІ на сьогоднішній день досить ефективний інструмент для захисту конфіденційної інформації тільки в інтеграції з іншими сервісами безпеки і актуальність інтегрованих рішень буде з часом тільки збільшуватися. Тому, впровадження програмних продуктів щодо запобігання витоків електронної документації з локальної мережі підприємтва постає досить значною необхідністю в роботі всього електроного документообыгу.

Кваліфікаційна робота (проєкт) "Розроблення засобів забезпечення інформаційної безпеки для систем електронного документообігу в локальній мережі установи" присвячена розробці комплексу програм для захисту локальної мережі підприємства від несанкціонованого доступу до конфіденційної інформації, за рахунок побудови Системи захисту інформації на основі отпимальних алгоритмів для моніторингу мережі, а також можна використовувати для контролю дій персоналу в робочий час.

Програмне забезпечення написане мовою програмування C# та Python на основі розробленого алгоритму для Windows додатків, визначених політиками інформаційної безпеки. Проаналізовано можливості роботи данної системи для підприємства. Проведені експерименти показали високу ефективність даного підходу при вирішенні завдань обмеження несанкціонованого доступу до конфіденційної інформації. Для IT-відділів і фахівців з інформаційної безпеки, програмний продукт дозволяє поглянути на задачу контролю над діями з конфіденційними документами, мінімізувати недоліки на рівні технології.

Кваліфікаційна робота (проєкт) містить аналіз діяльності системи захисту інформації в локальній мережі установи, розробку технічного завдання, проект програмного забезпечення, результати розробки, розділ економіки, правові

аспекти безпеки, а також текст програми, програму і методику випробувань та інструкцію для користувача.

Виконано розрахунок економічної ефективності програмного забезпечення, який показує ефективність його використання. Проаналізовано найпопулярніші програмні засоби в галузі захисту локальної мережі підприємства, окреслено їх плюси та мінуси.

Кваліфікаційна робота (проєкт) виконаний на 105 сторінках, містить 33 рисунки, 7 таблиць, 7 додатків та список використаної літератури з 41 найменувань.

Також, були розглянуті основні підходи до організації діагностики комп'ютерної мережі, показані переваги ведення документування мережі, за допомогою спеціальних систем документування, визначені і детально розглянуті етапи проведення комплексної діагностики мереж.

Результатом виконання кваліфікаційної роботи (проєкту) є створений програмний продукт для СЗІ в локальній мережі установи. На основі СЗІ та поліпшений алгоритмів розроблена нова програма для використання постійних моніторингів подій в операційній системі Windows, її в додатках, які визначених політикою ІБ. Розроблений продукт програмного забезпечення задовольняє вимогам, які поставлені у технічному завданні.

Програмне забезпечення може працювати під управлінням операційних систем Windows і Linux.

Тестування даного програмного продукту показало, що програмне забезпечення успішно справляється з поставленими перед ним задачами щодо захисту інформації в локальній мережі підприємсва

Програмне забезпечення розроблено мовою програмування C Sharp на основі інтерфейсу програмування додатків (API) Windows Forms, а також з виккористанням бази даних під управлінням СУБД MySQL. Розроблена система забезпечує захист інформації в локальній мережі та поліпшення функціонування електроної документації на підприємстві для будь-якої галузі.

На закінчення хотілося б підкреслити, що ніякі апаратні, програмні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпека даних у комп'ютерних мережах. У той же час звести ризик втрат до мінімуму можливо лише при комплексному підході до питань безпеки [4].

Проведене дослідження в перспективі відкриває можливості створення компактних, швидкодіючих та енергонезалежних систем штучного інтелекту. При всьому цьому відзначимо, що СЗІ на сьогоднішній день – досить ефективний інструмент для захисту конфіденційної інформації тільки в інтеграції з іншими сервісами безпеки і актуальність інтегрованих рішень буде з часом тільки збільшуватися. Тому, впровадження програмних продуктів щодо запобігання витоків електронної документації з локальної мережі підприємства постає досить значною необхідністю в роботі.

Удосконалення процесу документообігу за допомогою впровадження електронної бази даних вже охопило низку державних структур, і стає все більш необхідним і у вищих навчальних закладах [24-26]. У перспективі розглядається можливість розробки спільних рекомендацій щодо захисту інформації локальних мереж для подібних організацій, заводів, установ, і створення типової інструкції щодо забезпечення безпеки інформації в системах обробки даних. Зокрема, в подальшому постає необхідність в розробці алгоритму штучних нейронних мереж, які будуть більш детально і краще посилювати швидкість розпізнання образів мережевого екрану СЗІ та якість програмного забезпечення вказаного в даному дослідженні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. **Kirsten Korosec**. Tesla подає в суд на колишніх співробітників за крадіжку комерційних секретів [Електронний ресурс] / Kirsten Korosec // TechCrunch. – 2019. – Режим доступу до ресурсу: https://techcrunch.com/2019/03/21/tesla-sues-former-employees-zoox-for-alleged-trade-secret-theft/.

2. **Infowatch**. Глобальні дослідження витоків інформації починаючи з 2007 року [Електронний ресурс] / infowatch.. – 2018. – Режим доступу до ресурсу: https://www.infowatch.ru/analytics/leaks_monitoring.

3. **Торокін А. А**. Інженерно-технічний захист інформації: навч. Посібник для вузів / А. А. Торокіна .- М.: Геліос АРВ, 2005 .- 960с.

4. **С. Е. Остапов, С. П. Євсеєв, О.Г. Король**. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

5. **Рибальський О.В.** Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.6.

6. **Хорошко В. О.** Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020.

7. **Євдокимов С.О., Устенко С.А.** . Розробка системи захисту інформації в локальній мережі підприємства // Геометричне моделювання та інформаційні технології: науковий журнал / за ред. Сергія Устенка. – № 1 (7), квітень 2019. – Миколаїв: МНУ імені В.О. Сухомлинського, 2019. С. – 103 с.

8. **Євдокимов С.О., Лукьянчиков С.Д.** Актуальні проблеми кібербезпеки автоматизованої банківської системи // Інформаційні технології в моделюванні:

науковий журнал / за ред. Сергія Устенка. – № 1 (5), квітень 2018. – Миколаїв: МНУ імені В.О. Сухомлинського, 2018. С. – 120 с.

9. **Євдокимов С.О**. Згорткові нейронні мережі для розпізнавання образів // Інформаційні технології в моделюванні: Матеріали ІІІ-ої всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (22-23 березня 2018 р., м. Миколаїв). – Миколаїв: МНУ імені В.О. Сухомлинського, 2018. – 175 с.

10. **Загинайлов Ю. Н** «Теория информационной безопасности и методология защиты информации» http://window.edu.ru/resource/984/71984 (дата обращения 18.03.2016).

11. **Артамонов В. А., Артамонова Е.В.** «Каналы утечки информации» http://media.professionaly.ru/processor/topics/original/2013/09/24/utechki kanal.pdf (дата обращения 18.03.2016)

12. **Філоненко, С. Ф**. Система попередження витоку персональніх даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко // Ukrainian Scientific Jornal of Information Security. — 2014. — Vol. 20, № 3. — P. 279–285.

13. **Habimana N., Muhoza D., Nyirimanzi J.C.** та ін. Statistical YearBook 2017. National Institute of Statics of Rwanda. URL: http://www.statistics.gov.rw/publication/statistical-yearbook-2017 (дата звернення 31.03.2019).

14. **Нестеров С. А.** Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

15. **Олифер В., Олифер Н.** Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.: ил. — (Серия «Учебник для вузов»).

16. **В.И. Ярочкин.** Информационная безопасность (Учебник для вузов). М. Фонд «Мир» и Изд-во «Академический проспект». 2006.

17. **Торокин,** Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. — М.: Гелиос АРВ, 2005. - 960 с.

18. **Євдокимов С.О., Устенко С.А.** Розробка DLP-системи захисту інформації для локальної мережі підприємства // Інформаційні технології в моделюванні: Матеріали IV-ої всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (21-22 березня 2019 р., м. Миколаїв). – Миколаїв: МНУ імені В.О. Сухомлинського, 2019. – 169 с. – С. 129.

19. **Домарев В.В.** Безопасность информационных технологий. Методология создания систем защиты К.: ТИД ДиаСофт, 2002. – 688 с. — ISBN 966-7992-02-0.

20. **Домарев В.В**. Защита информации и безопасность компьютерных систем К.: ТИД ДиаСофт, 1999. — 480 с. — ISBN 966-7393-29-1.

21. **Зайцев А.П.,** Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: Машиностроение, 2009. — 508 с. — ISBN 978-5-94275-454-9

22. **Домарев В.В.** "Системный подход к созданию СЗИ" - К.:ООО ТИД «Диасофт», 2004.-992 с.

23 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" — Указ Президента України; Стратегія від 26.08.2021 № 447/2021

24. **Charles Petzold**. Programming Microsoft Windows with C# (Developer Reference). – Microsoft Corporation, 2001. – 1328 с.

25. **Дубовцев В.А.** Безопасность жизнедеятельности. / Учеб. пособие для дипломни-ков. - Киров: изд. КирПИ, 1992.

26. Хван, Т.А. Безпека життєдіяльності / Т.А. Хван, П.А.Хван. - Ростов н / Д: «Фенікс», 2013. - 418 с

27. **Шерман М.І.** Навчальна дисципліна «Електронний документообіг та захист інформації» як складова системи формування комп'ютерно-інформаційної компетентності магістрів державної служби/ Інформаційні технології в освіті: Збірник наукових праць. Випуск 15. – Херсон: ХДУ, 2013. – С. 96-102 Несторенко Т.П. Роль електронного урядування в розвитку інституціональної інфраструктури міста: вітчизняний та зарубіжний досвід. Зб. матеріалів Всеукраїнської конференції „Інформаційні технології та розвиток місцевого самоврядування". Чернівці: ДрукАрт, 2008. 15-17 грудня 2008. – С.62-69.

28. **Хофман, Л. Дж.** Современные методы защиты информации / Л. Дж. Хофман. – Москва : Советское радио, 1994. – 264 с.

29. **Л.Матвієнко, В.Волков**. Процес розробки програмного забезпечення. Від теорії до практики.-К., 2008.-ТОВ "Інформаційні програмні системи".-117 с.

30. 100+ покликань на матеріали з R. URL: https://pairach.com/2012/02/26/r-tutorials-from-universities-around-the-world/

31. Методичні рекомендації з підготовки та оформлення випускний кваліфікаційної роботи (проекту) для технічних напрямів підготовки 09.03.01 Інформатика та обчислювальна техніка, 09.03.04 Програмна інженерія, 12.03.01 Приладобудування, 23.03.01 Технологія транспортних процесів / уклад. Л.Н.Буйлушкіна. - Нижньовартовськ, 2017. - 35с

32. **Євдокимов С.О**. Нейронні мережі хопфілда для розпізнавання образів// Інноваційні наукові дослідження в науці та практиці: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 11 серпня 2021 р.). Полтава: ЦФЕНД, 2021. 28 с.

33. **Шерман М.І., Степаненко Н.В.** Електронний документ як об'єкт інформаційної діяльності посадової особи органів місцевого самоврядування/ Державна політика щодо місцевого самоврядування: стан, проблеми та перспективи : збірник матеріалів конференції / за заг. ред. Ю.М. Бардачова, І.П. Лопушинського, О.А. Тертишної. – Херсон: Олді-плюс, 2012. – с. 185-186

34. Проблеми та перспективи підготовки магістрів державної служби в умовах інформаційного суспільства/ Матеріали II міжнародної науково-методичної конференції «Інноваційні технології як чинник оптимізації педагогічної теорії і практики» / Наук.ред. Юзбашева Г.С. Херсон: Айлант, 2012. Випуск 15. - С. 15-17

35. Методичні рекомендації до виконання розділу "Охорона праці та безпека в надзвичайних ситуаціях" у дипломному проекті для студентів освітньо-кваліфікаційних рівнів "спеціаліст", "магістр" усіх спеціальностей усіх форм навчання / укл. О. В. Северинов. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2014. – 32 с. (Укр. мов.)

36. **Білова Т. Г.** Інформаційна технологія управління процесами документообігу / Т. Г. Білова // Новітні інформаційні технології в освіті : матеріали міжвузівської наук. конф. – Харків: ХДАК, 2008. – С. 52-55.

37. **Якіменко А.В.** Основи документообігу та документознавства: Виробниче видання / А. В. Якіменко. – М. : Экзамен, 2003. – 192 с.

38. **Бізлі Д.Python.** Докладний довідник. - Пер. з англ. - СПб .: Символ-Плюс, 2010. -864 с., Іл.

39. **Слатків. Бретт.** Секрети Python: 59 рекомендацій з написання ефективного коду .: Пер. з англ. -М .: ТОВ ii.д. Вільямс ", 2016. - 272 с .: іл. - Парал. Тит. Англ.

40. **Саидерс, Крис.,** Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд. : Пер. с англ. - СПб. : ООО "Диалектика", 2019 - 448 с. : ил. - Парал. тит. англ.

41. **Парасрам Шива, Замм Алекс, Херіянто Теді, Алі Шакіл, Буду Даміан, Йохансен Джерард, Аллен Лі.**, Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. — 448 с.: ил. — (Серия «Для профессионалов»). ISBN 978-5-4461-1252-

Додаток А

Технічне завдання на розробку ПЗ

1 Вступ

Назва розроблюваного проекту: "СЗІ", далі – "Програмний продукт".

Програмний продукт повинен використовуватися адміністратором, менеджером, та іншими уповноваженими особами підприємства будь-якої галузі, для полегшення і автоматизації обліку роботи персоналу та захисту електронного документообігу від несанкціонованого доступу та витоку за межі.

2 Підстави для розробки

Розробка ведеться на підставі навчальної програми Херсонського державного університету згідно з завданням переддипломної практики.

3 Призначення розробки

3.1 Функціональне призначення програми

Функціональним призначенням програми є захист локальної мережі підприємства будь-якої галузі (обмін електронною документацією, робота персоналу та їх моніторинг, формування звітів).

3.2 Експлуатаційне призначення програми

Програма може та повинна проводити моніторинг локальної мережі підприємства, при необхідності проводити дії щгідно політики конфіденційності. Користувачами програми повинні бути співробітники підприємства, що використовує даний програмний продукт.

4 Вимоги до програмного виробу **(**комп‘ютерної системи**)**

4.1 Вимоги до функціональних характеристик

4.1.1 Вимоги до складу виконуваних функцій

Програма повинна виконувати та мати функцію авторизації для розподілу прав доступу на: адміністраторів, менеджерів, робітників підприємства та клієнтів.

З правами доступу користувача як адміністратор підприємства, програма повинна надати можливість виконувати наступні функції:

1) Додання, пошук, редагування, перегляд, видалення інформації в локальній мережі;

2) Редагування, додання, пошук, перегляд інформації та видалення;

3) Додавання, редагування, пошук, перегляд та видалення необхідної документації.

4) Надавати права доступу менеджерам, робітникам або обмежити їх в доступі.

5) Формування звітів.

З правами доступу користувача як менеджера підприємсва, програма повинна надати можливість виконувати наступні функції:

– пошук і перегляд інформації про роботи підлеглих;

– моніторинг локальної мережі;

– оформлення звітів;

– надавати права доступу робітникам чи обмежувати їм доступ.

З правами доступу користувача як робітника підприємства, програма повинна надати можливість виконувати наступні функції:

– пошук і перегляд інформації наданою менеджерами чи адмінами;

– додавання і редагування певної інформації;

– Видалення інформації заданої правам доступу до редагування.

З правами доступу користувача як клієнта, програма повинна надати можливість виконувати наступні функції:

– пошук і перегляд інформації, заданої менеджерами або адміністраторами.

4.1.2 Вимоги до організації вхідних та вихідних даних

Введення тексту здійснюється за допомогою клавіатури. Данні для пошуку та увесь текст вводяться вручну. Додавання товару до виробника,

постачальника та клієнта можливе також зі списків на вибір користувача. Всі дані, що зберігаються на сервері потребують місця на локальному диску електронно-обчислювальної машини.

Інформація, яка отримана з переглядів та пошуків даних, виводиться на сторінках браузера. При бажані вона може бути скопійована та роздрукована на папері.

4.1.3 Вимоги до часових характеристик

Вимоги до часових характеристик програми не висуваються

4.2 Вимоги до надійності

Програмний продукт повинен нормально функціонувати при безперебійній роботі ПК та постійному підключенні до мережі Інтернет. При виникненні збоїв в роботі, відновлення нормальної роботи повинне проводитися після перезавантаження браузера.

Для забезпечення надійності інформації повинна використовуватися СУБД, що забезпечує цілісність транзакцій і несе відповідальність за цілісність інформації.

Система повинна продовжити коректно функціонувати при втраті частини інформації. У випадку неможливості продовження коректної роботи має бути повідомлено про це.

У разі введення користувачем некоректної інформації система повинна повідомити про помилку і надати можливість виправити її.

4.3 Вимоги до умов експлуатації

Необхідний рівень підготовки користувачів: навики в користуванні комп’ютером та роботи з локальною мережею. Для експлуатації даного програмного забезпечення потрібен сучасний ПК, вихід до локальної мережі, а також всі необхідні вимоги для нормальної роботи ПК.

Комп'ютер призначений для роботи в закритому опалювальному приміщенні при наступних умовах навколишнього середовища:

– температура навколишнього повітря від +10 ° С до +35 ° С;
– атмосферний тиск від 630 до 800 мм ртутного стовпа;

– відносна вологість повітря не більше 80%;

– запиленість повітря не більше 0,75 мг / м ³.

4.4 Вимоги до складу та параметрів технічних засобів

Даний програмний продукт потребує від комп’ютеру, на якому він буде встановлений, наступних характеристик, які треба розглядати як мінімальні:

– процесор Intel або AMD від 2.81 GHz та вище;

– 4Gb оперативної пам'яті і більше;

– 512 Gb вільного простору на жорсткому диску і більше;

– ОС Microsoft Windows 7/8/10 або ОС Linux.

Для роботи з даним програмним продуктом необхідна наявність сучасного браузеру та можливість виходу в мережу Інтернет.

4.5 Вимоги до інформаційної та програмної сумісності

Даний програмний продукт призначений для розгортання на сервері, який має Apache, PHP5, СУБД MySQL або LiteSQL.

Мова розробки даної системи: C#, PHP.

Технології: .NET, WindowsForms, PHP, HTML, CSS.

4.6 Вимоги до маркування та упакування

Програма не повинна розповсюджуватися. Поширення даного продукту на фізичних носіях не передбачається.

4.7 Вимоги до транспортування та зберігання

Транспортування та зберігання не передбачаються у зв'язку з відсутністю фізичних носіїв.

5 Вимоги до програмної документації

Програмна документація повинна містити:

– технічне завдання;

– технічний опис програми;

– опис застосування програми;

– інструкція з експлуатації програми;

– програма і методика випробувань.

6 Техніко-економічні показники

Техніко-економічні показники для даного програмного продукту не розраховуються.

7 Стадії та етапи розробки

Стадії та етапи розробки представлені в таблиці А.1.

8 Порядок контролю та приймання

Тестування програмного продукту повинно проводитися у відповідності до узгоджених заздалегідь із замовником програмного продукту методики випробувань. Тестування проводиться в зазначені строки.

Кожна стадія розробки повинна бути представлена в зазначені строки та узгоджена з викладачем. В ході проведення здавально-приймальних випробувань, документуючи за допомогою протоколу проведення випробувань. На підставі протоколу проведення випробувань виконувач сумісно з замовником підписують акт прийомки-здачі програми в експлуатацію.

Таблиця А.1 – Стадії та етапи розробки:

Стадії розробки	Етапи робіт	Термін виконання робіт	
		початок етапу	кінець етапу
1 Технічне завдання	1.1 Обгрунтування необхідності розробки програми	02.11.20	09.11.20
	1.2 Розробка технічного завдання	10.11.20	28.12.20
	1.3 Затвердження технічного завдання	29.11.20	06.12.20
2 Ескізний проект	2.1 Розробка ескізного проекту	07.12.20	20.12.20
	2.2 Затвердження ескізного проекту	21.10.20	28.12.20
3 Технічний	3.1 Розробка технічного проекту	29.12.20	06.01.21

проект	3.2 Затвердження технічного проекту	07.01.21	14.01.21
4 Робочий проект	4.1 Розробка програми	15.01.21	28.02.21
	4.2 Розробка програмної документації	29.02.21	05.03.21
	4.3 Випробування програми	06.03.21	13.03.21

Додаток Б

Текст програми

Лістинг 1

```
namespace ClientLogIn
{
   public partial class Login : System.Web.UI.Page1
   {
      protected void Page1_Load(object sender, EventArgs e)
      {
      }

      protected void LogButton_Click(object sender, EventArgs e)
      {
         if (AuthenticateUser(userNameTextBox.Text, passwordTextBox.Text))
         {
            Response.Cookies.Add(new HttpCookie("name_user", name_userTextBox.Text));
            Response.Cookies.Add(new HttpCookie("password", passwordTextBox.Text));
            Response.Cookies.Add(new HttpCookie("logged", "true"));
            Response.Redirect("Default1.aspx");
         }
      }

      private bool AuthenticateUser(string username, string password)
      {
         return true;
      }
   }
}

namespace ClientLogIn
{
   public partial class Default : System.Web.UI.Page1
   {
      bool isAdmin;

      protected void Page1_Load1(object sender, EventArgs e)
      {
         if (Request.Cookies["loggedin"] == null || Request.Cookies["loggedin"].Value != "true")
         {
            Response.Redirect("Log.aspx");
         }
         else
         {
            if (Request.Cookies["name_user"].Value == "Admin")
            {
               isAdmin = true;
            }
         }
         DataBind();
      }

      public override void DataBind()
      {
         base.DataBind();
         if (isAdmin)
         {
            userTypeLabel.Text = "Admin";
         }
         else
         {
            userTypeLabel.Text = "Not Admin";
         }
      }
   }
}
```

```
public bool Cancel_PrintJOB(string Print_Name, int print_JobId)
{
   bool Action_Performed = false;
   string searchQuery = "SELECT * FROM Win32_PrintJOB";
   ManagementObjectSearcher PrintSearchJOB = new ManagementObjectSearcher(searchQuery);
   ManagementObjectCollection PrintJOB_Collect = PrintSearchJOB.Get();
   foreach (ManagementObject PrintJOB in PrintJOB_Collect)
   {
      string NAME_JOB = PrintJOB.Properties["Name"].Value.ToString();
      char[] ListARR = new char[] { ',' };
      string jobPrinterName = NAME_JOB.Split(ListARR)[0];
      int JOB_ID = Convert.ToInt32(NAME_JOB.Split(ListARR));
      string documentName = PrintJOB.Properties["Document"].Value.ToString();
      if (jobPrinterName == Print_Name)
      {
         PrintJOB.Delete();
         Action_Performed = true;
         break;
      }
   }
   return Action_Performed;
}

ManagementObjectSearcher searchPrintJobs = new ManagementObject- Searcher(searchQuery);
ManagementObjectCollection prntJobCollection = searchPrintJobs.Get();
foreach(ManagementObject prntJob in prntJobCollection)
{
string jobName = prntJob.Properties["Name"].Value.ToString();
char[] splitArr = new char[] { ',' };
string jobPrinterName = jobName.Split(splitArr)[0];
string documentName = prntJob.Properties["Document"].Value.ToString();
if (jobPrinterName == printerName)
{
printJobCollection.Add(documentName);
}
}
return printJobCollection;
}
public bool CancelPrintJob(string printerName, int printJobId)
{
   bool isActionPerformed = false;
   string searchQuery = "SELECT * FROM Win64_PrintJob";
   ManagementObjectSearcher searchPrintJobs = new ManagementObjectSearcher(searchQuery);
   ManagementObjectCollection prntJobCollection = searchPrintJobs.Get();
   foreach (ManagementObject prntJob in prntJobCollection)
   {
      string jobName = prntJob.Properties["Name"].Value.ToString();
      char[] splitArr = new char[] { ',' };
      string jobPrinterName = jobName.Split(splitArr)[0];
      int jobId = Convert.ToInt32(jobName.Split(splitArr);
      string documentName = prntJob.Properties["Document"].Value.ToString();
      if (jobPrinterName == printerName)
      {
         prntJob.Delete();
         isActionPerformed = true;
         break;
      }
   }
   return isActionPerformed;
}

protected override void OnClosed(EventArgs e)
{
   base.OnClosed(e);
   ChangeClipboardChain(this.WindowHandle, m_nextClipboardViewer);
   if (m_hwndSource != null)
   {
      m_hwndSource.RemoveHook(WndProc);
   }
}

[DllImport("User32.dll", CharSet = CharSet.Auto)]
private static extern int SendMessage(IntPtr hwnd, int wMsg, IntPtr wParam, IntPtr lParam);
```

```
case WM_CHANGECBCHAIN:
{
if (wParam == m_nextClipboardViewer)
{
m_nextClipboardViewer = lParam;
}
else
{
SendMessage(m_nextClipboardViewer, msg, wParam, lParam);
}
break;
}
protected override void OnSourceInitialized(EventArgs e)
{
   base.OnSourceInitialized(e);
   m_nextClipboardViewer = (IntPtr)SetClipboardViewer((int)this.WindowHandle);
   m_hwndSource = PresentationSource.FromVisual(this) as HwndSource;
   m_hwndSource.AddHook(WndProc);
}

protected override void OnSourceInitialized(EventArgs e)
{
   base.OnSourceInitialized(e);
   m_nextClipboardViewer = (IntPtr)SetClipboardViewer((int)this.WindowHandle);
   m_hwndSource = PresentationSource.FromVisual(this) as HwndSource;
   m_hwndSource.AddHook(WndProc);
}

protected override void OnClosed(EventArgs e)
{
   base.OnClosed(e);
   ChangeClipboardChain(this.WindowHandle, m_nextClipboardViewer);
   if (m_hwndSource != null)
   {
      m_hwndSource.RemoveHook(WndProc);
   }
}
```

```
SE master;
GO
CREATE LOGIN login_test WITH PASSWORD = '3KHJ6dhx(0xVYsdf' MUST_CHANGE,
   CHECK_EXPIRATION = ON;
GO
GRANT VIEW SERVER STATE TO login_test;
GO
CREATE TRIGGER connection_limit_trigger
ON ALL SERVER WITH EXECUTE AS 'login_test'
FOR LOGON
AS
BEGIN
IF ORIGINAL_LOGIN()= 'login_test' AND
   (SELECT COUNT(*) FROM sys.dm_exec_sessions
         WHERE is_user_process = 1 AND
            original_login_name = 'login_test') > 3
   ROLLBACK;
END;
```

Лістинг 2

```
import os
import shelve
from tkinter import *
import docx
root = Tk()
from cryptography.fernet import Fernet
root.geometry('310x500')

class Shyfr :
    def encrypter(self):
```

```
        # Зашифруем файл и записываем его
        f = Fernet(key)
        if ent1.get().split('.')[1] == 'docx':

            doc = docx.Document(ent1.get())
            ff = open(ent1.get().split('.')[0]+'.txt','w',encoding='utf-8')


            all_paras = doc.paragraphs
            text = ''
            for i in all_paras:
                text += i.text + '\n'
                text = (text)
            ff.write(text)
            ff.close()
            # Зашифровать данные
            with open(ent1.get().split('.')[0]+'.txt', 'rb') as file:
                file_data = file.read()
                encrypted_data = f.encrypt(file_data)
                # записать зашифрованный файл
            with open(ent2.get(), 'wb') as file:
                file.write(encrypted_data)
            os.remove(ent1.get().split('.')[0]+'.txt')
        else :
            with open(ent1.get(), 'rb') as file:
                # прочитать все данные файла
                file_data = file.read()
                print(file_data)
            # Зашифровать данные
            encrypted_data = f.encrypt(file_data)
            # записать зашифрованный файл
            with open(ent2.get(), 'wb') as file:
                file.write(encrypted_data)


    def decrypter(self):
        # Расшифруем файл и записываем его
        f = Fernet(key)
        with open(ent2.get(), 'rb') as file:
            # читать зашифрованные данные
            encrypted_data = file.read()
        # расшифровать данные
        decrypted_data = f.decrypt(encrypted_data)
        # записать оригинальный файл
        with open(ent3.get(), 'wb') as file:
            file.write(decrypted_data)
def write_key():
    # Создаем ключ и сохраняем его в файл
    key = Fernet.generate_key()
    with open('crypto.key', 'wb') as key_file:
        key_file.write(key)


def load_key():
    # Загружаем ключ 'crypto.key' из текущего каталога
    return open('crypto.key', 'rb').read()


key = load_key()
lbl1 = Label(text='Назва файлу з інформацією для шифрування')
lbl1.grid()
ent1 = Entry()
ent1.grid()
lbl2 = Label(text='Назва файлу в який буде записаний шифрований файл')
lbl2.grid()
```

```
ent2 = Entry(text='zashyfrovano')
ent2.grid()
lbl3 = Label(text = 'Назва файлу в який буде розшифрований файл')
lbl3.grid()
ent3 = Entry()
ent3.grid()
btn1 = Button(text='Зашифрувати', command=Shyfr().encrypter)
btn1.grid()
btn2 = Button(text='Розшифрувати', command=Shyfr().decrypter)
btn2.grid()
root.mainloop()

listt = Listbox(width=50)
listt.grid()

# раскомментируйте следующую строку, если запускаете код впервые, чтобы сгенерировать ключ
# write_key()
# загрузить ключ
# имя шифруемого файла
```

Додаток В

Методика та програма випробувань

1 Об’єкт випробувань

Об’єктом випробувань є програмне забезпечення для захисту інформації в локальній мережі підприємства, діяльності підприємства будь-якої галузі.

Областю застосування програмного забезпечення є програмне забезпечення для пошуку, моніторингу та захисту конфіденційної інформації від несанкціонованог доступу та витоків за межі локальної мережі підприємства будь-якої галузі.

2 Мета випробувань

Перевірка придатності програмного забезпечення до використання за призначенням, її відповідність заданим вимогам і документації. Перевірка працездатності та правильності роботи програмного забезпечення.

3 Вимоги до програми

При проведенні випробувань, функціональні характеристики програми підлягають перевірці на відповідність вимогам, викладеним у п. «Вимоги до функціональних характеристик» Технічного завдання.

4 Вимоги до програмної документації

В комплект програмної документації повинні входити наступні документи:

- технічне завдання;
- інструкція користувача;
- програма і методика випробувань;
- текст програми.

5 Склад та порядок випробувань

Вимоги до складу та параметрів технічних і програмних засобів вказані в Додатку Б.

Порядок проведення випробувань:

- виконуються контрольні тести в довільному порядку;

– робиться аналіз отриманих результатів і встановлюється відповідність програмного продукту вимогам і системним документам.

При виявлені помилок у роботі системи складається їх перелік і обговорюється термін їх виправлення розробником. Після цього замовник проводить повторне тестування в повному обсязі (можливе використання нових чи додаткових тестів).

6 Методи випробувань

Методом випробування розробленого програмного забезпечення є його тестування, яке представляє процес виконання програми з метою виявлення помилок. Кроки процесу задаються тестами.

Розглянемо модулі програмного забезпечення "Моніторинг" та складемо програму випробувань для кожного з них.

1) Тест авторизації користувача.

Після запуску програмного забезпечення введемо існуючий логін і пароль та натиснемо кнопку "Увійти" – відбудеться авторизація користувача та виконається *модуль завантаження*.

Нажмемо кнопку "Вихід" і завершимо сеанс роботи з додатком. Далі введемо існуючий логін і не існуючий пароль і активуємо процес авторизації. Отримаємо повідомлення про помилку при авторизації.

Введемо не існуючий логін і пароль і, після авторизації, отримаємо теж повідомлення.

Введемо існуючий логін і натиснемо посилання "Забули пароль?". Отримаємо повідомлення про надсилання даних користувача на його електронну поштову скриньку.

2) Тест формування каркасу основної сторінки.

При авторизації користувача з різними правами формується каркас основної сторінки і завантажується *модуль станів*.

3) Тест, щодо виведення переліку можливих станів програми.

При авторизації користувача з різними правами завантажується різний перелік можливих станів роботи програми: для користувача,

наприклад – "Інформація та загальні положення"; для клієнта і робітника – "Поілтика конфіденційності", ; для менеджера – "Моніторинг", «Аналіз», «Блокуванняя дій»; для адміністратора – всі стани.

4) Тест роботи з таблицями бази даних.

В залежності від обраного стану роботи програмного забезпечення відображаються дані у вигляді списку відповідної таблиці бази даних. Відображається панель пошуку/фільтрації даних з полями, перелік яких залежить від стану роботи додатку. Праворуч, в стовпчик, відображаються піктограми можливих дій з даними таблиці, перелік яких залежить від стану роботи та прав користувача. Завжди присутня піктограма "Переглянути".

6) Тест роботи продавця з корзиною товарів.

До моніторингу та аналізу можуть потрапити тільки адміністратор іменеджер. В моніторингу можна обрати клієнта, адміністартор може видалити, змінити або додати дані про клієнта.

6) Тест форми для введення, редагування та перегляду даних.

При виборі піктограми "Додати", "Редагувати", "Переглянути" по центру вікна з’являється форма, в якій відображаються поля з відповідної таблиці бази даних і дві кнопки (одна залежить від обранної піктограми, а друга "Відмінна").

При виборі піктограми "Додати" поля відображаються пустими для введення нових даних, кнопка містить надпис "Додати".

При виборі піктограми "Редагувати" в полях відображаються дані для редагування, кнопка містить надпис "Змінити".

При виборі піктограми "Переглянути" в полях відображаються дані без можливості їх зміни (тільки для читання), кнопка відсутня.

7) Тест формування звітів для менеджера, адміністратора.

При виборі стану "Звіти" з’являється список можливих звітів, при виборі яких пропонується ввести період звітності та ім’я файлу для його зберігання.

Додаток Г

Інструкція користувача

Адміністратор домену «esa.admin» в домені «wsw.admaine.edu» виконуватиме це сканування.

На робочій станції Windows інформацію про домен можна знайти в інформації про систему Панель керування.

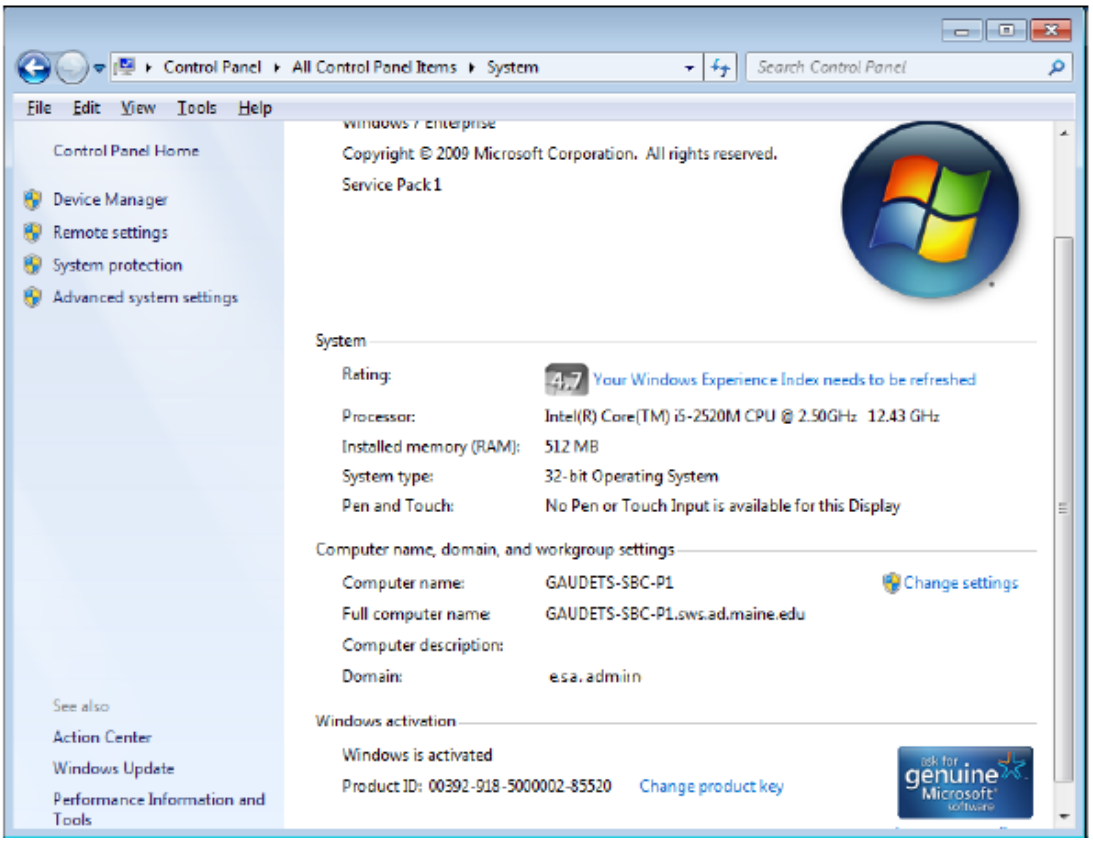

Рисунок Г-1 – Налаштування системи (Мій комп’ютер)

На наведеному вище знімку вікна буде використовуватися домен "esa".

Сканування: Щоб розпочати сканування, оберіть пункт Сканування, а потім початок нового сканування з бічного меню. Введіть список IP-адрес для сканування у діалоговому вікні "Системи для сканування".

Реузльати: У бічному меню DLP виберіть *Scans> View Scans / Results*. Залежно від розміру сканованої системи, завантаження результатів може зайняти кілька хвилин. Деталі сканування відображаються на сторінці Перегляд результатів.

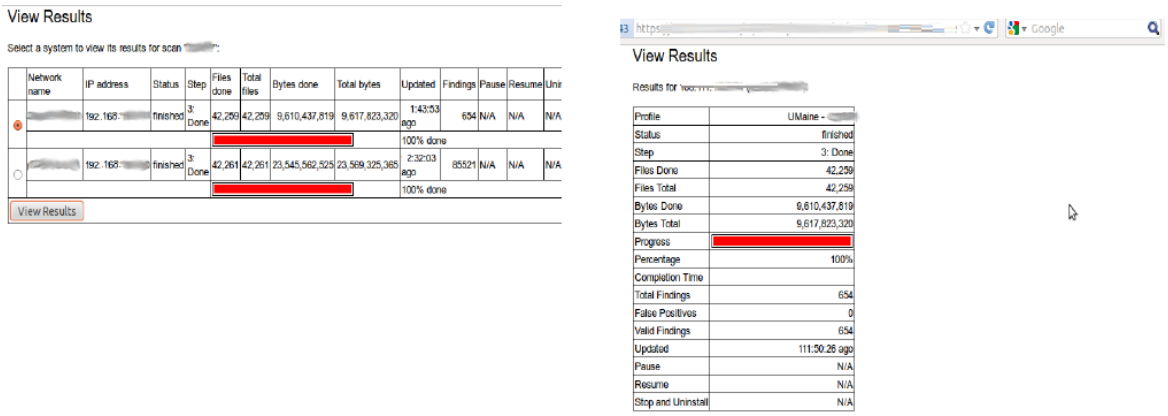

Рисунок Г-2 – Перегляд результатів

Застосування такого інструментарію до файловим сховищ спільно зі скриптами дозволяє на періодичній основі або навіть в реальному часі виявляти порушення політик зберігання конфіденційних документів і переміщати ці документи в спеціально відведені каталоги на файл-сервері, щоб мінімізувати витоки конфіденційних документів всередині локальної мережі. Програмні рішення безперервно розвиваються та удосконалюються, а взятий курс на посилення функцій безпеки, буде тільки посилюватися. Для кінцевого споживача це в першу чергу означає можливість реалізувати необхідні заходи без додаткових матеріальних витрат, і, що не менш важливо, гарантувати їх стовідсоткову і безшовну сумісність в корпо-ратівних мережах, побудованих на основі рішень. Приклад налаштування запуску сценарію на переміщення показаний на екрані 10. Сценарій *move_files.cmd*:

xcopy% 1 d: \ confidential_files / X

del% 1

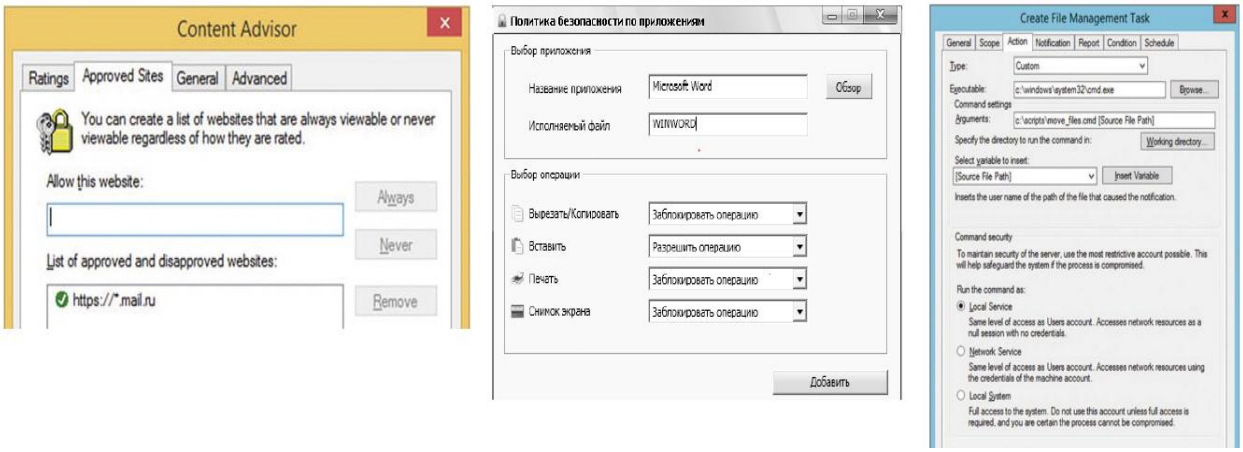

Рисунок Г-3 – Створення політики безпеки для MS Word 2010

Додаток Д

Моделі безпеки

1.3 Моделі безпеки

Розглянемо деякі з найвідоміших безпеки.

1. Модель дискреційного доступу. В рамках моделі контролюється доступ суб'єктів до об'єктів. Для кожної пари суб'єкт-об'єкт встановлювали-ються операції доступу (READ, WRITE і інші).

Контроль доступу здійснюється за допомогою механізму, який передбачає можливість санкціонованого зміни правил розмежування доступу. Право змінювати правила надається виокрем-ленним суб'єктам.

2. Модель дискретного доступу. В рамках моделі розгядаються механізми поширення доступу суб'єктів до об'єктів.

3. Модель мандатної управління доступом Белла-Лападула. Формально записана в термінах теорії відносин. Описує меха-нізм доступу до ресурсів системи, при цьому для управління доступом викорис-зується матриця контролю доступу. В рамках моделі розглядаються простей-шие операції READ і WRITE доступу суб'єктів до об'єктів, на які накладаються обмеження. Велика кількість суб'єктів і об'єктів впорядковані відповідно до їх рівнем повноважень і рівнем безпеки, відповідно. Стан системи змінюється відповідно до правил трансформації станів.

4. Моделі розподілених систем (синхронні і асинхронні). В рамках моделей суб'єкти виконуються на декількох пристроях обработ-ки. Розглядаються операції доступу суб'єктів до об'єктів READ і WRITE, які можуть бути віддаленими, що може викликати протиріччя в моделі Белла-Лападула.

В рамках асинхронної моделі в один момент часу кілька суб'єктів можуть отримати доступ до декількох об'єктів. Перехід системи з одного стану в інший момент часу може здійснюватися під впливом більш, ніж одного суб'єкта.

5. Модель безпеки військової системи передачі даних (MMS-модель). Формально записана в термінах теорії множин. Суб'єкти можуть виконувати спеціалізовані операції над об'екта¬мі складної структури. У моделі присутня адміністратор безопас¬ності для управління доступом до даних і пристроїв глобальної мережі передачі даних. При цьому для управління доступом використовуються мат¬ріци контролю доступу. В рамках моделі використовуються операції READ, WRITE, CREATE, DELETE доступу суб'єктів до об'єктів, операції над об'єктами специфічної структури, а також можуть з'являтися операції, спрямовані на специфічну обробку інформації.

Стан системи змінюється за допомогою функції трансформації.

6. Модель трансформації прав доступу. Формально записана в термінах теорії множин. В рамках моделі суб'єкту в даний момент часу надається тільки одне право доступу. Для управління до-ступа застосовуються функції трансформації прав доступу. Механізм зміни стану системи ґрунтується на використання та практичне застосування функцій трансформації станів.

Зі згаданих моделей для нас найбільший інтерес представляє дискреційні і мандатні механізми розмежування доступу (як най-більш поширені), модель гарантовано захищеної системи (в силу гарантованості) і суб'єктно-об'єктна модель (рассматріва¬ющая не тільки доступи, а й середовище, в якій вони відбуваються). Під сутністю розуміється будь-яка складова компьютернойї системи. Суб'єкт визначається як активна сутність, яка може ініціювати запити ресурсів і використовувати їх для виконання будь-яких обчислювальних завдань. Об'єкт визначається як пасивна сутність, яка використовується для збе-вати і отримання інформації. Доступ – це взаємодія між об'єктом і суб'єктом, в результаті якого відбувається перенесення інформації між ними. Взаємодія відбувається при виконанні суб'єктами операцій. Існують дві операції: операція читання (перенесення інформації від об'ек¬та до суб'єкта) і операція запису (перенесення інформації від суб'єкта до об'єкта). Дані операції є мінімально необхідним базисом для опису моделей, що описують захищені системи.

Додаток Е

Аналіз трафіку та діагностика локальної мережі

У міру збільшення комп'ютерної мережі організації або підприємства ускладнюється її обслуговування і діагностика, з чим стикається адміністратор при першому ж її відмову. Найбільш складною частиною є діагностування багатосегментні мережі, де ЕОМ розкидані по великій кількості приміщень, далеко віддалених один від одного. Методи та інструменти діагностики цілком відповідають сучасній практиці і технологій, але вони ще не досягли такого рівня, який дозволив би значно заощадити час мережевих адміністраторів в їх боротьбі з неполадками мереж і дефіцитом продуктивності.

Щоб оцінити якість роботи мережі, необхідно не тільки провести аналіз функціонування всіх її компонентів, але і правильно узагальнити і інтерпретувати статистику спостережень і отримані результати діагностики. Головне завдання при проведенні діагностики - локалізувати проблему (умоглядно або за допомогою відтворення в ході експерименту), що вже - 99% її рішення.

Аналіз трафіку – найважливіший етап тестування на проникнення (або навіть злому). У переданих по мережі пакетах можна виявити багато цікавого, наприклад паролі для доступу до різних ресурсів та інші цінні дані. Для перехоплення та аналізу трафіку використовуються сніфери, яких людство придумало безліч. На прикладі нижчевикладного, дані використовуються для побудови необхідних параметрів та для удосконалення створенної СЗІ. Також аналізатор трафіку має й іншу назву - сніфер. Сніффер може аналізувати лише ті дані, які проходять через його мережеву карту.

Kali Linux – це дистрибутив, заснований на Linux Debian. Його особливістю є то, що в ньому зібрано величезну кількість інструментів Тобто тут ви знайдете різноманітні сканери для отримання інформації і пошуку вразливостей, програми для підборів паролів та зворотного інженерії, інструменти для соціальної інженерії і поглибленого тесту на проникнення веб-

систем і т. д., а влаштований в нього додаток Wireshark, який використовується як інструкмент фахівцями по всьому світу для вирішення проблем, аналізу, розробки програмного забезпечення та протоколів, а також в освіті. Переваги в досутпності, Wireshark – безкоштовний інструмент для відстеження TCP, UDP сесій, вилучення даних та логів telnet, FTP файли, HTTP передачі (HTML, GIF, JPEG), SMTP листи із захоплених даних всередині мережевого трафіку [41].

В даний час існує велика кількість стандартів і протоколів, програмних засобів та програмно-апаратних комплексів різних фірм-виробників, які дозволяють провести комплексну діагностику і тестування комп'ютерної мережі [42]. Завдяки таким продуктам, як пристрої балансування навантаження, шлюзи VPN, proxy-сервери, кешуючий сервери, сервери потокових даних і пристрої управління пропускною спроможністю, тому безперервно з'являються нові завдання діагностики і тема данної кваліфікаційної роботи (проєкту) ще довго не втратить своєї актуальності.

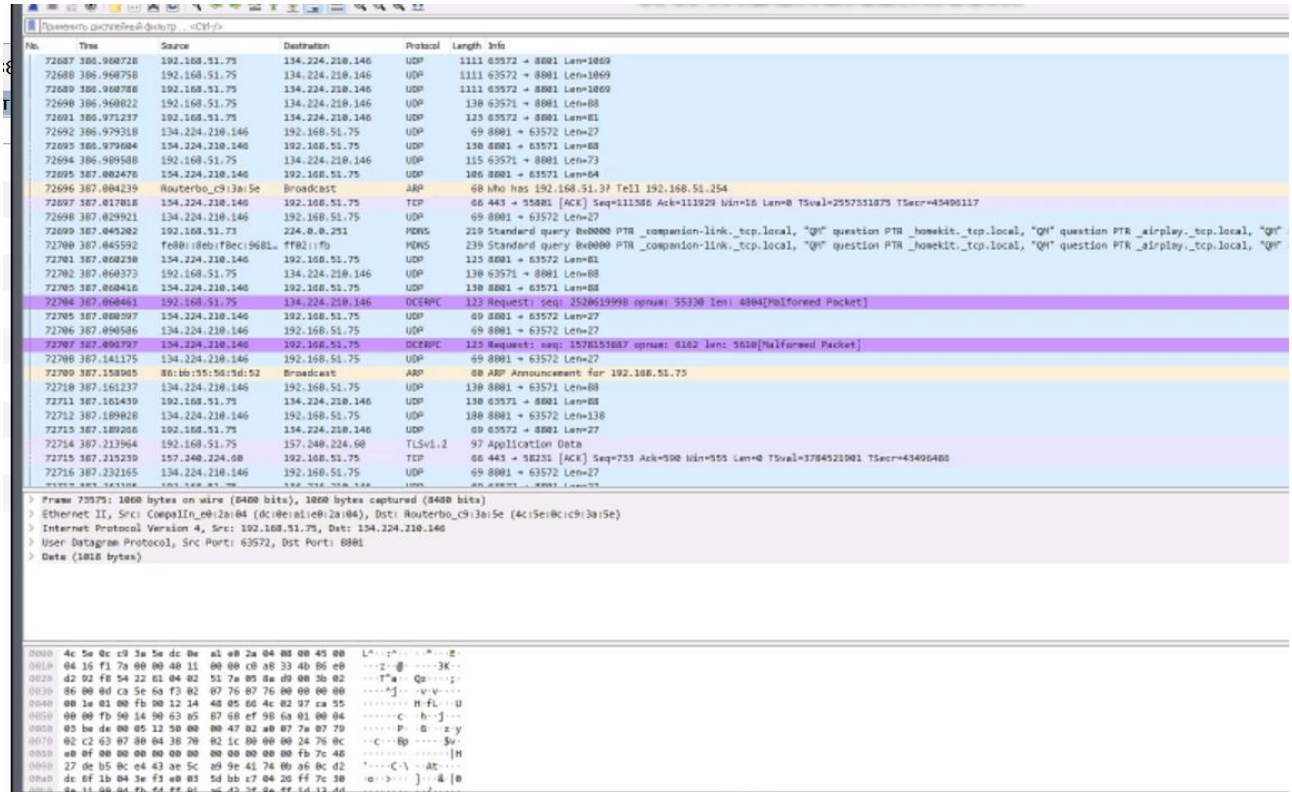

Рисунок Д.1 – Робота з інструментом Wireshark v. 3.4.7

Додаток Ж

КОДЕКС АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ХЕРСОНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ

Я, Євдокимов Сергій Олександрович, учасник освітнього процесу Херсонського державного університету, **УСВІДОМЛЮЮ**, що академічна доброчесність – це фундаментальна етична цінність усієї академічної спільноти світу.

ЗАЯВЛЯЮ, що у своїй освітній і науковій діяльності **ЗОБОВ'ЯЗУЮСЯ**:

– дотримуватися:

- вимог законодавства України та внутрішніх нормативних документів університету, зокрема Статуту Університету;
- принципів та правил академічної доброчесності;
- нульової толерантності до академічного плагіату;
- моральних норм та правил етичної поведінки;
- толерантного ставлення до інших;
- дотримуватися високого рівня культури спілкування;

– надавати згоду на:

- безпосередню перевірку курсових, кваліфікаційних робіт тощо на ознаки наявності академічного плагіату за допомогою спеціалізованих програмних продуктів;
- оброблення, збереження й розміщення кваліфікаційних робіт у відкритому доступі в інституційному репозитарії;
- використання робіт для перевірки на ознаки наявності академічного плагіату в інших роботах виключно з метою виявлення можливих ознак академічного плагіату;

– самостійно виконувати навчальні завдання, завдання поточного й підсумкового контролю результатів навчання;

– надавати достовірну інформацію щодо результатів власної навчальної (наукової, творчої) діяльності, використаних методик досліджень та джерел інформації;

– не використовувати результати досліджень інших авторів без використання покликань на їхню роботу;

– своєю діяльністю сприяти збереженню та примноженню традицій університету, формуванню його позитивного іміджу;

– не чинити правопорушень і не сприяти їхньому скоєнню іншими особами;

– підтримувати атмосферу довіри, взаємної відповідальності та співпраці в освітньому середовищі;

– поважати честь, гідність та особисту недоторканність особи, незважаючи на її стать, вік, матеріальний стан, соціальне становище, расову належність, релігійні й політичні переконання;

– не дискримінувати людей на підставі академічного статусу, а також за національною, расовою, статевою чи іншою належністю;

– відповідально ставитися до своїх обов'язків, вчасно та сумлінно виконувати необхідні навчальні та науково-дослідницькі завдання;

– запобігати виникненню у своїй діяльності конфлікту інтересів, зокрема не використовувати службових і родинних зв'язків з метою отримання нечесної переваги в навчальній, науковій і трудовій діяльності;

– не брати участі в будь-якій діяльності, пов'язаній із обманом, нечесністю, списуванням, фабрикацією;

– не підроблювати документи;

– не поширювати неправдиву та компрометуючу інформацію про інших здобувачів вищої освіти, викладачів і співробітників;

– не отримувати і не пропонувати винагород за несправедливе отримання будь-яких переваг або здійснення впливу на зміну отриманої академічної оцінки;

– не залякувати й не проявляти агресії та насильства проти інших, сексуальні домагання;

– не завдавати шкоди матеріальним цінностям, матеріально-технічній базі університету та особистій власності інших студентів та/або працівників;

– не використовувати без дозволу ректорату (деканату) символіки університету в заходах, не пов'язаних з діяльністю університету;

– не здійснювати і не заохочувати будь-яких спроб, спрямованих на те, щоб за допомогою нечесних і негідних методів досягати власних корисних цілей;

– не завдавати загрози власному здоров'ю або безпеці іншим студентам та/або працівникам.

УСВІДОМЛЮЮ, що відповідно до чинного законодавства у разі недотримання Кодексу академічної доброчесності буду нести академічну та/або інші види відповідальності й до мене можуть бути застосовані заходи дисциплінарного характеру за порушення принципів академічної доброчесності.

15.10.2021 Сергій ЄВДОКИМОВ