Міністерство освіти і науки України

Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Воловатова Антона Віталійовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1] ***Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз рівня захищеності системи електронного документообігу Обласного господарського суду***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Воловатов А.В.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1] ***Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз рівня захищеності системи електронного документообігу Обласного господарського суду***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від _29.11.18__ № 2025-л _____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***Система електронного документообігу***

Предмет досліджень ***Рівень захищеності системи електронного документообігу***

Мета ***Аналіз рівня захищеності системи електронного документообігу та дослідження підписання медійних файлів з допомогою електронного підпису***

Вихідні дані для проведення роботи ***матеріали науково – дослідної та преддипломної практик***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***Аналіз можливості реалізації атаки «заміна шрифту» та спосіб підписання медійного файлу***

Практична цінність ***Запобігання реалізації атаки «заміна шрифту», підтвердження оригінальності та цілісності медійних файлів***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Відповідність методичним рекомендаціям до підготовки та захисту дипломної роботи та вимогам нормативним документів та законів в сфері електронного документообігу

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***Запобігання фінансових затрат у разі реалізації атаки на електронний документ***

Соціальний ефект ***Підтвердження оригінальності та цілісності медійних файлів***

7 ДОДАТКОВІ ВИМОГИ

Відповідність вимогам українського законодавства, відомчих нормативно – правових актів та міжнародних стандартів

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: с., рис., табл., додатків, джерел.

Об’єкт дослідження: система електронного документообігу

Мета роботи: проведення аналізу рівні захищеності системи електронного документообігу.

Метод дослідження – аналіз і випробування.

У роботі проведено аналіз популярних систем електронного документообігу як об’єкта досліджень. Проведено дослідження вразливості електронного документа на атаку «заміна шрифту», на основі якої визначено, що реалізація цієї атаки неможлива.

В економічному розділі наведено обгрунтування потреби проведення аналізу систем електронного документообігу.

Практичне значення роботи полягає у зменшенні часу та фінансових витрат при відновленні системи електронного документообігу та втрачених електронних документів. Результати здійснених у дипломній роботі досліджень можуть бути використані для наступних аналізів систем електронного документообігу

Наукова новизна дослідження полягає у виявленні нових імовірних вразливостей електронного документообігу та аналіз методів підписання медійних файлів з допомогою електронного підпису .

Напрямки подальших досліджень полягають у аналізі інших імовірних вразливостей електронного документу, що не були розглянуті у даній роботі.

СИСТЕМА, ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, ВРАЗЛИВІСТЬ, ЕЛЕКТРОННИЙ ДОКУМЕНТ, МЕТОДИКА, АНАЛІЗ.

РЕФЕРАТ

Пояснительная записка с., рис., табл., приложений, источников.

Объект исследования: система электронного документооборота

Цель работы: проведение анализа уровня защищенности системы электронного документооборота.

Метод исследования - анализ и испытания.

В работе проведен анализ популярных систем электронного документооборота как объекта исследований. Проведено исследование уязвимости электронного документа на атаку «замена шрифта», на основе которой определено, что реализация этой атаки невозможна.

В экономическом разделе приведены обоснования необходимости проведения анализа систем электронного документооборота.

Практическое значение работы состоит в уменьшении времени и финансовых затрат при восстановлении системы электронного документооборота и потерянных электронных документов. Результаты проведенных в дипломной работе исследований могут быть использованы для следующих анализов систем электронного документооборота

Научная новизна исследования заключается в выявлении новых возможных уязвимостей электронного документооборота и анализ методов подписания видео файлов с помощью электронной подписи.

Направления дальнейших исследований заключаются в анализе других возможных уязвимостей электронного документа, которые не были рассмотрены в данной работе.

СИСТЕМА, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ, ВПЕЧАТЛИТЕЛЬНОСТЬ, ЭЛЕКТРОННЫЙ ДОКУМЕНТ, МЕТОДИКА, АНАЛИЗ.

ABSTRACT

Explanatory note: p., Rice, tabl., Applications, sources.

Object of research: system of electronic document circulation

Purpose: to analyze the level of security of the electronic document management system.

Method of research - analysis and testing.

In the special part it is proved that the system of electronic document management has vulnerabilities.

The paper analyzes the popular systems of electronic document circulation as an object of research. The study of the vulnerability of the electronic document to the "replacement of the font" attack was conducted, on the basis of which it was determined that the realization of this attack is impossible.

The economic section provides a justification for the need for an analysis of electronic document management systems.

The practical value of the work is to reduce the time and financial costs of restoring the electronic document flow system and lost electronic documents. The results of the thesis research can be used for the following analyzes of electronic document management systems

The scientific novelty of the study is to identify new likely vulnerabilities in electronic document circulation and to analyze the methods of signing media files with the help of electronic signature.

The direction of further research is to analyze other likely vulnerabilities of the electronic document, which were not considered in this paper.

SYSTEM, ELECTRONIC DOCUMENT COURSES, VARIABILITY, ELECTRONIC DOCUMENT, METHODOLOGY, ANALYSIS.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕД – електронний документ

ЕП – електронний підпис

СЕД – система електронного документообігу

КМУ – Кабінет Міністрів України

AVI – Audio Video Interleaved

RIFF – Resource Interchange File Format

WMV – Windows Media Video

ASF – Advanced Systems Format

MKV – Matroska Multimedia Container

MPEG – Moving Picture Experts Group

ЗМІСТ

С.

ВСТУП

В даний час всі державні служби переходять від паперової форми документообігу до електронного документообігу. На даний момент в Україні , розроблена законодавча база яка сприяє введення в дію електронного документообігу. В зв’язку з стрімким переходом від паперового документообігу до електронного документообігу, виникає питання з реалізації рівня захисту системи електронного документообігу та електронних документів.

Вразливості систем електронного документообігу та електронних документів підписаних з допомогою електронного підпису, дають змогу зловмисникам провести ряд атак та в результаті змінити або знищити електронний документ. Також в зв’язку імовірними змінами, шо до форматів електронних документів, можлива імовірність, що медійні файли згодом прийдеться також підтверджувати його цілісність та оригінальність.

Об’єкт дослідження: Система електронного документообігу.

Мета роботи: проведення аналізу рівні захищеності системи електронного документообігу.

У роботі проведено аналіз імовірних вразливостей електронних документів, а також аналіз методів підписання медійних файлів з допомогою електронного підпису.

Практичне значення роботи полягає в виявленні імовірних вразливостей електронного документу та запобігання реалізації імовірних атак.

Наукова новизна дослідження полягає в аналізі та виявленні вразливостей системи електронного документообігу та аналіз методів підписання медійних файлів.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Нормативно-правова база в сфері електронного документообігу.

На даний час в Україні досі триває процес по переходу від паперового документообігу до електронного документообігу. Питання в правовому урегулюванні цього процесу є актуальним. Електронний документообіг регулюється законами України, такими як:

- Конституція України;
- Цивільним кодексом України;
- Закон України «Про інформацію»;
- Закон України «Про захист інформації в автоматизованих системах»;
- Закон України «Про державну таємницю»;
- Закон України «Про телекомунікації»;
- Закон України «Про обов'язковий примірник документів»;
- Закон України «Про Національний архівний фонд та архівні установи»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про основні засади забезпечення кібербезпеки України»;
- Закон України «Про електронні довірчі послуги»;
- Закон України «Про електронний цифровий підпис»(втратив чинність від 05.10.2017);

Також постанови Кабінету Міністрів України:

- Постанова від 28 жовтня 2004 *року* «Типовий порядок встановлює загальні правила документування в органах виконавчої влади управлінської діяльності в електронній формі і регламентує виконання

дій з електронними документами з моменту їх створення або отримання до відправлення чи передачі до архіву органу виконавчої влади»;(не є дійсна на теперішній час)

- Постанова від 26 травня 2004 року «Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу»;
- Постанова від 17 січня 2018 року «Деякі питання документування управлінської діяльності»;
- Наказ Державного Комітета Архівів України «Про затвердження порядку зберігання електронних документів в архівних установах» (на теперішній час не дійсний);
- Наказ Міністерства Юстиції України «Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання».

Один з основних регулюючих законів України в сфері електронного документообігу є Закон України «Про електронні документи та електронний документообіг».

Основні поняття:

- Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.
- Електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Також в законі України «Про електронні документи та електронний документообіг», визначенні організаційно-правові засади щодо відправлення та одержання документів , зберігання електронних документів, перевірка та підтвердження цілісності та оригінальності електронного документа, правовий

статус електронного документа. Згідно цього закону електронний документ має таку юридичну силу як и паперова його копія. Але для підтвердження цілісності та оригінальності електронного документа використовують – електронний цифровий підпис або електронну печатку.

«Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України "Про електронні довірчі послуги»

Згідно з законом України «Про електронні довірчі послуги» який почав свою дію від 05.10.2017, з'явились деякі зміни. Органи виконавчої влади почали використовувати кваліфіковані печатки та кваліфікований цифровий підпис, також з'явились кваліфіковані центри сертифікації ключів. Кваліфікований електронний підпис – це удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа.

Кваліфіковані надавачів електронних довірчих послуг, кваліфіковані печатки та кваліфікований електронний цифровий підпис з'явились в наслідок прийняття Постанови КМУ від 19.09.2018 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності» та наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про вимоги з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації». Одна з проблем даного наказу, це прийняття за основу міжнародні стандарти, деякі з них навіть не мають перекладу на державну мову, а трактуються на оригінальній мові.

Кваліфіковані надавачі електронних довірчих послуг- це так звані акредитовані центри сертифікації ключів. В Україні на даний час налічується 21 кваліфікований надавач електронних довірчих послуг.

Згідно цього закону до складу електронних довірчих послуг відносяться:

- створення, перевірка та підтвердження удосконаленого електронного підпису чи печатки;
- формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки;
- зберігання удосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності. Згідно закону України «Про електронні довірчі послуги». Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису (КЕП) чи печатки надається кваліфікованим постачальником електронних довірчих послуг та включає:

- надання користувачам електронних довірчих послуг засобів кваліфікованого електронного підпису чи печатки для генерації пар ключів та/або створення кваліфікованих електронних підписів чи печаток, та/або перевірки кваліфікованих електронних підписів чи печаток, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки;
- технічну підтримку та обслуговування наданих засобів кваліфікованого електронного підпису чи печатки.

Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо:

- перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису чи печатки;
- перевіркою встановлено, що відповідно до вимог цього Закону на момент створення кваліфікованого електронного підпису чи печатки був

чинним кваліфікований сертифікат електронного підпису чи печатки підписувача чи створювача електронної печатки;

- за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача чи створювача електронної печатки;
- під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки;
- під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов’язаний цей кваліфікований електронний підпис чи печатка.

Згідно з цим законом кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

Згідно з законодавства України електронний документ який підписаний електронним підписом, має юридичну силу як і його паперова копія.

Згідно з Законами України «Про електроні документи та електронний документообіг» та «Про електронні довірчі послуги» можемо зробити такий висновок, що однією з головних складових електронного документа є КЕП. Так як за допомогою КЕП підтверджується оригінальність та цілісність електронного документа.

Наступне, питання яке розглянемо більш детальніше, це постанова КМУ від 28 жовтня 2004 року «Типовий порядок встановлює загальні правила документування в органах виконавчої влади управлінської діяльності в електронній формі і регламентує виконання дій з електронними документами з

моменту їх створення або отримання до відправлення чи передачі до архіву органу виконавчої влади».

В цій постанові вказано яким чином повинно здійснюватися документування в органах виконавчої влади управлінської діяльності в електронній формі і регламентує виконання дій з електронними документами з моменту їх створення або одержання до відправлення чи передачі до архіву органу виконавчої влади. Але на даний час ця постанова не є дійсною. Заміна цієї постанови відбулась 17 січня 2018 року постанова КМУ «Деякі питання документування управлінської діяльності». Згідно з теперішньою постановою КМУ, до неї входять таки розділи як :

- типова інструкцію з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну;
- типова інструкцію з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади;

Інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві та електронного міжвідомчого обміну, регламентує такі дії як :

- порядок проходження електронного документа з моменту його створення, відправлення або одержання до моменту передавання до архіву установи;
- засади організації документування управлінської інформації в електронній формі для установ, які тимчасово створюють документи у паперовій формі;
- загальні засади функціонування та використання системи електронної взаємодії органів виконавчої влади (далі - система взаємодії);
- оперативний інформаційний обмін з використанням службової електронної пошти.

Згідно з цією інструкцією всю організацію електронного документообігу в установі покладається на її службу діловодства, яка забезпечує:

- розроблення в установі єдиного порядку документування управлінської інформації та роботи з документами незалежно від форми їх створення;
- розроблення номенклатури справ установи;
- реєстрацію та облік документів;
- методологію та контроль за дотриманням установленого порядку роботи з електронними документами в структурних підрозділах установи;
- організацію документообігу, формування справ, їх зберігання та підготовку для передавання до архівного підрозділу установи;
- впровадження та нагляд за дотриманням структурними підрозділами установи вимог інструкцій з діловодства та національних стандартів;
- здійснення заходів із зменшення обсягу службового листування в установі та в установах, що належать до сфери її управління;
- використання системи електронного документообігу, ведення та актуалізацію електронних довідників в установі;
- дотримання вимог до підготовки електронних та паперових документів та організації роботи з ними;

Також служба діловодства повинна розробляти інструкцію з діловодства установи, якою одночасно регламентується питання організації діловодства в паперовій та електронній формах.

Система електронного документообігу установи повинна відповідати вимогам законодавства до форматів даних, сервісу інтеграції до системи взаємодії та вимогам нормативно-правових актів у сфері захисту інформації.

Далі розглянемо питання міжвідомчого обміну електронними документами. Обмін електронними документами через систему взаємодії здійснюється виключно з дотриманням вимог до встановлених форматів даних електронного документообігу в установах. Система взаємодії забезпечує гарантовану доставку електронних документів від їх відправників до їх одержувачів (адресатів).

Приймання вхідних електронних документів, виконуються за деякими правилами:

- електронні документи які приходять до установи через систему взаємодії, приймаються службою діловодства;
- електронний документ, що завантажився із системи взаємодії до системи електронного документообігу або надійшов до веб-модуля системи взаємодії установи, вважається доставленим адресату;
- попередній розгляд електронного документа здійснюється в електронній формі службою діловодства установи з використанням системи електронного документообігу або у разі її відсутності веб-модуля системи взаємодії.

За результатами попереднього розгляду отриманий через систему взаємодії електронний документ підлягає реєстрації, крім випадків, коли:

- електронний документ надійшов не за адресою;
- електронний документ надійшов повторно;
- заявлений склад електронного документа не відповідає фактичному;
- реквізити вхідного електронного документа не збігаються з реквізитами, зазначеними в електронному документі;
- на електронному документі відсутній електронний цифровий підпис підписувача чи відсутня електронна печатка установи, наявність якої на ньому передбачена цією Інструкцією;
- на документ накладено електронний цифровий підпис особи, яка не є підписувачем документа або особою, що виконує його обов’язки;
- відсутня електронна позначка часу;

В цій інструкції ідеться також мова, яким чином відбувається надсилання вихідних електронних документів.

Надсилання електронних документів через систему взаємодії їх адресатам здійснюється автоматично та централізовано, за фактом їх завантаження в автоматизованому режимі із системи електронного документообігу (веб-модуля системи взаємодії) установи в систему взаємодії одразу після їх реєстрації.

Не може бути відправлений через систему взаємодії електронний документ, цілісність якого не підтверджено електронним цифровим підписом або електронною печаткою згідно з вимогами цієї інструкції .

Із системи електронного документообігу установи до системи взаємодії завантажуються зареєстровані електронні документи або засвідчені електронні копії документів.

1.2 Аналіз електронного документообігу та типових структурних схем електронного документообігу.

Актуальність цієї теми зумовлена тим, що однією з найскладніших сфер для впровадження автоматизованих інформаційних систем в Україні є передусім документообіг державних структур. І це є значною проблемою, бо документообіг у нашій державі є системою, що забезпечує роботу з документами, які надходять ззовні та готуються всередині установи, насамперед реєструються, передаються працівникам організації, допомагають здійснювати контроль за виконанням певних робіт, вести довідкову роботу і врешті-решт зберігати. Документообіг є дуже важливою складовою частиною процесів управління і прийняття управлінських рішень. Без добре і надійно організованого документообігу сьогодні жодна установа не може якісно та ефективно працювати, адже він впливає на оперативність, економічність і надійність функціонування апарату управління організацією, культуру праці управлінського персоналу і власне на якість управління, займає доволі важливе місце в роботі державних органів.

Електронний документообіг є актуальним, тому що має велику кількість переваг перед паперовим документообігом. Одні з головних аргументів на користь електронного документообіг є :

- створення єдиного інформаційного простору в масштабах підприємства й реалізація всіх процесів саме в системі;
- прискорення та прозорість проходження документів і надання послуг;

- оптимізація процесів, пов’язаних з документообігом, поліпшення контролю над усіма інформаційними потоками і процесами на підприємстві;
- розмежування повноваження, доступу до документів і дії над ними;
- можливість спільної роботи в межах єдиної інфраструктури;
- підвищення швидкості пошуку документів на підприємстві;
- запобігання втраті важливої інформації через недбалість персоналу;
- підвищення рівня інформаційної безпеки за рахунок механізмів електронного цифрового підписів;
- забезпечення всіх документаційних процесів з одночасним застосуванням електронних і паперових версій документів;
- підтримка змішаного документообігу (підготовка документів з паперовим носієм і звітів за шаблонами, облік місця зберігання оригіналів документів);
- створення структурованого реєстру документів відповідно до номенклатури справ підприємства;
- централізоване, структуроване й систематизоване зберігання документів в електронному архіві.

Але електронний документообіг має також і недоліки, такі як:

- придбання програм та самої системи;
- їх упровадження, модернізація й подальше обслуговування.

Але сам електронний документообіг – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно із законодавством. Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних,

телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ. Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

В зв’язку з появою електронного документа , постало питання підтвердження його оригінальності та цілісності. Тому було вирішено використовувати електронний підпис , електронну печатку та електронної позначки часу згідно з Постановою КМУ від 17 січня 2018 року «Про деякі питання документування управлінської діяльності».

Електронний документообіг має типову структурну схему. Данна типова структурна схема, можлива для використання в орган виконавчої влади.

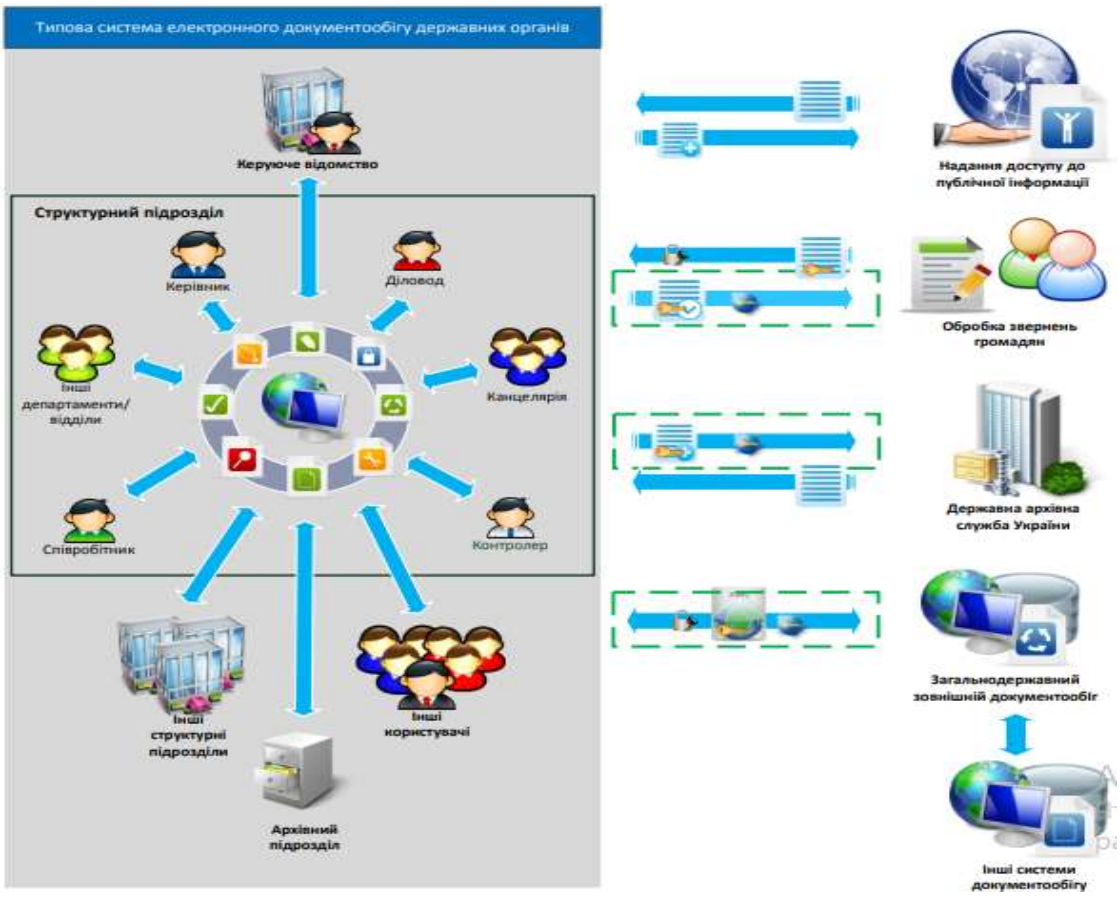


Рисунок 1.1 - Типова структурна схема електронного документообігу

На цій схемі зображено, яким чином можлива побудова систем електронного документообігу та які функції вона може виконувати. Такі як, доступ до внутрішніх документів, обмін між відомостями, надання певної інформації зовнішнім користувачам. Також можемо бачити ,що кожен підрозділ має доступ до системи але з різними правами. Деякі зовнішні зв'язки відбуваються по захищеному каналу зв'язку. На типовій структурній схемі зображенні відділи які в ходять в систему електронного документообігу. Кожен з відділів відповідає за певні функції та мають різноманітний рівень прав. Також зображено яким чином відбувається обмін електронними документами між іншими відомостями. Наприклад обмін ЕД з загально держаними документообігом по захищеному каналу зв'язку, та документи підписанні за допомогою ЕП.

1.3 Системи електронного документообігу.

Таблиця 1.1 Види систем електронного документообігу

№	Системи електронного документообігу органів виконавчої влади	Системи електронного документообігу банків та підприємств різного роду діяльності.
	АСКОД - В обсязі функцій, зазначених в документі «Часткове технічне завдання на розробку захищеного від НСД компонента «Система електроного документообігу АСКОД. Програмне забезпечення АСКОД Корпоративний», сукупність яких визначається функціоналним профілем захищеності: КА-2, КО-1, ЦА-1, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НИ-3, НК-1, НО-3.	Система «Lotus Notes» - забезпечує розроблення і розміщення прикладних програм групового забезпечення, дозволяє користувачам одержувати, відслідковувати, спільно використовувати і створювати інформацію для обробки документів.

Продовження таблиці 1. Види систем електронного документообігу

	Система «Діло» - призначена для автоматизації управлінської діяльності у вітчизняних міністерствах і відомствах, територіальних органах влади, на підприємствах різних сфер діяльності.	Optima Workflow — це комплексне рішення, яке інтегрується з різними електронними системами, створеними для автоматизації бізнес-процесів і оптимізації діяльності на підприємстві. Електронний документообіг прискорює обробку документації, збільшуючи ефективність. Впровадження системи електронного документообігу на базі Optima Workflow дозволяє відмовитися від паперового ведення справ, що істотно оптимізує діяльність компаній і державних установ.
	Система «Кодекс: Документообіг» - це комплекс взаємозалежних систем діловодства, банків документів і корпоративних сервісів, що забезпечують автоматизоване розв' язання задач діловодства і документообігу в органах державної влади й інших організацій.	

Розглянемо кожну систему окремо, які функції вона має, які можливості реалізує. Першою системою яку ми розглянемо буде «Аскод».

Система електронного документообігу АСКОД™ призначена для автоматизації процесів діловодства, службового, господарського та управлінського документообігу, для організації колективної роботи над документами з використанням без паперових технологій та для забезпечення електронного документообігу із застосуванням електронного цифрового підпису (ЕЦП). Сучасна версія системи електронного документообігу

АСКОД™ функціонує на платформі системи управління базами даних ORACLE.

Система електронного документообігу АСКОД™ підтримує такі функції:

- автоматизація уніфікованих технологічних процедур діловодства та службового документообігу (облік, проходження, передача на виконання та опрацювання документів в електронній формі будь якого формату і звичайних паперових документів);
- автоматизація процесів опрацювання вхідних, вихідних, внутрішніх, організаційно-розпорядчих, нормативних та інших видів документів;
- автоматизація процесів опрацювання звернень громадян:
- автоматизація процесів опрацювання запитів на публічну інформацію;
- автоматизація процесів опрацювання заявок на надання послуг;
- автоматизація процесів надання адміністративних послуг;
- можливість автоматизації процесів ведення різноманітних реєстрів;
- автоматизація процесів обліку договорів і контролю їх виконання;
- управління заявками на закупівлю та оплату ТМЦ;
- управління відрядженнями;
- наскрізний контроль строків виконання документів, оповіщення виконавця і контролера про наближення строків виконання, про невиконані в строк документи;
- підтримка версій документів;
- застосування електронного цифрового підпису;
- формування описів справ для передачі на архівне зберігання;
- автоматизація архівного зберігання документів відповідно до вимог чинного законодавства;
- формування основних звітів щодо документообігу та контролю виконання з можливістю відбору даних за визначеними критеріями;

- розмежування прав доступу на рівні: функціональних модулів, функцій, групи операцій, окремих операцій, атрибутів реєстраційної картки, групи документів, окремих документів;

Система АСКОД™ підтримує обмін даними і документами з системою електронної взаємодії центральних органів виконавчої влади.

Система АСКОД™ забезпечує можливість формування переліку публічної інформації(даних та електронних копій документів) для публікації на WEB-сайтах. Система АСКОД™ має у своєму складі функціонал - АРМ Керівника, який надає можливість керівникам підприємства (установи) підписувати документи електронним цифровим підписом, здійснювати розгляд документів, приймати рішення щодо їх виконання (накладати резолюцію, формулювати доручення та завдання) та здійснювати контроль за їх виконанням. АРМ Керівника може функціонувати як на настільних персональних комп'ютерах так і на мобільних планшетних засобах (на базі операційних систем Windows, iOS та Android).

Система АСКОД™ дозволяє впровадити технологію централізованого документообігу для підприємств (установ) з територіально-розподіленою організаційною структурою та забезпечує повноцінну роботу територіально-віддалених користувачів системи через WEB-доступ.

Система базується на певних функціональних профілях захисту, а саме:

- КА-2 – базова адміністративна конфіденційність;
- КО-1 – повторне використання об'єктів;
- ЦА-1 – мінімальна адміністративна цілісність;
- ЦО-1 – обмежений відкат;
- ДР-1 – квоти;
- ДС-1 – стійкість при обмежених відмовах;
- ДЗ-1 – модернізація;
- ДВ-1 – ручне відновлення;

- НР-2 – захищений журнал;
- НИ-2 – одиночна ідентифікація і автентифікація;
- НИ-3 - множинна ідентифікація і автентифікація;
- НК-1 - однонаправлений достовірний канал;
- НО-3 - розподіл обов'язків на підставі привілеїв;
- НЦ-1 - КЗЗ з контролем цілісності;
- НТ-2 - самотестування при старті;
- НА-2 - автентифікація відправника з підтвердженням;
- рівень гарантії – 2.

Наступна система електронного документообігу яку розглянемо – система «ДІЛО». Система "ДІЛО" - комплексний промисловий розв'язок, що забезпечує автоматизацію процесу діловодства, а також ведення повністю електронного документообігу організації. Система ефективно використовується як у невеликих комерційних компаніях, так і в розподілених холдингових або відомчих структурах.

Переваги системи:

- швидкий пошук документів;
- відстеження руху документа на всіх етапах його життєвого циклу;
- ефективний контроль і звітність по виконанню резолюцій;
- скорочення строків підготовки й узгодження документів;
- зручна робота над проектами документів;
- можливість делегування повноважень;
- швидка й зручна реєстрація документів за допомогою розгорнутої системи різних довідників;
- відстеження ходу виконання резолюцій;
- зручний і швидкий пошук по будь-яких реквізитах реєстраційної картки(РК) як документів, так і проектів (РКПД);

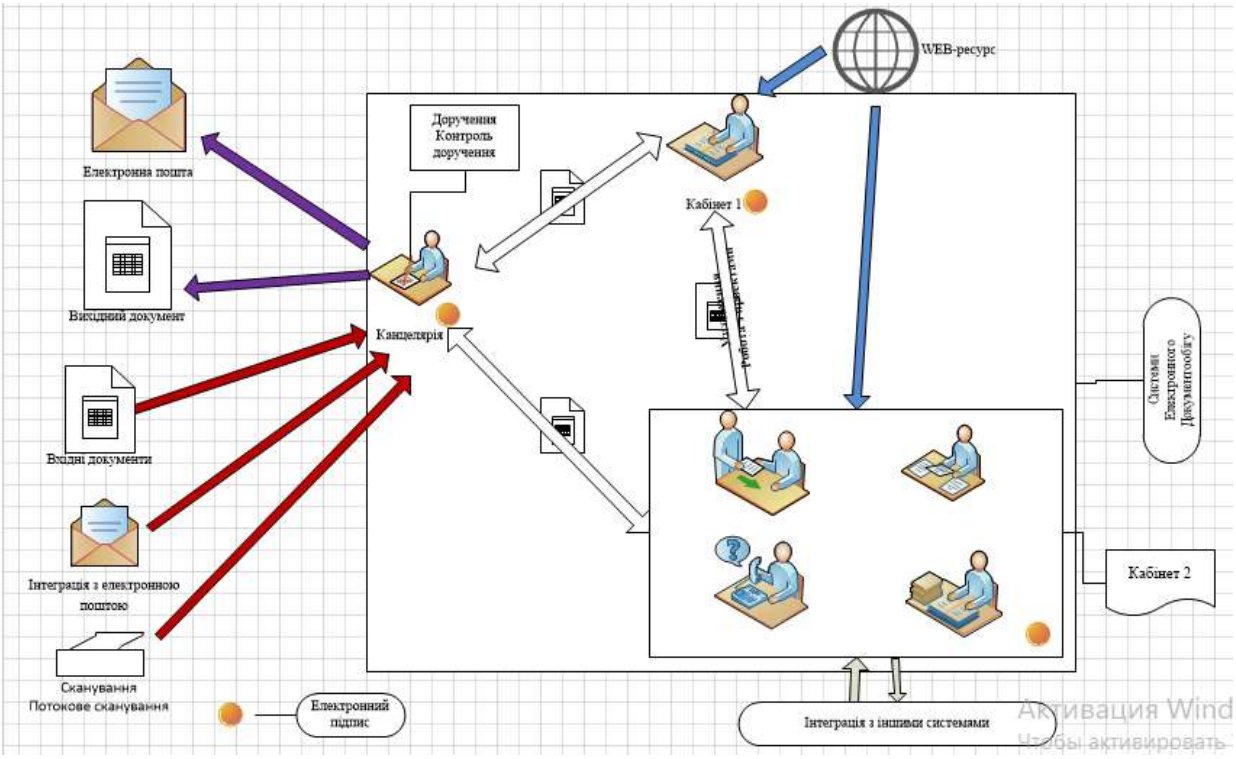


Рисунок 1.2 - «Типова структурна схема побудови системи ДІЛО в організації »

Основні характеристики системи «ДІЛО»:

- масштабна й гнучка в настроюванні, легко адаптується до специфіки документообігу в організаціях будь-якого розміру від одного робочого місця й до тисячі;
- забезпечує необхідний рівень конфіденційності інформації й відповідність усім нормативним вимогам як російського, українського, білоруського діловодства, так і міжнародних стандартів (ISO 15489 "Інформація й документація - Керування документами" і ISO/IEC 17799:2000 "Інформаційні технології - Практичний посібник з керування інформаційною безпекою");
- забезпечує захищений електронний документообіг з використанням електронного підпису (ЕП) і спеціальних криптографічних засобів. Компанія "Електронні Офісні Системи" має всі необхідні сертифікати для використання засобів захисту інформації у своїх продуктах;

- має можливості масового переводу паперових документів в електронний вид і переміщення їх у базу даних системи за допомогою опції "Потокове сканування";
- підтримує повний цикл роботи із проектами документів, у тому числі їх маршрутизацію і версії;
- має відкриту архітектуру й надає можливість інтеграції з іншими програмними засобами як компанії ЕОС, так і інших виробників програмних продуктів.

Кожна система реалізує сам процес електронного документообігу. В системі циркулюють електронні документи різних форматів. Існують безліч форматів які вважаються електронними документами та підлягають підписанню за допомогою ЕП. На об’єкті дослідження циркулюють електронні документи таких форматів як:

- PDF - повна назва: Portable Document Format/Archival-1 – відкритий міжоперабельний формат для обміну електронними документами/архівний - частина 1. Тип формату: текстово-графічний формат для довгострокового зберігання електронних документів. Використання електронного цифрового підпису у документах, сформованих у форматі PDF/A, повинно здійснюватися відповідно до вимог наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованого у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (із змінами).
- DOCX – без сумнівів, документ Microsoft Word, сама популярна програма для роботи текстами. Word є в наявності всіх версій офісного пакету Microsoft Word. Файли форматів DOCX, містять різноманітну інформацію о форматуванні тексту – шрифти, вирівняння тексту, відступ, абзаци, списки, колонки и т.д. Документи Microsoft Word також

можуть включати в себе зображення, діаграми, таблиці, сценарії. Окрім різноманітних об’єктів, тексту та інформації про форматування, файл містить параметри документа.

Документ Word насправді це не один файл, це сукупність конфігураційних файлів.

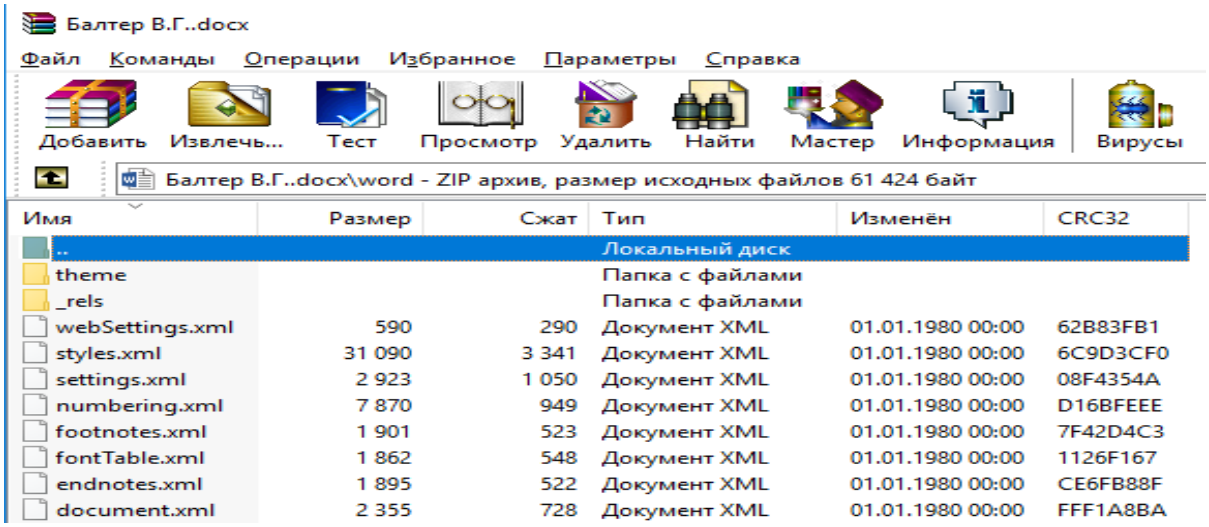


Рисунок 1.3 – Структура документа Word.

В цьому архіві файлів Word документа, знаходяться безліч конфігураційних файлів. Файли які відповідають за шрифт, файли відповідаючи за форму та структуру самого документа.

Важливо враховувати також, якого виду інформація циркулює в електронних документах. Інформація може бути відкритого типу, службова, з обмеженим доступом(конфіденційна та таємна). Треба розуміти які види захисту приймати для видів інформації. Деякі електронні документи захищають їх цілісність не тільки за рахунок ресурсів електронного підпису, а за допомогою інших програмних продуктів. З кожним роком з’являються все більше різноманітних атак на електронні документи підписанні за допомогою електронного підпису.

Для ретельнішого аналізу рівня захищеності систем електронного документообігу, розглянемо на прикладі системи електронного документообігу виконавчого органа влади «Обласного господарського суду».

Розглянемо структурну схему електронного документообігу на прикладі об’єкта дослідження «Господарський суд». Організаційна структура суду, складається з керівника апарату суду, відділ канцелярії, відділ діловодства,

архів, відділ захисту інформації та адміністрування, серверна, судді та їх помічники.

В суді використовують систему електронного документообігу «Діло». В даній системі відбувається розмежування всіх підрозділів. В системі електронного документообігу «Діло», введенні такі терміни як домен, сектор, канцелярій та інші відділи. Сектор – це найменування судді, за кожним суддею закріплений окремий сектор. Домени- це керівник апарату , відділ захисту інформації та адміністрування та серверна.

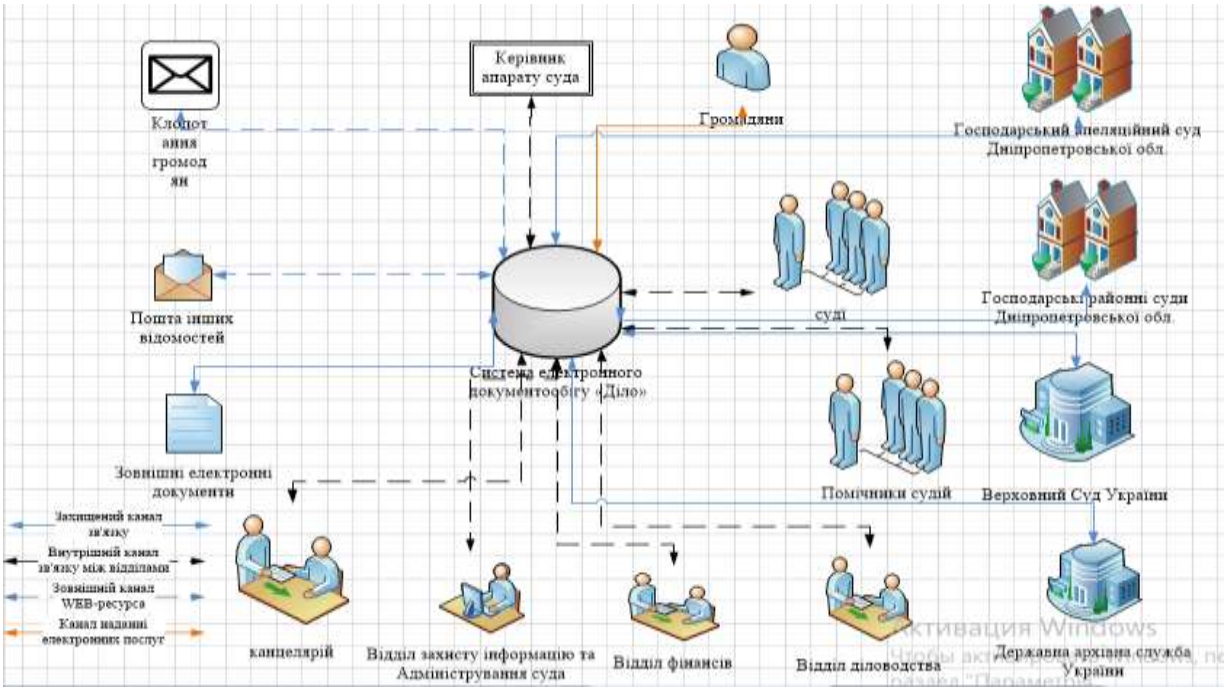


Рисунок 1.4 - Структурна схема електронного документообігу господарського суду.

На структурній схемі зображено яким чином реалізується електронний документообіг в Господарському Суді. Суд має як зовнішній захищений канал зв’язку між іншими виконавчими органами влади, такими як Господарський Апеляційний Суд та інші Господарські суди області. Також має і внутрішній захищений канал зв’язку , який надає змогу обміну електронними документами між відділами та секторами. Пошта та клопотання громадян надходять по зовнішньому каналу WEB-ресурса.

На об’єкті, присутні файли медійних форматів, в зв’язку з веденням судових засідання в вигляди відео-конференції. Ці файли записуються на сервер та на дискові носії, та зберігаються в суді.

1.4 Електронний підпис

Будь який електронний документ, формату Docx. або PDF та навіть медійного формату, не має юридичної сили якщо він не підписаний за допомогою електронного підпису та не має відмітки часу. В наслідок цього, виникає питання яким чином органи виконавчої влади отримує ЕП.

На теперішній час в зв’язку з прийняттям Закону України «Про електроні довірчі послуги», втрачає свою чинність Закон України «Про електронний цифровий підпис». В наслідок таких змін, виникають нові терміни такі як:

- електронний підпис - електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис. Заміна минулого терміну електронний цифровий підпис;
- кваліфікований електронний підпис - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;
- кваліфікований надавач електронних довірчих послуг - юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам Закону України «Про електронні довірчі послуги» та відомості про яку внесені до Довірчого списку;

На даний час в Україні діють 21 кваліфікований надавач електронних довірчих послуг. В зв’язку з прийняттям Закона України «Про електронні довірчі послуги», був затверджений Наказ Адміністрації Державної служби

спеціального зв’язку та захисту інформації України, що до «Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації». Наказ регламентує яким вимогам повинні відповідати кваліфіковані надавачі електронних довірчих послуг, для отримання змогу і далі продовжувати надавати електронні довірчі послуги.

Електронний підпис має безліч атак, за допомогою яких можливо порушити цілісність електронного підпису та змісту файла який підписаний ЕП. Виділяють 3 напрямки атак:

- атака з використанням відкритого ключа;
- колізії першого і другого роду;
- Соціальні атаки.

1.5 Висновок по першому розділу

Проаналізувавши нормативно-правову базу в сфері електронного документообігу. Розглянувши типові структури побудови електронного документообігу та різновид систем які забезпечують сам процес електронного документообігу. Засади електронного документообігу та електронного підпису та різноманітність форматів файлів які підлягають підписанню за допомогою ЕП. Висновок аналізу виглядає таким чином, питання аналізу рівня захищеності систем електронного документообігу є актуальним. В зв’язку з появою нових та різноманітних атак на електронний підпис, модернізацію та оновлення систем електронного документообігу. Це питання потребує більш детальнішого аналізу.

1.6 Постановка задачі

Задача даної дипломної роботи становить, провести аналіз рівня захищеності систем електронного документообігу. Виявлення вразливих моментів ЕП. Та яким чином можливо запобігти атакам на ЕП в системі електронного

документообігу. Також розгляд медійних файлів як електронного документа та як реалізувати ЕП на медійному файлів з меншою вірогідністю зміни змісту файлу.

2. Розділ 2. СПЕЦІАЛЬНИНЙ РОЗДІЛ

2.1 Аналіз рівня захищеності системи електронного документообігу.

Об’єктом дослідження даної дипломної роботи є система електронного документообігу обласного Господарського Суду. В даній установі використовується система електронного документообігу «Діло». Система мала великий попит серед органів влади України.

Перед тим як перейти к аналізу системи електронного документообігу, вважаю вважливо виділити джерело загрози. В установі знаходиться понад 50 судів, кожна суддя має помічника, керівник апарату суду. Також різноманітні відділи такі як: канцелярія, відділ фінансового забезпечення, відділ діловодства, відділ захисту інформації та адміністрування систем, відділ кадрі. Всі відділ певним чином приймають учать в системі електронного документообігу. Розглянемо організаційно-структурну схему обласного Господарського суду.

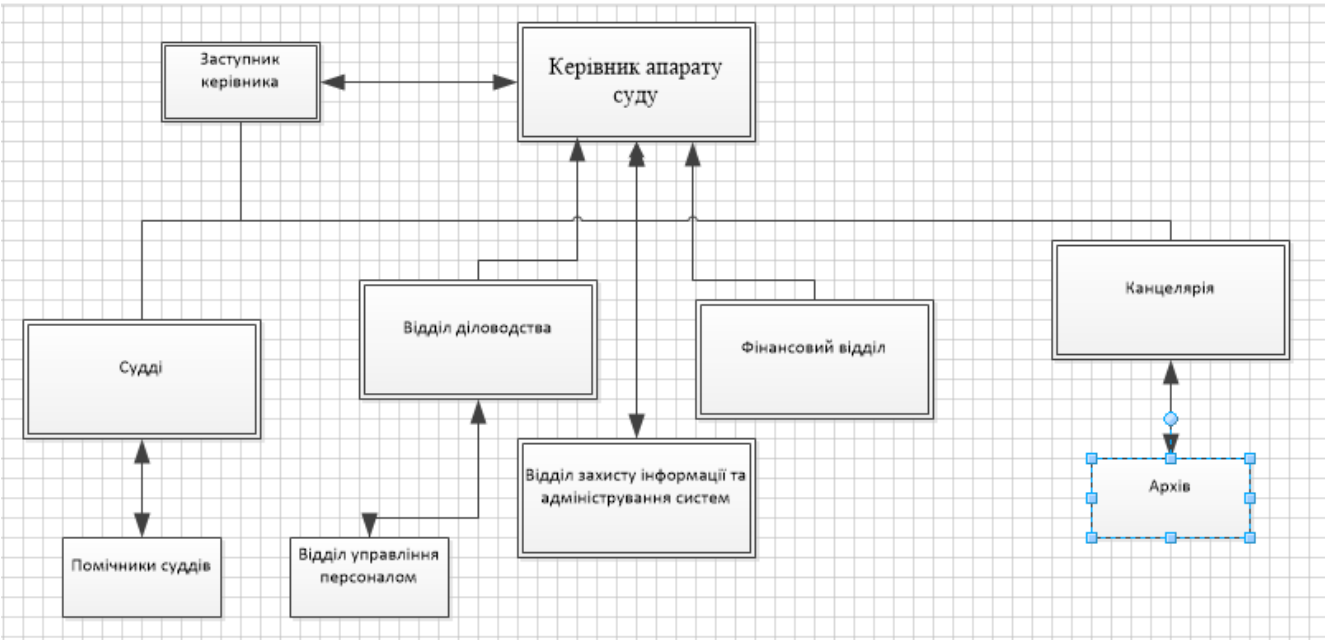


Рисунок 2.1- Організаційна структура обласного Господарського суду

Кожен з відділів є учасником електронного документообігу, та має певні права в цій системі. Тому кожен з них несе загрозу цілісності ЕД.

Тому за допомогою системи «Діло», кожен з цих учасників має різний рівень прав та можливостей в системі електронного документообігу. Деякі з них можуть лише мати право на розгляд документа чи ознайомлення з ним, інші можуть редагувати документ. Право на накладання на документ ЕП лише у керівника апарату суду його заступника та у суддів господарського суду.

Розмежування прав не виключає всі вразливості системи та ЕП. В наш час дуже стрімко з'являються різноманітні способи як реалізувати атаку на ЕП з метою заволодіти інформацією або змінити її.

2.2 Аналіз імовірних атак ЕП.

На даний час існує безліч різноманітних атак на ЕП. Деякі з них потребують великих витрат часу. Розглянемо які атаки існують на даний час та є актуальними:

- атака на основі відомого відкритого ключа (key-only attack) – найслабша з атак, практично завжди доступна для зловмисника;
- проста атака з вибором підписаних повідомлень (generic chosenmessage attack) – зловмисник має можливість обрати певну кількість підписаних повідомлень, при цьому відкритий ключ він отримує після такого вибору;
- спрямована атака з вибором повідомлень (directed chosen-message attack) – обираючи підписані повідомлення, зловмисник знає відкритий ключ;
- адаптивна атака з вибором повідомлень (adaptive chosen-message attack) – зловмисник знає відкритий ключ; вибір кожного наступного підписаного повідомлення він може робити на основі знання припустимого підпису попереднього обраного повідомлення.
- Колізії першого та другого роду;
- Соціальні атаки.

Деякі атаки більш спрямовані на шахрайські дії, такі атаки як соціальні. Ці атаки не потребують дії над ЕП. Соціальні атаки більш спрямовані на власників ЕП або інших членів системи електронного документообігу.

Не мало важливий факт, яка інформація міститься в електронному документі. Деяка інформації потребує більше рівнів захисту ніж ЕП.

Під час аналізу літератури та різноманітних інформаційних джерел, Було виділено цікаву статтю, в якій розповідалось про атаку на електронний документ підписаний електронним підписом з допомогою заміни шрифту. В статті розповідається, що можливо зміна змісту електронного документа після підписання, таким чином щоб ці зміни не були виявленні при перевірці ЕП. Суть цієї атаки полягає в тому, що є в наявності електронний документ в форматі DOCX. підписаний електронним підписом, з певним змістом. Без порушення значення ХЕШ-функції ЕП, за допомогою заміни шрифту змінюється зміст документа на розсуд злочинця. Який в свою чергу використовує безкоштовний програмний продукт FontForge – за допомогою якого можливо не лише модифікувати стандартні шрифти, а створити свій унікальний шрифт.

2.3 Реалізація атаки на електронний документ з допомогою підміни шрифту.

Перед самою реалізацією розглянемо в яких випадках атака має сенс, а в яких далі не треба продовжувати .Приведемо це в якості блок схеми. На блок-схемі зображено які можуть бути варіанти реалізація атаки на основі заміни або модернізації шрифту. Атака не має сенсу продовжуватись якщо при спробі модернізації або заміні шрифту, система Microsoft Windows 10 забороняє проводити будь які модернізації або заміни системних шрифтів. В випадку якщо вдалося замінити шрифт і зміст ЕД був змінений але при перевірці ЕП зафіксував зміни ЕД, атака вважається не реалізованою. Та в випадку якщо при

перевірці ЕП не зафіксував змін ЕД, то атака вважається успішною, а КЗЗ потребує аналізу та внесення поправок.

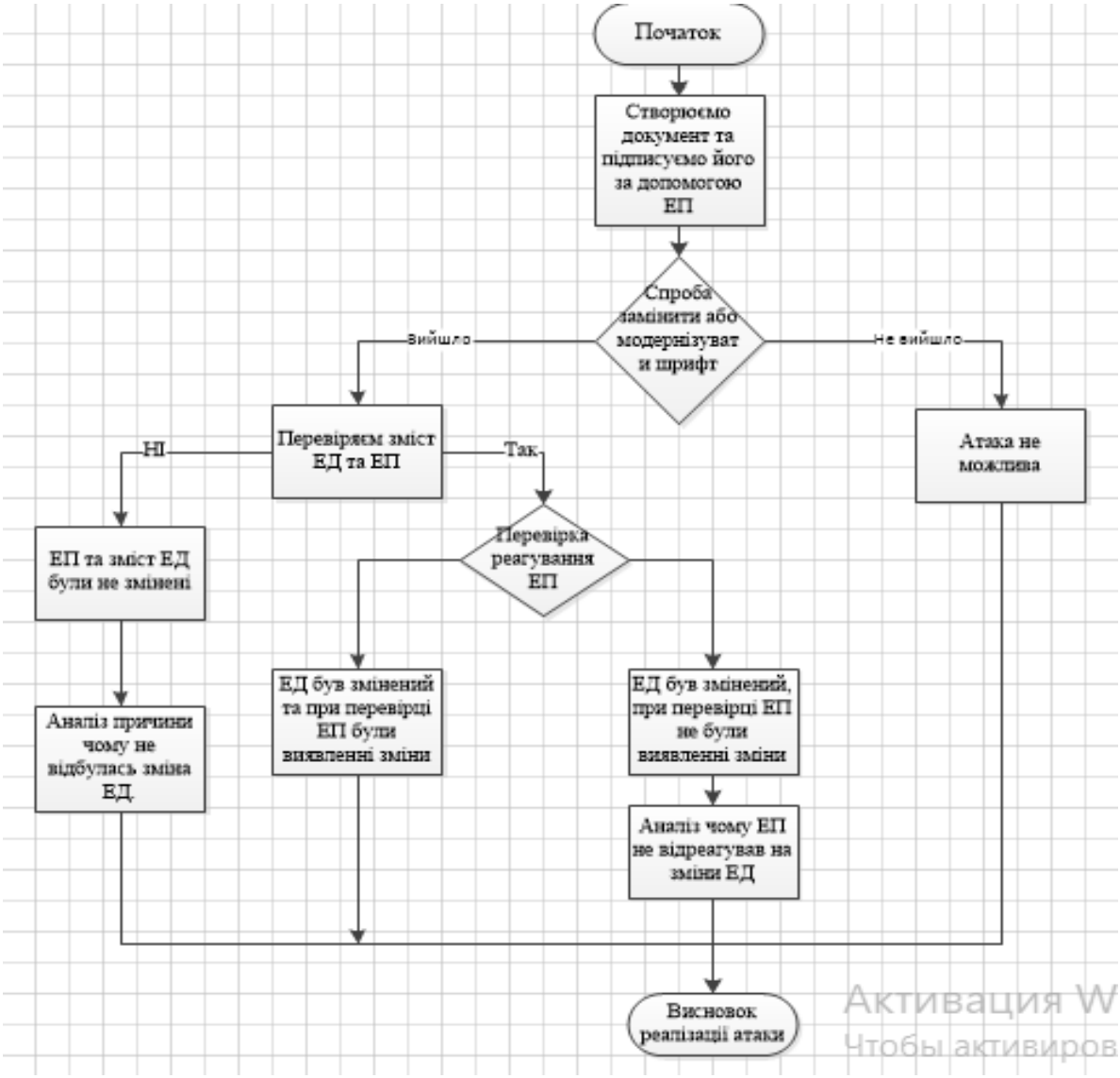


Рисунок 2.2 –Алгоритм реалізації атаки

Для початку потрібно створити документ Test.doc та підписати цей документ за допомогою електронного підпису . Документ повинен бути Microsoft Word 2003, внаслідок того що програмне забезпечення АЦСК ПАО КБ «ПРИВАТБАНК», має обмеження та підписує документи лише до версії Microsoft Word 2003, документи створені в більш новіших версіях виникають труднощі в вигляді відмови підписання документа.

Внаслідок цього обмеження, треба чітко розуміти, що саме підписує ЕП. Сам документ Word має форму архіву та складається з різних конфігураційних

файлів. Розглянемо порівняння документу Microsoft Word 2003 та документу Microsoft Word 2016.

Таблиця 2.1 Порівняння документів Word версій 2003 та 2016.

Характеристика документа Microsoft Word 2003	Характеристика документа Microsoft Word 2016
Конфігураційні файли : - Contents Type – файл містить конфігурації щодо шрифту, стилю та змісту документу. - TemeManager – файл містить конфігурації щодо теми документа.	Конфігураційні файли: - Document – файл містить конфігурації щодо змісту документа. - Styles – файл відповідає за стиль оформлення документа - FontTable – файл відповідає за шрифти які використовуються при оформленні документа - Settings – файл налаштування - Theme1 – файл конфігурації теми документа.

Внаслідок того що зміст конфігураційних файлів відрізняється. Виникає потреба з’ясування які файли потребують підпису з допомогою ЕП. В документі Word версії 2016 року, кожен файл відповідає за окрему складову, внаслідок цього можна зробити висновок, що підписання файл конфігурації який відповідає тільки за зміст документ, не досить тому як є не важливі файли. Такі як : файл який відповідає за шрифт який використовується при формуванні документа, файл який відповідає за стиль документа.

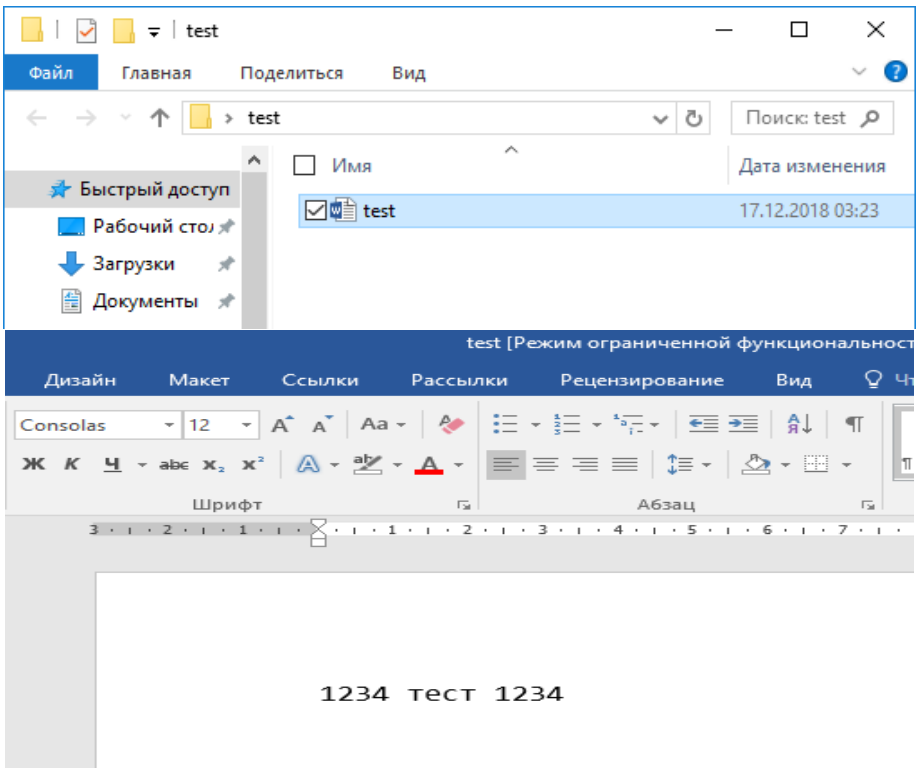
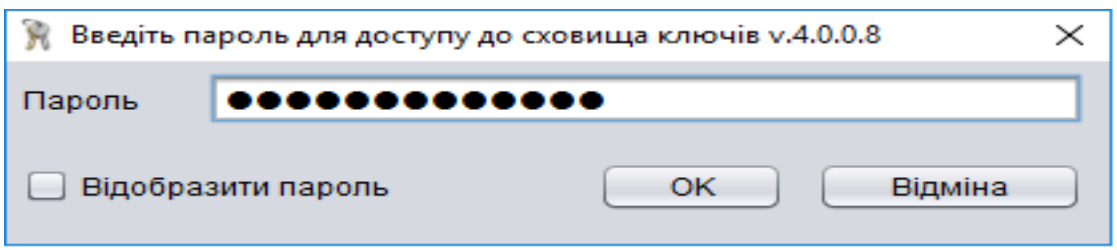


Рисунок 2.3 – Створений документ

Наступний крок підписання документа за допомогою електронного підпису. Для цього нам знадобиться сертифікат ЕП та програмне забезпечення з допомогою якого і відбудеться підписання документа. Підписання документа реалізуємо за допомогою програми АЦСК ПАО КБ «ПРИВАТБАНК». Але є один недолік програми, програма має обмеження та в зв'язку з цим обмеження вона не може накладати ЕП на документи які зроблені у версіях Word документів вище версії Microsoft Word 2003. Внаслідок цього, це несе певні складнощі тому що структура документа Microsoft Word 2016 досить відрізняється від структури документа Microsoft Word 2003.



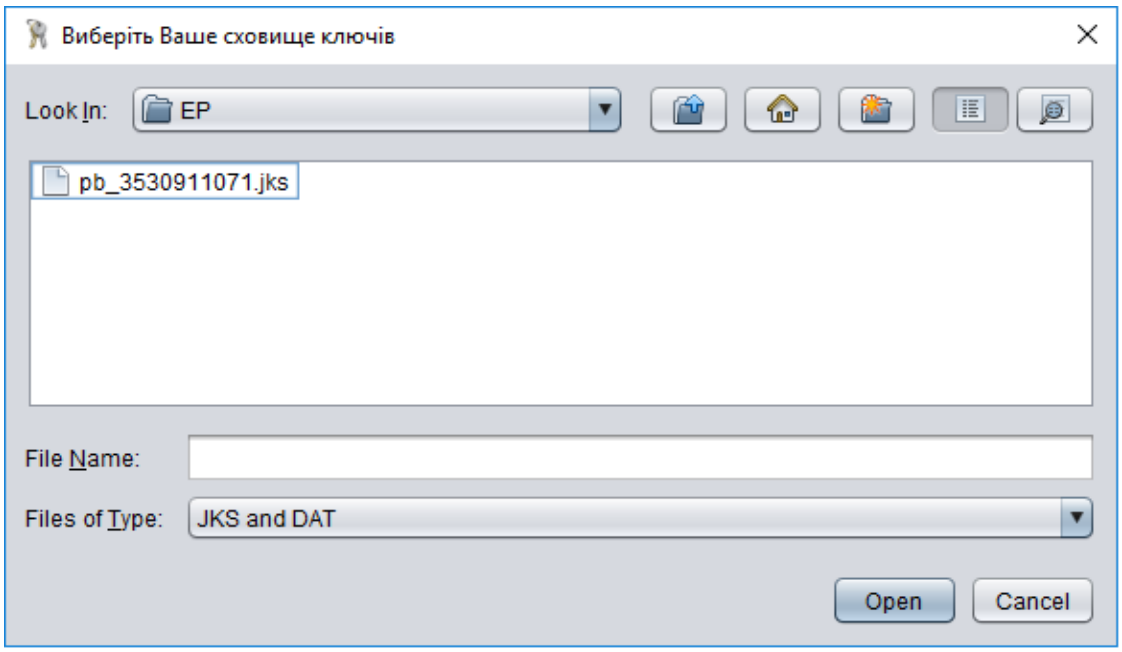
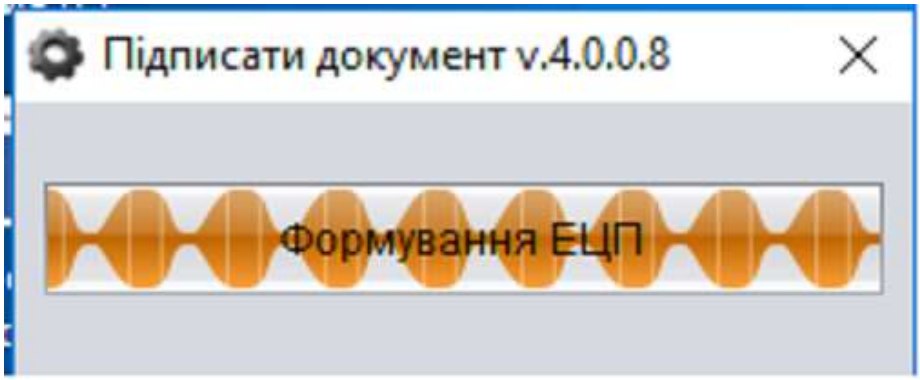
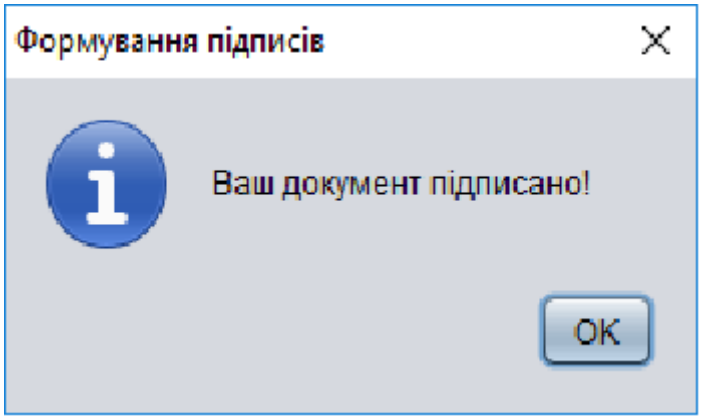


Рисунок 2.4 – Процес підписання документа

Входимо до сховища ключів та вибираємо за допомогою якого ключа будем підписувати документ. Далі вибираємо ключ та підписуємо вибраний нами





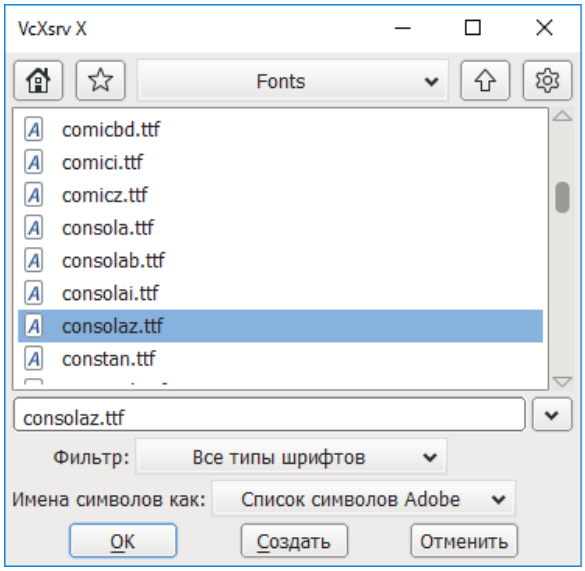
документ.

Рисунок 2.5 – процес підписання документа

При спробі підписання документа Microsoft Word 2016, та перевірці ЕП, програма показувала, що документ не має ЕП. Але при спробі підписання ЕП конфігураційних файлів, було виявлено, що файл підлягає підпису. Внаслідок цього можна зробити висновок, що замість самого документу можна підписати його конфігураційні файли та захистити файл від змін.

Наступний крок, вибір програми для модернізації або створення нового шрифту. Є досить різноманітний вибір програм за допомогою яких можливий процес модернізації шрифту або створення нового. Серед всіх програмних ресурсів які дають змогу реалізувати цей процес, було вибрано програма Font Forge. Причина вибору цієї програми становить в тому, що даний продукт є в вільному доступі та має досить великий спектр функцій. Після встановлення відкриваємо програму та намагаємось модернізувати або замінити шрифт Consolas. За допомогою цього шрифту був створений зміст нашого тестового документу.

Для того щоб модернізувати або замінити шрифт, нам потрібно для початку вибрати директорію в якій знаходяться всі шрифти Microsoft Word. Ця папка знаходить на локальному диску C/ Windows/Fonts. Наступний крок, відкриваємо програму Font Forge, обираємо потрібну нам директорію, та



шукаємо шрифт за допомогою якого був створений текст нашого документа.

Рисунок 2.6 – Вибір шрифту

Після того як потрібний нам шрифт був вибраний, натискаєм «Создать», та переходимо безпосередньо до модернізації шрифту.

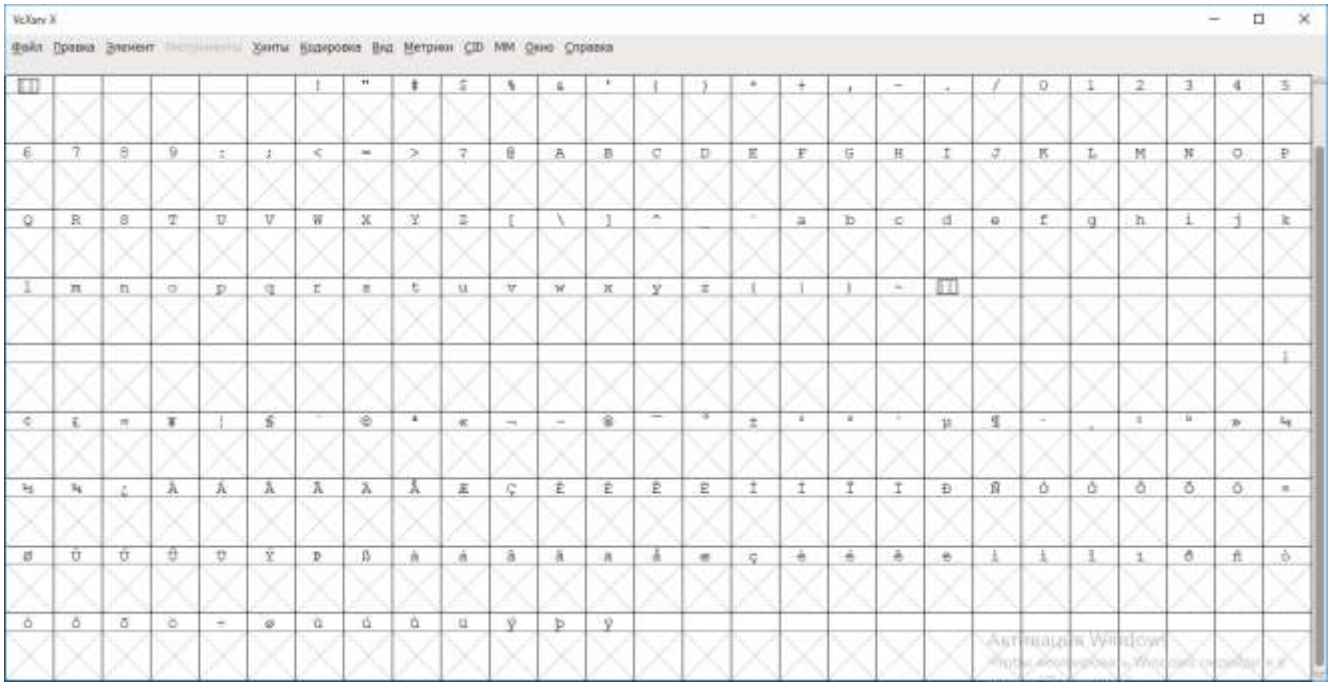
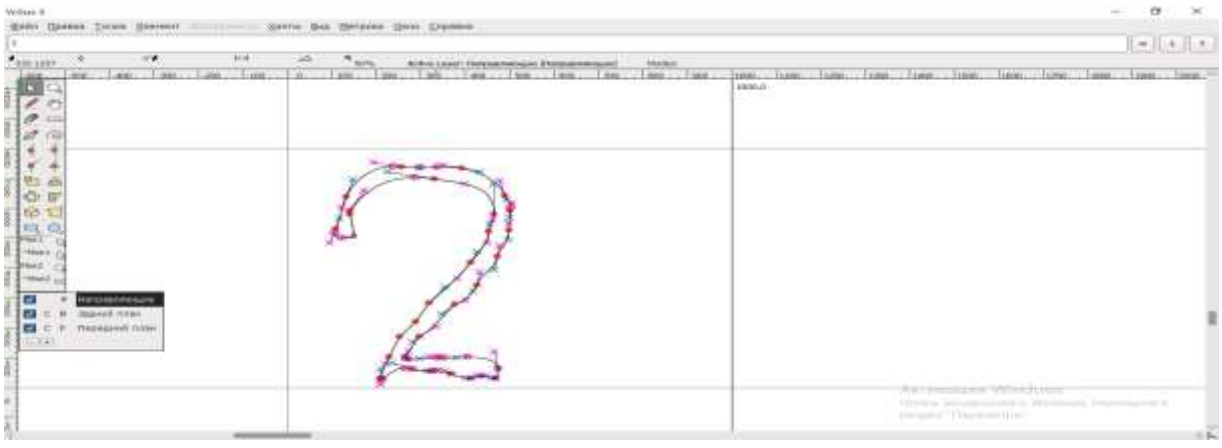


Рисунок 2.7 – Вигляд шрифту в програмі Font Forge

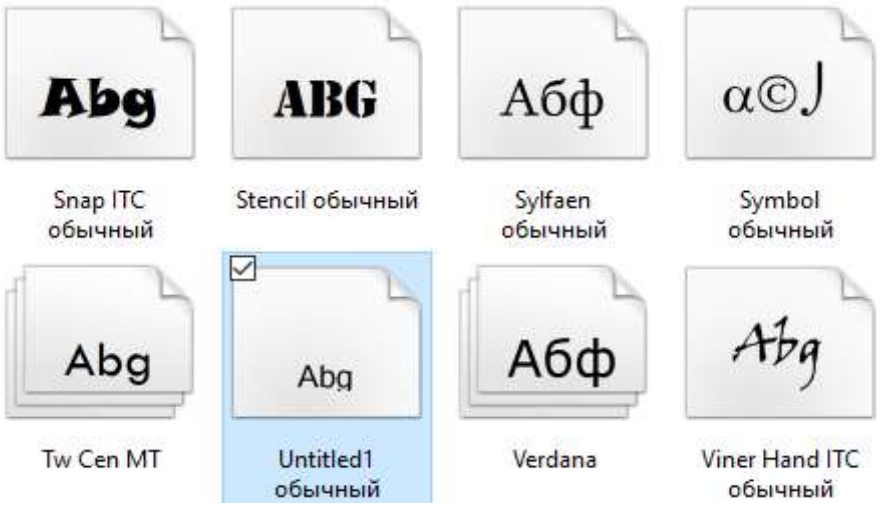
Такий вигляд має вибраний шрифт через програму Font Forge. Шрифт складається з безлічі гліфів, кожен з них має своє певне значення. Для зміни змісту нашого електронного документу, нам не потрібнно змінювати всі гліфи цього шрифту. Лише достатньо замінити декілька гліфів для перевірки чи можлива атака на базі заміни шрифту. Тому замінимо гліф з позначкою «1» на любий інший символ. Для того щоб замінити гліф , нам потрібно вибрати гліф який нам потрібно замінити , після цього з’явиться вікно в якому потрібно



зобразити символ на який ви хотіли б щоб замінили гліф «1».

Рисунок 2.8.- Зміна гліфу

На скриншоті зображен символ на який буде замінений гліф. Після заміни документ повинен замінити значення «1» на «2». Спробуємо зберегти



модернізованний шрифт, та замінити ним оригінальний шрифт.

Рисунок 2.9. – Підстановка шрифт

Модернізований шрифт був вдало встановлений в директорію з стандартними шрифтами, але при збереженні був змінена його назва на «Untitled1». Тепер треба спробувати видалити шрифт «Consolas», для того щоб його замінити модернізованим шрифтом.

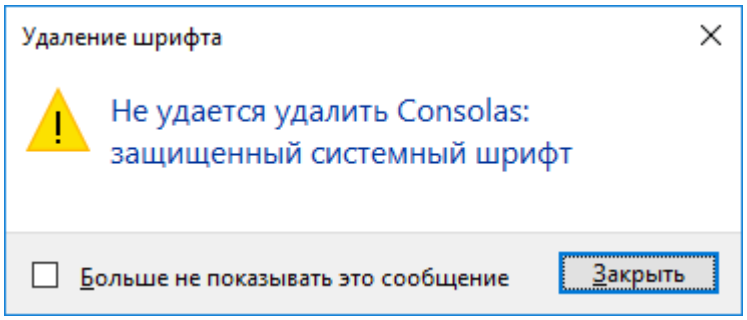


Рисунок 2.10 – Відмова системою Windows в модернізації або зміні шрифту

Але нам не вдається цього зробити, тому що цей шрифт вважається системним шрифтом, система Microsoft Windows не дає змогу видалити його. Тому шляхом заміни шрифту в дерикторії атака не можлива.

Але документ Word, як було приведено вище це певного роду архів, з безліч конфігураційних файлів. Серед цих конфігураційних файлів, є файл який відповідає які шрифти використовувати в даному документі, спробуємо через нього провести заміни так , щоб змінився зміст але ЕП цих змін не відобразила.

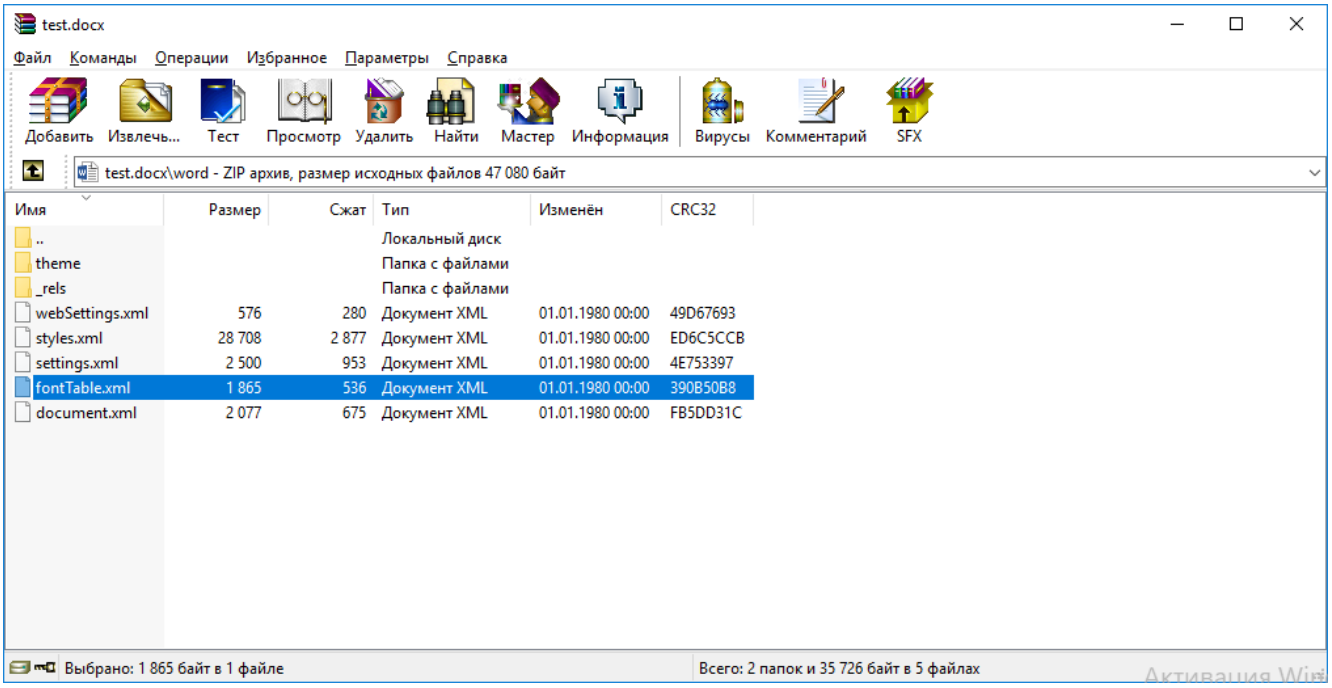


Рисунок 2.12 – Перелік конфігураційних файлів

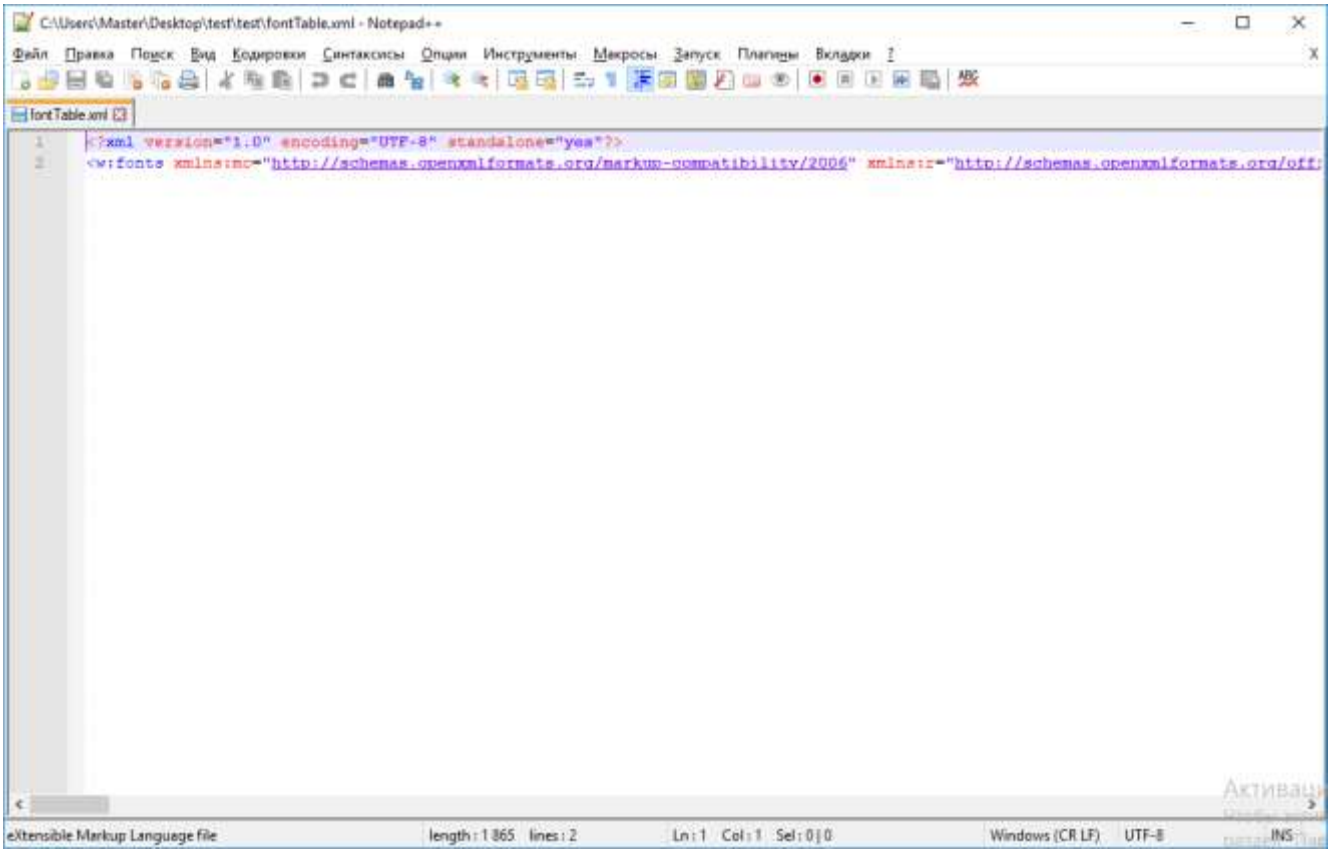


Рисунок 2.11 – Файл конфігурації шрифту

Спробуємо в цьому конфігураційному файлі, назви шрифтів замінити на назву шрифту який ми створили. Після зміни конфігураційного файлу, зміст електронного документ не змінився. По причині того що програма WinRAR не давала замінити файли конфігурації.

В наслідок отриманих даних, можливо зробити висновок, що атака по підміні шрифту не є актуальною. В зв’язку з тим, що без допоміжних програмних заходів, лише за допомогою ресурсів системи Windows Microsoft вдалося уникнути зміни змісту електронного документу.

2.4 Аналіз питання , яким чином підписати медійний файл за допомогою ЕП та які варіанти атак можливі на медійні файли

Орган влади «Обласний Господарський суд», моє змогу вести судові засідання між іншими господарськими судами. За допомогою відео-конференції. Кожне засідання записується, та запис зберігається певний час. В зв’язку з цим виникає питання, яким чином підписувати медійні файли з допомогою ЕП, так щоб забезпечити цілісність та оригінальність файлу. Медійний файл вважається один із видів електронного документа який циркулює в системі електронного документообігу. Відео запис засідання суду може бути використаним як доказ при поданні в апеляцій суд. Але для того щоб підтвердити оригінальність та цілісність медійного файлу, він потребує накладання ЕП. В цьому питанні виникають, інші підпитання. Підписувати потрібно весь медійний файл, або досить лише ключових кадрів. Яким чином підписати медійний файл, щоб стала менше вірогідність заміни змісту медійних файлів.

Розберем характеристики різних медійних файлів. Існують різноманітні формати медійних файлів, кожен формат має свої особливості. Розглянемо кожен формат окремо.

Формат відео файлу визначає структуру відео файлу, - то, як зберігається файл на носії інформації (CD, DVD, жорсткому диску або каналі зв'язку). Зазвичай різні формати мають різні розширення файлу (* .avi, * .mpg, * .mov і ін.).

Комп'ютерне цифрове відео являє собою послідовність цифрових зображень і пов'язаний з ними звук. Елементи відео зберігаються в цифровому форматі.

Існує безліч способів захоплення, зберігання та відтворення відео на комп'ютері.

З появою комп'ютерного цифрового відео стихійно стали виникати найрізноманітніші формати представлення відеоданих, що спочатку призвело до деякої плутанини і викликало проблеми сумісності.

Однак, завдяки зусиллям Міжнародної організації зі стандартизації (ISO - International Standards Organisation) вироблені єдині стандарти на формати відеоданих, які ми і розглянемо.

AVI (Audio / Video Interleaved) - стандарт відео файлу, розроблений Microsoft, в якому аудіо та відео дані чергуються між собою і при відтворенні ділянку звукової доріжки синхронізується з відеофрагментів. AVI є спеціальним випадком формату RIFF. Аудіо та відео послідовності в AVI файлі не містять тимчасових міток і не створюють індекси. Дані упорядковуються в часі послідовно, відповідно до їхнього порядку в AVI файлі. Додаток (відеоплеєр) має відображати кадри відеопослідовності і аудиопоток згідно частоті кадрів і частоті дискретизації відповідно, зазначених в заголовку файлу.

AVI - це формат відео контейнера, в якому визначена структура розміщення аудіо та відео потоків. Сам AVI не визначає, чим саме повинні бути закодовані відео дані, що дозволяє зберігати аудіо і відео дані різними способами. Зазвичай AVI контейнер використовують такі кодеки як M-JPEG, Indeo, DivX та ін. Тип кодека, використаного для кодування відеоданих, вказане за допомогою FourCC коду знаходиться в заголовку AVI файлу. Файл цього формату складається з блоків, які в свою чергу складаються також з блоків. Верхній блок – Riff- містить ідентифікатор форми «avi_», який власне і показує, що має справу з AVI- файлом. Для ідентифікатора файлу призначено 4 символи, але четвертий ніколи не використовується.

AVI-файл містить мінімум 2 блока даних: заголовок та данні. Заголовок містить інформацію про частоту кадрів, формат аудіо, зображення. Блок даних, зазвичай відображається у вигляді послідовності записів, кожний запис складається з одного кадру і відповідного звукового супроводу.

Записувати в форматі AVI можливо як без стискування так і з стискуванням даних.

WMV (Windows Media Video) - цифровий відео формат, створений і контрольований компанією Microsoft ©. WMV - відео файл, записаний в форматі Windows Media. WMV - це універсальне назву комплексного

технологічного рішення, що почався з версії 7 (WMV7), в якому Microsoft використовувала власний формат кодування MPEG-4 відео (і як це не дивно не сумісного з іншими MPEG-4 технологіями).

Файли WMV містяться в контейнері ASF - Advanced Systems Format. Файли цього формату можуть містить як відео дані Windows Media Video, так і аудіо дані Windows Media Audio. Файли WMV мають змогу підтримувати використання засобів захисту DRM, які не дозволяють користувачеві копіювати інформацію. Саме із-за цієї характеристики, формат файлів WMV є дуже популярним серед компаній які займаються продажом цифрових копій відеороликів та аудіозаписів.

Файли WMV стискаються за допомогою кодеків, розроблених компанією Microsoft. Формат контейнера ASF – кодує дані за допомогою кодека WMV. Кодек Windows Media Video 9 Professional дозволяє користувачеві отримувати потоки з дозволом більше ніж 300 000 пікселів, а також бітрейтом в 1000 Кб/с.

MKV - це відео-контейнер, схожий на MOV і AVI, який підтримує необмежену кількість доріжок аудіо, зображень та субтитрів (наприклад, SRT або USF). Контейнер Matroska Multimedia Container являє собою відкритий стандарт, безкоштовний формат файлу, який може містити необмежену кількість відео, аудіо, зображень або доріжок субтитрів у одному контейнері. Призначений для використання в якості універсального формату для зберігання мультимедійного загального контенту, такого як фільми або телешоу. У порівнянні з формат AVI, MKV концептуально схожий на технологічне рішення таких форматів, як MP4 або Advanced Systems Format (ASF). Зміст файлу повністю розкрито в специфікації: реалізація складається з програмного забезпечення з відкритим вихідним кодом.

Всупереч поширеній думці, MKV файли є форматами мультимедійних контейнерів, а не форматом стиснення аудіо або відео. Контейнер може укладати аудіо, відео і субтитри в один файл, навіть якщо ці елементи використовують різні типи кодування. Наприклад, у вас може бути файл MKV, який містить відео H. 264 і щось зразок MP3 або AAC для аудіо. Сам контейнер

MKV також підтримує практично всі аудіо - і відеоформати, що робить його високо адаптивним і простим у використанні.

Можливості формату MKV:

- Трансляція через Інтернет (протоколи HTTP і RTP);
- Швидке перемотування по файлу;
- Стійкість до помилок;
- Екранні меню (як на DVD). (НЕ реалізовано через відсутність специфікації);
- Розбиття файлу на глави (Chapters);
- Модульна розширюваність.

MPEG - це абревіатура від Moving Picture Experts Group (Експертна Група з Рухомим Зображеннях) - що займається розробкою форматів MPEG. Ця група визначає стандарти в цифровому відео, серед яких MPEG-1 - стандарт, використовуваний в Відео компакт-дисках, MPEG-2 стандарт, використовуваний на DVD і SVCD, DVB (цифрове телебачення), MPEG-4 стандарт, використовуваний в потоковому відео і що лежить в основі таких технологій як DivX, XviD і 3ivx. Як формат, в порівнянні з M-JPEG, цей стандарт забезпечує скорочення загального обсягу даних на 75-80% без втрати візуальної якості. Ця експертна група працює під спільним керівництвом двох організацій - ISO (Організація за міжнародними стандартами) і IEC (Міжнародна електротехнічна комісія). Офіційна назва групи - ISO / IEC JTC1 SC29 WG11. Її завдання - розробка єдиних норм кодування аудіо- і відеосигналів. Стандарти MPEG використовуються в технологіях CD-i і CD-Video, є частиною стандарту DVD, активно застосовуються в цифровому радіомовлення, в кабельному і супутниковому ТБ, Інтернет-радіо, мультимедійних комп'ютерних продуктах, в комунікаціях по каналах ISDN і багатьох інших електронних інформаційних системах.

MPEG-1 – перший представник сімейства MPEG стискування. Як стандарт був затверджений у 1992 році, а як формат реалізований в 1993 році. Швидкість

відеопотока в форматі MPEG-1 обмежена 150 Кб/с. Зараз MPEG-1 може бути реалізованим в вигляді формата NTSC 352x240, з швидкістю 30 кадрів/с або в форматі PAL/SECAM 352x288, з швидкістю 25 кадрів/с.

У форматі MPEG-1 всі кадри медійного файлу діляться на 3 типи кадрів: I- , P- і B- кадри. До першого типу (I- кадри, Intra Frames) відносяться опорні кадри. Їх зображення зберігається в повному об’ємі у форматі JPEG. Для P-кадрів (Predicted Frames) записуються тільки відмінності від попереднього I-кадру, що вимагає набагато менше дискового простору. Для B- кадрів (Bi - DirectiOnallyInterpolated Frames) зберігаються відмінності від попереднього і наступного I - або P- кадру.

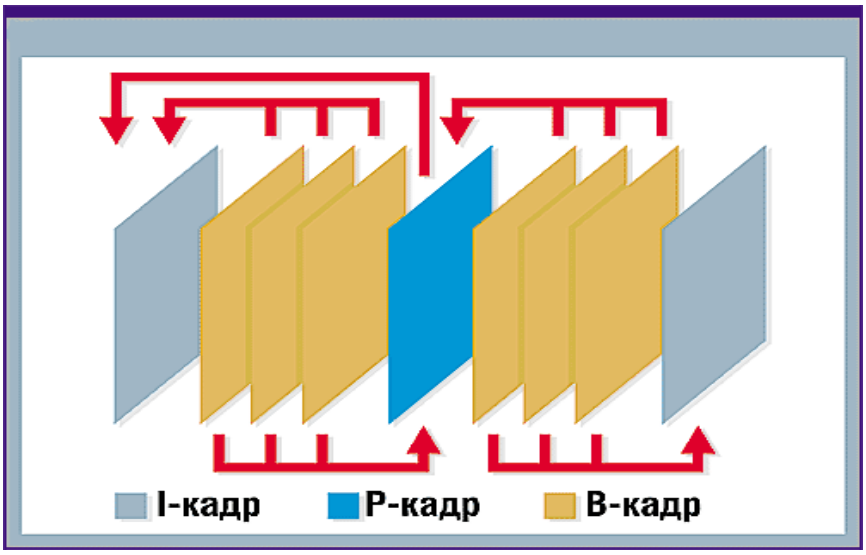


Рисунок 2.12 – Схема кадрів формату MPEG

Проаналізувавши існуючі формати медійних файлів, можливо виділити два формата які підходять для підписання за допомогою ЕП. Формати WMV та MPEG більш вигідно підходять для збереження відео-конференцій засідань та підписання за допомогою ЕП.

Виникає питання яким чином підписати медійний файл великого розміру за допомогою ЕП. Проаналізувавши всі інформаційні джерела в сфері цього питання, були виділенні декілька способів підписання медійного файлу.

За допомогою Хеш- функції кожного кадру. Підписувати кожний кадр, в результаті в нас буде захищений кожен кадр від змін, але не зможемо гарантувати захист послідовності кадрів. В зв’язку з цим виникає можливість зміни медійного файлу, за допомогою видалення деяких кадрів або зміною послідовності кадрів. Можна розділити відео файл на рівні частини, та підписати їх окремо, в наслідок цього будуть захищені всі кадри та їх послідовність, але може статись так, що кадр який нас цікавить потрапить на границю 2 частин. Також деякі системи за допомогою яких накладається ЕП мають обмеження розміру файлу який підлягає підписанню.

Єдине вірне рішення, це при підписанні враховувати не тільки значення хеш-функції поточного кадру, а також значення попереднього кадру. Таким чином ми захистимо від зміни не тільки кожен кадр а і послідовність. Але в цього рішення є вразливість колізії, можливий підбір хеш-функції попереднього кадру таким чином, що при перевірці ЕП змін не буде виявлено. Тому пропонується використовувати файли формата MPEG, так як формат складається с головного кадра-I та кадрів P та B. Якщо враховувати хеш-функцію кадра I та суму хеш функцій кадрів P або B, вірогідність того, що можливий підбір кадрів прирівнюється до 0.

.

2.5 Висновок по другому розділу

В наслідок аналізу рівня захищеності системи електронного документообігу обласного Господарського Суду. Було виявлено деякі види джерел загроз ЕД підписаних за допомогою ЕП.

Після спроби реалізації атаки по заміні шрифту, було виявлено що атака не є актуально в зв’язку з тим, що за рахунок ресурсів системи Microsoft Windows атака по заміні шрифту можлива для реалізації, тому що система не дає змогу реалізовувати будь які дії з системними шрифтами.

В питанні про медійні файли, було прийнято рішення, що формат MPEG є найбільш вигідним для підписання за допомогою ЕП. Також в результаті аналізу, було прийнято рішення, що підписувати треба тільки хеш-функцію поточного кадру, а брати показники попереднього кадру для упевненості в не зміні кадру та його послідовності.

РОЗДІЛ 3. ЕКОНОМЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ ПРОВЕДЕННЯ АНАЛІЗУ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

3.1 Вступ

Метою розділу є обґрунтування економічної доцільності аналізу рівня захищеності системи електронного документообігу та способів підписання медійних файлів з допомогою електронного підпису.

В зв’язку з аналізом системи електронного документообігу обласного суду, та виявлення деяких засад в рівнях захисту, приведених у другій частині магістерської роботи. Є актуальним прорахування скільки імовірних збитків може понести орган державної влади, якщо будуть реалізовані атаки. Та який обсяг коштів можна зберегти внаслідок відвертання імовірних атак.

Щоб визначити ефективність необхідно розрахувати:

– капітальні витрати на аналіз рівня захищеності систем електронного документообігу;

– трудомісткість витрати на проведення аналізу рівня систем електронного документообігу та аналізу методів підписання медійних файлів з допомогою електронного підпису ;

– річні експлуатаційні витрати на підтримку системи електронного документообігу та сертифікатів електронного підпису;

– показники економічної ефективності проведення аналізу рівня захищеності системи електронного документообігу обласного господарського суду.

3.2 Розрахунок фіксованих (капітальних) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на проведення аналізу рівня захищеності Кпз складаються з витрат на заробітну плату виконавця аналізу рівня захищеності Ззп і вартості витрат машинного часу, що необхідний для опрацювання на ПК Змч:

$$K_{аз} = З_{зп} + З_{мч} \quad (3.1)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{ПР}, \quad \text{грн}, \quad (3.2)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата.

Розрахуємо час, який буде витрачено на створення програми і методики:

$$t = t_{тз} + t_{втз} + t_{ае} + t_{сп} + t_{вз} + t_{ор}, \text{ годин}, \quad (3.3)$$

де $t_{тз}$ – тривалість складання технічного завдання на проведення аналізу рівня захищеності;

$t_{втз}$ – тривалість вивчення технічного завдання;

$t_{ае}$ – тривалість аналізу рівня захищеності системи електронного документообігу та аналізу методів підписання медійних файлів ;

$t_{сп}$ – тривалість складання методики підписання медійних файлів з допомогою електронного підпису;

$t_{вз}$ – тривалість випробувань захищеності системи електронного документообігу;

$t_{\text{ор}}$ – тривалість опрацювання результатів;

У таблиці 3.1 представлена трудомісткість процесів.

Назва процесу	Трудомісткість, год.
Складання технічного завдання для проведення аналізу рівня захищеності системи електронного документообігу	24
Вивчення технічного завдання	8
Аналіз рівня захищеності системи електронного документообігу та аналіз методів підписання медійних файлів	72
Тривалість складання методики підписання медійних файлів з допомогою електронного підпису	56
Тривалість випробувань захищеності системи електронного документообігу	136
Опрацювання результатів	80

$$t = 24 + 8 + 72 + 56 + 136 + 80 = 376 \text{ годин.}$$

$З_{\text{пр}}$ – середньогодинна заробітна плата фахівця з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_{м}}{t_m} = \frac{11000}{160} = 68.75 \text{, грн/год,} \qquad (3.4)$$

де $З_{\text{м}}$– середня заробітна плата фахівця з інформаційної безпеки – 11 000 грн., t_m – робочій час на місяць -160 год.

$$З_{\text{зп}} = 376 \cdot 68{,}75 = 25\,850, \text{ грн}$$

Вартість машинного часу для проведення аналізу рівня захищеності та аналізу методів підписання медійних файлів, розраховується за формулою:

$$З_{мч} = (t_{опр} \cdot С_{мч} + t_{д}), \text{ грн,} \quad (3.5)$$

де $t_{опр}$ – трудомісткість налогодження всіх необхідних операцій на ПК, годин (80 год);

$t_д$ – трудомісткість підготовки документації на Пк, годин (40 год);

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}}, \text{ грн} \quad (3.6)$$

де $Р$ – встановлена потужність ПК, 0.5 кВт;

$С_е$ – тариф на електричну енергію, 1.68 грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на початок року, 8000 грн.;

$Н_а$ – річна норма амортизації на ПК, 0.1 частки одиниці;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920 год).

$$С_{мч} = 0,5 \cdot 1,68 + \frac{8000 \cdot 0,1}{1920} = 1,25, \text{ грн/год}$$

$$З_{мч} = 80 \cdot 1,25 + 40 = 140 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проведення аналізу рівня захищеності системи електронного документообігу та аналізу методів підписання медійних файлів з допомогою електронного підпису становлять :

$$К_{пз} = 140+25\ 850 = 25\ 990, \text{ грн} \quad (3.7)$$

Оскільки в даній роботі розглядається тільки перевірка елементів захисту модуля «Проактивний захист», перевірка повної системи вимагає більше часу, а відповідно більші капітальні витрати. Пердбачається, що для повної перевірки капітальні витрати становитимуть у 2 рази більше.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні (експлуатаційні) витрати на функціонування системи електронного документообігу:

$$С = С_а + С_з + С_{ел} + С_{тос}, \text{ грн}, \quad (3.8)$$

де $С_а$ - Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ)

$$С_а = К_{пз} /2 =(25\ 850)/2=12\ 925, \text{ грн}, \quad (3.9)$$

Сз - Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему електронного документообігу та допоміжних систем ,складає:

$$С_з = (Зм+ 22\%) \cdot m = 13\ 420 \cdot 12 = 161\ 040 \text{ грн}, \quad (3.10)$$

де m – кількість місяців.

До річного фонду заробітної плати додається єдиний внесок (22%) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = Р \cdot Fр \cdot Ц_е , \text{ грн,} \quad (3.11)$$

де Р – встановлена потужність апаратури на якій реалізована система електронного документообігу, 0.5 кВт;

$F_р$ – річний фонд робочого часу системи електронного документообігу (за 40-годинного робочого тижня $F_р$ = 2080 год);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин, 1.68 грн/кВт·година.

$$С_{ел} = 0,5 \cdot 2080 \cdot 1,68 = 1\ 747,2 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати складають:

$$С = 12\ 325 + 161\ 040 + 1\ 747,2 = 175\ 712,2 \text{ грн.}$$

3.4 Оцінка можливого збитку від атаки

Упущена вигода від простою атакованої системи електронного документообігу становить:

$$U = П_п + П_в + V, \quad (3.12)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників обласного господарського суду, грн;

$П_в$ – вартість відновлення системи електронного документообігу та електронних документів які були атаковані (переустановлення системи, відновлення електронних документів та ін.), грн;

V – втрати від зниження працездатності апарату суду.

Втрати від зниження продуктивності співробітників атакованої системи електронного документообігу являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \ , \qquad (3.13)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч);

$З_с$ – заробітна плата співробітників апарату господарського суду, грн на місяць;

$t_п$ – час простою системи електронного документообігу та відновлення електронних документів змінених або знищених внаслідок атаки, годин.

$$П_п = \frac{11000 + 7000}{176} \cdot 3 = 306 \text{, грн}$$

Витрати на відновлення працездатності системи електронного документообігу включають кілька складових:

$$П_в = П_{ви} + П_{пв}, \qquad (3.14)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення електронних документів, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованих відділів апарату $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ВИ} \ , \qquad (3.15)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого відділу апарату суду, годин;

$$П_{ви} = \frac{5000 + 5000 + 8000}{176} \cdot 16 = 1636 \text{, грн}$$

Витрати на відновлення вузла або сегмента системи $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_{В} \ , \qquad (3.16)$$

де Зо – заробітна плата обслуговуючого персоналу (адміністратора), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує систему електронного документообігу, годин.

$$П_{ПВ} = \frac{11000}{176} \times 8 = 500 \text{ , грн}$$

Витрати на відновлення працездатності системи електронного документообігу включають кілька складових:

$$П_в = 1\ 636 + 500 = 2\ 136 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента системи визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ}) \ , \qquad (3.17)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч;

$$V=0 \text{ , грн}$$

Упущена вигода від простою атакованого вузла або сегмента системи становить:

$$U = 306 + 2\ 136 + 0 = 2\ 442 \text{ , грн}$$

Таким чином, загальний збиток від атаки на систему електронного документообігу складе

$$B = \sum_i \sum_n U \, , \qquad (3.18)$$

де i – число атакованих електронних документів ;

n – середнє число атак на рік.

$$В = 10 \cdot 120 \cdot 2\,442 = 2\,930\,400 \text{ грн.}$$

3.5 Загальний ефект від впровадження рекомендацій

Загальний ефект від впровадження системи електронного документообігу визначається з урахуванням ризиків порушення системи електронного документообігу і становить:

$$E = B \cdot R - C, \qquad (3.19)$$

де В – загальний збиток від атаки систему електронного документообігу і, тис. грн;

R – очікувана імовірність атаки на систему електронного документообігу та зміни електронних документів частки одиниці(0,3 найбільш ймовірній відсоток);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 2\,930\,400 \cdot 0{,}3 - 175\,712{,}2 = 703\,407{,}8 \text{ грн}$$

3.6 Економічне обґрунтування

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

– коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на системи електронного документообігу, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.20}$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;
K –капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = \frac{703407}{25990} = 27$$

Нормативне значення коефіцієнта повернення інвестицій визначається з наступних міркувань.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань), то в якості $E_н$ варто приймати бажану норму прибутковості альтернативних варіантів вкладення коштів К (наприклад, у цінні папери, інші проекти, на депозитний рахунок у банку, тощо) з урахуванням інфляції. Визначити бажане значення коефіцієнта ефективності можна також виходячи з прийнятної для підприємства індивідуальної норми прибутковості, якак б, принаймні, не знижувала ринкову вартість фірми.

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (Nдеп – Nінф)/100), \quad (3.21)$$

де Nдеп – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

Nінф – річний рівень інфляції, 13,7%.

$$27 > (18\text{-}13{,}7)/100$$

$$27 > 0{,}043$$

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій T_o.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{25990}{703407} = 0{,}036 \approx 2 \text{ дні.}$$

3.7 Висновки до економічного розділу

В результаті розрахунку витрат на проведення аналізу рівня захищеності системи електронного документообігу було визначено, що розмір капітальних витрат складатиме 25 9906 грн, а щорічні експлутаційні витрати 175 712,2 грн. для забезпечення повної перевірки системи

Коефіцієнт повернення інвестицій ROSI показав, що 27 грн додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження програми і методики.

Загальний ефект від впровадження програми і методики визначається з урахуванням ризиків порушення інформаційної безпеки і становить 703 407, 78 грн

Було доведено, що застосування програми і методики в організації збереже від збитків у розмірі від 1 до 2 930 400,45 грн та окупиться лише за 2 дні.

ВИСНОВКИ

У дипломній роботі було проведений аналіз рівня захищеності систем електронного документообігу, на основі якого було проведенно дослідження імовірних вразливостей електронного документу.

Оскільки стрімко з’являються нові вразливості системи електронного документообігу, важливо проводити аналіз рівня захищеності кожного року, щоб розуміти які види атак можливі в реалізації на системі електронного документообігу.

Перевірялися електронні документи які циркулюють в системі електронного документообігу за допомогою реалізації атаки «заміни шрифту». Внаслідок було виявлено, що реалізація цієї атаки є не можливою завдяки ресурсам захисту Microsoft Windows. Також було проаналізовано яким методом та які формати мультимедійних файлів більш підходять для підписання за допомогою електронного підпису.

Оскільки для реалізації електронного підпису на медійні формати треба знати структура формату, був проведений аналіз структур медійних форматів.

Проведено огляд системи електронного документообігу та розглянуто можливість реалізації атаки «заміна шрифту».

В економічному розділі наведено обгрунтування проведення аналізу систем електронного документообігу.

Практичне значення роботи полягає зменшення часу та фінансових витрат при проведенні аналізу рівня захищеності систем електронного документообігу. Результати здійснених у дипломній роботі досліджень можуть бути використані для проведення наступних аналізів системи електронного документообігу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про електронні документи та електронний документообіг» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/851-15
2. Закон України «Про електронні довірчі послуги» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2155-19
3. Постанова від 28 жовтня 2004 року «Типовий порядок встановлює загальні правила документування в органах виконавчої влади управлінської діяльності в електронній формі і регламентує виконання дій з електронними документами з моменту їх створення або отримання до відправлення чи передачі до архіву органу виконавчої влади» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1453-2004- п
4. Постанова від 17 січня 2018 року «Деякі питання документування управлінської діяльності» [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/55-2018- п
5. Системи електронного документообігу [Електронний ресурс]. – Режим доступу: https://fossdoc.com/vybor-sed
6. Увеличиваем себе премию в два раза, или как взломать документы, подписанные усиленной квалифицированной подписью [Електронний ресурс]. – Режим доступу: https://habr.com/company/ascon/blog/347016/
7. ЭЦП видеопотока [Електронний ресурс]. – Режим доступу: https://habr.com/post/409625/
8. Формат MPEG — спецификация и возможности [Електронний ресурс]. – Режим доступу: http://video-practic.ru/content/format-mpeg-vozmozhnosti

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	4	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	23	
6	А4	2 Розділ	18	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на елетронному носії

1. Магістерська робота Воловатов А_В_125м-17-1.docx – Пояснювальна записка Воловатов А_В.pptx – Презентація

ВІДГУК

на дипломну роботу магістра на тему:

«Аналіз рівня захищеності системи електронного документообігу обласного господарського суду»

студента групи 125м–17–1 *Воловатова Антона Віталійовича*

Мета дипломної роботи – забезпечення безпеки системи електронного документообігу обласного господарського суду.

Тема дипломної роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – випробування та поліпшення систем захисту.

Задачі дипломної роботи (аналіз особливостей функціонування та вразливостей системи електронного документообігу обласного господарського суду, аналіз існуючих систем електронного документообігу, проведення тестування та обробка отриманих результатів, обґрунтування способів реалізації цифрового підпису) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Практичне значення результатів проектування полягає у обґрунтуванні способів реалізації цифрового підпису при зміні технологій обробки документації.

До недоліків дипломної роботи відносяться:

- відсутність оцінки ефективності запропонованих рішень;
- проведення випробувань не в повному обсязі;
- структура викладення програми та методики випробувань відрізняється від рекомендованої.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Воловатов А.В. виявив себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до дипломної роботи магістра, заслуговує оцінки “добре”, а Воловатов А.В. присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н, проф. _____ В.І. Корнієнко

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)