Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська дипломна робота на тему:
«Система захисту електронного документообігу Вінницької міської ради»

Виконав: студент 4 курсу групи 1БС-21мс
спеціальності 125 Кібербезпека
_____ Солончук О.Б.

Керівник: к.ф-м.н., доцент каф. ЗІ
_____ Дудатьєв А. В.
«19» червня 2023 р.

Рецензент: к.т.н., доцент каф. ПЗ
_____ Хошаба О.М.
«19» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти - І бакалаврський
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо – професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф
В. А. Лужецький
«20» березня 2023 року

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Солончуку Олександру Богдановичу

1. Тема роботи: «Система захисту електронного документообігу Вінницької міської ради».

керівник роботи: Дудатьєв Андрій Веніамінович, к.т.н., доцент кафедри ЗІ, затверджено наказом ректора ВНТУ від 20 березня 2023 року №67.

2. Строк подання студентом роботи 19 червня 2023.

3. Вихідні дані до роботи:

– використовуваний тип документів і стандартів ЕЦП: ЦЕП

– electronic signature ESNF : основні криптографічні протоколи ЕЦП : ISO/IEC 9796-2:2010; ISO/IEC 14888-1:2008 ; ISO/IEC 14888-2:2008;

– тип документів систем ЕДО :*.doc; *.pdf; *.jpg; *.rtf; *.txt; інші;

– тип шифрування в системах ЦЕП - синхронне і асинхронне: AES; DES; RSA.

4. Зміст текстової частини: Вступ. 1.Аналітичний огляд технологій електронного документообігу і його інформаційного захисту. 2. Аналіз загроз і вразливостей систем електронного документообігу. 3. Підвищення безпеки передачі даних у системах ЕДО і організація надійного інформаціного захисту ЕД. 4. Оцінки і дослідження захисту інформаційних систем електронного документообігу. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстрованого матеріалу.

Структурна схема моделі захисту (плакат, А4). Структурна схема і креслення моделі і структури засобу захисту процесу передачі і підходів шифрування (плакат,А4). Структурна схема засобу інформаційного захисту ЕДО і ЕД в них(плакат, А4). Отримані в результаті обчислень графічні залежності (плакати, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Дудатьєв А. В., доц. кафедри ЗІ	20.03.2023	16.06.2023
2	Дудатьєв А. В., доц. кафедри ЗІ	20.03.2023	16.06.2023
3	Дудатьєв А. В., доц. кафедри ЗІ	20.03.2023	16.06.2023

7. Дата видачі завдання: 20 березня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	06.03 – 14.03	
2	Розробка технічного завдання	15.03 – 17.03	
3	Аналіз інформаційних джерел за напрямком БДР. Аналіз проблем ІБ ЕДО	18.03 – 31.03	
4	Розробка рішень, моделей, алгоритмів, методів	01.04 – 15.04	
5	Практична реалізація, моделювання, експериментування, результати	16.04 – 01.05	
6	Аналіз виконання ТЗ, висновки	02.05 – 10.05	
7	Оформлення пояснювальної записки	11.05 – 18.05	
8	Попередній захист БДР	18.05 – 21.05	
9	Виправлення зауважень, підготовка ілюстративного матеріалу	22.05 – 30.05	
10	Представлення БДР до захисту, рецензування	01.06 – 15.06	
11	Захист БДР	20.06 – 23.06	

Студент _____ Олександр СОЛОНЧУК

Керівник роботи _____ Андрій ДУДАТЬЄВ

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота складається з 61 сторінок формату А4, на яких є 37 рисунків, 1 таблиця, 31 найменування списку використаних джерел .

Бакалаврська робота присвячена розробці та реалізації системи інформаційного захисту електронного документообігу. У бакалаврській дипломній роботі проведено аналіз сучасного стану розвитку систем електронного документообігу та систем інформаційного захисту від них. Встановлено об'єкт, предмет, завдання та методи роботи, сформульовано мету. В роботі проведено аналіз існуючих проблем інформаійноїх безпеки електронного документообігу (ЕДО) і передачі електронних документів (ЕД) у них. Запропоновано нові моделі і метод підвищеного захисту електронної інформації та електронних документів (ЕД) в системах передачі документів. Запропоновано технологію системи підвищеного захисту на базі вдосконаленої моделі електронного цифрового підпису – ЦЕП+. Проведено оцінки і виявлено основні загрози систем ЕДО і контроль передачі і інформаційних захист систем ЕДО. Розроблено основні засади створення інформаційних систем підвищеного захисту систем ЕДО та структури систем захисту ЕДО. Було реалізовано структура захищеної інформаційної системи ЕДО, яка складається з таких компонентів: клієнт, сервер і база даних. Реалізовано окремі програмні модулі для достідження вразливостей і виявлення проблемних місць ЕДО.

Розглянуті основні чинники впливу і фактори кіберзагроз для ЕДО, які проявляються у каналах зв'язку ЕДО, а також можливості несанкціонованого втручання і зчитування інформації ЕДО у інформаційних системах та їх наслідки. Розглянуто перспективи розвитку і підходи покращеного методу і моделі захищеної більш передачі даних у ІМ ЕДО.

Отримані в бакалаврській дипломній роботі результати можна використати для підвищення захисту існюючиї ІМ ЕДО, та для тестування інформаційної захищеності і підвищення рівня захисту систем ЕДО із якісним покращенням системи зв'язку.

Ключові слова: ЕДО, шифрування даних, ЕД, ЦЕП, КЕП, ІМ, інформаційні мережі, система ЕДО, Інтернет-канали, інформаційний захист.

ABSTRACT

The bachelor's qualification work consists of 61 pages of A4 format, on which there are 37 figures, 1 table, the list of used sources contains 19 items.

The bachelor thesis is devoted to the development and implementation of the system of information protection of electronic document management (EDO). In the bachelor's thesis, an analysis of the current state of development of electronic document management systems and information protection systems against them was carried out. The object, subject, tasks and methods of work have been established, the goal has been formulated. The paper analyzes the existing problems of information security of electronic document management (EDO) and transmission of electronic documents (ED) in them. New models and methods of increased protection of electronic information and electronic documents (ED) in document transmission systems are proposed. The technology of the enhanced protection system based on the improved model of electronic digital signature - ECP+ is proposed. Assessments were made and the main threats to EDO systems and transmission control and information protection of EDO systems were identified. The basic principles of creating information systems for increased protection of EDO systems and the structure of EDO protection systems have been developed. The structure of the secure EDO information system was implemented, which consists of the following components: client, server and database. Separate software modules have been implemented to detect vulnerabilities and identify EDO problem areas.

The main influencing factors and factors of cyber threats to EDO, which are manifested in EDO communication channels, as well as the possibility of unauthorized intervention and reading of EDO information in information systems and their consequences, are considered. Prospects for the development and approaches of an improved method and model of more secure data transmission in IM EDO are considered.

The results obtained in the bachelor thesis can be used to improve the protection of the existing IM EDO, and to test information security and increase the level of protection of EDO systems with qualitative improvement of the communication system.

Keywords: EDO, data encryption, ED, CEP, KEP, IM, data networks, EDO, data protection.

ЗМІСТ

ВСТУП

Сучасний розвиток технологій передачі і обробки інформації сприяв розвитку і розробки нових, більш ефективних і комфортних методів документообігу і контролю за рухом окремих процесів і інформаційних даних в організацях і між суб'єктами господарювання і ділової взаємодії. Таким є електронний документообіг – ЕДО, що передбачає рух електронних документів (ЕД) між користувачами в інформаційній системі . Також розвиток мережі Інтернет і сучасних підходів сприяв розвитку систем електронного документообігу (ЕДО), який дозволяє швидко, комфортно та ефективно вирішувати задачі руху і контролю документів, ділової інформації. Це сприяє пришвидшенню та підвищенню ефективності бізнес-процесів і ділової активності із паралельним зменшенням бюрократичних процедур і часу на прохлодження певних етапі отримання документів.

Електронний документообіг (ЕДО), або обіг електронних документів (ЕД) — це організована окрема сукупність процесів створення, оброблення, правлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із перевіркою автентичності.

Переваги запровадження системи ЕДО очевидні це – економія часу, ресурсів, оптимізація бізнес-процесів і підвищення комфортності та іміджевості системи електронного документообігу, зменшення бюрократії системи ЕДО.

Недоліками і проблематика запровадження системи ЕДО є інформаційна безпека і конфіденційність даних системи, яка є критичним місцем в окремих моментах і потребує детального розгляду і покращення. Також це – складність і необхідність встановлення додаткових засобів : програмних і апаратних для запровадження системи ЕДО, що несе окремі витрати для організації.

Сучасні системи ЕДО та їх електронні пристрої досить активно і стрімко розвиваються в останні роки і впроваджуються у все ширші сфери і колда на різних підприємствах і організаціяї і в електронних систем. Останні тренди показують, що розвиток цифрових та інформаційних технологій електронного документообігу досить стрімко розвивається: від впровадження в традиційні сфери побутового життя і

електроних систем користувача (і персональних пристроїв користувачів) до професійних корпоративних і банківських систем на базі складної автоматизації і цифрових технологій високого рівня, які впроваджуються у промисловості вже не один рік.

Сучасні розробки і автоматизація систем ЕДО гарантують, що рівень безпеки самої сигнатури підпису є досить високим. Безпека і стабільність роботи цих пристроїв – напряму залежить від стабільності і кібербезпеки обчислювального процесу і середовища системи, де ЕДО розгорнута і реалізується ці процеси. Використання шифркування і прогресивних алгоритмів накладення цифрових сигнатур в сфері прогресивних спеціалізованих систем і критичних систем, в якості основних ланок керування автентичність підвисання документів в бізнес- процесах дозволяє гарантувати високий рівень безпеки.Безпека роботи мікропрограм і алгоритмів ЦЕП в складі ЕДО дозволяє в більшості стабільно, надійно і нормально функціонувати системам автентичності документообігу і контролю за процесами обішу документів в системах – це вирішує першочергове завдання автентичності авторства для забезпечення роботи електронних систем документообігу, в які запроваджені алгоритми накладання ЕЦП і КЕП входить. Сучасні ЕДО мають прогресивні архітектури, різні обчислювальні спеціалізовані блоки, стабільність роботи яких є ключовим фактором роботи всіх бізнес –систем і логістики підприємства чи організації.

Але за рахунок недосконалості інших ланок системи ЕДО мають місце вразливі ланки і «слабкі» в плані кібербезпеки місця в іеформаційнійсистемі підприємства. Де ЕДО запроваджена. Це несе в свою чергу високри ризики для бізнес-процесів підприємства і самої ключової економічної і інформаційної безпеки підприємства чи організації в цілому. Це ставить проблему інфомроаційної безпеки ЕДО із ЦЕП на ключові позиції в рамках задача по розгортанню і оптимізації основних бізнес-процесів в інформаційній системі підприємства і її ІКС.

В останні роки набуває розвитку і швидкого темпу збільшення інтенсивності атак і різних втручань в інфраструктуру організацій, їх інформаційні мережі, із витоками даних і спотворенням і втратою ключової інформації, що виливається в досить серьозні наслідки для компаній. Це важливо і для систем із ЕДО, де

підвищення інтенсивності інформаційних впливів та інформаційних загроз на ЕДО із ЕЦП у різних галузях також спостеріагється сьогодні в різних організаціяї. Кількість інформаційних кібезагроз для ЕДО із КЕП та ЕЦП пропорційно збільшується із ростом числа і функціоналу цифрових технологій [1, 2].

Метою БДР є підвищення рівня інформаційної захищеності інформаційної системи електронного документообігу шляхом запровадження нового методу і моделі пркащеного шифрування і захисту інформації в системі ЕДО.

Задачі, які необхідно вирішити для досяггнення мети:

– провести аналіз і оцінки впливу базових сучасних, найбільш актуальних кіберзагроз і інформаційних впливів в системах ЕДО ;

– проаналізувати вразливі місця і технології здійснення атак і впливів на ЕДО;

– провести аналіз і визначення основних принципів стабільного захищеного функціонування інформаційної системи ЕДО і розгядом технології КЕП і ЦЕП для на дійного документообігу;

– розробка нової, покращеної моделі і методу ЕДО із підвищеним інформаціним захистом в ЕЦП , що дозволить підвищити захист і підвищити контроль за системою;

– оптимізувати систему ЕДО, зробити оцінки стабільності їй роботи;

– визначити основні точки втрати і оптимізувати модель захисту системи ЕДО в результаті її функціонування в складі електронних систем;

Предметом БДР є процес підвищення рівня інфомраційного захисту електронного документообігу організаціях.

Об’єктом БДР є інформаційний захист електронного документообігу в організаціях та захист інформації в інформацйно-компютерних системах ЕДО.

1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ І ЙОГО ІНФОРМАЦІЙНОГО ЗАХИСТУ

1.1. Загальні положенні і принципи функціонування ЕДО. Проблематика галузі та стан сучасних інформаційних технологій електронного документообігу.

Сучасний розвиток технологій передачі і обробки інформації сприяв розвитку і розробки нових, більш ефективних і захищенихметодів документообігу і контролю за рухом окремих процесів і інформаційних даних в організацях і між суб'єктами господарювання і ділової взаємодії. Також розвиток мережі Інтернет і сучасних підходів сприяв розвитку систем електронного документообігу (ЕДО), який дозволяє швидко, комфортно та ефективно вирішувати задачі руху і контролю за документами., що сприяє пришвидшенню та підвищенню ефективності бізнес-процесів і ділової активності із паралельним зменшенням бюрократичних процедур і часу на проходження певних етапів отримання ЕД.

ЕДО із застосуванням перевірки підпису ЕЦП та їх автентичності на певних етапах бізнес-процесу в такій документальні інформації часто використовується в організаціях , як це показано на рис. 1.1 та рис.1.2.

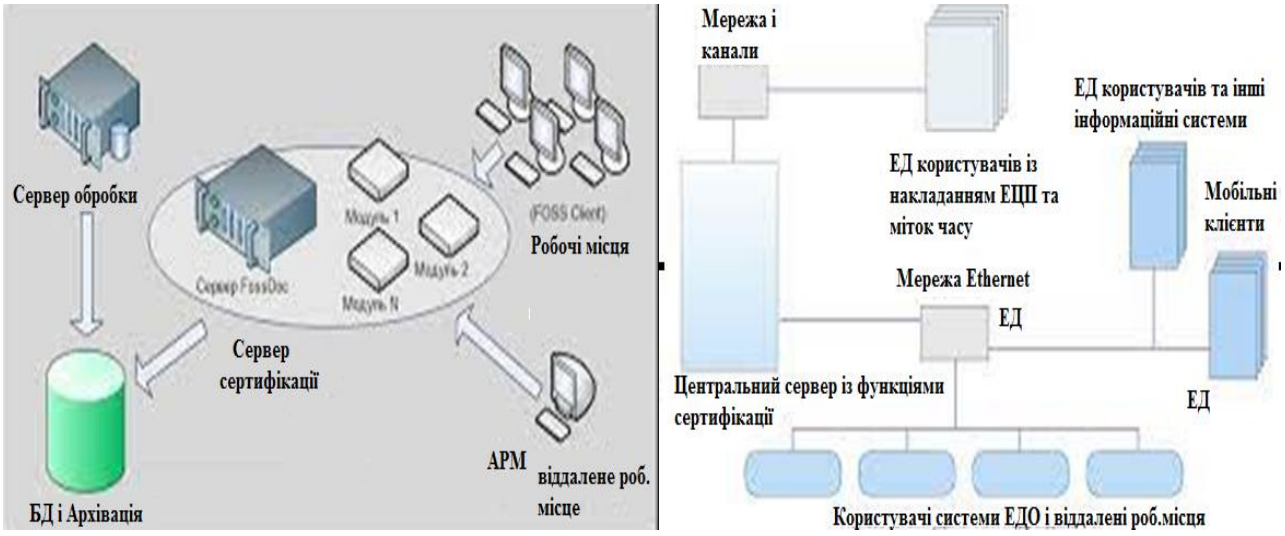


Рисунок 1.1 – Узагальнена схема інформаційної мережі документообігу (ЕДО)

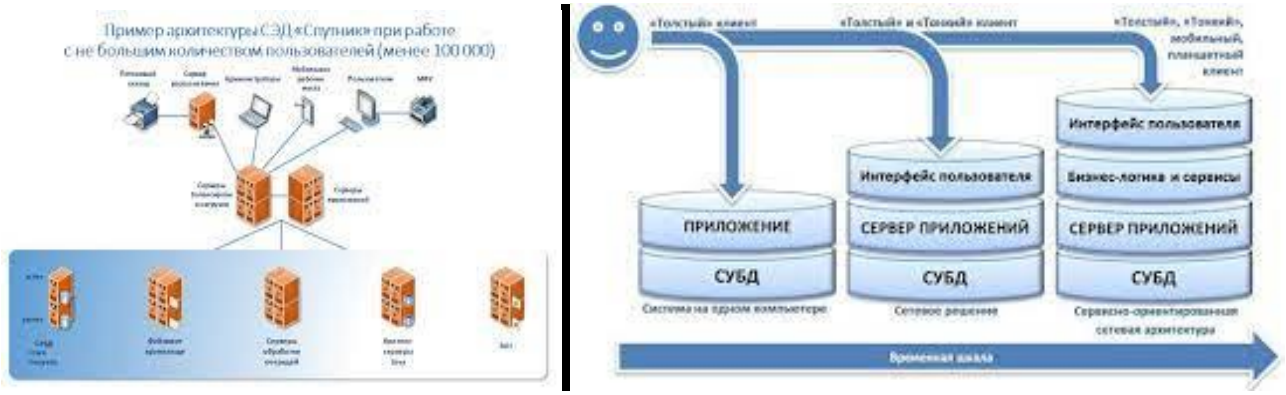


Рисунок 1.2 – Узагальнена схема організації захищених мереж для ЕДО

1.2 Порядок здійснення функціонування ЕДО

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством. Це пояснення наведено і розглянуто в статті 9. в Законі України «Про електронні документи та електронний документообіг» від 22 травня 2003 року N 851-IV[1], а також Закону України « Про інформацію».

Електронний документообіг (ЕДО) — це процес створення, погодження, надсилання, отримання та зберігання електронних документів у цифровому форматі. Основними складовими ЕДО є електронний документ (ЕД) та засоби ЕДО. – Електронний документ (ЕД)— документ з обов’язковими реквізитами, де дані відображаються в електронному вигляді. ЕД може бути перетворений у візуальну форму, придатну для сприйняття людиною, а також повинен зчитуватись системами. Архітектура системи ЕДО показана нга рис .1.3 Позначка (мітка) часу є обов’язковим реквізитом при накладанні КЕП на електронний документ із використанням процесів накладання. Вона фіксує дату та точний час у момент підписання документу, що присвоюється електронному підпису. Позначку часу видає сервер центру сертифікації ключів OCSP. Загальні принципи формування запитів на формування даних ЕД в ЕДО.

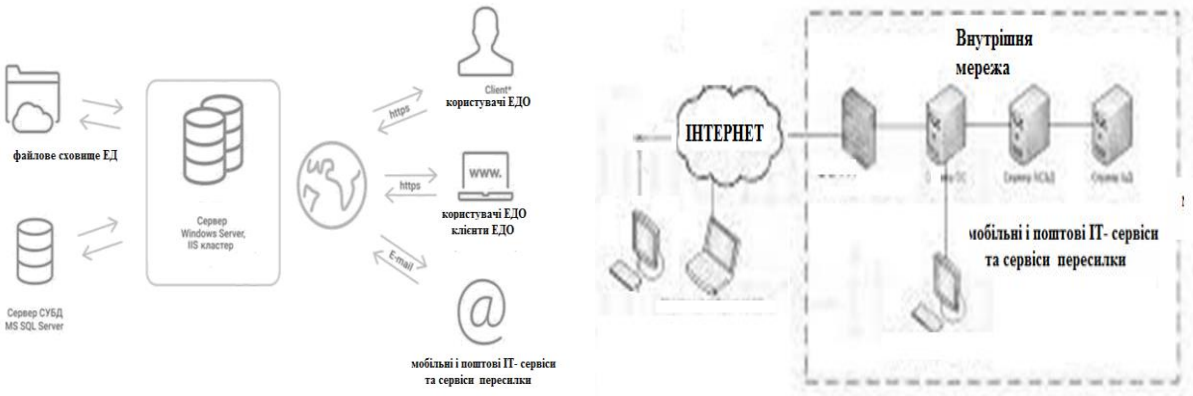


Рисунок 1.3 – Архітектура системи ЕДО із базовим захистом даних і контролем ЕД

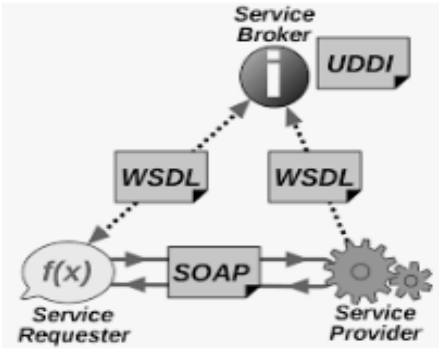


Рисунок 1.4 – Загальні принципи формування запитів на формування даних ЕД в ЕДО

Особливості (ЕДО) електронного документообігу:

– відправлення та передавання електронних документів здійснюється між сторонами в електронній формі;

– зберігання електронних документів та архіви електронних документів також здійснюється в електронній формі;

– перевірка автентичності здійснюється засобами ЦЕП (Електронного цифрового підпису) за допомогою ключа цифрового електронного підпису (КЕП);

– ЕЦП і КЕП, які за допомогою спеціальних алгоритмів в складі спеціалізованого ПЗ (програмного забезпечення) яке накладає унікальну сигнатуру електронного цифрового підпису, що дозволяє підтвердити автонтичність ЕД.

Рисунок 1.5 – Загальна ілюстрація процесу накладення ЕЦП автором із використнаям комп’ютерних засобів в системах ЕДО

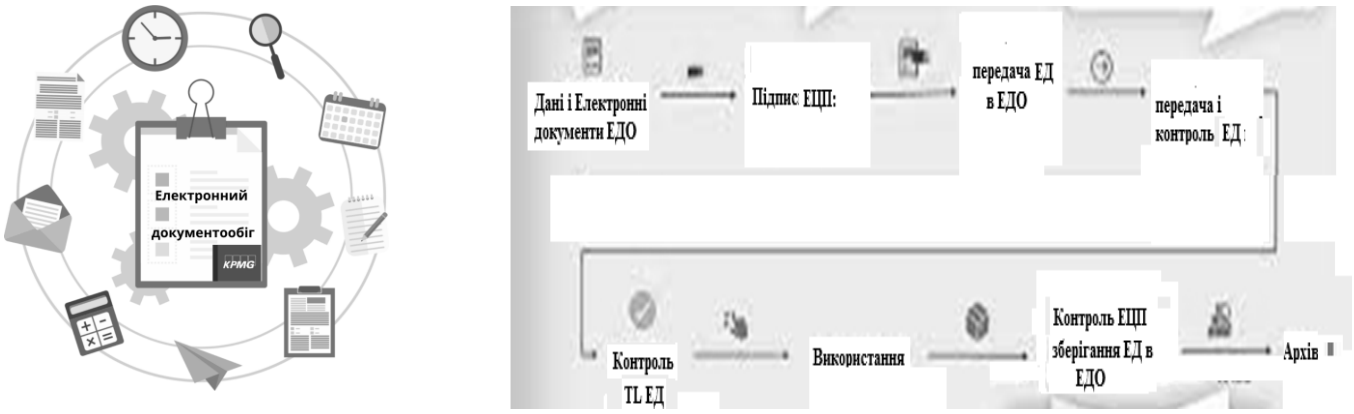


Рисунок 1.6 – Узагальнена схема руху ЕД в інфраструктурі підприємства

Одним з можливих способів представлення схеми обміну електронними документами є наступне:

– в процесі обміну даним в ЕДО при електронному документообігу, відправник створює ЕД і підписує його електронним підписом і надсилає через програму документообігу чи іншими засобами адресату;

– при цьому отримувач ставить свій електронний підпис на отриманому документі. Відправник отримує завізований екземпляр;

– протягом процесу підписання адресат отримує повідомлення з проміжними статусами документів, такими як доставлено, погоджено, відхилено.

1.3 Принципи функціонування і організації надійного і стабільного документообігу в системах ЕДО

Згідно зі сучасними тенденціями до впровадження новітніх технологій та зменшення бюрократичних процедур, необхідні нові підходи у всіх сферах, включаючи обмін електронними документами(ЕД). Багато звичайних методів пересилання паперових документів і використання поштових служб більше не ефективні, оскільки ціни і час на фізичну доставку документів зросли. Тому ми потребуємо переходу до електронного документообігу (ЕДО) з використанням нових методів та підходів.

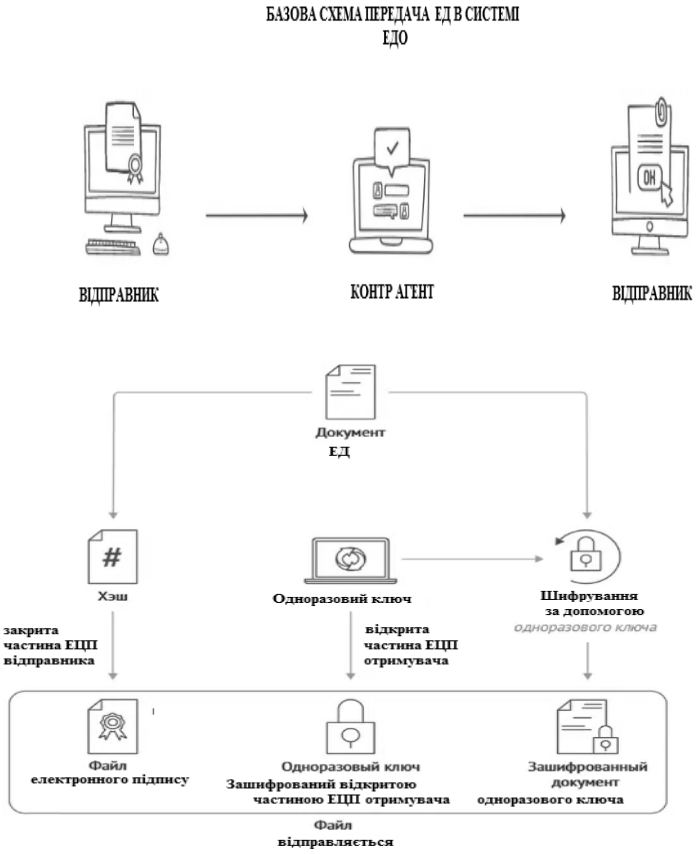


Рисунок 1.7 – Схема руху ЕД в схемі ЕДО

Саму повну і максимально надійну схему обміну електронними документами рис. 1.4 , яка враховує обов’язкові етапи – інформаційний захист даних можна представити основними 3-ма процедурами:

Формування відправником електронної документації (електронний документ – ЕД);

– підпис відправником його електронним підписом (ЦЕП - КЕП) ;

– надсилання через програму документообігу адресату;

– інформаційний захист ЕДО та відправлення ЕД на всіх етапах;

– інформаційний кіберзахист середовища та мережі і інфомрції ЕДО;

– отримувач ставить свій КЕП на отриманому документі;

– відправник отримує завізований екземпляр;

при чому в процесі підписання адресати отримують повідомлення з проміжними статусами документів: доставлено, погоджено чи відхилено.

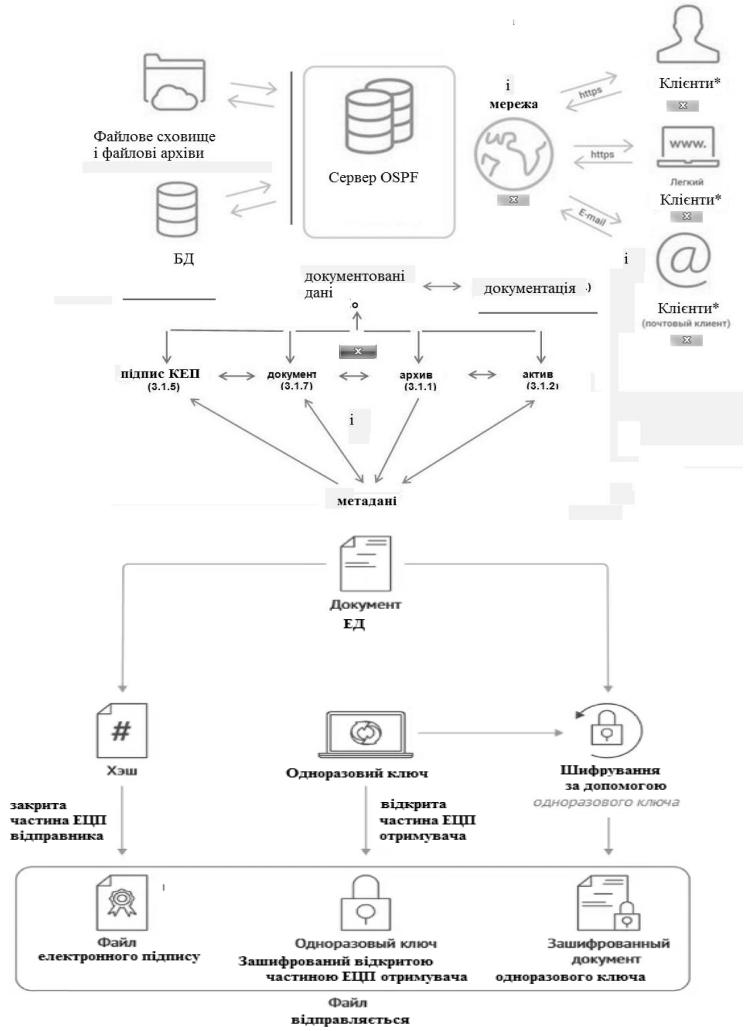


Рисунок 1.8 – Схема руху ЕД в схемі ЕДО із базовим захистом ЕЦП

Схема накладання ЕЦП за допомогою КЕП на електронні документи показана на рис.1.5 та рис.1.6.

Рисунок 1.9 – Базова схема руху і підписанння ЕД в схемі ЕДО за допомогою КЕП, а також регламент функціонування ЕДО

Зазвичай користувачі ЕДО найчастіше підписують електронні документи базовим одним ЕЦП. При великому обсязі документообігу організація отримує інструкцію щодо ведення електронного документообігу (ЕДО) та встановлює порядок використання електронного підпису (ЕП). Ключ електронного підпису, відомий як КЕП (кваліфікований електронний підпис), складається з секретного (особистого) ключа та сертифіката відкритого ключа, які використовуються тільки як пара. Секретний ключ КЕП генерується як унікальна послідовність випадкових символів, а сертифікат відкритого ключа обчислюється на основі секретного ключа: неможливо отримати секретний ключ з сертифікату.

Сертифікат відкритого ключа ЦЕП містить персональну інформацію власника (наприклад, ім'я, унікальний реєстраційний номер, видавця сертифіката та термін його дії) і підписується секретним ключем Центру сертифікації ключів. Цей сертифікат може бути згенерований Центром сертифікації ключів. Під час підписування електронного документа за допомогою КЕП його вміст не змінюється. Замість цього додається блок даних, який є електронним підписом. Процес отримання цього блоку складається із декількох етапів (рис.1.10).

Рисунок1.10 – Базова Схема підписання ЕД в схемі ЕДО за допомогою КЕП

При модифікації ЕД зміниться його цифровий відбиток(signature), і тоді документ не пройде перевірку: кореляцію процедури ЕЦП. Таким чином, цифровий відбиток (ЦВ - ЕЦП) захищає документ від змін третіми особами після накладання КЕП, а шифрування секретним ключем підтверджує авторство документу. Також змінюється і сама Hash-функція (або контрольні суми) самого документа, що можу слугувати свого роду «індикатором» модифікації вмісту або інформаційного втручання в системах ЕДО.

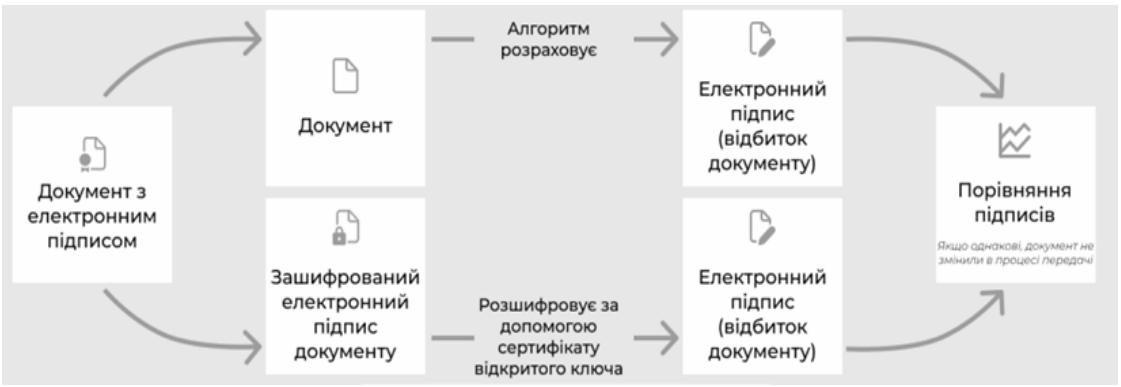


Рисунок 1.11 – Схема контролю і перевірки підписання ЕД із КЕП в схемі ЕДО

Розшифрувати електронний цифровий підпис (ЕЦП) та одержати початковий відбиток, що відповідатиме документу, можна тільки за допомогою сертифікату відкритого ключа автора за спеціальним алгоритмом ЕЦП. Перевірка ЕЦП отриманого документа проводиться кількома етапами:

– отримувач ЕД визначає унікальний цифровий відбиток одержаного документу за допомогою спеціального алгоритму формування і накладення сигнатури ЕЦП;

– розшифровує електронний підпис документа(signature), за допомогою сертифікату відкритого ключа автора та одержує відбиток початкового ЕД;

– зрівнює відбитки документу та розшифрованого ЕЦП, якщо вони однакові – це означає, що документ не модифікувався в процесі передачі.

1.3.1 Підходи формування, база і різновиди ЕД

Загалом, ЕДО можна розподілити на два типи:

1) внутрішній електронний документообіг – це обмін електронними документами всередині компанії. Сюди входять кадрові документи, накази, розпорядження та інші типи документів, що використовуються в роботі організації. Для цих цілей можна використовувати програму BAS ;

2) зовнішній електронний документообіг – це обмін документами між підприємствами та державними установами. Сюди входять договори, додаткові угоди, рахунки-фактури, акти виконаних робіт, видаткові накладні, довіреності, офіційні листи та інші. Будь-які паперові документи можна перетворити у цифровий формат.

Які переваги отримує компанія при переході на ЕДО 1.

1) зменшення витрат на канцтовари, друк та доставку документів;.

2) укономія часу співробітників та швидкість обміну документами;

3) стандартизація документів та зручний і швидкий пошук за номером, датою, типом документу чи будь-яким іншим idßреквізитом;

4) зменшення ризику втрати документів, завдяки резервному копіюванню;

5) захист від отримання інформації третіми особами.

6) здатність працювати 24/7 за рахунок доступу до ЕДО із будь – якої точки світу в захищеній мережі.

7) контроль робочих процесів і монеторинг документів ЕДО ;

8) ккологічність та скорочення кількості спожитого паперу;

9) висока технологічність та привабливість, іміджевість ЕДО.

1.3.2 Проблематика технологій захисту даних в каналах ЕДО

Основна проблема інформаційної безпеки і необхідність запровадження високого захисту даних при електронному документообігу – це втрата інформації в каналах:

1.4 Проблеми інформаційної безпеки систем ЕДО і захисту ЕД

Основними проблемами і інформаційними загрозами в система ЕДО є :

1) витік конфіденційних документів в системі ЕДО;
2) несанкціоноване спотворення;
3) несанціоновианий витік документів ЕДО;
4) знищення і видалення документів, а також пошкодження;
5) модифікація підпису (*потенц. загроза) чи використ. інших сигнатур ЕЦП;
6) втручанні зловмисників і взлам систем ІКС і систем безпеки ЕДО;
7) витік інформації і витік секретних даних ключів і підпису КЕП до зловмисників, що дозволяє неавторизований підпис документів зловмисником;
8) недостатньо складні паролі і дані авторизації в системах ЕДО;
9) загрози 0-го дня та невиявлені критичні вразливості ;
10) вразливості безпеки в програмному забезпеченні систем ЕДО і ЦЕП;
11) ненадійно захищені носії ключів системи цифрового підпису (КЕП);
12) загрози комплексного доступу і перевищення прав доступу;
13) загрози схожої подібності ідентифікаційних даних.

Це далеко не всі існуючі загрози і в тому числі загрози несанкціонованого доступу. Інколи постає проблема про потребу друкувати та зберігати електронні документи.

1.5 Основні засади розвитку і вдосконалення захисту систем ЕДО

Впровадження систем електронного документообігу (СЕД) дозволяє компаніям отримати ряд переваг, таких як зниження витрат, прискорення обігу документів та ефективне виконання завдань. Однак, для успішного впровадження

СЕД необхідно вжити заходів для забезпечення безпеки електронного обігу та збереження документів. Робота будь-якого суб'єкта господарювання із ЕДО. Основою будь-якої системи електронного документообігу (СЕД) є сам електроний документ (ЕД). У межах системи це представляє собою файл або запис у базі даних. Відповідно до Закону України "Про електронні документи та електронний документообіг", електронний документ (ЕД) визначається як документ, в якому інформація фіксується у вигляді електронних даних і містить обов'язкові реквізити, які визначаються законодавством. Електронний документ може бути створений, переданий, збережений і перетворений за допомогою електронних засобів у візуальну форму, яка може бути відображена електронно або надрукована на папері таким чином, що її можна розуміти людиною. Тільки електронний цифровий підпис (ЕЦП) має правовий статус, еквівалентний фізичному підпису, тоді як інші види електронного підпису не мають такого статусу.

1.6 Аналіз літературних джерел в галузі ЕДО

В галузі систем електронного документообігу існує ряд літературних джерел, які досліджують та описують цю тему. Деякі з них включають:

1) "Electronic Document Management Systems: A Portable Consultant" (автор: Thomas M. Koulopoulos) - ця книга надає введення в системи електронного документообігу та їх роль у сучасному бізнесі. Вона розглядає проблеми, виклики та переваги впровадження таких систем.

2) "Electronic Document Management Systems: A Case Study" (автор: David A. Smith) – ця книга пропонує вивчення конкретного випадку впровадження системи електронного документообігу в організації. Вона аналізує етапи впровадження, виклики та результати.

3) "Electronic Document Management Systems: Assessment and Implementation" (автор: Larry W. Kavanagh) – ця книга надає розгорнуті поради та

стратегії для оцінки та впровадження систем електронного документообігу. Вона охоплює такі аспекти, як аналіз потреб, вибір системи та впровадження.

4) "Managing Electronic Records: Methods, Best Practices, and Technologies" (автори: William Saffady та Charles Dollar) - ця книга зосереджується на управлінні електронними записами та системами документообігу. Вона розглядає принципи, методи та технології управління електронними записами в організаціях.

Серед українських джерел в галузі систем ЕДО можна відмітити такі :

1) "Електронний документообіг: теорія та практика" (автор: Василь Матвійчук) - ця книга присвячена електронному документообігу в українському контексті. Вона охоплює теоретичні аспекти, методи впровадження та організацію електронного документообігу.

2) "Електронний документообіг: організація та використання" (автор: Лариса Василюк) - ця книга надає практичні рекомендації та поради щодо організації та використання систем ЕДО в українських організаціях.

3) "Системи електронного документообігу: організація, використання, безпека" (автор: Юрій Лисиця) – ця книга розглядає аспекти організації, використання та безпеки систем електронного документообігу в українському контексті.

Ці джерела можуть надати українську перспективу і особливий погляд на принципи і схеми систем електронного документообігу та їх впровадження. Також ці літературні джерела можуть бути корисними для отримання детальнішої інформації про системи електронного документообігу та їх впровадження в різних контекстах.

Сучасні технології і прилади передачі даних високої захищеності в ЕДО і функціональності базаються на комплексних методах захисту і покращеного шифрування в т.ч. на додаткових методах захисту, а також на захищених каналах і мережах , на яких організовується зв’язок і передачі ЕД.

В українських джерелах в галузі ЕДО, проведений аналіз уразливостей інформаційних систем, пов'язаних з документообігом і описані критичні слабкі місця. Серед таких джерел, список може включати наступні:

1) "Аналіз уразливостей інформаційних систем" / автори: В.П. Кір'янов, О.С. Колісник, О.В. Чумаченко, І.О. Хомич. Ця книга зосереджена на загальному аналізі

уразливостей інформаційних систем, включаючи аспекти, пов'язані з документообігом. Вона надає інформацію про типові уразливості, методи їх виявлення та заходи забезпечення безпеки.

2) "Інформаційна безпека організацій" / автор: І.М. Глушко. Ця книга включає розділи, присвячені аналізу уразливостей інформаційних систем і методам їх захисту. Вона також враховує аспекти, пов'язані з документообігом і безпекою електронних документів.

3) Наукові статті і публікації українських вчених та фахівців в галузі інформаційної безпеки та кібербезпеки. Багато з цих робіт зосереджені на виявленні уразливостей і заходах забезпечення безпеки інформаційних систем, включаючи системи електронного документообігу.

Ці джерела можна знайти в наукових бібліотеках, університетах або відповідних онлайн-ресурсах, спеціалізованих на інформаційній безпеці та кібербезпеці в Україні.

2 АНАЛІЗ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Аналіз інформаційних загроз в системах ЕДО

В результаті аналізу і на основі практичного досвіду, нині багато підприємств, які впроваджують системи електронного документообігу СЕД ЕДО, висловлюють занепокоєння щодо можливого навмисного або випадкового знищення чи втрат електронних документів (ЕД). У той же час, коли розглядаються паперові версії документів, також практично неможливо забезпечити 100% захист від крадіжок, копіювання, фотографування і втрат або навмисного знищення чи несанкціонованого прочитання. Однак, ЕДО надає можливість захистити дані на кількох рівнях.

Перед тим як розглядати конкретні загрози для системи електронного документообігу (ЕДО), важливо забезпечити безпеку обміну електронними документами, що є однією з найважливіших вимог до будь-якої СЕД ЕДО. Згідно з Законом України від 5 липня 1994 року № 80/94-ВР "Про захист інформації в інформаційно-телекомунікаційних системах", захист інформації - це набір заходів, спрямованих на запобігання несанкціонованим діям щодо інформації в системі. Відповідальність за забезпечення захисту інформації покладається на власника системи. Основними загрозами безпеки систем ЕДО є:

1) Загроза цілісності інформації і цілісності ЕД в ЕДО — пошкодження, знищення або перекручення інформації ЕД із ЕЦП, як не навмисне (в разі помилок і технічних збоїв), так і зловмисне через інформаційні впливи і взлами;

2) Загроза конфіденційності даних і документів ЕДО — будь-яке порушення конфіденційності, зокрема крадіжка, перехоплення інформації, зміна маршрутів доставки, витоки до зловмисників та інше тощо,

3) Загрози для роботи і основного функціоналу системи ЕДО — загрози, реалізація яких може призвести до порушення або припинення роботи ЕДО та

ЦЕП (умисні атаки, помилки користувачів, збої в устаткуванні і програмному забезпеченні);

4) Загроза доступності даних ЕДО і систем ЕЦП — здійснення зловмисних дій, які унеможливлюють чи ускладнюють доступ до ЕДО, зокрема, створення таких умов, при яких доступ до послуги чи інформації або заблокований, або не можливий за час, для інших цілей.

Рисунок 2.1. – Джерела загроз для інформації і ЕД в системах ЕДО

5) Користувачі ЕДО та ЕЦП є потенційним внутрішнім зловмисником, які можуть нашкодити свідомо чи із необережності. Водночас спектр можливих загроз від легальних користувачів також доволі.

6) Внутрішні загрози і ненадійний персонал IT-служби підприємства із ЕДО чи суміжних аутсортингових IT-послуг – є особливою загрозою і групою ризику, до якої слід поставитися із особливою увагою. Зазвичай цей тим загрози важко виявити, а такі спеціалісти мають широкі, а нерідко і практично необмежені повноваження і доступ до сховищ і функціоналу обробки даних.

7) Зовнішні зловмисники, то тут все залежатиме від сфери діяльності підприємства, організаційної форми, наявності конкурентів тощо.

Як правило модель зовнішнього зловмисника описується моделлю класичнго хакінгу системи ЕДО «із зовні» за допомогою сканування і виявлення вразливостей із подальшою їх експлуатацією. Також сюди можна віднести прямі і не прямі методи доступу і контролю об’єктів, різні ін’єкції ШПЗ і модулів.

2.2 Способи інформаційного захисту систем ЕДО

Безпосередній захист системи ЕДО на підприємстві можна організувати різними способами. Як уже зазначалося, багато власників інформації та документів все ще побоюються вводити електронний документообіг саме з причин безпеки, втрачаючи при цьому час і кошти. Для аналізу надійності системи ЕДО , можно використати декілька показників:

1) Забезпечення збереження ЕД в складі ЕДО**.** Насамперед це - резервне копіювання ЕД в складі ЕДО. Також сюди входить зберігання ЕД в архіві ЕДО, який знаходиться в захищеному хмарному середовищі.

2) Закритий доступ до ЕДО**.** Щоб увійти всвій акаунт, користувач ЕДО має пройти аутентифікацію. Це може бути один спосіб, наприклад, пароль, і захищений USB-ключ (токен) із відбитком пальця.

3) Доступ багатоетапний**,** що містить кілька кроків: *пароль* і ключ або пароль і біометрична фіксація. Максимально надійний для проведення ідентифікації й подальшої аутентифікації спосіб — біометричний, за якого користувач ідентифікується за своїми біометричними даними (відбиток пальця, сканування сітківки ока, голос). Однак у цьому випадку вартість захисту ЕДО є вищою. До того ж техніка користувачів має відповідати вимогам біометричної фіксації даних.

4) Розмежування прав доступу в системі ЕДО. Цей функціонал дає змогу мати доступ до окремих документів лише певному колу користувачів. Інші користувачі, відповідно, такого права позбавлені.

5) Ступінь конфіденційності даних в ЕДО. Для дотримання конфіденційності в ЕДО можуть застосовуватися криптографічні методи шифрування даних, які ніхто, крім їх власника і призначених ним користувачів, не зможе бачити. Застосування криптографії значно підвищують інформаційну безпеку і конфіденційність ЕД навіть у разі його потрапляння ЕД до сторонніх осіб.

6) Забезпечення високої захищеності і достовірності інформації в ЕДО**.** Поки що основним і практично єдиним із запропонованих на ринку рішенням для забезпечення достовірності документа є ЕЦП. Зрозуміти, що

документ чинний можна за наявності ЕЦП. Більшість виробників систем і ПЗ ЕДО вже мають вбудовані у свої системи, розроблені засоби ЕЦП.

7) Протоколювання і легування дій користувачів ЕДО. Це один із важливих елементів захисту електронного документообігу. За умови його правильного налаштування та реалізації в ЕДО протоколювання дає можливість відстежувати всі неправомірні дії користувачів та знаходити загрози .

8) Надійний парольний захист і кібергігієна конфіденційних даних на робочих місцях в системах ЕДО. Особливе значення надається системам контролю паролів і даних авторизації в системах ЕДО, ннадійності формування цих жданих їх крипостійкості і інших характеристик. Інші підходи і політики збереження конфіденційних даних (паролі, КЕП, логіни) .

9) При переході на технологію ЕЦП в ЕДО, паперові документи передаються в в архів і залишається в організації, допоки не завершиться термін їз зберігання (для паперових документів, (згідно чинних норм Мінюсту України він складає 3 роки). Фіз. точки зору безпеки і інформаційної захищеності, підробити ЕД, підписаний підписом ЕЦП (документи, що візуються КЕП), - практично не можливо або досить важко, але існують інші загрози. Різновиди електронного підпису :

- кваліфікований електронний підпис (КЕП);
- удосконаленим електронний підпис (УЕП).

Відмінності між кваліфікованим (КЕП) та удосконаленим (УЕП) електронним підписом в тому, що як і хмарний захищений носій – ці типи підпису мають різний рівень захисту. Тип ЕЦП - УЕП — це підпис старого зразка, який розміщується на інформаційному носії : комп’ютері, флешці чи CD-диску. Тип КЕП — це електронний підпис, що зберігається виключно на захищеному носії токені або на захищеній хмарі провайдера. Обидві технології забезпечують достатньо стабільні, але все одно мають недоліки і існують потенційні можливості для їх компрометації.

Рисунок 2.2 – Відомі системи розподіленого ЕД із базовими процесами

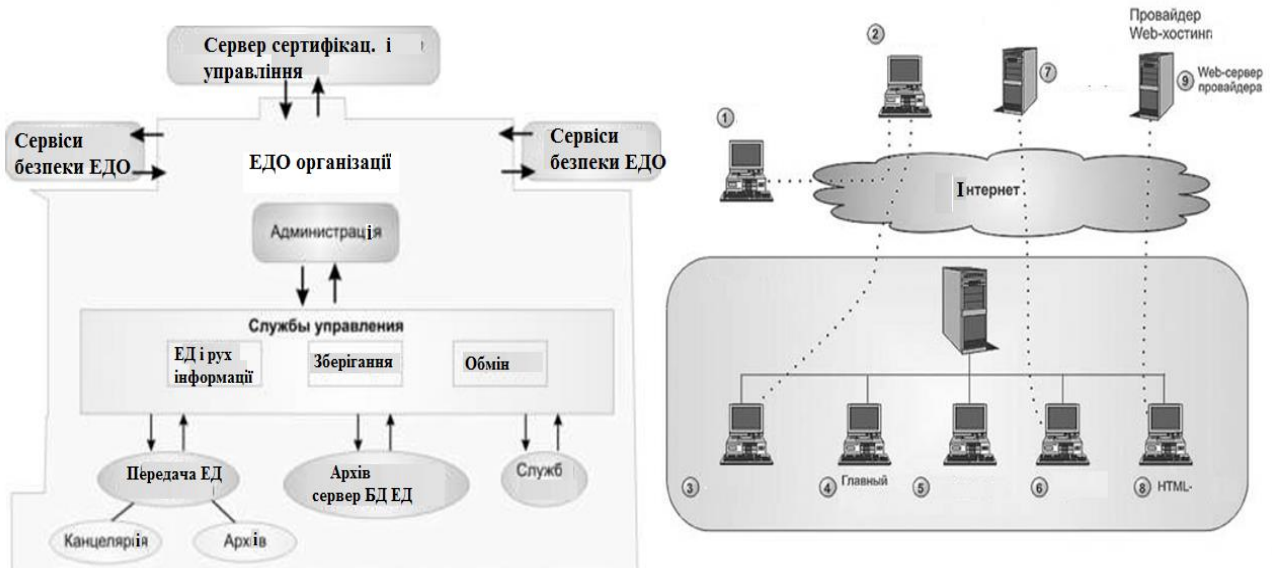


Рисунок 2.3 – Використання систем розподіленого ЕДО (електронного документообігу) у складі ІКС організацій і побудова захищених мереж і каналів

Проблема інформаційної безпеки в системах електронного документообігу ЕДО досить складна, гостро стоїть і завжди актуальна і становить серйозну загрозу для організацій і фізичних осіб, які експлуатують технології ЕДО, оскільки неправильне або недостатнє захисту інформації може призвести до витоку конфіденційних даних, порушення їх цілісності та доступності ЕД, а також спричинити ризик фальсифікації документів.

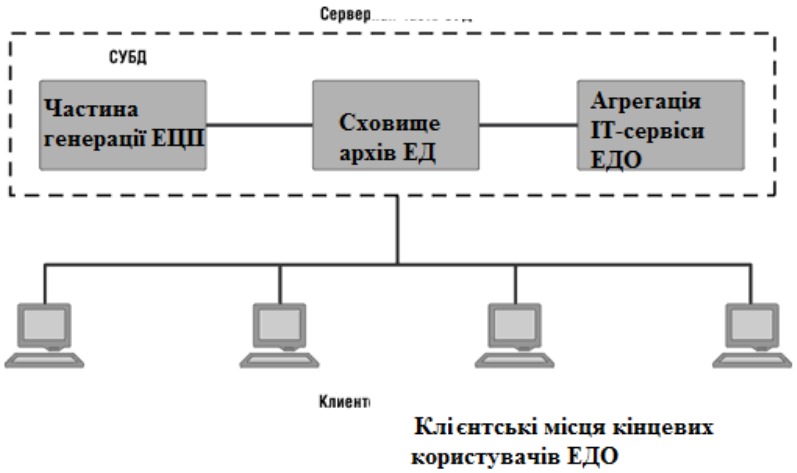


Рисунок 2.4 –Базова структура ЕДО із розподіленою обробкою і передачею ЕД ., яка інтегрується в інфрастукруту підприємства

2.3 Ключові проблеми інформаційної безпеки систем ЕДО при недостатньому інформаційному захисті

Ось деякі основні проблеми інформаційної безпеки, з якими можуть стикатися системи електронного документообігу:

1) недостатня аутентифікація та авторизація: Відсутність надійних механізмів аутентифікації та авторизації може призвести до несанкціонованого доступу до документів та систем, а також може дозволити зловмисникам підробити підписи або використовувати чужі облікові записи;

2) незахищена передача даних і незахищене середовище: Недостатні заходи безпеки під час передачі даних по мережі можуть призвести до їх перехоплення або модифікації і може спричинити порушення конфіденційності та цілісності документів.

3) вразливості програмного забезпечення і вразливості середовищ передачі: Наявність вразливостей в програмному забезпеченні, яке використовується для електронного документообігу, може бути використана зловмисниками для отримання несанкціонованого доступу до системи або внесення шкідливого коду;

4) втрати даних: Несправність апаратного забезпечення, помилки в програмному забезпеченні або несанкціоновані дії можуть призвести до втрати даних, що зберігаються в системі ЕДО. Це може мати серйозні наслідки для роботи;

Розглядаючи проблему інформаційної безпеки в широкому змісті, можна відзначити, що в цьому випадку мова йде про інформаційну безпеку всього суспільства і його життєдіяльності, при цьому на інформаційну безпеку покладає завдання по мінімізації всіх негативних наслідків від загальної інформатизації й сприяння розвитку всього суспільства при використанні інформації як ресурсу.

Слід зазначати, що основними вразливостями є:

1) несанкціонований доступ: Недостатня автентифікація та контроль доступу можуть призвести до несанкціонованого доступу до системи ЕДО;

2) втрата чи крадіжка даних: Недостатня захищеність даних може призвести до їх втрати. Якщо зловмисники отримають доступ до ЕД або БД ЕДО, це може створити значні ризики;

3) соціальний інжиніринг: Зловмисники можуть використовувати методи соціального інжинірингу для отримання доступу до системи ЕДО;

4) вразливості програмного забезпечення: Наявність вразливостей у програмному забезпеченні, таких як система управління документами або сервери, може стати причиною зламу системи електронного документообігу;

5) недостатня шифрування та захист даних: Якщо дані в системі електронного документообігу не шифруються або недостатньо захищені, зловмисники можуть перехоплювати та читати конфіденційну інформацію. Це може стати наслідком значних витоків і проблем безпеки організації вцілому ;

Основна вразливість у програмному коді систем електронного документообігу може полягати у недостатньому перевірці та обробці вхідних даних, що може призвести до атак ін’єкцій шкідливого коду (code injection attacks), таких як SQL-ін'єкція або XSS (Cross-Site Scripting).

Наприклад, ось приклад коду у системі електронного документообігу, який має вразливість XSS: phpCopy code:

```
$userInput = $_GET['message'];
echo "<div>".$userInput."</div>";
```

У цьому прикладі вхідний параметр message не перевіряється на наявність шкідливого коду. Якщо зловмисник вставить скриптовий код у значення параметра message, наприклад:

<script>alert('XSS вразливість!');</script>

То цей код буде відображений на веб-сторінці і виконаний в браузері користувача, що може призвести до виконання шкідливих дій, таких як крадіжка сесійних файлів або перенаправлення на фішингові сторінки.

Для запобігання цій вразливості, необхідно правильно перевіряти та екранувати вхідні дані перед їх використанням. В даному випадку, можна використовувати функцію htmlspecialchars для екранування HTML-тегів у вхідних даних:

Php Copy code

```
$userInput = $_GET['message']; $encodedInput = htmlspecialchars($userInput); echo
"<div>".$encodedInput."</div>";
```

Regenerate response

Таким чином, вхідні дані будуть відображені як звичайний текст, а не виконуваний код у веб-сторінці. Це допомагає запобігти XSS-атакам та забезпечити безпеку системи електронного документообігу. У цьому зв'язку основними завданнями інформаційної безпеки в ЕДО є:

- захист інформації і ЕД в ЕДО і державної таємниці;
- захист секретної і конфіденційної інформації, комерційних даних, або даних власністю держави, від несанкціонованого доступу і маніпулювання;
- захист прав громадян на володіння, розпорядження й керування приналежної їм інформацією і документів ;
- захист прав підприємців при здійсненні ними комерційної діяльності;
- захист конституційних прав громадян на таємницю листування.

Розглядаючи проблему інформаційної безпеки ЕДО, відзначимо, що в цьому випадку мова йде про сукупність методів і засобів надійного захисту інформації і ЕД ЕДО на її матеріальних носіїв, спрямованих на забезпечення цілісності, конфіденційності і доступності документів ЕДО.

2.4 Аналіз основних протоколів захищеного зв’язку для каналів інформаційних мереж ЕДО

У ІС системах ЕДО, як і у будь яких інформаційних системах існує проблема надійної захищеної комунікації при передачі даних і ЕД. Ця проблема надійного і захищеного підключення кінцевих і проміжних клієнтів ЕДО є однією із основних проблем безпеки ЕДО . Саме через ненадійне зєднання і «відкритість» потоків даних вібуваються основні втрати інформації і ЕД в ситемі ЕДО та атаки типу MITM. Прокладка нових надійних і захищених кабельних мереж вимагає великих капіталовкладень, а в ряді випадків – не можлива, особливо в умовах щільної міської забудови. Оптимальним рішенням проблеми є використання додаткового обладнання для захищеного зв’язку. Поверх традиційних і існуючих мереж або безпровідних ліній передачі [8,9]. Так, стандарт IEEE 802.11 і IEEE 802.15 передбачає для цих цілей використання захищених протоколів зв’язку, а також захисту каналів безпровідної передачі.

Враховуючи це, необхідною є використання надійних протоколів шифрування і кодування для надійного захисту даних в кналах ЕДО – як основної складової системи захисту. Розробка нового метода і моделі повинна базуватись саме на цих принципах . Протоколи повинні використовувати надійні алгоритми шифрування : із AES-DES-RSA – шифруванням і надійним захистом із 128-бітним (не менше) ключем захисту. Це дозволить засобам захисту надійно захищати ЕД в системах ЕД і робити передачі даних для каналів ІМ ЕДО надійною і стабільною, що можуть використовуватись у критичній інфраструктурі ЕДО.

Забезпечення безпеки передачі даних трафіку каналів інформаційно-компютерних мереж ЕДО і систем (ІКС) ЕДО із використанням тунелювання VPN – э другим принципом передачі даних .Безпека WEB-комунікацій і WEB-API э третім принципом створення надійної моделі захисту ЕДО.

У зв'язку з тим, що протокол HTTP призначений для передачі незашифрованих символьних даних, особи, які мають доступ до каналу передачі даних між клієнтом і сервером, можуть легко переглядати трафік і

використовувати його для несанкціонованих дій. Щоб забезпечити захист цих даних, запропоновано використовувати розширення HTTPS, яке "упаковує" дані, передані по протоколу HTTP, в криптографічний протокол SSL або TLS.

HTTPS використовує TCP-порт 443, і для підготовки веб-сервера до обробки HTTPS з'єднань адміністратор повинен отримати та встановити сертифікат для цього веб-сервера. Протокол SSL (Secure Sockets Layer) є криптографічним протоколом, який забезпечує безпечну передачу даних по мережі Інтернет. Він створює захищене з'єднання між клієнтом і сервером, використовуючи шифрування з відкритим ключем для підтвердження дійсності передавача й одержувача.

Пізніше протокол SSL був замінений стандартом TLS (Transport Layer Security) на основі протоколу SSL 3.0. TLS, який використовує шифрування з відкритим ключем та коригувальні коди і безпечні хеш-функції для забезпечення надійності і захищеності передачі даних.

Протоколи SSL і TLS використовуються як протоколи запису на нижньому рівні транспортного протоколу, такого як TCP, і вони інкапсулюють різні протоколи (наприклад, POP3, IMAP, SMTP або HTTP). Вони забезпечують підтвердження надійності клієнт-серверних комунікацій, виконують алгоритми шифрування даних в каналах ЕДО.

На нижньому рівні багаторівневого транспортного протоколу в системах ЕДО протоколи запису і використовується для інкапсуляції різних протоколів (POP3, IMAP, SMTP або HTTP) при передачі даних. Для кожного інкапсулірованого протоколу він забезпечує умови, при яких сервер і клієнт можуть підтверджувати один одному свою дії, виконувати алгоритми шифрування і робити обмін криптографічними ключами, перш ніж протокол прикладної програми почне передавати й одержувати дані. Для доступу до веб-сторінкам, захищеним протоколом SSL, у URL замість схеми http, як правило, підставляється схема https, що вказує на те, що буде використовуватися SSL-з'єднання. Стандартний TCP-порт для з'єднання по протоколі https — 443. Для роботи SSL потрібно, щоб на сервері мався SSL-сертифікат. У мережі WEB(Веб) підтримуються 3 типи аутентифікації при клієнт-серверних взаємодіях:

– Basic – базова аутентифікація, при якій ім'я користувача і пароль

передаються в заголовках http-пакетів. Пароль при цьому не шифрується і є присутнім у чистому виді в кодуванні base64. Для даного типу аутентифікації використання SSL є обов'язковим;

– Digest – дайджест-аутентифікація, при якій пароль користувача передається в хешованому виді. За рівнем конфіденційності паролів цей тип мало чим відрізняється від попереднього, тому що атакуючому все рівно, чи дійсно це дійсний пароль або тільки хеш від нього: перехопивши посвідчення, він усе рівно одержує доступ до кінцевої точки. Для даного типу аутентифікація використання SSL є обов'язковим;

– Integrated – інтегрована аутентифікація, при якій клієнт і сервер обмінюються повідомленнями для з'ясування дійсності один одного за допомогою протоколів NTLM або Kerberos у ЕДО. Цей тип аутентифікації захищений від перехоплення посвідчень користувачів, тому для нього не потрібен протокол SSL;

Тільки при використанні цього типу аутентификації можна працювати за відкритою схемою у ЕДО, у всіх інших випадках необхідно використовувати схему https. Загальні положення архітектури мережевої безпеки викладені в рекомендації Міжнародного союзу електрозв'язку: ITU-T-U X.805.X - ITU-T X.509.X [10, 12]. Ця рекомендація закладає основи для розробки загальних і детальних рекомендацій з цих питань для конкретних мереж незалежно від їх технології та відповідності еталонним моделям OSI або TCP/IP у ЕДО. При викладі матеріалу цієї роботи термін «мережева безпека» часто буде замінений широко використовуваним в літературі рівноцінним терміном «інформаційна безпека в мережах» або в даній роботі просто «інформаційна безпека» (ІБ). Під загрозою відповідно до рекомендації ITU-T-Г X.800.X у системах ЕДО розуміється потенційна можливість порушення безпеки даних.

Принципи виконання функцій захисту жаних протоколами інформаційної безпеки на прикладному рівні (протокол pfübcne XGP), на транспортному рівні (протокол SSL / TLS), на межсетевом рівні (протокол IPSec) є базовмим для надійного захисту даних електронних окументів (ЕД) у ЕДО .

До основних захищених протоколів і технологій безпеки в каналах ІС ЕДО

можна віднести: PGP і BGP; L2TP;P2TP; S2TP;IPSec ; ESP.

Всі вони використовують захищені схеми обміну клбючами:

IKE (Inter Key Exchange). Це базові і основні протоколи захисту, які використовуються для надійного шифрування потоків даних в ЕДО і самих ЕД в процесі їх передавання між абонентами А і В в каналах ІМ ЕДО, Ці протоколи входять та підтримуються більшістю сучасних систем сучасного канального та мережевого обладнання і систем організації інформаційних мереж.

Протоколи захищеної передачі даних із шифруванням є протоколами захисної оболонки передачі ,яка використовує пари ключів для створення захищеного шифрованого з'єднання і проведення захищеної передачі ЕД в ЕДО. Протоколи захисту шифрують пакети даних в каналах ЕДО і пакети ЕД, що забезпечує конфіденційність повідомлень, аутентифікацію і захист. Шифрування і дешифрування повідомлень по протоколам захисту наведено на рис. 2.6. Повідомлення М шифрується загальним ключем Ks за допомогою традиційної симетричною криптографії. Цей ключ генерується на стороні абонента А і шифрується відкритим ключем абонента В. Шифрування проводиться асиметричною чи семетричною криптографією ЕР за допомогою відкритого ключа Ев одержувача повідомлення. Зашифрований загальний ключ ЕВ (Ks(T)) (який іноді називають цифровим конвертом) і зашифроване цим ключем повідомлення С = Ks (Т) передаються по каналах ІМ абоненту В (рис.2.5).

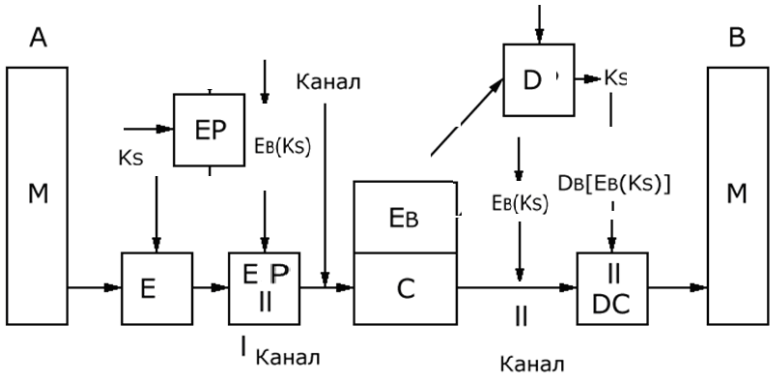


Рисунок 2.5. – Шифрування і дешифрування повідомлень протоколами захищеної передачі в каналах ЕДО

На стороні абонента В (Рис. 2.5.) за допомогою його закритого ключа Dв проводиться дешифрування DP. В результаті перетворень отримується ключ симетричного шифрування Ks = Dв (EB (Ks(T))), відправлений зашифрованим на стороні абонента А. І цим ключем проводиться дешифрування DC зашифрованого повідомлення М (тобто С =(Ks (M(T))) за допомогою симетричного криптографії із загальним ключем. Аутентифікація повідомлення із ЕДО в ЕДО протоколами захисту виконується за допомогою цифрового підпису протоколу (не слід плутати із ЕЦП для ЕД) з використанням криптографії з відкритим ключем і профілю повідомлення. Створення ЕЦП ЕД на базі подібного протоколу – це окремий механізм із окремими своїми ключами шифрування, які діють в рамках канального механізму передачі.

В цьому випадку, закритий ключ протоколу відправника є тільки у нього, користувач впевнений в тому, що дану підпис міг створити тільки власник відповідного секретного ключа. Надійність алгоритму хешування SHA-1 (SHA-X) дає одержувачу впевненість також в цілісності даних, тобто в тому, що ніхто інший не міг створити ще одне повідомлення з відповідним хеш-кодом і, отже, за підписом його оригінального повідомлення. Таким чином, схема рис. 2.5 забезпечує впевненість в автентичності джерела повідомлень і цілісності даних повідомлень (тобто аутентифікацію повідомлення). Криптографія ЕД в ЕДО з відкритим ключем має недолік в низькій швидкості а тому застосовується при шифруванні/ дешифрування коротких повідомлень і невеликих ЕД (ключа симетричного шифрування, хеш-коду).

2.5 Встановлення захищеного зв’язку в каналах ЕДО

На рис. 2.8 показана схема обміну захищеними повідомленнями при встановленні захищеного зв'язку SA між клієнтом і сервером в ЕДО. У мережах ЕДО на базы WiFi і WiMAX клієнтом є бездротовий користувач, а сервером аутентифікації RADIUS-сервером ЕДО. Процес встановлення захищеного зв'язку можна уявити що складається з наступних чотирьох етапів [4]. Процес ініціалізується клієнтом, який відправляє серверу повідомлення «client-hello» в ЕДО із параметрами: версія, випадкові значення, ідентифікатор сеансу, комплект шифрів, метод стиснення. На

рис.2.6 показаний детальний опис 2-х із цих параметрів: ідентифікатор сеансу і комплект шифрів. Випадкові значення використовуються для захисту від загрози «повтор передачі пакета». Ідентифікатор сеансу забезпечує роботу TLS і ідентифікує сеанс зв’явку і описує 2 важливих поняття – «сеанс» і «з'єднання». Сеанс визначає набір параметрів захисту, які можуть використовуватися декількома з'єднаннями. Ідентифікатор сеансу говорить про намір клієнта створити новий «сеанс» або створити нове «з'єднання» в рамках того ж «сеансу».

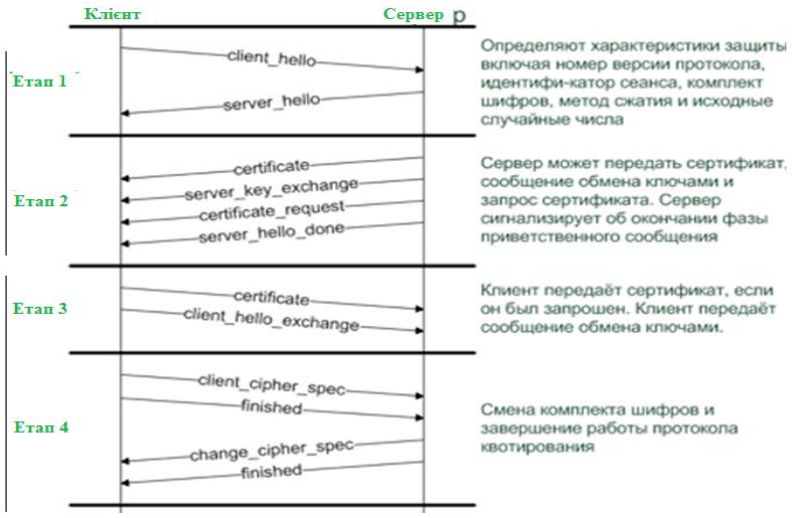


Рисунок 2.6 – Схема захищеного обміну повідомленнями в ЕДО (захищене з'єднання)

Кожен комплект шифрів визначає алгоритм обміну ключів і список, що складається з окремих наборів і полів. Зараз доступно для використання велика кількість різних алгоритмів шифрування: алгоритм асинхронного шифрування (RC4, DEA, IDEA і ін.); алгоритми хеш-функції (SHA-1, MD5); потоковий, блоковий тип шифру. Важливою є 2 парамтери шифрування в будьякому алгоритмі:

– довжина хеш-коду;
– довжина вектора ініціалізації блокових кодів.

Протокол TLS підтримує такі методи обміну ключів для шифрування з загальним ключем і обчислення значень відкритих ключів за протоколом HMAC (додаток Д, розділ Д2). Алгоритм RSA формує секретний ключ і відкритого ключ RSA, повідомлення прицбьому шифрується за допомогою обох ключів. Для цього відправнику повинен бути доступний сертифікат відкритого ключа одержувача. Найчастіше використовується метод Діффі-Хеллмана з фіксованими параметрами

(Fixed Diffie-Hellman Alg). Метод обміну ключами за схемою Діффі-Хеллмана, при якому сертифікат сервера містить відкриті параметри алгоритму Діффі-Хеллмана, підписані центром сертифікації. Для захисту інформації в ньому використовується криптограіччний алгоритм і ключ:

– Алгоритм – послідовність математичних дій, за допомогою яких відбувається перетворення інформації;

– Ключ - секретний прихований код (числова послідовність), який необхідний для читання, зміни або перевірки даних.Клієнт повідомляє свої параметри алгоритму Діффі-Хеллмана або в сертифікаті, якщо потрібно аутентифікація клієнта, або в повідомленні обміну ключами.

Це забезпечує захист від загрози «людина посередині» MITM (додаток Д, розділ Д3) за допомогою "Метод Діффі-Хеллмана з одноразовими параметрами (Ephemeral Diffie-Hellman). Цей метод застосовується для створення тимчасових (одноразових) секретних ключів. У цьому випадку сторони обмінюються відкритими ключами Діффі-Хеллмана, підписаними закритим ключем RSA відправника. Одержувач для перевірки підпису може використовувати відповідний відкритий ключ. Для аутентифікації відкритих ключів застосовуються сертифікати. Це забезпечує захист від загрози «людина посередині» (додаток Д, розділ Д3). Передбачає використання базового алгоритму Діффі-Хеллмана, але аутентифікація не виконується. Іншими словами, кожна зі сторін надсилає свої відкриті параметри для алгоритму Діффі-Хеллмана іншій стороні без аутентифікації. Для забезпечення вимог надійного шифрування і виконання надійних криптографічних алгоритмів пртоколи захисту в ЕДО використовують стандартні але надійні механізми криптографії – інформація захищається шляхом гешування та шифрування надійним математичним алгоритмом.

Посилення захисту протоколів ІБ ЕДО прикладного рівня захищений канал ЕДО, реалізований на прикладному рівні, захищає тільки певну службу (файлову, передачу . передачу ЕД в ЕДО, гіпертекстову, поштову передачу і ін.). При цьому для кожного прикладного протоколу необхідно розробляти власні засоби захисту.

Використання протоколів захисту IProtocolSec підсилює захист механізмів забезпечення ІБ, вбудованих в прикладний рівень (такі, як протоколи електронної комерції та інші). На рис. 3.4 показаний приклад використання IProtocolSec. Тут приведена корпоративна мережа з двох локальних обчислювальних мереж, що знаходяться в різних місцях. Під корисним вантажем тут розуміється поле даних, в яке входять заголовки і інформація рівнів вище мережевого (тобто транспортного і прикладного). Пакети IP, які підлягають захисту захищеним протоколом IProtocolSec, обгортаються, але не заголовок IP. AH в транспортному режимі передбачає аутентифікацію корисного вантажу IP і деяких частин заголовка IP.

Тунельний режим забезпечує захист всього пакета IP в каналах ЕДО. Коли електронний документ (ЕДО) підлягає передачі, він розбивається на пакети і кожен із цих пакетів захищається протоколоам захисту і шифрування I ProtocolSec, що забезпечує високий стйпінь захисту. І навіть при успішній реалізації MITM атак в інформаційних системах ЕДО, із подальшим зчитуванням документа ЕД . шифрований його формат зробить його вміст недоступним для зовнішнього зловмисника поза каналом. Щоб виконати це завдання шифрування, після додавання до пакету IP полів AH або IProtocolSec весь пакет разом із полями захисту розглядається як корисний вантаж деякого нового «зовнішнього» пакета IP з новим зовнішнім заголовком IP. Весь вихідний (внутрішній) пакет при цьому пересилається через «тунель» від однієї точки мережі IP до іншого, і жоден з маршрутизаторів на шляху не може перевірити внутрішній заголовок IP. Оскільки пакет инкапсулирован в новий, більший пакет, цей новий пакет може мати зовсім інші параметри джерела і адресата, що, очевидно, посилює захист. Тунельний режим використовується тоді, коли один або обидва кінці захищеного зв'язку є шлюзами захисту, наприклад граничними маршрутизаторами, які використовують захищений протокол IProtocolSec.

У механізмах аутентифікації і конфіденційності для передачі даних між двома хостами ЕДО ротокол I ProtocolSec передбачає попереднє виконання наступних двох кроків (фаз) [2].

1) Кожен хости ЕДО івузол ІМ ЕДО в мережі повинен бути, перш за все, аутентифікований (див. Додаток. А, розділ А.2 і додатки В, Г). Різні реалізації захищених протоколів I ProtocolSec (наприклад, протокол IPSec) може передбачати різні методи і підходи шифрування із використанням алгоритмів захисту і «огортання» пакетів. Створюється захищений канал зв’язку в інформаційній системі ЕДО для захищеної передачі інформації і передачі захищених даних про параметри в ході другої фази захисту .

2) Ця фаза є ключовою в захищених протоколах I ProtocolSec (наприклад, IPSec або ESP) і полягає в створенні захищеного зв'язку SA (Security Authentication). При цьому відправник X і одержувач Y повинні домовитися про застосовувані протоколах шифрування|дешифрування, визначити ключі, часи їх дії, а також інші параметри зєднняня і сесії зв’язку . У кожному протоколі передачі I ProtocolSec наводиться і використовується свій власний список параметрів захищеного зв'язку, в залежності від алгоритму. Захищений зв'язок створюється процедурою управління ключами за допомогою одного із механізмів обміну ключами IKE (Internet Key Exchange) в кожному протоколі захищеної передачі I ProtocolSec. Організовувати високоефективне надійне і шифроване зєднання із керуванням та моніторинг інформаційних процесів і захищену передачі інформації у сучасних ЕДО – ключова задача для забезпечення високого інформаційного захисту. Створення надійної передачі ЕД в ЕДО на базі захищених процесів і в системах із захищеними протоколами заявку через організовані закриті канали на базі Інтернет-комунікацій віддаленого зв’язку відповідає концепції захищених закритих систем передачі і концепції надійного застосування ЕДО і захищеного обміну ЕД.

Не зважаючи на захист шифруванням в ЕДО потрібні ще й додаткові заходи захисту інформації ЕД, не тільки ІМ каналах передачі ЕД а й у самій ЕДО.

Підсумки проміжного аналізу надійності і кіберстійкості систем ЕДО.

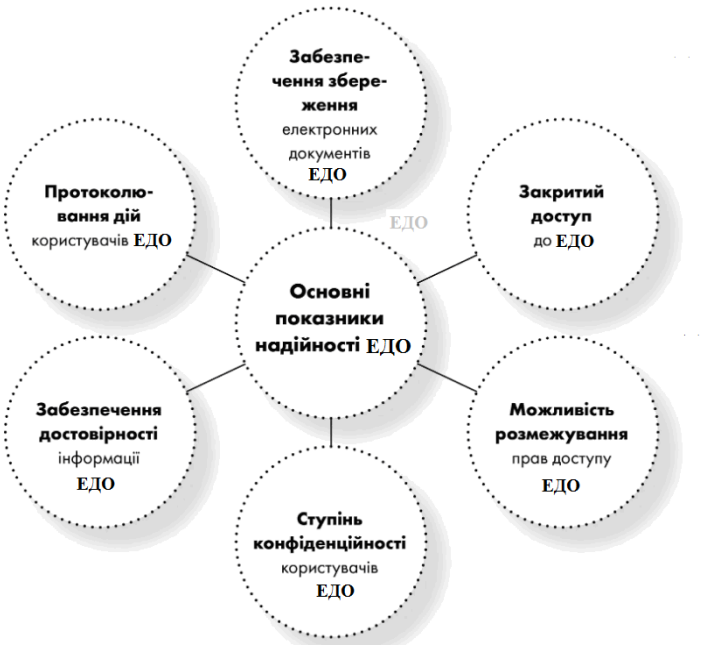


Рисунок 2.7 – Основі фактори і показники, які впливають на надійніст ЕДО

апаратних засобів системи, ПК, периферії та інших пристроїв;

Крім технічних аспектів також необхідно враховувати організаційні заходи забезпечення безпеки ЕДО. Навіть якщо система електронного документообігу (ЕДО) та криптографія мають ефективний захист, мало що може завадити третій особі прочитати документ, наприклад, якщо вона стоїть за спиною користувача, який має законний доступ до цього документа. Існує можливість, розшифровування інформацію із ЕД, використовуючи ключ, який залишений працівником у відкритому доступі, наприклад, на робочому столі під час його відсутності. Основним проблемним місцем в організації захисту ЕДО є не тільки технічні засоби, але і відношення користувачів до ІБ. Важливо розуміти, що коли документ потрапляє до користувача – повна його конфіденційність вже є порушеною. Підхід до захисту ЕДО повинен бути комплексним. Важливо чітко розуміти та об'єктивно оцінювати потенційні загрози та ризики ЕДО. Захист ЕДО не обмежується лише захистом документів і каналів передавання даних ІМ. Крім того, є важливою перевагою можливість відокремлення системи ЕДО у спеціальний сегмент ІС ІКС мережі ЕДО. Тому при виборі засобів інформаційного захисту ЕДО необхідно оцінювати потенційні втрати від розголошення або спотворення інформації та порівнювати їх з вартістю засобів, які потрібно впровадити для їх захисту.

2.6 Розроблення структурної та математичних моделей захисту інформації ЕД в системах ЕДО

2.6.1 Розробка математичної моделі загроз і захисту даних в ЕДО системах

Стандартні моделі захисту ЕДО передбачають використання стандартних ЕДО, що передбачають аналіз видів можливих загроз і моделей загроз інформаційних систем і формування правил ІБ із створенням дієвих механізмів і систем захисту ЕД і ЕДО від більшості загроз і з кожного із типів загроз і напрямків захисту. Стандартна модель захисту інформаційної системи ЕДО і системи захисту для створення моделі захисту даних від загрозв в ЕДО полягає у створенні шаблону еталону факторів впливу і самогообєкта інформцінйог орпоцесу ЕДО.

Етап 1 моделі. Повністю перерахувати і проаналізувати всі загрози і об'єкти системи ЕДО , що підлягають захисту від впливів порушника *Oi*.

Етап 2 моделі. Повністю перерахувати і проаналізувати всі можливі варіанти дій зловмисників і загроз, тобто вказати всі потенційні загрози інформації: формується набір загроз інформаційної безпеки $З_Н$.

Етап 3 моделі. Визначити в кількісному вираженні заходи відповідної загрози для кожного зазначеного раніше об'єкту. Кожна загроза, позначена на етапі 2, має ймовірність появи, що і визначається на даному етапі: результаті утворюється граф моделі захисту ЕДО, де ребро (t_i,про$_j$) означає, що загроза t_i дозволяє отримати доступ до об'єкта Пр O_j..

Етап 4 моделі. Сформувати засоби комплексного захисту інформації в системі ЕДО. Мета засобів захисту інфлормації ЕДО – створити бар'єр для доступу до інформації ЕДО по кожному ребру графа. Так формується набір засобів забезпечення захисту інформації *М*. Один і той же засіб безпеки може захищати декілька об'єктів і протистояти кільком загрозам.

Етап 5. Визначити в кількісному вираженні міри можливості протидії загрозам в системах ЕДО. Якщо ці заходи перевищують рівень загрози в ЕДО, то така система захисту ЕДО вважається достатньою.

Різновиди моделей ІБ ЕДО:

3) 1)Модель системи розмежування доступу до ресурсів системи ЕДО;

4) 2)Модель системи захисту ЕДО із застосуванням шифрування ЕД;

До одним і тим же ресурсів можуть звертатися кілька користувачів, при цьому, якщо ресурси вимагають захисту, то доступ до них здійснюється лише за наявності у користувача повноважень на це.

Недоліки даних моделей:

5) На практиці часто досить складно визначити всі шляхи негативних дій по відношенню до системи ЕДО, що погіршує адекватність результатів моделі;

6) Відсутність ребра (t_i,o_j) не означає, що система повністю захищена;

7) Не враховуються витрати на захист системи і отримуваний від цього ;

Традиційна модель захисту ЕДО., описана у [23] показана на рисунку 2.10.

Рисунок 2.8 – Модель загроз і захисту даних в системах ЕДО із оцінками загроз

Дана модель (рис.2.8) враховує комплексний фактор реалізації ризиків в каналах і інфомраційно-комунікаційних трактах реалізації передавання даних в біомедичних системах, їх оцінку та шляхи нейтралізації.

Об'єктивні показники моделі:

– Канальні загрози інформаційній безпеці, що характеризуються ймовірністю реалізації, пропорційною кількості комунікацій в системі;

– Вразливі точки (точки реалізації загроз інформаційної системи або системи запобігання загрозам (системи інформаційної безпеки);

– Враховується ризики - чинники, що відображує можливі наслідки від реалізації загрози організації в результаті реалізації загрози ІБ: втрата/ модифікація інформації та її несанкціонованого зчитування .

Також відомою є модель, що передбачає використання оцінки ризиків і запровадження заходів інформаційної протидії (рис. 2.8).

Для побудови збалансованої системи інформаційної безпеки потрібно спочатку провести комплексний аналіз ризиків у сфері інформаційної безпеки біомедичної системи передачі даних . Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику.

2.6.2 Методика проведення аналізу по моделі захисту ЕДО

Методика дозволяє повністю проаналізувати і зафіксувати та оцінити вимоги щодо гарантування інформаційної безпеки послуг, що надаються, і гарантій безпеки майнових прав та інтересів клієнтів. Досягти поставлених цілей можна при вирішенні таких основних завдань:

Оцінка ризиків по всім комунікаціям в системах і комплексна оцінка фактору безпечності;

– віднесення і класифікація інформації до категорії ступенів захисту;

– прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів причин і умов, що сприяють порушенню функціонування об'єкта ІС;

– створення умов функціонування з найменшою вірогідністю реалізації загроз;

– створення механізму і умов оперативного реагування на загрози інформаційній безпеці та прояви негативних тенденцій у функціонуванні;

– уникнути витрат на зайві заходи безпеки, що можливі у разі оцінки ризиків;

– здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;

– забезпечити проведення робіт в короткі терміни та оцінити ефективність.

Побудова моделі інформаційної технології захисту ЕДО при побудові моделі захисту ІБ систем ЕДО слід враховувати взаємозв'язки між ресурсами ЕДО. Наприклад, реалізації сценарію витоку даних, вихід із ладу якогось вузла ЕДО може призвести до втрати даних або виходу з ладу іншого критичного елемента ЕДО. Ці взаємозв'язки визначають основу побудови моделі організації інформаційної безпеки. Ця модель, відповідно до пропонованої методики, буде такою: для виділених ресурсів визначають їх цінність огляду і «вагу», атакож потенційні ризики і загрози втрати даних, визначають порушення функціоналу і проводять відповідні оцінки заходів протидій цим ризикам. Потім описують взаємозв'язки ресурсів, визначають загрози безпеці й оцінюють вірогідність їх реалізації.

2.6.3 Математична модель кіберзагрози в системах ЕДО

Для успішного застосування і оцінки захисту в ЕДО при передачі інформації електронних документів пропонується використати математичні моделі оцінки і захисту від загроз (модель безпеки даних в ЕДО):

Значення коефіцієнтів $k=10^{-4} – 10^{-6}$ вважався задовільним, то в наш час завдяки розвитку технологій вважається прийнятним $k=10^{-6}$. Тому будь-яка система повинна бути розроблена із запасом надійності і передбачати деякий «запас безпеки», щоб передбачати різкі зміни умов впливу кіберзагрози на основін компоненти і середовище інформаційної системи ЕДО. Загасання і спад захисту при різних умовах явищах, зокрема при збільшенні інтенсивності інформаційних загроз можливе при збільшенні коефіцієнту загроз $-\alpha(\lambda)$ при збільшенні їх інтенсивності λ , яка можна досить високих значень в екстремальних умовах і при критичному впровадження. Це передбачено в моделі загроз. Це можно точно змоделювати. Наприклад, прямі втручання і ін’єкції шкідливого коду і функціоналу ШПЗ в ЕДО легко формалізуються розширеною моделлю втручання:

$$G(x,y,f) = f_0(\lambda,x,e) \exp[-\alpha(\lambda)\, q_k(x)\, I\, k\,] \qquad (2.4)$$

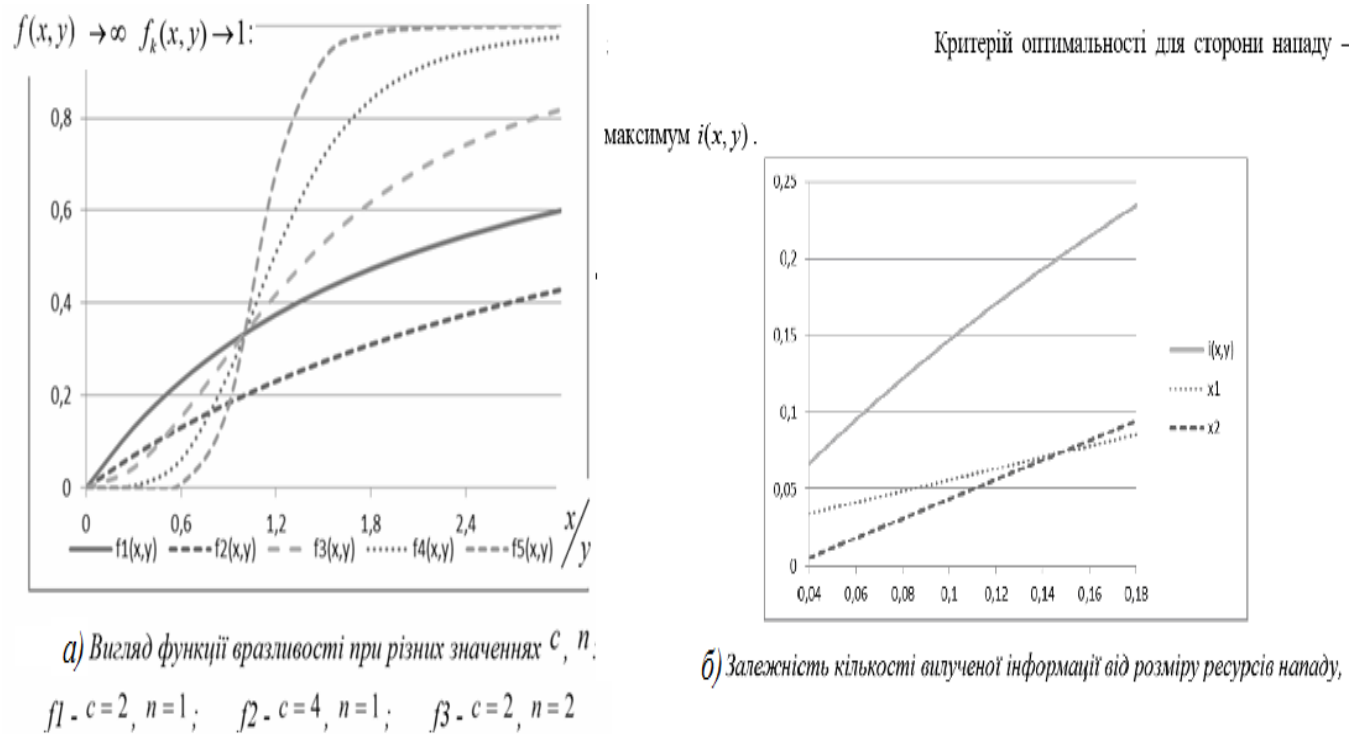
У цьому розділі всю увагу приділено функції $q_k(x)$, як показника котрий характеризує дії нападника.

$$f(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n+c} \tag{2.5}$$

Окремий випадок формули (2.4) із врахуванням

(2.5) $$G(x,y)=0.4\frac{x_1/0.05}{x_1/0.05+4}+0.6\frac{x_2/0.05}{x_2/0.05+8}.$$

для досліжень дав змогу т=отримати графік функції (2.4), який показаний на рис. 2.9.



а) Вигляд функції вразливості при різних значеннях c, n:

f1 - c = 2, n = 1; f2 - c = 4, n = 1; f3 - c = 2, n = 2

б) Залежність кількості вилученої інформації від розміру ресурсів нападу,

Рисунок 2.9 – Графіки функцій (2.4) моделі втручання в систему ЕДО

Ця модель може стати основою при оцінці інформаційних загроз і може використовуватись при розробки зовнішнії засобів захисту систем ЕДО, які послідовно підключаються до/або функціонують в складі основної архітектури інших приладів і систем електронного діловодства і електронного документообігу, а також засобів для непрямого аналізу і вимірювання вмісту шкідливого ПЗ та інформац. загроз в коді основниї програми і інформаційного потоку ЕД даних, що підлягаються обробленню. Аналіз і нейтралізація

шкідливого коду в трафіку і ЕД і в складі обчислювального процесу ЕДО відбувається в режимі наближеного дор реального часу та в режимі реального часу. Використання комплексу технологій мережевого захисту, використання в кнаалах захищених основних мережевих протоколів і вінформаійного захисту обчислювальних процесів, а також захисту трафіку передбачає умовно максимальну мінімізацію кіберзагроз та ризиків їх появи $r_{сх}$:

$$r_{сх} \rightarrow [\max(\min T_r) \; , T_r \; \epsilon \; M_r] \; ;$$

$$'Tr = \sum_{i}^{n} Tr_i \rightarrow N * T_r s \qquad (2.6)$$

де T_r – узагальнена ймовірність появи інфомраціних ризиків в системі ($T_r \; \epsilon \; M_r$), де M_r– множина інформаційних ймовірностей загроз (мапа кіберзагроз).

Дана модель безпеки ЕДО забезпечує оцінкузначно вищу ефективність захисту даних ЕД в ЕДО при аналізі і передаванні інформації ЕД і інших даних порівніно з іншими не примими методами а може використовуватись для швидкого і попереднього аналіз і блокування нешифрованого трафіку і інформаційних потоків в внформаційних мережах передачі даних ЕДО на базі Ір -протоколу ю Використовується шифрування IProtocolSec для передачі даних моніторингу, відтворення і передавання біологічних показників людини, а також є економіно вигідним, оскільки не потребує застосування високотехнологічних і дорогоцінних прийьомів і засобів. Запропоновані моделі оцінки інформац. загро*зи для ЕДО* може з достатньо високою ефективністю використовуватись у комерційні практиці впровадження систем ЕДО.

3 ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У СИСТЕМАХ ЕДО І ОРГАНІЗАЦІЯ НАДІЙНОГО ІНФОРМАЦІНОГО ЗАХИСТУ ЕД

3.1 Оцінка захисту і вразливостей систем ЕДО

Як відомо, для надійного захисту ЕД, Електронний документообіг в системах ЕДО, повинен здійснюватися за правилами внутрішнього розпорядку і бути обмеженим для сторонніх осіб. Але досить часто цього недостатньо для повнофункціональнго надійного захисту, що потребує розробки і впровадження нових підходів : зокрема нових моделей і методів покращеного захисту, що дозволить підвищити ступінь захисту систем електронного документообігу ЕДО.

Базові традиційні підходи до захисту систем ЕДО полягають:

- використання антивірусних систем запобігання вторгнень IPS;
- використання мережевих систем екранування (Active & Pasive Firewall);
- використання тунельованих каналів звязку (VPN) із шифруванням і захистом по одному із протоколів шифрування (IPSec; L2Tp PPTP; P2P;BGP SPTP інше);
- використання додаткового шифрування ЕД та авторизованного доступу до них;
- використання додаткових методів захисту і в тому числі моделей;
- використання надійних сертифікатів шифрування (1024 -2048);
- використання комплексних додаткових методів і систем захисту (КЗСІ).

Варто відзначити, що електронний документ як і електронна довірча послуга *(ЕДП) – це послуги і суміжні ІТ сервіси, які надаються для забезпечення електронної взаємодії між 2-ма або більше суб'єктами, які довіряють надавачу електронних довірчих послуг. При виборі провайдера електронного документообігу, який надає такі електронні довірчі послуги, необхідно звертати

увагу на ряд факторів, що забезпечать повноцінну та захищену роботу з даними підприємства-замовника.

Вразливості і загрози для ЕДП та ЕД теж мають місця в системах ЕДО і можуть бути використані зловмисниками для генерації шкідливого трафіку і вторинного зламу ІКС систем ЕДО.

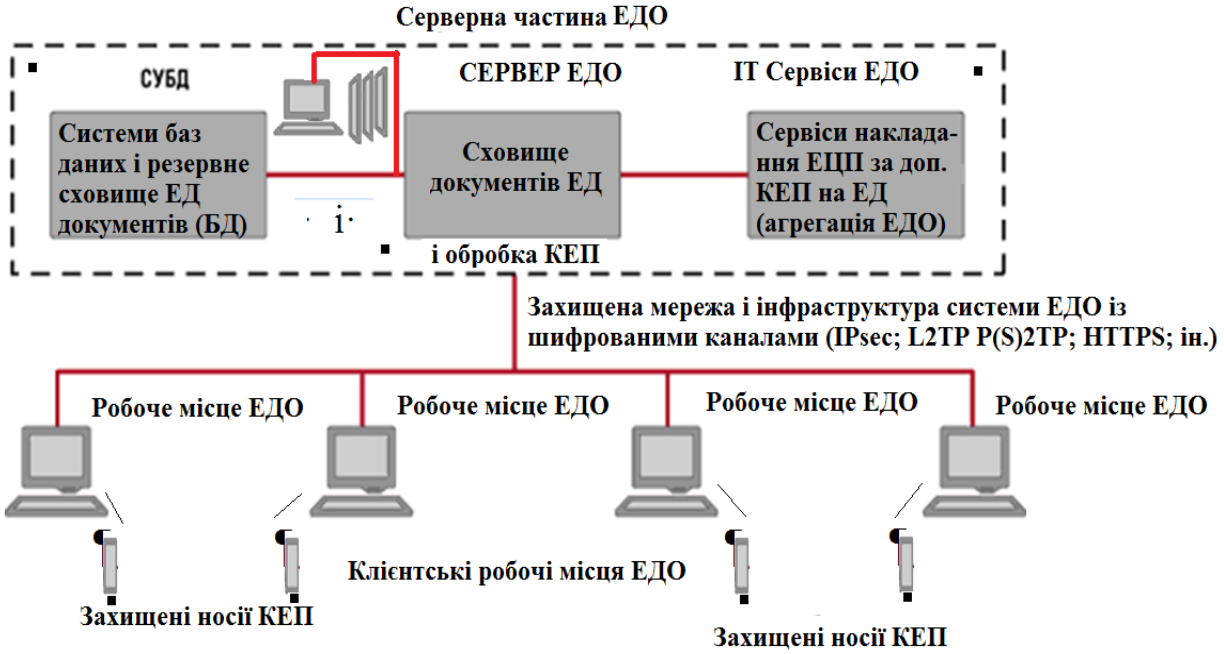
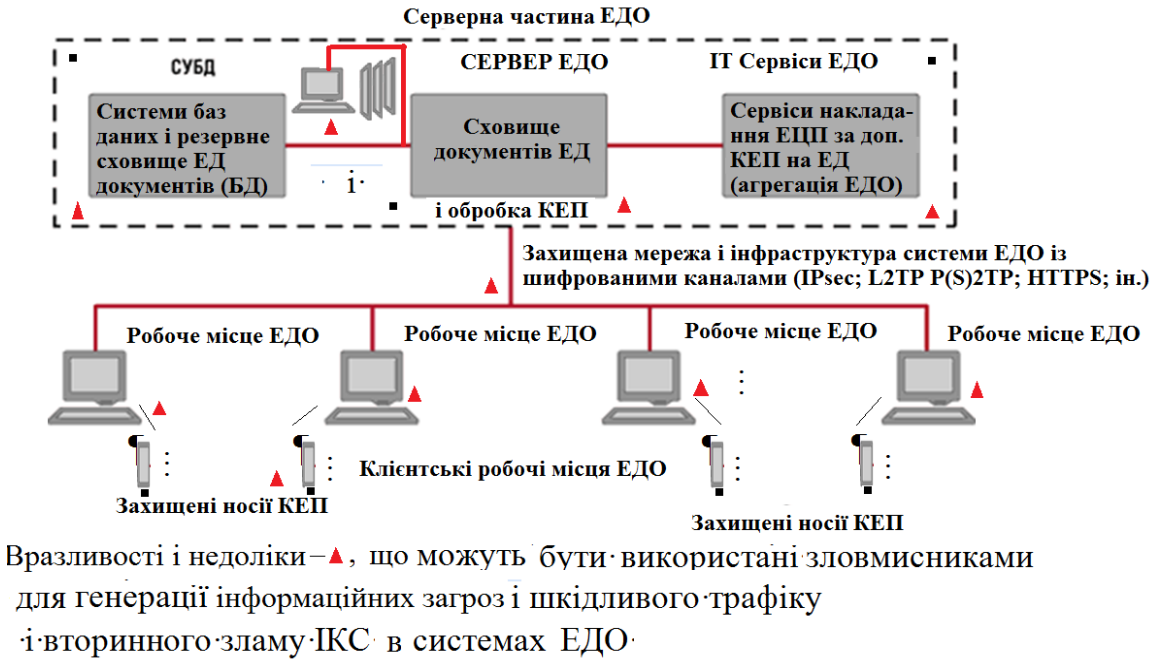


Рисунок 3.1. – Структура ЕДО, яка інтегрована в інфрастукруту підприємства

Також , відповідно до проведеного аналізу загроз для систем ЕДО, в ході аналізу виявлено, шо можуть бути використані недосконалості і існуючі вразливості в системах ЕДО, які можуть в подальшому бути експлуатовані(рис.3.2).



Вразливості і недоліки, що можуть бути використані зловмисниками для генерації інформаційних загроз і шкідливого трафіку і вторинного зламу ІКС в системах ЕДО

Рисунок 3.2. – Структура ЕДО, яка вміщує в себе вразливості і недосконалдості

Окремим місцем є інформаційні мережі і інфраструктура систем ЕДО, яка потребує окремої уваги з точки зори інформаційної безпеки самої ЕДО, так як вона може бути джерелом загроз і втрат інформації. Структура інформаційної мережі ЕДО показана на рис. 3.3а та рис.3.3б.

Рисунок 3.3 – Узагальнена схема руху електронних документів в мережі ЕДО врамках інфраструктури підприємства

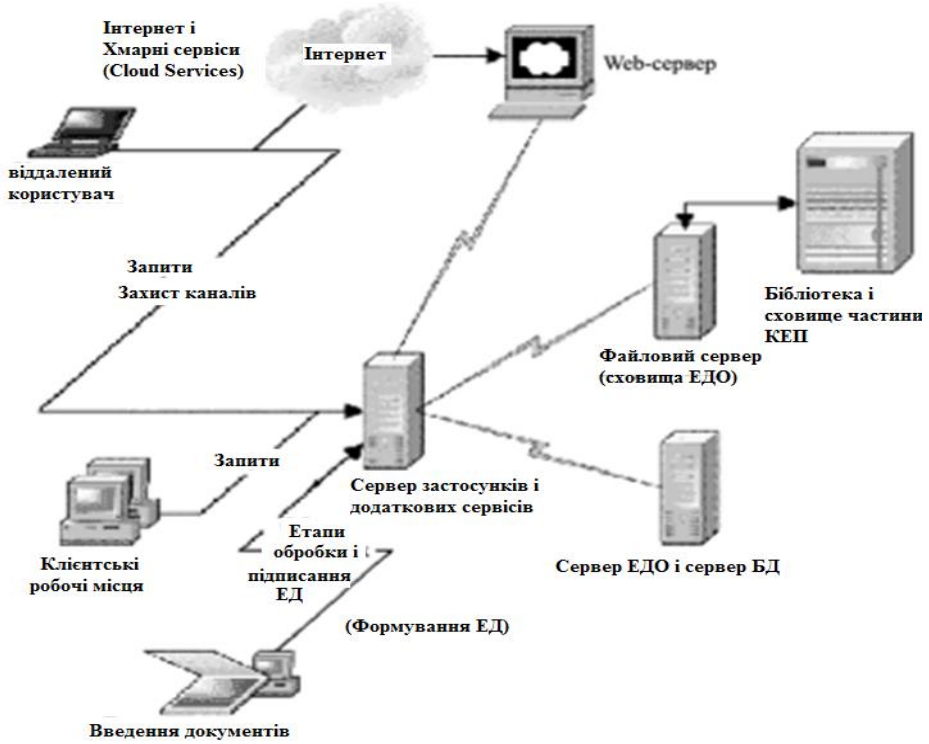


Рисунок 3.4 – Структура інформаційної мережі ЕДО із базовим захистом

Базова структура передбачає базовий захист, але його часто недостатньо для повноцінного захисту і це потребує ретельного вивчення і застосування нових підходів захисту і в тому числі комплексних підходів на різних ділянках і вузлах ЕДО із використанням комплексної системи захисту інформації (КЗСІ).

3.2 Аналіз вразливостей і джерел загроз для систем ЕДО

Існують різні уразливості, які можуть впливати на інформаційні системи документообігу. Деякі з найпоширеніших уразливостей включають :

1) недостатня автентифікація та контроль доступу: Слабкі методи аутентифікації, використання слабких паролів, недостатній контроль доступу до системи можуть дозволити несанкціонований доступ до ЕД та можливість їх змін.

2) незахищений обмін даними: Відсутність шифрування під час передачі документів між користувачами може призвести до перехоплення ЕД.

3) вразливості програмного забезпечення: Помилки у програмному забезпеченні, недостатнє оновлення та патчі можуть створювати ризики і загрози.

4) соціальний інжиніринг: Зловмисники можуть використовувати соціальний інжиніринг, щоб ввести в оману користувачів та отримати доступ до ЕДО .

5) втрати даних в каналах (MiTM) і вузлах (MiTN) : Погрози включають випадкове або навмисне видалення даних, втрату даних через атаки чи проблеми.

6) фізичний доступ до обладнання і технології КЕП в складі ЕДО: Несанкціонований фізичний доступ до серверів, комп'ютерів або іншого обладнання.

7) спам та фішинг: Атаки електронною поштою, спамові повідомлення та фішингові атаки на користувачів системи ЕДО з метою отримання несанкц. доступу.

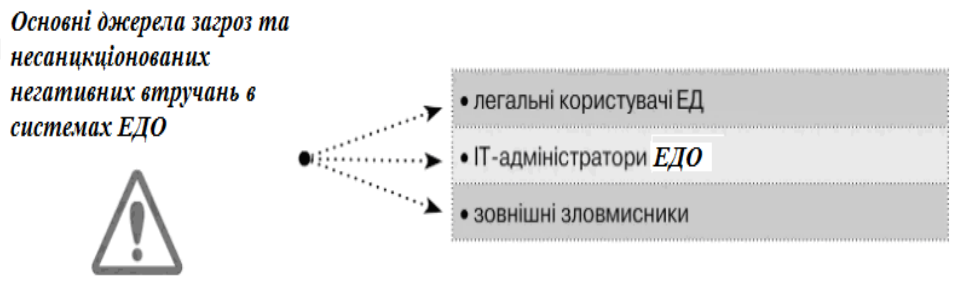


Рисунок 3.5 – Джерела загроз для основних вразливостей ЕДО

Ці уразливості потребують систематичного аналізу та оперативного реагування і закриття.

3.3 Аналіз вразливостей інформаційних систем, пов'язаних з електронним документообігом

Одним із надзвичайно важливих аспектів є регламентація електронного документообігу. Базові резюмуючі висновки по аналізу часитини вразливостей ЕДО (рис.3.5):

– базовий захист в існуючих ЕДО є недостатнім для високого рівня ІБ;

– окремі вузлу і місця ЕДО є більш вразливими до зовнішніх атак і впливів;

– потрібні нові і додаткові методи і заходи захисту для високорівневого комплексного і стабільного захисту даних в сучасних ЕДО (рис.3.6) ;

– потрібна запровадження нових засобів і заходів захисту інформації ЕДО.

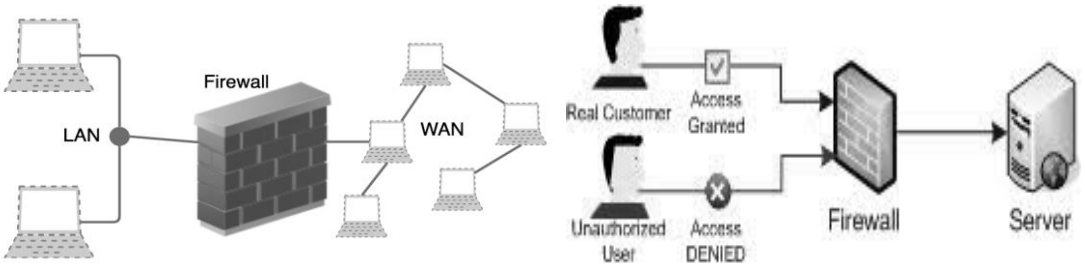


Рисунок 3.6 – Основні проблеми і загрози інформаційних втручань у мережі ЕДО

Сучасні прилади і компоненти (програмні і апаратні) ЕДО досить широко охоплюють всі сфери сучасного життя від побутових систем ЕДО до персональних ЕЦП і корпоративних систем ЕДО для використання професійних промислових функцій. Розвиток мережі Інтернет сприяє розвитку засобів ЕДО, які являють собою сукупність пристроїв і ПЗ, як персональних пристроїв користувачів так і програмних систем для захисту електронних лрокументів і інформації користувача, а також окремих вузлів і пристроїв із використанням Інтернет - каналів і інтерфейсів. Сучасні системи ЕДО є високоінтелектуальними ІС і містять засоби захисту і тракти зв’язку із іншими окремими ІС системами або програмами в їх складі. У сучасних ЕДО комплексна інформаційна безпека і ризики – значна проблема для даних ЕД.

Із зростанням популярності технології ЕЦП і суміжних систем ЕДО, а також портативних мобільних пристроїв і смарт-пристроїв користувачів, і суміжних сервісів зростає й інтенсивність інформаційних загроз.

Тренди сучасних років говорять, що основними хакерськими загрозами у системах каналах ЕДО є:

– перехоплення і спотворення інформації в каналах і інтерфейсах ЕДО, MITM-атаки і інформаційні впливи в ЕДо і ЕД;

– включення шкідливих ПЗ модулів і вірусів в ЕДО, а також хакерських даних іх модифікацією основного ПЗ і втратою функцій ЕДО і перехопленого потоків даних в каналах ЕДО та/або перехоплення ЕД;

– хакерські загрози і різного роду атаки із підміною технічних паркаметрів каналів і підміною самої інформації та інше;

– Втручання в потоки ядра ПЗ ЕДО і операційних систем ЕДО;

– Втрата управління ЕДО і втрата ЕД (витоки даних) в ЕДО через канали зв’язку і через спеціальніс або неуважні дії адміністраторів чи користувачів ЕДО;

– інформаційні загрози для пограничних пристроїв ЕДО;

– прямі та не прямі хакерські атаки і втручання в інформаційні процеси ЕДО в ЕД через вторинні і сторонні потоки і інтерфейси зв’язку ;

– перехоплення керування та/або спотворення даних ЕД в ЕДО і в каналах;

– модифіковане і неоригінальне програмне забезпечення ЕДО;

– шкідливі посилання, фішинг і соціальні атаки на користувачів і співробітників систем ЕДО: соціальна інженерія та припрацювання співробітників ;

– ризики фальсифікації підпису та порушення процесів передачі ЕД в ЕДО.

3.4 Створення нового методу і моделі більш захищеного обміну інформацією і ЕД в системах ЕДО

Основні засади і тезими фундаменту запропонованих підходів при розробці методу і моделі підвищеного інформаційного захисту :

– використання 2-ї сигнатури на кожному важливому ЕД за другим КЕП;

– використання контролю Геш – функцій (Hash-функцій) електронних документів (ЕД) на кожному етапі їх проходження в системі ЕДО (на базі різних алгоритмів обчислення Геш-функцій : Hash-функцій – Схема: $\mathbf{A} -_{\mathbf{Hash}} \mathbf{B} -_{\mathbf{Hash}} \mathbf{C}$;

– використання шифрування в каналах передачі різними протоколами *(.SP);

– використання авторизації доступу для особливо важливих ЕД за паролем доступу і їх відкриття – використання технології архівування;

– використання регулярних бекапів ЕД на різних розподілених сховищах;

– використання поліпшеного і захищеного сховища КЕП – флешок із біометрією ;

– використання шифрування і доступу і захисту файлових систем ПК/серверів на розподілених джерелах ЕКП ЦЕП (КЕП) в складі ЕДО;

– контроль дата процесів і дата –потоків (Data-flows);

– виконанн політик кібергігієни і комплексного захисту даних;

– використання систем моніторингу процесів SIEM в ЕДО і КСЗІ;

– використання підходу «диференційованого рівня захисту ЕДО»: - тобто для документів і інформації, яка має вищий рівень цінності і секретності – запроваджуються більш високо рівневі заходи захисту, і навпаки – для інформації, яка має менший ступінь захисту – запроводжується менш високо рівневі заходи ІБ:

$$/ \text{Esec Level} = ki \times Pi \times IDLi \ / . \qquad (3.1)$$

де k – коефіцієнт пропорційності захисту; Esec Level – загальний рівень захисту ланки системи ЕДО; Pi – питома вартість реалізації і впровадження заходів і засобів захисту і –ї ланки системи ЕДО; IDLi – питомий рівень інформаційної захищеності при впровадженні заходів і засобів захисту і –ї ланки системи ЕДО;

Основна ідея і раціональне правило : вартість захисту ланки системи ЕДО повинна бути меншою за вартість її основного функціоналу Pi MAIN FUNC , тобто характерне правило Pi < Pi MAIN FUNC і/та вартість захисту ланки системи ЕДО повинна бути співмірною повинна із вартістю її основного функціоналу Pi ≈ Pi MAIN FUNC

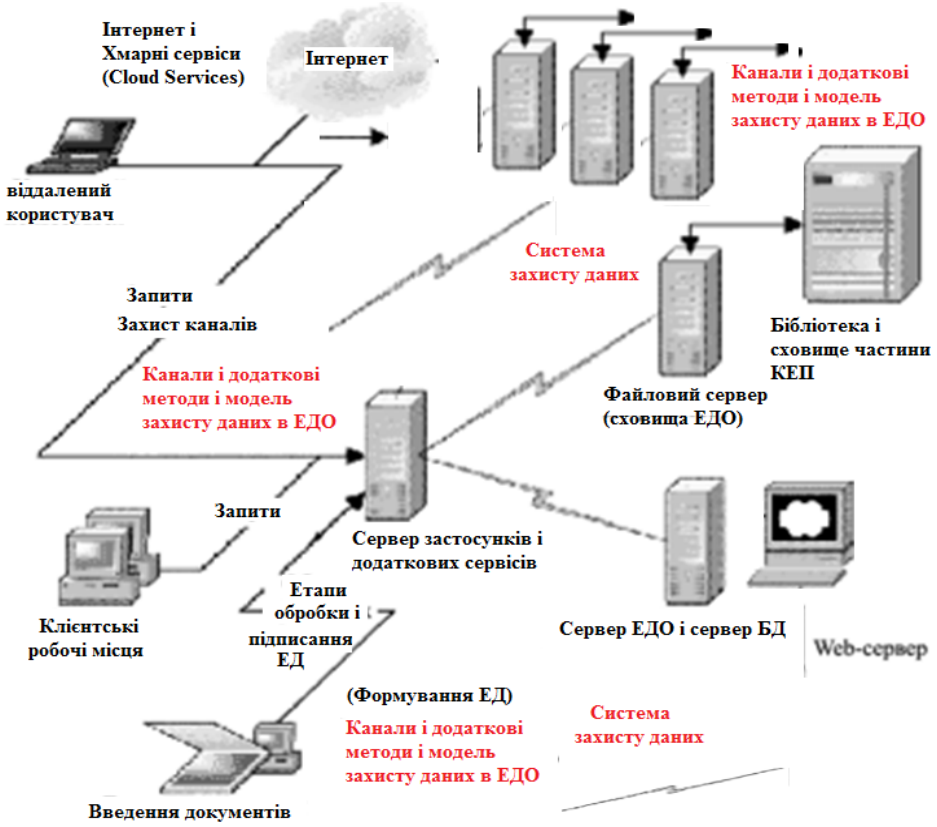


Рисунок 3.7 – Структура ІМ ЕДО із підвищеним захистом і підходами додаткового захисту

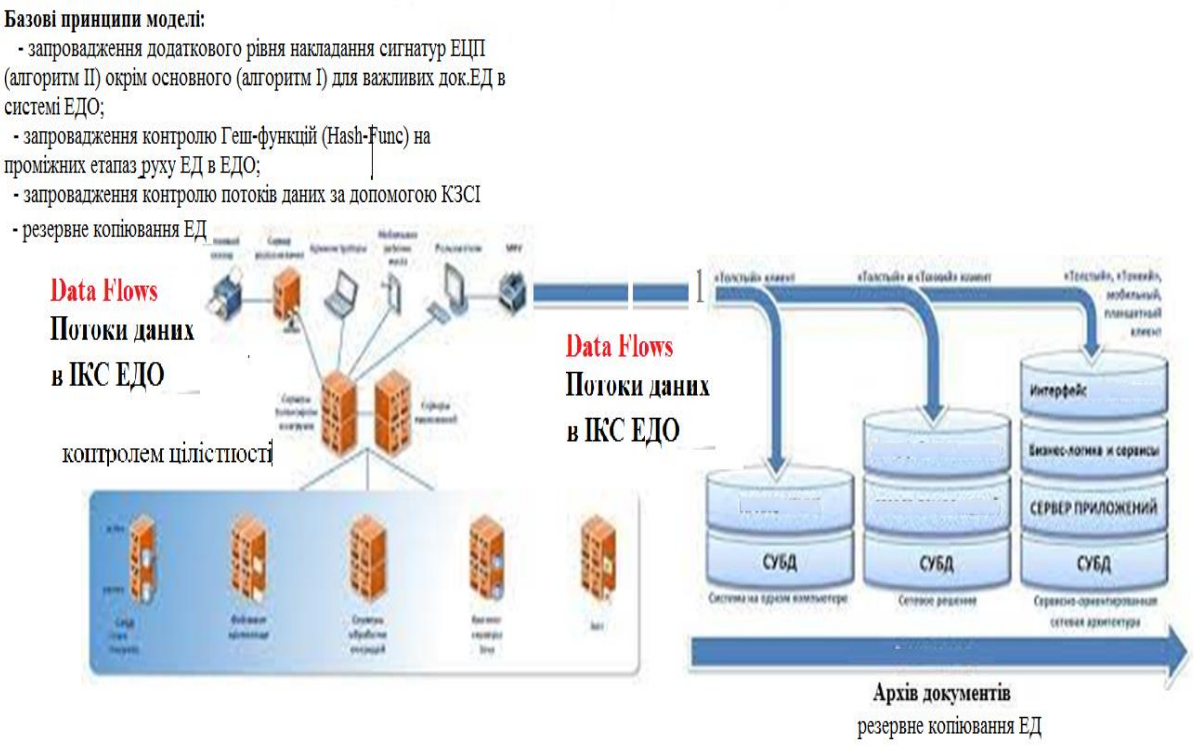


Рисунок 3.8 – Узагальнена схема і засади методу і моделі покращення захисту даних в ЕДО організації із використанням захищених ІМ для ЕДО

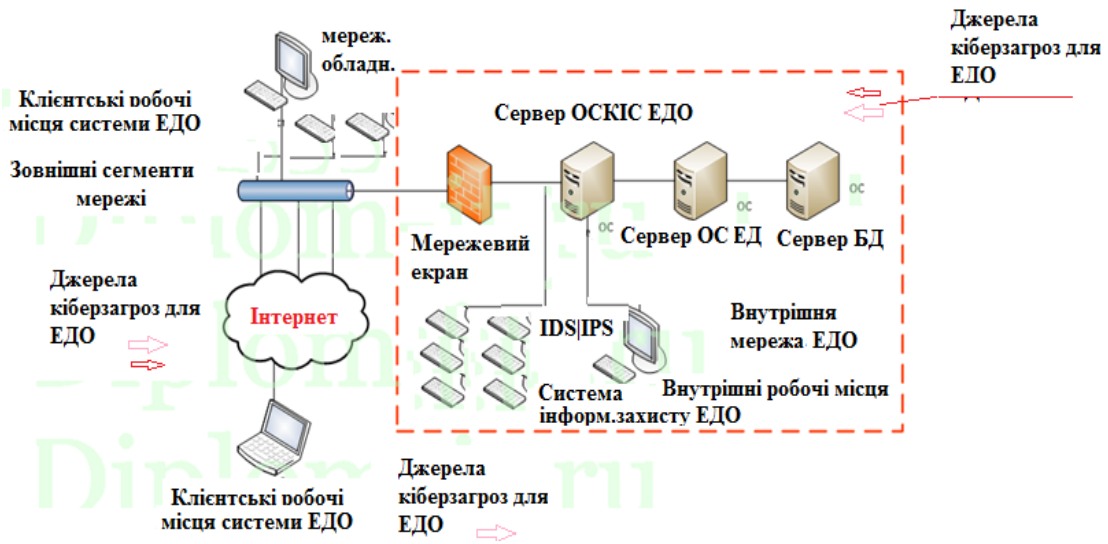


Рисунок 3.9 – Структура захищеної інформаційної мережі ЕДО із підвищеним рівнем захисту і підходами додаткової ІБ із контролем цілістності

Для забезпечення безпечного документообігу і передачі і електронного підпису ЦЕП (КЕП) (рис.3.6 – рис.3.9)даних ЕД в системах ЕДО в безпечних умовах, із контролем їх цілісності і додатковим рівнем ІБ, як показано на структурі (Рис. 3.10).

Так, принцип додаткового захисту полягає :

– відправник із безпечністю отримує завізований і захищений ЕД;

– в процесі підписання адресати отримують повідомлення з проміжними статусами документів: доставлено, погоджено чи відхилено із мітками часу і погоджено та підписано одним або двома ЕЦП (в залежності від необхідного рівня захисту документа);

– дані передаються в захищених каналах ІМ в захищеній мережі ЕДО;

– здійснюється контроль цілісності за допомогою механізму Геш-функції.

На рисунку 3.10 показано схему руху документів в захищеному режимі.

Покращена схема накладання ЕЦП за допомогою накладання 2-го КЕП на електронні документи і проміжного контролю ілістності (порівняно із відомою схемою : рис.1.5 , див. розділ 1), яка враховує накладання другого КЕП (Алгоритм II) і проміжного контролю цілісності на проміжних етепах передачі документа, який є і формує додатковий рівень захисту для більш важливих ЕД, який показана на рис. 3.11 .

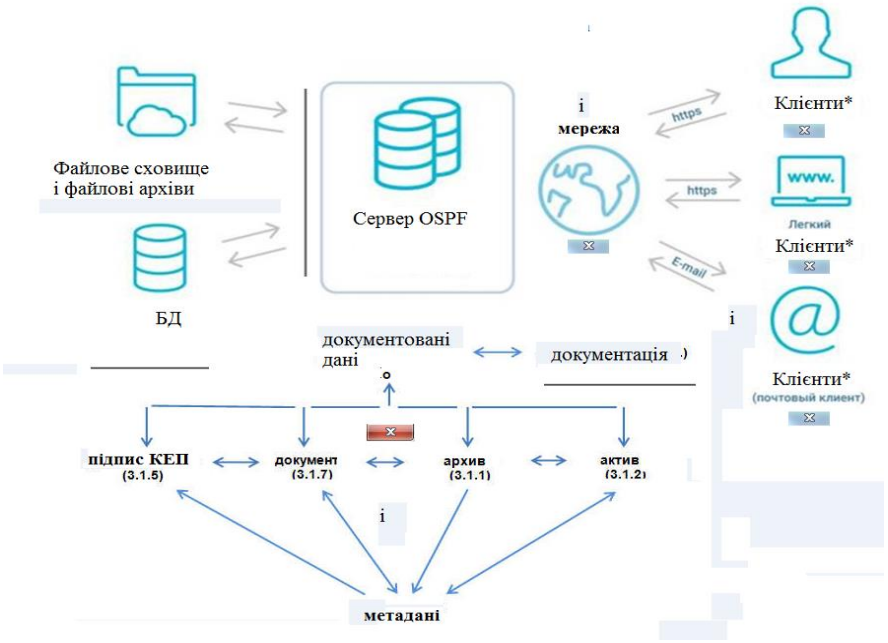


Рисунок 3.10 – Схема руху ЕД в схемі ЕДО

Рисунок 3.11 – Схема руху підписаного ЕД в схемі ЕДО за допомогою КЕП

Зазвичай спеціалісти і користувачі ЕДО: керівники та юристи найчастіше підписують електронні документи 1-м КЕП. При великому обсязі документообігу організація отримує інструкцію щодо ведення електронного документообігу (ЕДО) та встановлює порядок використання електронного підпису (ЕП). Для білтш важливих документів може бути паралельно використаний КЕП 2 за допомогою алгоритма 2. Таким, чином кожен співробітник компанії і користовуач ЕДО може на свій васний розсуд. Адо керуабчисб нормативами сам вазначати ступінь важливості документа і приймати рішення про накладання додаткового КЕП (КЕП 2) (рис.3.11 – рис.3.12)– для додаткового рівня захисту системи ЕДО системи отримати свої власні електронні ключі

згідно з цією інструкцією. Тепер давайте розберемося, що таке 2-й електронний підпис (ЕП2 чи КЕП 2), та яким чином підписуються документи електронним підписом алгоритмом 2 (КЕП 2).

Рисунок 3.12 – Схема підписання і руху ЕД за допомогою додаткового рівня захисту (КЕП I + КЕП II і з контролем Геш-функцій файлу)в загальній схемі ЕДО

Електронний підпис ЦЕП КЕП 2, який пропонується використати як однин із варіантів додаткового захисту , відомий як КЕП 2 (кваліфікований електронний підпис II) для більш важливих документів, складається з 2-го секретного (і особистого) ключа та 2-о сертифіката відкритого ключа, які використовуються тільки як 2-га пара. Секретний ключ КЕП 2 генерується аналогічно як і КЕП 1, але за другим алгоритмом як унікальна послідовність випадкових символів, а сертифікат 2 відкритого ключа 2 обчислюється на основі секретного ключа 2, але для вищої криптостійкості обчислюється за допомогою 2-го іншого алготритму. Зауважте, що неможливо отримати секретний ключ із самого сертифікату, як при використанні КЕП1 (традиційний захист) так і з використанням додаткового КЕП 2 (додатковий захист), так і із їх комбінативним поєднанням. Сертифікат відкритого ключа 1 і відкритого ключа 2 (рис.3.11 та рис.3.12)містить персональну інформацію власника (наприклад, ім'я, унікальний реєстраційний номер, видавця сертифіката та термін його дії) і підписується секретними ключемами 1 та 2 Центру сертифікації ключів за різними алгоритмами 1 та 2. Ці сертифікати можуть бути опублікований на веб-сайті Центру сертифікації ключів. ід час підписування електронного документа за допомогою КЕП I та КЕП II його вміст не змінюється. Замість цього додаються блоки даних, які є електронними підписами (основним та додатковими). Процес отримання цього блоку складається із декількох етапів, показаних на рис.3.12. При

модифікації ЕД зміниться його цифровий відбиток(signature), і тоді документ непройде перевірку електронного цифрового підпису(ЕЦП). Таким чином, цифровий відбиток (ЦВ) захищає документ від змінтретіми особами після накладання КЕП, а шифрування секретним ключем підтверджує авторство документу.

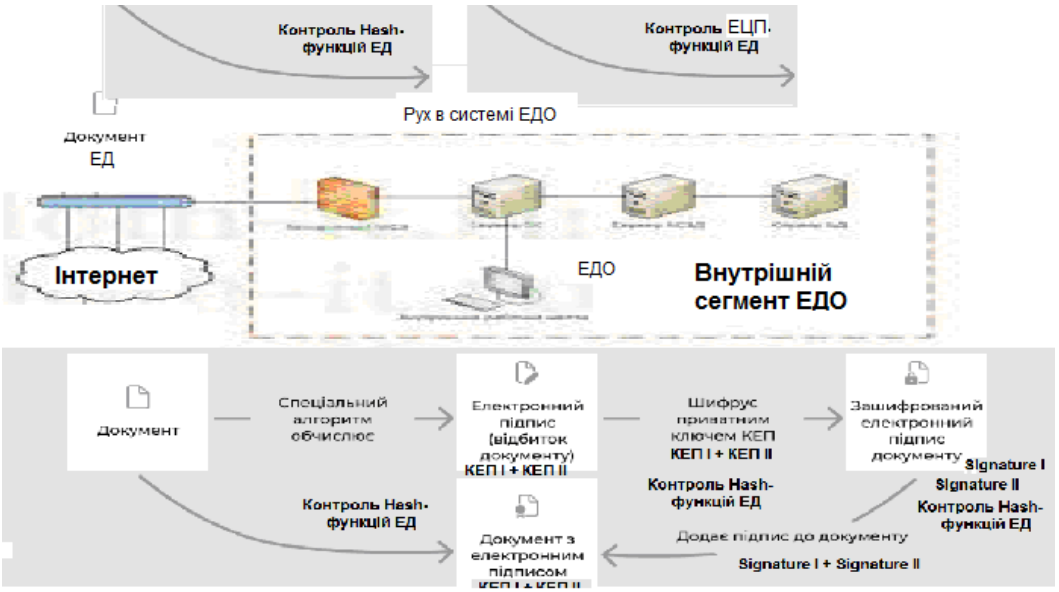


Рисунок 3.13 – Процес руху і контролю ЕД в структурі ті ІСК системи ЕДО із додатковим захистом даних на проміжних вузлах і точках

Цифровий Геш (Геш-функція) дозволяє контролювати цілісність дани на етапах проходження системи в ЕДО між її вузлами. Тобто, якщо цілісність змінилась – документ пошкодився або є інформаційні втручання в нього (допис іншої частини, спроба доступу, спроба запису вірусу, або додаткової частини та інше..) . Геш-функція (Hash-Functipon) – є індикатором цілістності і безпечності документа на шляху його руху в системах ЕДО.

Розшифрувати електронний цифровий підпис (ЕЦП: КЕП I та КЕП II)та одержати початковий відбиток, що відповідатиме документу, можна тільки за допомогою сертифікатів (I та II) відкритого ключа автора. Перевірка ЕП отриманого документа проводиться кількома етапами: 1.

Досить серьозну небезпеку створюють документи, яку можу тьпроходити скомпрометований вузол мережі ЕДО, в якому файл ЕД може бути заражений вірусмо чи пошкоджений. Що становить ризики для всієї системи ЕДО. Це

становить серйозну загрозу для організацій і фізичних осіб, які експлуатують технології ЕДО, оскільки неправильне або недостатній рівень захисту інформації ЕД в ЕДО може призвести до витоку конфіденційних даних, порушення їх цілісності та доступності, порушення безпеки всієї ЕДО та інших її вузлів, а також фальсифікації.

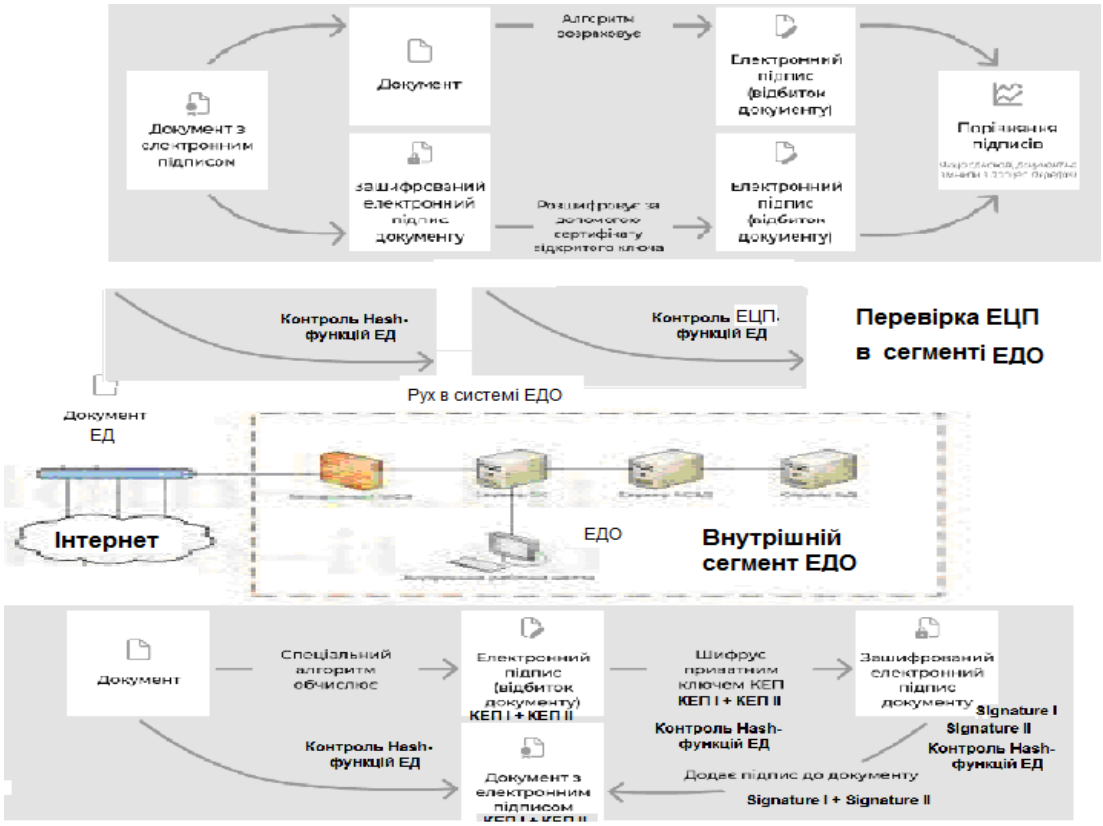


Рисунок 3.14 – Схема руху і контролю і перевірки підписання ЕД в схемі ЕДО

Отримувач більш захищеного ЕД із додатковим рівнем захисту визначає унікальний цифровий відбиток (КЕП I + КЕП II: signature S I + signature S II) одержаного документу за допомогою спеціальних алгоритмів 1 і 2;

Розшифровує електронний підпис документа (signature I+II) та одержує відбиток ЕД. Порівнює відбитки документу та розшифрованого ЕЦП, якщо вони однакові – це означає, що документ не модифікувався в процесі передачі.

3.5.Модель і метод додаткового захисту систем документообігу

На основі аналізу був розроблений і систематизований основний метод і модель додаткового інформаційного захисту системи електронного документообігу. Цей метод і модель полягає у наступному :

– використання 1-ї та 2-ї сигнаткрКЕП I + КЕП II на кожному важливому документі за других ключем і алгоритмом шифрування;

– використання контролю Геш – функцій (Hash-функцій) електронних документів на кожному проміжному етапі [j ….. j+1] їх проходження в системі ЕДО (на базі різних алгоритмів обчислення Геш-функцій) : Hash-функцій (MD5, CRS32 інш.);

– використання AES/DES шифрування даних при передачі в каналах ЕДО передачі за допомогою різних протоколів *(IPSec; L2TP; S2TP; HTTPS; Kerberos);

– використання авторизації доступу для особливо важливих документів за паролем доступу і їх відкриття – використанрня технології архівування;

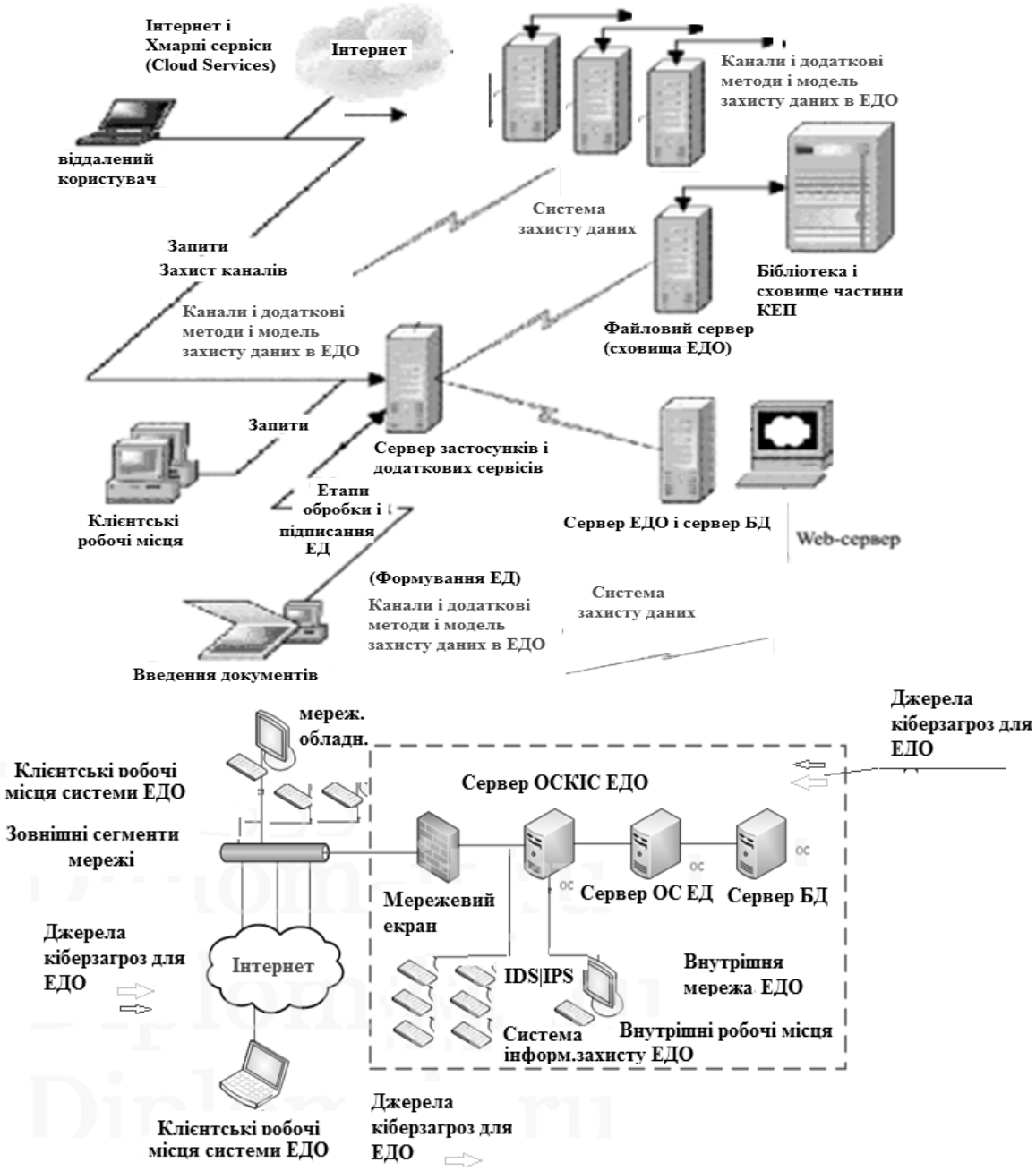


Рисунок 3.15 – Модель ІМ системи ЕДО із додатковим захистом ІМ

– використання регулярних бекапів (BackUp) ЕД на різних носіях;

– використання більш захищеного сховища КЕП – флешок із біометрією;

– використання шифрування і доступу і захисту файлових систем ПК/серверів на розподілених джерелах ЕКП -ЕЦП (ЕЦП КЕП+) в складі ЕДО;

– контроль дата-процесів і дата –потоків (Data-flows) в системі ЕДО;

– виконання політик кібергігієни даних і КЗСІ ІС в ЕДО;.

– використання систем моніторингу процесів і потоків даних за допомогою SIEM в ЕДО і КСЗІ (Комплексних систем захисту інформації);

– використання підходу «диференційованого рівня захисту ЕДО»: - тобто для ЕД, із вищим рівнем цінності і секретності – запроваджуються більш високорівневі заходи захисту, і навпаки – для ЕД із меншим ступенем цінності – менший захист. (див. формулу (3.1)).

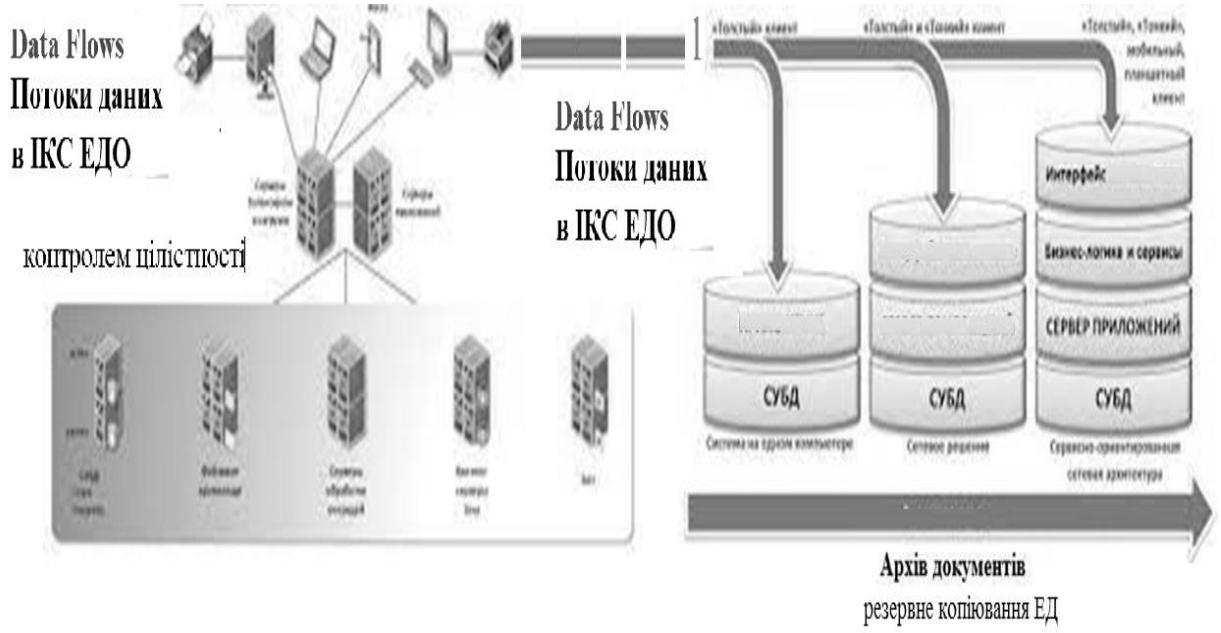
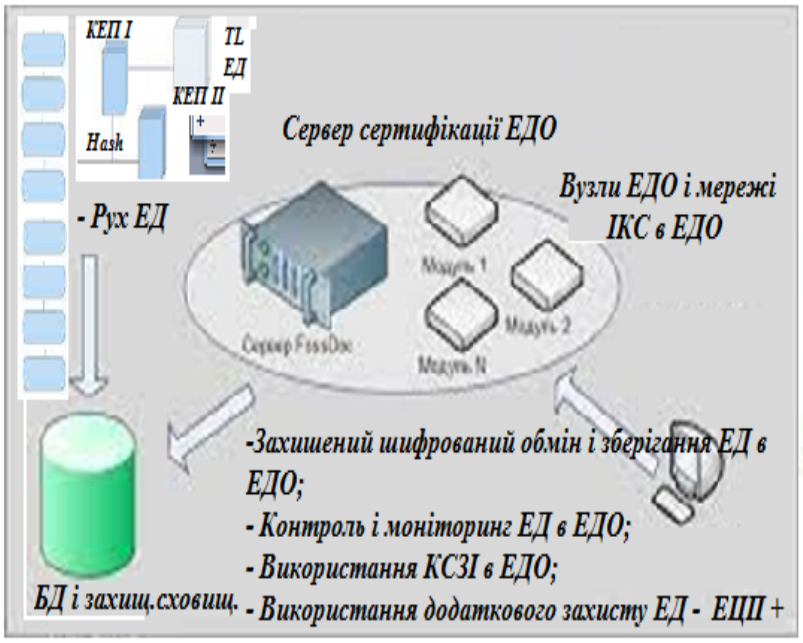


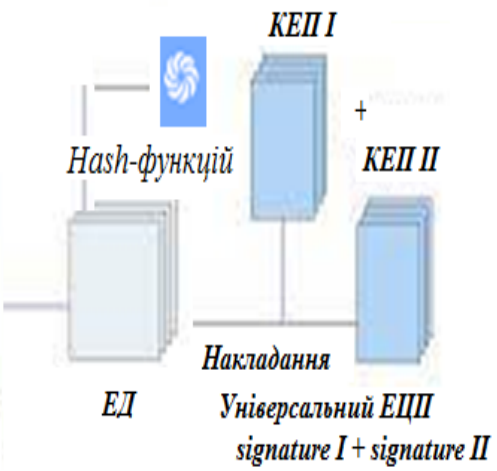
Рисунок 3.16 – Модель і мережа комплексного інформаційного захисту ЕДО

Модель комплексного інформаційного захисту ЕДО (рис.3.16 –рис. 3.17)на базі окремих структур і комплексних підходів передбачає використанн покращених структур захищеної інформаційної мережі ЕДО із підвищеним рівнем захисту і запровадженням підходів і методів додаткового захисту із контролем цілісності.

- *використання 1-ї та 2-ї сигнаткрКЕП I + КЕП II на кожному важливому документі за других ключем і алгоритмом шифрування;*

- *використання контролю Геш – функцій (Hash-функцій) електронних документів на кожному проміжному етапі [j ..... j+1] їх проходження в системі ЕДО (на базі різних алгоритмів обчислення Геш-функцій) : Hash-функцій (MD5, MD 4 SRS32 інш.);*





- *використання AES/DES шифрування даних при передачі в каналах ЕДО передачі за допомогою різних протоколів *(IPSec; L2TP; S2TP; HTTPS; Kerberos);*
- *використання авторизації доступу для особливо важливих документів за паролем доступу і їх відкриття – використанрня технології архівування;*
- *використання регулярних бекапів (BackUp) документів на різних розподілених сховищах і носія;*

Рисунок 3.17 – Розроблена модель і метод комплексного інформаційного захисту електронних документів (ЕД) в системі (ЕДО)

Розроблена модель і метод (Рис.3.16, рис.3.17), а також схема захищеної ІМ ЕДО для передачі потоків даних ЕД (рис.3.15) і підписаних документів в системі ЕДО базується на засадах методу і моделі покращеного захисту даних ЕЦП КЕП+. Тенденції останніх років і аналіз кіберзагроз в області ЕДО свідчать, що у 2022-2023 велика частка до 50-70% загроз у системах ЕДО із використанням глобальної мережі Інтернет припадає саме на галузь каналів і передачі даних в ЕДО на базі Інтернет-каналів, 25-44% із якої спрямовано саме на компрометацію і махінацію ЕД і ПЗ ЕДО на IoT користувачів, із підключенням до Інтернет.

4 ОЦІНКИ І ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

4.1. Аналіз уразливостей інформаційних систем, пов'язаних із документообігом

Аналіз вразливостей інформаційних систем ЕДО і систем, пов'язаних із документообігом є важливою складовою безпеки даних в організації. Традиційна модель ІКС ЕДО включає обробку, передачу та зберігання документів інформаційної системи. Існує кілька типових вразливостей, які можуть виникати в цьому контексті. Ось деякі з них:

1. Недостатня фізична безпека інформаційної системи ЕДО: Якщо фізичний доступ до пристроїв, серверів або документів не обмежений, це може призвести до несанкціонованого доступу до конфіденційної інформації.

2. Слабка аутентифікація та авторизація систем ЕДО: Якщо система не вимагає достатньо міцного пароля або не забезпечує правильну авторизацію та контроль доступу до документів, хакер може отримати доступ.

3. Недостатнє шифрування і захист ЕД за допомогою ЕЦП , а також в каналах і на кінцевих точках: Якщо документи не зашифровані на високому рівні, то під час передачі або зберігання, вони можуть стати легкою мішенню.

4. Вразливості програмного забезпечення та інформаційних систем і мереж: Застосунки і ПЗ ІКС ЕДО, можуть мати вразливості, які можуть бути використані для несанкціонованого доступу або атаки на ІС ЕДО.

5. Соціальний інжиніринг і фішинг: Зловмисники можуть використовувати методи соціального інжинірингу для отримання доступу до конфіденційної інформації, шляхом маніпулювання користувачами системи.

6. Інсайдерські загрози. Вплив ненадійних і скомпрометованих співробіткинів на систему ЕДО ззовні.

Для аналізу уразливостей інформаційної системи едо та забезпечення заходів захисту системи ЕДО, пов'язаної з документообігом, рекомендується проводити такі кроки:

1. Тестування на проникнення систем ЕДО;
2. Регулярне оновлення і моніторинг систем і ІКС ЕДО;
3. Регулярне оновлення ключів КЕП;
4. Вибір та надійна зберігання паролів та даних авторизації в ЕДО;
5. Надійне зберігання ключів КЕП на надійних фізичних носіях (бажано із біометричною ідент.по відбитку пальця.(Такі Flash- є наявні на ринку);
6. Регулярний перегляд і дотримання правил політики кібергігієни поводженя із електронним ключем КЕП;
7. Робота в тестових режимах для тестування безпеки систем ЕДО;
8. Використання комплексних засобів інформаційного захисту ЕДО і правил кіберогігієни і кібербезпеки при роботі із інформацією ЕДО.

4.2 Дослідження проблем інформаційної безпеки систем ЕДО

Проведений аналіз показав, що серед основних проблем електронного документообігу і проблем суміжних систем, пов'язаних із ЕДО є такі:

1. Відповідність електронного документообігу застосованим комп'ютерним технологіям: У багатьох випадках перехід до ЕДО відбувається без врахування особливостей обліку підприємства та використаних ІКС.

Рішення: Проведення аналізу поточного документообігу та розробка проекту створення та впровадження електронного документообігу, який враховуватиме особливості обліку підприємства та структуру бухгалтерської комп'ютерної системи.

2. Оптичне введення документів з паперового носія та обробка графічної інформації: Автоматизоване перетворення паперових первинних документів можливе лише за допомогою сканувального обладнання (сканеру). Хоча процес сканування є швидким, подальша обробка електронного графічного файлу в дані, які можуть бути оброблені комп'ютерним ПЗ, займає багато часу та потребує значних зусиль.

Рішення: Розумним рішенням є використання потужних програм для обробки відсканованих документів. Розробка уніфікованих форм документів, які легко піддаються обробці після сканування. Заповнення документів друкованими літерами з метою швидкого їх розпізнавання програмою.

3. Контроль за правами доступу та захист електронного документа і його реквізитів: Опис: Користувачі бухгалтерської ІКС можуть мати доступ до ЕД, до якої вони не мають прав доступу. Під час зберігання електронного документа виникає ризик його пошкодження або зміни.

Рішення: Необхідно розрізняти доступ до інформації для відповідних користувачів ЕДО за допомогою різних засобів контролю доступу. Захист електронного документа повинен бути забезпечений різними апаратними та програмними засобами, зокрема методом і моделлю комплексного захисту.

4.3 Оцінка інформаційної безпеки ЕДО і ПЗ ЕДО

Оцінка інформаційної безпеки є одним з найважливіших аспектів загальної економічної безпеки підприємств, організацій і державних структур. Вона використовується для оцінки рівня захищеності бізнес-середовища організації. Захист інформації ЕДО є спеціалізованим напрямком діяльності, спрямованим на запобігання витоку даних ЕД

Метод оцінки ризиків повинен дозволяти власникові інформаційної системи ефективно оцінити застосовність та ефективність методу з необхідним рівнем точності. Математична модель оцінки інформаційної безпеки повинна враховувати велику кількість ризикових факторів і дозволяти створювати ефективні числові алгоритми обробки інформації. Існують методи оцінки ризиків інформаційної безпеки, які дозволяють оцінити можливі загрози, які можуть призвести до відмов або зменшення функціональності інформаційної системи. До найпоширеніших методів оцінки ризиків належать:

1) Методика оцінки ризиків, яка базується на моделі загроз та вразливостей.

2) Методика оцінки ризиків, яка базується на створенні моделі загроз ЕД.

Перший метод використовує головним чином статистичні та експертні дані про кіберзагрози та вразливості. Для оцінки ризиків у інформаційній системі підприємства спеціалісти спочатку встановлюють рівень захищеності кожного важливого ресурсу шляхом оцінки ймовірності реалізації кіберзагроз, які можуть впливати на ці ресурси компанії. Оскільки ризики інформаційної безпеки пов'язані з використанням сучасних інформаційних технологій, які визначають ефективність професійної діяльності компанії в інноваційному аспекті, вони відносяться до категорії "інноваційному аспекті (Наприклад, із використаттям методів штучного інтелекту Аі або технологій ML чи rapidML). Інноваційні ризики відносяться до категорії ризиків, пов'язаних з інноваційним аспектом впровадження інформаційних загроз. Якщо визначити інноваційні ризики як ймовірність втрати $p_{i\ innov}(t_i)$, через неправильну мету

$$(p_{sum}{}' = Sum_{i=1}^{n}[p_{i\ innov}(t_i)]),\ ' \qquad (4.1)$$

то при оцінці ризиків відмови в працездатності системи оптимальним підходом буде використання параметра і витрат P_i, як загальної вартості і матеріальних витрат, на відновлення функціонування системи і ймовірностей $P_i \cdot p_{i\ innov}(t_i)$, тобто:

$$S' = '\ P_{sum}{}' \cdot\ p_{sum}{}' = Sum_{i=1}^{n}[P_i \cdot p_{i\ innov}(t_i)]. \qquad (4.2)$$

З урахуванням експертних даних про ризики, уразливості та витрати для кожного ресурсу, можна побудувати модель загроз та вразливостей, які є актуальними для інформаційної системи організації. Це дозволить проаналізувати працездатність ІКС ЕДО з точки зору мінімізації ризиків відмови або зменшення працездатності системи.

4.4 Оцінювання ризиків кіберзагроз для інформаційних систем та програмного забезпечення ЕДО і суміжних систем ІКС

Програмне забезпечення ПЗ ЕДО являє собою сукупність програм, призначених для розв’язання завдань на комп’ютері та опрацювання ЕД. Програма ЕДО– це впорядкований набір команд для рішення задач ЕДО. Програмне та апаратне забезпечення ЕДО працюють взаємопов’язано і в неперервній взаємодії. Будь-який апаратний пристрій ЕДО управляється

програмно. Програмне забезпечення ЕДО можна поділити на три класи : системне ПЗ, прикладне ПЗта інструментальне ПЗ ЕДО. Інтеграція програмного забезпечення ЕДО призвела до того, що практично будь-яка програма ЕДО і опрацюванн ЕД має риси кожного класу. Системне програмне забезпечення ЕДО здійснює управління роботою обчислювальної системи і обчислювальним процесом ЕДО. Як правило, системні програми забезпечують взаємодію інших програм з апаратними складовими, організацію інтерфейсу користувача. Сюди відносять операційні системи, сервісні системи ЕДО. Прикладне програмне забезпечення ЕДО призначене для розв’язання прикладних завдань ЕДО фахової діяльності і опрацювання ЕД користувачів системи. Спектр таких програм ЕДО надзвичайно широкий: від одиничних до комплексних індустріальних програмних комплексів ЕДО. Сюди відносять розрахункові, навчаючі, моделюючі програми ЕДО , комп’ютерні модулі ЕДО, тощо. Інструментальне програмне забезпечення ЕДО призначене для розробки всіх видів інформаційно-програмного забезпечення. При цьому під інформаційним забезпеченням розуміють сукупність попередньо підготовлених даних ЕД, необхідних для роботи ПЗ ЕДО. Наприклад, будь-яка сучасна програма ЕДО має вбудовану довідку і опис (документацію)для роботи з ним. Файл довідки ПЗ являє собою програмно-інформаційне забезпечення ЕДО. До інструментального програмного ЕДО забезпечення відносять: редактори (текстові, графічні, музичні), системи табличної обробки даних (табличні процесори), системи управління базами даних, транслятори мов програмування, інтегровані системи діло виробництва, тощо. Кожен користувач ЕДО , перш ніж здійснювати які-небудь дії в комп'ютерній системі ЕДО, повинен ідентифікувати себе для роботи із дозволеними йому ЕД. У свою чергу, система повинна перевірити достовірність особи користувача ЕД, тобто що він є саме тим, за кого себе видає. Стандартним засобом перевірки достовірності є аутентифікація користуачів ЕДО – пароль та логін, а також додаткові засоби, хоча у принципі можуть використовуватися також особисті картки, біометричні пристрої (сканування рогівки ока або відбитків пальців) або їх комбінація, тощо.

4.5 Розрахунок і оцінка стабільності програмного засобу і моделі комплексного захисту даних системи ЕДО

Для оброблення-передавання інформаційних даних із вищим ступенем безпеки було запропоновано використання нових моделі методу покращеного захисту, які ґрунтуються на комплексному підході.

Для цього визначення інтенсивність кіберзагроз для елементів чи вузлів системи ЕДО з урахуванням умов експлуатації і потенційного середовища використання [12]:

$$\lambda_i = n \cdot \lambda_{0i} \cdot K_1 \cdot K_2, \quad (4.3)$$

де λ_{0i} – номінальна інтенсивність відмовлень елементів при кіберзагрозі в вузлі 0i; K_1,K_2 – питомі корекційні коефіцієнти, що впливають на фактор кіберзагроз, в залежності від впливу факторів впливу чи кіберзагрози на той чи інший елемент в залежності від впливу інтенсивності потенційно-небезпечного ПЗ (K_1= 1.1…1,93; K_2 = 1,034..1.036); залежності; n – кількість елементів системи ЕДО.

Визначаємо ймовірність стабільної та беззагрозливої роботи ПЗ системи ІКС ЕДО в плані заданого наробітку часу (0, t_p) [12]:

$$P(t) = e^{-\sum_{i=1}^{n}(\lambda_i \cdot t_p)}, \quad (4.4)$$

де n - число елементів блоків/модулів в складі ПЗ; t_p =100..1000 год. – період часу стабільної роботи. (інколи слід брати t_p=1..24 год для оцінки режиму 24/7)

При цьому інтенсивність відмовлень при інформаційній загрозі в і-му блокові (компоненту) ЕДО того чи іншого програмного продукту ЕДО складе:

$$\Lambda = \sum^{n}\lambda_i = 50.162*10^{-6}\ 1/ч., \quad (4.5)$$

$$P(t) = \exp(-50.162*10^{-6}*500) = 0,982. \quad (4.6)$$

Розраховуємо середній час стабільної роботи (роботи без кібезагрози) в умовах підтримки повного функціоналу :

$$Tср = 1/\Lambda, \quad (4.7)$$

$$Tср = 1/50.162*10^{-6} = 18710. \quad (4.8)$$

$$Tср = 18710 \text{ год (середнє)} \quad (4.9)$$

Визначаємо коефіцієнт готовності до інформаційної загрози/кібератаки:

$$К_Г = ir /(ir +\lambda), \quad (4.10)$$

де ir – інтенсивність збоїв ПЗ компонентів і втрати функціоналу, $ir = 1,6*10^{-3}$.

$$К_Г = 1,6*10^{-3}/(1,6*10^{-3}+50.762*10^{-6}) = 0,979. \quad (4.11)$$

Таблиця 1. – Коефіцієнти загроз для різних системних компонент ЕДО

Найменування *модель базової ЕДО із N-клієнтів із 1сервер БД	**Кіл**.елем., шт. в системі ЕДО	**R_0*10^{-6}, 1/г**	**$К_1 \cdot К_2 \cdot \cdot R_0 \times 10^{-6}$, 1/λ**	**$\lambda_i \times 10^{-6}$, 1/λ**
Модулі ПЗ і апаратури передавання(вузли передеачі і шифрування даних ядро ОС)	5 6	0,32 0,012	0,872 0,109	8.72 0.163
Модулі ПЗ вводу виводу даних, шифрування	5	0,123	1,526	0,526
Модулі ПЗ і рограмні методи і біблікотеки накладання ЕЦП в ЕД в загальній системі ЕДО	4 3	0,523 0,0242	0,436 0,245	0.172 0.22
Інші вузли системи ЕДО і драйвери обладнання	5	0,0522	0.342	0.532
Модулі обробки даних ЕДО і обробки документів	6	0,042	0.0531	0.431

$$P(t) = \exp(-50.162*10^{-6}*500) = 0,982. \quad (4.6)$$

Розраховуємо середній час стабільної роботи (роботи без кібезагрози) в умовах підтримки повного функціоналу :

$$Tср = 1/\Lambda, \quad (4.7)$$

$$Tср = 1/50.162*10^{-6} = 18710. \quad (4.8)$$

$$Tср = 18710 \text{ год (середнє)} \quad (4.9)$$

Визначаємо коефіцієнт готовності до інформаційної загрози/кібератаки:

$$К_Г = ir /(ir +\lambda), \quad (4.10)$$

де ir – інтенсивність збоїв ПЗ компонентів і втрати функціоналу, $ir = 1,6*10^{-3}$.

$$К_Г = 1,6*10^{-3}/(1,6*10^{-3}+50.762*10^{-6}) = 0,979. \quad (4.11)$$

Таким чином, отримані в результаті проведення розрахунків показники стабільності програмного продукту/системи – ймовірність безвідмовної стабільної роботи і середній час стабільної роботи задовольняють необхідним вимогам.

4.6 Підходи і засади стабільної роботи ПЗ компонент ЕДО та оцінка ризиків для систем ЕДО та інших моделів ПЗ суміжних систем

Окремі параметри даних і інформаційних файлів широко використовуються для захисту доступу до ресурсів. Ряд сучасних атак та сучасне ПЗ для взламу можуть використовувати багато методів для розкриття даних користувачів та доступу до внутрішнього ПЗ та отримання несанкціонованого доступу до них із подальшою модифікацією або скачуванням. Особливо в актуальн часи, значно збільшилась ієрархія та еволюція методів та програмних систем як технічного характеру так і соціальної інженерії для отримання закритих даних та інформації із метою і подальшим використанням їх у шахрайських та кіберзлочинних цілях і здійснення злочинів економічного характеру.

Щоб як найкраще захистити дані в ЕДО і підвищити їх стабільність і функціонал, важливо розуміти, що робить надійним ці дані, як їх вміст можна ідентифікувати за допомогою унікального ідентифікатора та відтворити і перевірити в іншій точці (механізм контрольних сум/ Хеш-функцій). Особливість також складає і дані авторизації і забезпечення надійного виконання моделі двофакторнрої авторизації (MultiFactor Authentication MFA чи MFAAA, MultiFactor Authorization, Autoidentification & Acaunting), зокрема створення і надійних облікових записів при доступі до серверної частини ЕДО та ЕЦП і зокрема захисту КЕП і як однієї із складових частин політики безпеки інформаційних систем ЕДО вцілому. Створення надійної контрольної суми (Геш-функції) та паролів є невід‘ємною частиною заходів безпеки сучасних інформаційної системи ЕДО. Надійні ідентифікатори ЕД і надійні дані автонтифвкації мають відповідати вимогам, які перелічені в порядку важливості:

– Мають не змінний унікальний вміст і надійний функіонал ЕДО;

– Значення ідентифікаторів ЕДО, зокрема ідентифікаторів ЕД (signature 1n та signature 2n), а також Геш-функції ЕДО не повинні змінюватись як у точці створення самих інформаційних даних, так і у проміжних ікінцевих точках;

– Алгоритми роботи ЕДО не повинні забирати багато ресурсів ПЕОМ користувача чи сервера та не мати екстремумів функцій завантаженості (90-100%);

– Методи перетворення та порівняння ключ- ідентифікаторів КЕП даних

– не повинні бути складними та займати багато обчислювальних ресурсів ПЕОМ;

– Користувач повинен легко перевірити контрольні суми чи Геш-функцію та ЕЦП ЕД за допомогою КЕП, а також робочих файлів системи ЕДО.

– Ідентифікатори ЕД в системі ЕДО (зокрема електронний цифровий підпис : КЕП I та КЕП II: signature 1n та signature 2n) не повинні бути легко доступні для модулів перевірки функціоналу та повинні бути захищені від інших випливів та доступу. Геш–функції і контрольна суми, а також накладені сигнатури ЕЦП на ЕД мають бути відносно складними як і самі дані із згенерованою на базі них послідовностями додаткових отриманих даних.

Популярність використання надійних даних і мета даних ЕЦП і механізму контрольних сум чи Геш функцій у поєднанні із ЕЦП для перевірки цілісності даних зумовлена тим, що подібна перевірка просто реалізовується у цифровому середовищі і обладнанні ЕДО із підтримкою відповідного ПЗ, легко аналізується і добре підходить для виявлення і усунення загальних помилок і вразливостей ЕДО, слабкої криптостійкості (криптографічного захисту), викликаних наявністю шуму в каналах передачі даних і дір безпеки в інформаційних системах ЕДО.

ВИСНОВКИ

Тема БДР є актуальною і перспективною – інформаційний захист систем електронного документообігу є одним із ключових пріоритетів сучасного діловодства. і інформаційних систем організацій. Переваги запровадження системи ЕДО для ВМР очевидні це – економія часу, ресурсів, оптимізація локументальних-процесів і підвищення комфортності та іміджевості системи електронного документообігу, зменшення бюрократії системи ЕДО. Недоліками і проблематика запровадження системи ЕДО є недостаньо висока інформаційна безпека і конфіденційність даних системи, яка є критичним місцем в окремих моментах і потребує детального розгляду і покращення. Також це – складність і необхідність встановлення додаткових засобів: програмних і апаратних для запровадження системи ЕДО, що несе окремі витрати.

У БДР проведено аналіз сучасного стану розвитку систем електронного документообігу та систем інформаційного захисту від них. Встановлено об’єкт, предмет, завдання та методи роботи, сформульовано мету. В роботі проведено аналіз існуючих проблем інформаійної безпеки електронного документообігу (ЕДО) і передачі електронних документів (ЕД) у них. Визначено недоліки та вразливості систем електронного документообігу (ЕДО) та проведено аналіз інформаційних вразливостей процесу передачі електронного документу (ЕД). Також визначено вразливості і недоліки систем, суміжних із системами ЕДО.

В роботі розглянуто підходи покращення інформаційної безпеки і захищеного передавання електронних документів і даних в системах ЕДО і їх інформаційних мережах. Розглянуто основні чинники впливу і фактори кіберзагроз для ЕДО, які проявляються у каналах зв’язку ЕДО, а також можливості несанкціонованого втручання і зчитування інформації ЕДО.

В результаті досліджень і роботи запропоновано нові модель і метод підвищення інформаційного захисту електронної інформації та електронних документів (ЕД) у систамах ЕДО, які, на відміну від існуючих використовує покращену технологію захисту електронного документа: ЦЕП+ із використанням одночасно 2-х сигнатур ЕЦП, використовує додаткове надійне шифрування даних в

каналах передачі інформації ІМ ЕДО, використовує покращені технології зберігання КЕП із біометрією відбитка пальця і використовує Геш-функції для контролю руху ЕД в системі ЕДО. Також дані модель і метод передбачають покращений захист за допомогою систем КЗСІ в системах передачі документів в ЕДО. Запропоновано модель і технологія інформаційного захисту системи ЕДО має підвищеного захист на базі вдосконаленої методу електронного цифрового підпису – ЦЕП+ і структурного контролю і руху ЕД в захищеній інформаційній мережі.

В роботі проведено оцінки стійкості і виявлено основні загрози систем ЕДО, при контролі передачі і інформаційних даних і захисті їх в системах ЕДО. Розроблено основні засади створення інформаційних систем ЕДО із підвищеним захистом. Була оптимізована структура інформаційної системи ЕДО, зроблені оцінки стабільності їй роботи; визначені основні точки втрати даних і оптимізовано модель захисту системи ЕДО в результаті її функціонування в складі електронних систем;

Було реалізовано архітектуру і структуру захищеної інформаційної мережі ЕДО. Реалізовано окремі програмні модулі для достідження вразливостей і виявлення проблемних місць та інформаційних вразливостей ситем ЕДО. Розроблено програмну реалізацію і програмний код для тестування базових інформаційних функцій безпеки ЕД в ІМ та ІС, що може бути використаний для перевірки і тестування безпеки інформаційних систем ЕДО. Отримані в бакалаврській дипломній роботі результати і програмна реалізація можна використати для підвищення захисту ІМ ЕДО ВМР та тестування інформаційної захищеності і підвищення рівня захисту систем ЕДО із якісним покращенням системи зв’язку. Розроблений програмний продукт дає можливість автоматизувати процеси тестування за короткий проміжок часу.

Переглянуто методів і засобів розробки програмної системи. Обґрунтовано вибір створення програмної системи на базі веб-технологій та побудованої на триланковій архітектурі. Це дозволило покращити гнучкість і зручність системи, як у розробці та обслуговуванні, так і у використанні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

2) Лужецький В. А. Захист персональних даних : навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с. – ISBN 978-966-641-317-1.

3) Dua S., Du X. Data Mining and Machine Learning in Cybersecurity. – NY. : CRC Press, 2011. – 223 p.

4) Chio C., Freeman D. Machine Learning and Security. Protecting Systems with Data and Algorithms. – O'relly, 2018. – 385 p.

5) Малюк А.А. Інформаційна безпека: концептуальні та

6) методологічні засади захисту інформації: Навч. посібник. для вузів – К: Гаряча лінія - Телеком, 2004. – 280 с.

7) Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.

8) Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.

9) Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357 с.

10) Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регу-лювання. – К.: ВД "Гельветика", 2017. – 168 с.

11) Бармен С. Розробка правил інформаційної безпеки: [пер. з англ.] / Скотт Бармен – М. : «Вільямс», 2002. – 208 с. – ISBN: 5-8459-0323-8.

12) Мамаєв М., Технологія захисту інформації в інтернеті: [Спеціальний довідник] / Максим Мамаєв, Сергій Петренко - 2002. – 848 с. – ISBN 5-318-0244-7.

13) Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. – К.: ДУІКТ, 2006. – 126 с.

14) Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

15) Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко. – Луганськ: Ноулідж, 2012. – 480 с.

16) ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998.

17) Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.

18) Закон України «Про інформацію» : за станом на 1 січня 2019 р. / Верховна Рада України. — Офіц. вид. — [Електронний ресурс] http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

19) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : за станом на 1 січня 2019 р. / Верховна Рада України. — Офіц. вид. — [Електронний ресурс] http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0

20) Портал безпека [Електронний ресурс] www.bezpeka.com - Назва з екрану.

21) Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу/Google Академія - [Електронний ресурс] http://scholar.google.com.ua/

22) ISO/IEC, «Information technology — Security techniques-Information security risk management» ISO/IEC FIDIS 27005:2008

23) Kakareka, Almantas (2009). 23. У Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. с. 393. ISBN 978-0-12-374354-1.

24) Биков В.Ю., Лапінський В.В. Методологічні та методичні основи створення і використовування електронних засобів навчального призначення [Електронний ресурс] http://nbuv.gov.ua/UJRN/komp_2012_2_2

25) Алексейчук І.С. Про технологію створення системи тестування / І.С. Алексейчук // Нові технології навчання: Науково-методичний збірник.

26) Кріспін Л. Гнучке тестування: практична інструкція : пер. з англ. / Л. Кріспін., Д. Грегорі – М.: «Вільямс» [Електронний ресурс] http://eprints.cdu.edu.ua/1482/1/testyvan.pdf

27) What is REST? [Електронний ресурс] http://www.restapitutorial.com/lessons/whatisrest.html.

28) Markus Egger — MVVM Survival Guide for Enterprise Architectures in Silverlight and WPF [Електронний ресурс] https://www.packtpub.com/application-development/mvvm-survival-guide enterprisearchitectures-silverlight-and-wpf.

29) Martin Fowler — GUI Architectures. Часть 1 [Електронний ресурс] https://bit.ly/2CvCk1e.

30) Скотт Хокінс. Адміністрування веб-сервера Apache і керівництво по електронній комерції. [Електронний ресурс] https://muff.kiev.ua/files/books/Administririvanie.web-servera.Apache.pdf

31) MySQL. Довідник. MySQL AB. — М: «Вільямс»

32) Тестування програмного забезпечення [Електронний ресурс] https://kiev.lemon.school/uk/blog/osnovy-qa

ДОДАТКИ

Додаток А.
Протокол перевірки
бакалаврської дипломної роботи
на наявність текстових запозичень

Назва роботи: Система захисту електронного документообігу Вінницької міської Ради

Автор роботи: Солончук Олександр Богданович

Тип роботи: бакалаврська дипломна робота .

Підрозділ кафедра захисту інформації ФІТКІ .

Показники звіту подібності Unicheck

Оригінальність – 83,8%. Схожість – 16,2%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Солончук О.Б.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Мудрецов А.В.
(підпис) (прізвище, ініціали)

Додаток Б

Лістинг програми модуля аналізу вразливостей і відкритих ресурсів ЕДО

```
        import java.io.FileInputStream;
        import java.security.KeyStore;
        import java.security.PublicKey;
        import java.security.Signature;
        import java.net.*;
        import java.util.ArrayList;
        import java.util.List;

        public static void main(String[] args) {
        try {

        SignatureVerifier = new SignatureVerifier ();
        ConnectionScanner = ConnectionScanner ();

public class ConnectionScanner {
   public static void main(String[] args) {
      int timeout = 1000; // Таймаут підключення - 1000 мс
      List<Integer> openPorts = new ArrayList<>()
      try {
         InetAddress address = InetAddress.getLocalHost();
   System.out.println("IP-адреса: " + address.getHostAddress());
         for (int port = 1; port <= 65535; port++) {
            try {
               Socket socket = new Socket();
               socket.connect(new InetSocketAddress(address, port), timeout);
               System.out.println("Відкритий порт: " + port);
               openPorts.add(port);
               socket.close();
            } catch (Exception e) {
               // Порт закритий або сталася помилка підключення
            }
         }
      } catch (UnknownHostException e) {
         e.printStackTrace();
      }
      System.out.println("З'єднання на відкритих портах: " + openPorts);
   }
}

        public class SignatureVerifier {
           public static void main(String[] args) {
              try {
                 // Завантаження ключового контейнера з сертифікатом
                 String keystorePath = "path/to/keystore";
                 String keystorePassword = "keystore_password";
                 String alias = "alias";
                 String aliasPassword = "alias_password";
                 KeyStore keystore = KeyStore.getInstance("JKS");
                 FileInputStream fis = new FileInputStream(keystorePath);
```

```
            keystore.load(fis, keystorePassword.toCharArray());
            // Отримання публічного ключа з сертифіката
            PublicKey publicKey = keystore.getCertificate(alias).getPublicKey();
            // Завантаження підписаного повідомлення та його сигнатури
            String messagePath = "path/to/message";
            String signaturePath = "path/to/signature";
            FileInputStream messageFis = new FileInputStream(messagePath);
            FileInputStream signatureFis = new FileInputStream(signaturePath);
            byte[] messageBytes = new byte[messageFis.available()];
            messageFis.read(messageBytes);
            byte[] signatureBytes = new byte[signatureFis.available()];
            signatureFis.read(signatureBytes);
            // Ініціалізація об'єкту для перевірки сигнатури
            Signature signature = Signature.getInstance("SHA256withRSA");
            signature.initVerify(publicKey);
            // Оновлення об'єкту з підписаним повідомленням
            signature.update(messageBytes);
            // Перевірка сигнатури
            boolean isValid = signature.verify(signatureBytes);
            if (isValid) {
               System.out.println("Сигнатура вірна. Повідомлення не було змінено.");
            } else {
               System.out.println("Сигнатура невірна. Повідомлення може бути пошкодженим.");
            }
         } catch (Exception e) {
            e.printStackTrace();
         }
      }
}
}
}
```

ІЛЮСТРАТИВНА ЧАСТИНА

Система захисту електронного документообігу Вінницької міської ради

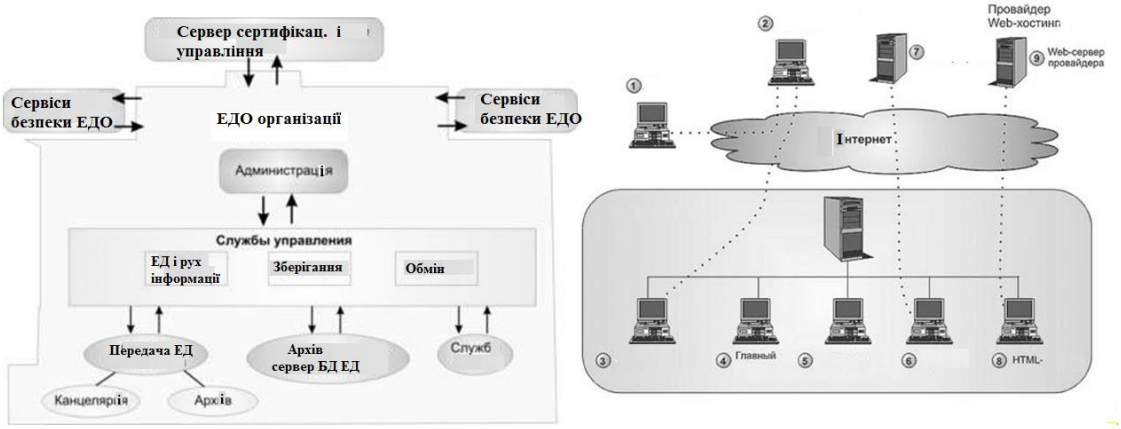
(Назва бакалаврської кваліфікаційної роботи)

Виконав: студент 4 курсу групи 1БС-21МС
спеціальності 125 Кібербезпека
_____ Олександр СОЛОНЮК
19 червня 2023 р.

Керівник: к. т. н., доцент каф. ЗІ
_____ Андрій ДУДАТЬЄВ
19 червня 2023 р.

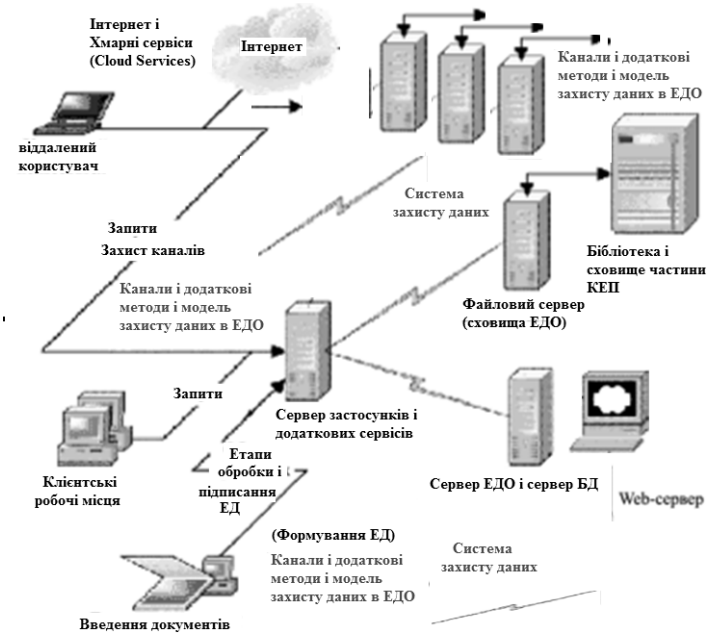
Структура захищеної інформаційної мережі ЕДО із підвищеним рівнем захисту і підходами додаткової ІБ із контролем цілістності

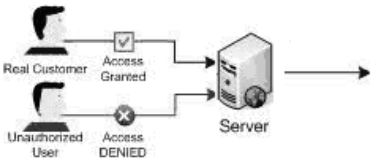
Структура захищеної інформаційної системи ЕДО



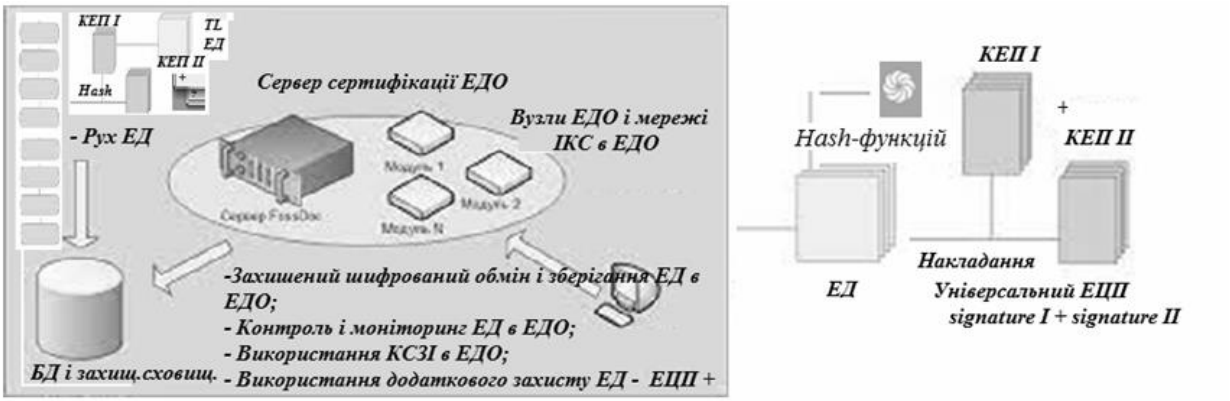
Структура моделі захищеної ІКС ЕДО із впровадженою системою комплексного захисту інформації (КЗСІ) і методом і моделлю захисту даних ЕД в ЕДО

Структурна схема захищеної інформаціної системи ЕДО





Розроблена модель і метод комплексного інформаційного захисту електронних документів (ЕД) в системі (ЕДО)



Структурна схема логічної схеми системи захисту ЕДО