ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення ефективності захисту процесу електронного документообігу конфіденційних даних корпоративної мережі об’єкту інформаційної діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності __125__ Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Микита ЧЕРНИШОВ

Виконав: здобувач вищої освіти групи СЗДМ 61
Микита ЧЕРНИШОВ

ІВАНЧЕНКО Ігорь .
к.т.н., доцент ___ ____
PI

Рецензент: _____
. *(ПРІЗВИЩЕ, Ім’я)*

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чернишову Микиті Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Підвищення ефективності захисту процесу електронного документообігу конфіденційних даних корпоративної мережі об'єкту інф
керівник кваліфікаційної роботи _____ Ігорь ІВАНЧЕНКО к.т.н., доцент .

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: опорний об'єкт інформаційної діяльності, інформаційно-комунікаційні канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні мережеві засоби захисту інформації від несанкціонованого витоку, програмно-технічні засоби електронного документообігу.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
4.1 Аналіз принципів побудови та можливостей систем електронного документообігу інформації в корпоративних мережах об'єкту інформаційної діяльності
4.2. Огляд каналів несанкціонованого витоку інформації через корпоративну мережу об'єкта інформаційної діяльності
4.3. Розробка рекомендації щодо удосконалення системи криптографічного захисту процесу електронного документообігу конфіденційних даних корпоративної мережі

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Микита ЧЕРНИШОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Ігорь ІВАНЧЕНКО
(підпис)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 80 сторінок, має 9 рисунків, 2 таблиці. Список використаних джерел містить 24 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності системи криптографічного захисту процесів обробки конфіденційних даних корпоративної мережі об'єкту інформаційної діяльності.

В кваліфікаційній роботі проведено огляд каналів несанкціонованого витоку інформації через корпоративну мережу об'єкта інформаційної діяльності проаналізовано принципи побудови та можливості систем електронного документообігу інформації в корпоративних мережах об'єкту інформаційної діяльності. Проведено огляд каналів несанкціонованого витоку інформації через корпоративну мережу об'єкта інформаційної діяльності. Досліджено напрямки та запропоновано рекомендації щодо удосконалення системи криптографічного захисту процесу електронного документообігу конфіденційних даних корпоративної мережі.

Апробація:

О.Ю. Панчук, М.О. Чернишов, Н.І, Осадчий. Основні загрози та ризики порушення цілісності інформації, що циркулює в корпоративній мережевій системі електронного документообіг. *Всеукраїнської науково-практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.43-44. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, КОРПОРАТИВНА МЕРЕЖА.

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 80 pages, has 9 figures, 2 tables. The list of sources used contains 24 items and takes up 3 pages.

The purpose of the qualification work is to increase the efficiency of the cryptographic protection system for the processing of confidential data of the corporate network of the object of information activity.

The qualification work reviews the channels of unauthorized information leakage through the corporate network of the object of information activity, analyzes the principles of construction and capabilities of electronic document flow systems in corporate networks of the object of information activity. Reviews the channels of unauthorized information leakage through the corporate network of the object of information activity. Researched directions and proposed recommendations for improving the cryptographic protection system for the process of electronic document flow of confidential data of the corporate network.

Approbation:

O.Yu. Panchuk, M.O. Chernyshov, N.I., Osadchy. Main threats and risks of violation of the integrity of information circulating in the corporate network system of electronic document management. All-Ukrainian scientific and practical conference: Current problems of security of information and communication systems. Kyiv, November 05, 2025, Kyiv: RVC DUIKT. – 2025. P.43-44. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: OBJECT OF INFORMATION ACTIVITY, INFORMATION WITH LIMITED ACCESS, CRYPTOGRAPHIC PROTECTION, CORPORATE NETWORK

.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД	–	Інформація з обмеженим доступом
СЕДО	–	Система електронного документообігу
ОІД	–	Об’єкт інформаційної діяльності
СТЗІ	–	Система технічного захисту інформації
ТКВІ	–	Технічний канал витоку інформації
ОТЗС	–	Основні технічні засоби і системи
ТЗПІ	–	Технічний засіб перетворення інформації
ДТЗС	–	Допоміжні технічні засоби системи ПЕМВ
	–	Побічні електромагнітні випромінювання
ТЗОС	–	Технічні засоби охоронної сигналізації

ВСТУП

Одним із найвагоміших та найактуальніших питань сьогодення є турбота про забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та комунікаційних мереж життєзабезпечення населення, які вважаються об'єктами інформаційної діяльності (ОІД). Тобто об'єкти, що є неналежними або не мають необхідної функціональності, можуть суттєво впливати на якість життя населення кожного регіону. Виходячи зі значних досягнень у науково-технічному розвитку, складності економічних життєвих процесів та соціальних відносин, а також розвитку різних технологій, що базуються на цих концепціях, можна зробити висновок, що одним із факторів, що сприяє якості функціонування ОІД, є різноманітність інформації. Частина цієї інформації підпадає під дію всіх видів правил щодо передачі, зберігання та захисту та вважається інформацією з обмеженим доступом (ІзОД).

Метою кваліфікаційної роботи є підвищення ефективності системи криптографічного захисту процесів обробки конфіденційних даних корпоративної мережі об’єкту інформаційної діяльності.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– проаналізовано принципи побудови та можливості систем електронного документообігу інформації в корпоративних мережах об’єкту інформаційної діяльності;

– проведено огляд каналів несанкціонованого витоку інформації через корпоративну мережу об’єкта інформаційної діяльності;

– досліджено напрямки та запропоновано рекомендації щодо удосконалення системи криптографічного захисту процесу електронного документообігу конфіденційних даних корпоративної мережі.

Об’єкт дослідження. Процес захисту інформації на об’єкті інформаційної діяльності.

Предмет дослідження. Система кібернетичного захисту центру електронного документообігу конфіденційних даних корпоративної мережі.

.

Розділ 1
УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ЦЕНТРУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ КОНФІДЕНЦІЙНИХ ДАНИХ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Особливості впровадження системи електронного документообігу в корпоративну мережу

В системах електронного управління записами (СЕД) бізнес-мереж.

Інформаційні об'єкти використовують різні методи збору, організації, зберігання, пошуку та перегляду цифрової інформації. У більшості СЕД використовується ієрархічна система зберігання файлів (за принципом "шафа/папка"). Кожен документ упаковується в досьє, яке потім розміщується на полиці тощо. Кількість потенційних рівнів вкладеності не визначена заздалегідь. Один і той самий документ може бути включений до кількох папок і полиць за допомогою механізму посилань (оригінальний документ у цьому випадку залишається незмінним і зберігається в місці, визначеному адміністратором СЕД). У кількох СЕД більша ємність для зберігання реалізується шляхом організації зв'язків між документами (ці зв'язки можна графічно редагувати та встановлювати).

Будь-який документ в СЕД приписується певному набору атрибутів (наприклад, його назва, автор документа, час створення тощо). Набір атрибутів може відрізнятися для різних типів документів (але він все одно залишатиметься однаковим у межах певного типу документа). Атрибути документа зберігаються в реляційній базі даних. Для кожного типу документа створюється картка за допомогою візуальних інструментів, які представляють назви атрибутів документа у вигляді чіткого графіка. Коли документ додається до SEDO, вибирається необхідний шаблон і картка заповнюється (вводяться значення атрибутів). Після заповнення форми виявляється адреса картки, пов'язана зі створенням документа.

Деякі експерти галузі вважають, що SEDO, ймовірно, стане основою корпоративної інформаційної системи на підприємстві чи в організації.

Як правило, серверна частина SEDO складається з таких логічних компонентів (які можуть бути розміщені на одному або кількох серверах):

1. Сховище атрибутів (атрибутів) документа;

3. Сховище документів;

4. Сервіси повнотекстового пошуку.

Сховище документів зазвичай називають сховищем документів. Сховище атрибутів та сховище документів часто синхронізуються під загальним терміном «архів документів». Важливо визнати, що значними перевагами SEDO є збереження документів у їхньому оригінальному форматі та автоматичне розпізнавання кількох типів файлів.

Останнім часом збереження документів разом з атрибутами в базі даних стало більш популярним. Цей метод має свої переваги та недоліки. Перевагою є значне підвищення безпеки доступу до документів, а головним недоліком – низька ефективність роботи з документами, які містять великий обсяг збереженої інформації. Цей метод також вимагає використання серверів з великим обсягом оперативної пам'яті та твердотільних дисків. Крім того, якщо база даних не може отримати документи, буде дуже важко відновити інформацію, що зберігається в ній.

Компоненти SEDO, що відповідають за переміщення документів, часто називають компонентами маршрутизації документів. Концепція вільного та жорсткого доступу до документів використовується для опису загальних концепцій. За допомогою «вільної» маршрутизації будь-який учасник потоку документів може змінити поточний маршрут документа або створити новий маршрут для потоку документів (або і те, й інше). За допомогою «жорсткої» маршрутизації документування маршрутів є суворим, і користувачам не дозволяється їх змінювати.

Однак за допомогою складної маршрутизації логічні процеси можуть виконуватися під час зміни маршруту, якщо виконуються заздалегідь визначені

умови (наприклад, надсилання документа керівництву, коли певний користувач перевищує свій авторизований діапазон).

У SEDO використовуються методи визначення повноважень та контролю доступу до документів. Зазвичай за їх допомогою розпізнаються такі типи доступу:

- повний контроль над процесом написання;

- можливість змінювати, але не знищувати письмовий документ;

- можливість створювати нові версії документа, але не змінювати його.

- можливість коментувати документ, але не змінювати його або створювати нові версії;

- право читати документ, але не змінювати його, чи це можливо?

- право доступу до картки, але не до вмісту документа;

- повна відсутність прав доступу до документа (під час роботи з SEDO кожна дія користувача записується, і, таким чином, всю історію його зв'язку з документами можна легко перевірити).

Під час роботи з документом, який має кількох авторів і потребує координації між різними екземплярами, дуже корисною функцією SEDO є можливість використання версій та підверсій документа.

Якщо виконавець спочатку створив першу версію документа, а потім передав її наступному користувачеві, це вважатиметься використанням документа. Другий користувач змінив документ і створив на його основі нову версію. Після того, як він передав свій чернетку документа наступній особі, він передав версію документа третьому користувачеві, який створив третю версію. Через визначений проміжок часу, автор першого чернетки ознайомився з коментарями та пропозиціями, після чого перший виконавець вирішує завершити оригінальний чернетку та на його основі створює контрофіційну версію документа. Перевага SEDO полягає в тому, що вона дозволяє користувачам автоматично відстежувати версії та підверсії документів (користувачі завжди можуть визначити, яка версія документа є найновішою, відстежуючи її до моменту створення).

Під час створення груп документів можливість додавання приміток є корисною. Оскільки користувачі часто позбавлені можливості вносити будь-які зміни до документа під час процесу затвердження, вони можуть натомість скористатися можливістю анотування. У більшості SEDO анотування здійснюється шляхом включення атрибута для анотації до картки документа та передачі прав на редагування цього поля користувачам. Однак це рішення не завжди практичне (особливо під час коментування візуального документа). У зв'язку з цим деякі SEDO мають функцію "червоного олівця", яку можна використовувати для візуалізації недоліків самого зображення.

1.2 Характеристика функціональних можливостей систем електронного документообігу

Проектування систем електронного документообігу здійснюється кількома компаніями окремо одна від одної, в результаті чого виникають проблеми під час взаємодії з різними системами управління документами від різних виробників. Як правило, ці проблеми пов'язані з розбіжністю між форматами представлення даних, відсутністю стандартизації системи та методами, що використовуються під час проектування системи.

Електронне документообіг (EDM) – це процедура створення, отримання, обміну, відстеження, аудиту, розповсюдження та зберігання документів та пов'язаної з ними інформації в певній інформаційній системі.

Управління електронною документацією полегшується програмним забезпеченням, спеціалізованим для цієї мети (EDMS, Enterprise Document Management Systems).

Серед найважливіших атрибутів систем електронного документообігу експерти зазвичай виділяють:

операційну систему;

типи, розміри та можливості документів;

стійкість системи;

максимальну кількість користувачів;

загальну кількість та кількість рівнів організації, що представляють властивості внутрішньої структури підприємства;

здатність працювати за стратегією «Звільнено», без надмірної прив'язаності до маршрутів;

методи створення схем маршрутів для письмового потоку;

Можливості регулювання потоку документів; методи повідомлення про випадки порушення правил документа, метод повідомлення посадових осіб,

Підтримка можливості роботи з кількома версіями документа, інтеграція з іншими програмами та налаштування програмного забезпечення відповідно до конкретних вимог замовника – все це особливості цього процесу.

Методи регулювання доступу та захисту від криптоаналізу.

Системи з розвиненими засобами workflow (WF)

Важливо розуміти деякі найважливіші визначення робочого процесу (Workflow), щоб зрозуміти цю концепцію:

Завдання, яке виконується без будь-якого врахування порядку чи послідовності одним або кількома членами робочої групи для досягнення спільної мети (IBM).

– повна або часткова автоматизація бізнес-процесу, документи, інформація або завдання передаються від одного учасника до іншого для виконання узгоджених дій;

– координація людей, інформації, об'єктів та подій для виконання послідовності дій та досягнення стану, який призводить до досягнення попередньо встановлених цілей (Workflow

ManagementCoalition).

Усі ці визначення стосуються бізнес-процесів, інформації та персоналу. Технологія робочого процесу включає:

– технології, що сприяють автоматизації робочих процесів; – автоматизації бізнес-процесів; – моделювання діяльності підприємства;

– контролю за всіма співробітниками компанії, як внутрішніми, так і зовнішніми, залученими до різних видів діяльності. У технології Workflow використовуються такі фундаментальні ідеї:

- об'єкт – бізнес-процес використовує об'єкт, специфічний для цього процесу (наприклад, документ, креслення або інструмент).

- подія – акт виконання дії над об'єктом (наприклад, підписання документа).

- операція – процес виконання дії, що є частиною бізнес-процесу, що розглядається (наприклад, перевірка правильності складання документа, внесення змін до документа).

- виконавець – посадова особа, якій доручено виконати бізнес-процес.

Кожен клас систем Workflow вирішує щонайменше три питання:

- опис бізнес-процесу;

- адміністрування бізнес-процесів; - нагляд за бізнес-процесами.

Управління виконанням робочого процесу включає:

- перевірку умов переходу між операціями; - передачу документів між виконавцями.

- інформування користувача про те, що йому потрібно зробити.

Основні компоненти системи електронного документообігу:

Масштабованість – важливо, щоб система могла обслуговувати будь-яку кількість користувачів, при цьому можливості системи обмежуються лише потужністю пов'язаного з нею програмного забезпечення.

Розподіленість – проектування систем управління документами повинно враховувати взаємодію між розподіленими платформами та документами в організаціях, що географічно розкидані.

Модульність – система повинна складатися з окремих компонентів, інтегрованих один з одним. Якщо користувач системи не впроваджує одразу всі компоненти системи управління документами, або сфера діяльності організації

менша, ніж весь спектр завдань управління документами, то система вважається модульною.

Таблиця 1.1 Функціональні можливості СЕДО

Функції	Зміст
Реєстрація документів	реєстрація і облік документів; ведення журналів реєстрації та обліку; ведення номенклатури справ
Контроль виконання	ведення контрольних завдань перенесення терміну виконання завдань ведення стану виконання зняття завдань з контролю згідно із звітами визначення результату виконання завдань підтримка завдань централізованого і децентралізованого рівня
Маршрутизація об'єктів документообігу	реєстраційних карток контрольних карток електронних версій документів звітів щодо виконання контрольних завдань
Колективна робота	ведення електронних версій документів
Пошук	атрибутивний пошук об'єктів документообігу, повнотекстовий пошук документів
Звітність	журнали реєстрації та обліку контрольні картки аналіз виконання завдань аналітичні і статистичні довідки
Адміністрування	розмежування повноважень управління технологічними процесами налагодження системи

Відкритість – система повинна мати відкриті інтерфейси, які можна розширювати та комбінувати з іншими системами.

Автоматизація управління документами здійснюється за допомогою окремих автоматизованих процесів, які об'єднуються у функціональні комплекси, типовими для яких є:

- комплекс написання документів за допомогою комп'ютера;

- система запису та перевірки електронних документів в оперативному цифровому архіві;

- складна система електронного зберігання, зберігання паперових документів та доступу до його інформації.

- кластер виконавчого контролю;

- проектування маршруту потоку низки складних документів;

- комплекс передачі даних;

- комплекс, що сприяє створенню статистичної та аналітичної звітності, а також оперативному аналізу.

- комплекс адміністративних та інформаційних завдань щодо нормативно-довідкової інформації.

- комплекс, що включає державні установи та установи;

У SEDO немає правил щодо складу чи змісту електронного документа.

У SEDO передаються такі дані:

- електронні записи;

- дані про реєстрацію, що зберігаються в електронному вигляді, щодо змісту електронного документа та його реєстрації.

- повідомлення відправнику, яке інформує його про прийняття (відображення) вхідного електронного документа службою управління офісом одержувача.

Інтерфейс між вами та SEDO дозволяє вам досягти цього:

- Ергономіка взаємодії користувача з SEDO;

- Взаємодія між користувачем та програмними компонентами SEDO базується на прозорому та інтуїтивно зрозумілому діалоговому вікні, що є інтерфейсом, що використовує піктограми, що представляють функції, режими та процедури;

- здатність користувача використовувати професійно-орієнтовані концепції предметної області управління офісом рідною мовою;

– можливість скасування дій користувача, а також обов'язкове підтвердження деструктивних дій користувача, які можуть призвести до зміни або відновлення даних;

– здатність користувача отримувати інформацію про функціональні атрибути SEDO (зокрема, отримувати на екрані підказки, що вимагають дій, функцій тощо).

SEDO може використовувати систему управління базами даних, яка надійно зберігає інформацію в різних форматах (як текстових, так і візуальних

або аудіоформатах). Ця система забезпечує швидкий доступ до інформаційних ресурсів для різних систем, які мають заплановану кількість користувачів.

1.3 Електронний цифровий підпис

Закон України «Про електронний цифровий підпис» зосереджений на регулюванні взаємодій щодо використання одного з видів електронного підпису – електронного цифрового підпису. Закон України про «електронні цифрові підписи» (Відомості Верховної Ради (ВВР), 2003, № 36, ст. 276) описує правову природу електронного цифрового підпису та регулює взаємодії, що виникають внаслідок його використання.

Електронні підписи, що походять з інших електронних записів або логічно пов’язані з ними, призначені для ідентифікації автора цих даних.

Електронний цифровий підпис – це форма електронного підпису, що походить від криптографічного перетворення.

Набір електронних записів, що додаються до цього набору записів або логічно інтегруються в нього.

Крім того, це сприяє автентичності документа та ідентифікації підписувача. Електронний цифровий підпис використовує закритий ключ для обробки та перевірки відкритого ключа. Унікальною характеристикою ЕЦП є використання протоколів криптографічної безпеки інформації.

Електронний цифровий підпис – це програмний інструмент, програмно-апаратний або апаратний пристрій, який створює ключі, використовує програмне або апаратне забезпечення для реалізації підпису та перевіряє його.

Закритий ключ – це компонент криптографічного процесу, який створює електронний підпис, цей компонент доступний лише підписувачу.

Відкритий ключ – це компонент криптографічного протоколу для перевірки електронного цифрового підпису, цей компонент доступний суб'єктам відповідних відносин.

Призначення електронного цифрового підпису

Коли електронні документи використовуються та передаються за допомогою телекомунікаційних засобів, безпеку інформації слід розглядати з максимальною ретельністю. Звичайний електронний документ, який не захищений від змін або несанкціонованого доступу, не вважається захищеним документом. Захист електронних документів здійснюється за допомогою електронного цифрового підпису.

Електронний цифровий підпис – це інформація, що вноситься до файлу даних його творцем, яка захищає файл від несанкціонованої зміни та однозначно ідентифікує підписувача.

Електронний цифровий підпис призначений для забезпечення дій фізичних та юридичних осіб, що здійснюються з використанням електронних документів. Він використовується фізичними та юридичними організаціями, які мають електронні документи, для розпізнавання підписувача та перевірки легітимності даних в електронній формі.

Цифровий підпис, створений електронними засобами, вважається еквівалентним власноручному підпису (печатці) за юридичною силою.

1) електронний цифровий підпис перевіряється за допомогою вдосконаленого сертифіката ключа, отриманого з надійного засобу цифрового підпису;

Під час процесу перевірки використовується потужніша пара ключів, яка була дійсною під час застосування електронного цифрового підпису.

3) закритий ключ підписувача ідентичний відкритому ключу, зазначеному в сертифікаті.

Електронна реалізація цифрового підпису не змінює процедуру підписання договорів та інших документів, які юридично зобов'язані укладати транзакції в письмовій формі.

3) закритий ключ підписувача ідентичний відкритому ключу, зазначеному в сертифікаті.

Електронна реалізація цифрового підпису не змінює процедуру підписання договорів та інших документів, які юридично зобов'язані укладати транзакції в

письмовій формі. Нотаріальні дії, що засвідчують легітимність цифрового підпису на електронних документах, здійснюються відповідно до протоколу, встановленого законом.

У випадках, коли необхідно засвідчити легітимність підпису на документах та відповідність копій документів оригіналу з печаткою, для автентифікації електронного документа використовується інший електронний цифровий підпис юридичної особи. Це спеціально призначено для цієї мети.

Процес використання цифрового підпису для державних організацій, установ та підприємств регулюється Кабінетом Міністрів України.

Процес використання електронного цифрового підпису в банківській справі регулюється Національним банком України.

Закриті та відкриті ключі

Система електронного цифрового підпису складається із закритого ключа, який створює електронний цифровий підпис, а також відкритого ключа, який його перевіряє.

Закритий ключ – це унікальний рядок символів довжиною 26 біт, призначений для створення ЕЦП в електронних записах. Закритий ключ діє лише з відкритим ключем.

Закритий ключ має зберігатися конфіденційно, оскільки будь-хто, хто його дізнається, зможе підробити електронний підпис.

Документ комплектується ЕЦП, який використовує закритий ключ. Цей ключ унікальний і існує лише в одному екземплярі у власника документа. Цей закритий ключ пов'язаний з відкритим ключем, який дозволяє перевірити відповідність ЕЦП його автору.

В результаті автор (підписувач) завжди зберігає свій секретний ключ, і ніхто не може легально підписати документ електронними засобами за нього. Крім того, будь-хто може використовувати відкритий ключ для автентифікації легітимності цього підпису та автора.

Процес накладання цифрового підпису електронними засобами здійснюється відправником (підписувачем) документа за допомогою свого

особистого ключа. Під час виконання цієї процедури дані, що підлягають підпису, та закритий ключ підписувача вводяться у відповідне поле програмного забезпечення.

Програма генерує з даних, використовуючи секретний ключ, унікальний блок даних фіксованого розміру (власний ЕЦП), який дійсний лише для закритого ключа та вхідних даних. Тобто, ЕЦП є цифровим підписом закритого ключа та документа.

Пізніше, ЕЦП зазвичай додається до вхідного документа (або розміщується в окремому полі документа), і ця комбінація інформації (документ + ЕЦП) створює захищений електронний документ.

Електронний цифровий підпис (ЕЦП) отриманого документа перевіряється одержувачем за допомогою відкритого ключа підписувача (відправника).

Для виконання цієї процедури необхідно отримати відкритий ключ відправника (наприклад, з каталогу). Крім того, необхідно отримати захищений документ (тобто дані, пов'язані з документом та ЕЦП). Програмний модуль, що відповідає підпису, перевіряє, чи дійсно цифровий підпис пов'язаний з документом та відкритим ключем. Якщо до самого документа або відкритого ключа було внесено зміни, буде перевірено, і це призведе до негативного результату.

Для повної функціональності системи електронного цифрового підпису (ЕЦП) одержувач повинен мати доступ до надійного дубліката відкритого ключа відправника та можливість перевірити, що цей дублікат дійсно належить цьому відправнику. Для досягнення цієї мети спеціальні директорії ключів, призначені для безпеки, створюються та підтримуються спеціальними установами, які називаються центрами сертифікації ключів (ЦСК). Відкритий ключ має бути затверджений ЦСК.

1.4 Система кібернетичного захисту від несанкціонованого доступу до даних корпоративної мережі

Фундаментальні концепції впровадження ефективних методів розробки та проектування технічних засобів захисту інформації в розподілених інформаційних системах з клієнт-серверною моделлю випливають з наступних правил:

1. Використання TCP/IP як основних протоколів транспортного та мережевого рівнів як основи ефективності проектування розподілених корпоративних додатків. Важливими інформаційними сервісами, що обробляють інформацію в корпоративній мережі, вважаються telnet, ftp, smtp, snmp, http, а також сервіси SQL-запитів.

2. До складу структури корпоративної мережі входять мережі передачі даних, що об'єднані мережею, окремі фізичні мережі, що не використовуються для забезпечення доступу до інформаційних ресурсів різного рівня секретності. Для забезпечення зв'язку процесів обробки даних використовуються стандартні протоколи. Відповідні модифікації програмного забезпечення, як для клієнта, так і для сервера, не реалізовані.

3. Розподіл механізмів безпеки за допомогою взаємодії на рівні зв'язку.

Здійснюється відповідно до протоколу ISO/OSI.

Виділення мережевих сервісів з метою захисту, на основі спеціалізованого протоколу для застосування, відбувається в рамках:

- Створення облікових записів у базі даних обмеженого доступу;

- Налаштування режимів роботи засобів захисту (сценарії реєстрації НРД, обслуговування запитів, що надходять, тощо);

- Створення віртуальних каналів зв'язку в оверлейній мережі, що захищені за допомогою шифрування каналів та вибіркового шифрування певних інформаційних полів (наприклад, для збереження цілісності транспортних зв'язків).

- Протоколу розширеної автентифікації, що використовує відкриту криптологію;

- Діагностики та документування стану захищених ресурсних об'єктів.

Для мінімізації втрат якості роботи програм використовується принцип потокової передачі. У рамках цього принципу розрізняються різні режими роботи, перший характеризується повнотою захисту, а другий вимагає витрат ресурсів, пов'язаних з комп'ютерами та комунікаціями, для виконання завдання.

У контексті реалізації фундаментальних принципів захисту інформації запропоновано модель багаторівневого захисту інформації. Комплексність захисту досягається включенням механізму, який запобігає потраплянню інформації під вплив усіх загроз у множині, класифікація яких базується на можливості їх усунення. Це приклади помилок та закладок у програмному забезпеченні, а також загроз, які не повністю усунуті, пов'язані з необхідністю доступу до інформації (доступ не може бути заборонений, як наслідок, неможливо усунути ці загрози). Багаторівневий захист передбачає використання додаткових технічних можливостей зі специфічними вимогами щодо проектування системи. При кількох рівнях захисту в корпоративних комунікаціях розглядаються такі напрямки розробки:

- Створення методів захисту робочих станцій та серверів, пов'язаних з корпоративною мережею, насамперед щодо захисту платформи, що на них використовується - операційної системи.

- Створення протоколу, специфічного для встановлення безпечного з'єднання "клієнт-сервер", яке реалізуватиме корпоративну мережу.

- Розробка спеціалізованих технічних засобів для захисту активів корпоративної мережі.

Важко гарантувати безпеку окремих комп'ютерів у внутрішній мережі.

В результаті ефективніше захищати всю мережу як єдине ціле. Щоб запобігти доступу до внутрішніх мереж людей ззовні компанії, використовується конструкція брандмауера. Брандмауер – це поєднання компонентів або система, розташована між двома мережами та має властивості, що визначаються захистом системи. Система постійно захищена від вторгнення. Брандмауер зазвичай має кілька різних компонентів, до яких належать бар'єри або екрани, що запобігають передачі певних типів трафіку, та канали. Шлюз –

це машина або серія машин, що виконують послуги, що компенсують наслідки обробки.

1.5 Архітектура типової системи електронного документообігу та критерії її обґрунтування

Сучасні системи електронного документообігу: EMC Documentum, LanDocs System, Megapolis Document Management, Optima-Flow.

Розглянемо систему EMC Documentum, яка інтегрована в інституційну структуру місцевих органів влади (рис. 5.1).

Система складається з чотирьох окремих підсистем, які були обрані на основі їхніх цільових функцій та технології, що використовується для їх реалізації:

1. Система управління обліково-аналітичною інформацією – це комплекс додатків, що надають користувачам інструменти для створення документів, участі в інтерактивних процесах з інформацією та автоматизованого аналізу діяльності підприємства. Основними обов'язками цієї підсистеми є: введення та ведення нормативних та інформаційних даних – класифікаторів, платіжних документів, актів тощо; створення та редагування первинних документів клієнтів, а також інших документів, створених на їх основі; навігація інформацією та пошук даних; аналіз інформації та створення зразків; підготовка та друк звітів.

Інтерфейс користувача підсистеми реалізовано в середовищі MS Access, яке підключено до MS SQL Server. Підсистема складається з таких компонентів:

Допоміжні: "Нормативні та інформаційні документи", "Документи прийняття та видачі", "Висновки експертів", "Платежі", "Контроль доступу"?

- основні: "Технічні пропозиції", "Інвестиційні угоди", "Виконавчі угоди", "Операційні рішення".

2. Підсистема, призначена для підтримки електронного сховища документів та сприяння потоку документів. Вона складається з Сервера управління документами (DMS) та компонента, що сприяє організації бізнес-

процедур (компонент, який називається робочим процесом). Він поєднується з ним. Основними функціями цієї підсистеми є: автоматизація бізнес-процесів, пов'язаних з координацією документів, автоматизоване захоплення сканованих документів у систему та організація роботи з системою, включаючи договірні та директивні документи.

3. Електронні публікації – це компонент системи публікації інформації про комп'ютери з певного книгарні, яка публікується онлайн. Ця підсистема включає веб-сервер та програму CGI, яка взаємодіє з банками даних через FTP. Основними обов'язками підсистеми є: підтримка та доступ до інформації через WWW; організація інтерактивного доступу до Інтернету та

Користувачі інформації інтрамережі повинні бути ідентифіковані, їхня автентичність має бути гарантована, а їм має бути наданий доступ до інтрамережі.

4. Компонент системного адміністрування та налаштування, який реалізується за допомогою стандартних функцій адміністрування Windows XP або інших версій MS Windows, він налаштовує правила для їх реалізації та пов'язану з ними документацію.

Система реалізована в архітектурі локальної мережі, що базується на серверах під керуванням Windows 2008 та має клієнтів, які працюють на тій самій системі. Програми працюють за протоколом "клієнт-сервер". Користувацька програма реалізована як окрема клієнтська програма, розміщена на файловому сервері та доступна для клієнтських станцій.

Серверна частина. У випадку типового мережевого протоколу використовується TCP/IP, що полегшує взаємодію комп'ютерів з веб-сервером (інтранет/інтернет). Електронний архів та потік документів забезпечується системою управління документами (DMS) DOCS Open, яка поєднується з модулем організації бізнес-процедур WorkRoute та модулем сканування зображень документів Deltalmage. Створення документів, введення та адміністрування нормативної та іншої інформації, аналіз окремих документів та

напрямків діяльності, статистичне обстеження загальної діяльності корпорації та підготовка звітів реалізуються через користувацьку програму, що є оригінальною для SQL Server. База даних MS SQL Server 6.5 є основним сховищем інформації (SQL). Таблиці SQL містять всю інформацію, необхідну для роботи сервера DMS та аналітичних користувацьких програм.

Клієнтська частина. Клієнти використовують комп'ютери, що працюють під управлінням операційної системи Windows. Доступ до веб-сервера через протокол TCP/IP здійснюється через стандартний браузер MS Internet Explorer.

Доступ здійснюється через стандартний протокол TCP/IP.

Налаштування клієнтів централізоване системним адміністратором.

Використання сучасних методів проектування під час розробки технічних вимог до програмних продуктів сприяє ідентифікації модулів, які мають спільну функцію в інших проектах.

Метод розробки схем баз даних заслуговує на особливу увагу. Ці рішення вимагають використання СУБД Oracle, MS SQL та InterBase.

Майже всі сучасні завдання складаються з розподілених систем, які побудовані відповідно до модель клієнт-сервер або використовувати електронну пошту для передачі документів або для повної реплікації бази даних компонентів системи.

Наприклад, ініціатива системи електронного управління документами (EDMS) включає клієнтські поштові пункти, які сприяють організованому розподілу документів між пов'язаними системами. EDMS походить від специфікацій X.400, X.425 та X.435, які стосуються способу взаємодії прикладних систем одна з одною. Під час розробки системи були розглянуті питання захисту документів від відтворення та несанкціонованого доступу.

Під час розробки програмного продукту максимально використовувалися стандартні інтерфейси для розробки програмного забезпечення, такі як MAPI, включаючи IDAPI, який є інтегрованим інструментом управління базами даних, та IBDE, який є інтегрованим інструментом розробки програмного забезпечення. Програмний інтерфейс IDAPI призначений для роботи з базами

даних, що дозволяє використовувати будь-яку базу даних. Це рішення є вигідним, оскільки дозволяє користувачам використовувати вже наявну базу даних, а не купувати SQL Server, рекомендований розробником.

Те саме стосується інтерфейсу між програмою та електронною поштою. Для зв'язку з поштовою системою використовується інтерфейс Microsoft MAPI, що дозволяє використовувати будь-яку електронну пошту (та пов'язаний з нею криптографічний захист), яка підтримує MAPI.

Якщо користувач не може використовувати MAPI, доступна альтернатива -використання Spooler (спулер, програма, яка буферизує дані), який має загальнодоступний інтерфейс до поштових систем.

В результаті можна сказати, що побудована система є доступною та має потенціал для зростання з точки зору розмірів бази даних та компонентів електронної пошти. Цей метод сприяє розширенню системи новими функціями, додаванню нових типів документів.

Завдяки короткому обговоренню основних методологічних принципів створення корпоративної системи електронного документообігу можна визначити основні методологічні принципи, які були задіяні при створенні цих систем (електронна публікація, системи підтримки клієнтів та електронне урядування).

1. Використовуючи процедурно-орієнтований підхід до управління документацією, цей метод дозволяє створювати документи, які є логічно узгодженими та підтримують весь життєвий цикл документа в організації.

2. Впровадження системи цифрового документообігу в кілька кроків, що зрештою призводить до завершення роботи системи на рівні кінцевих одержувачів. Це сприяє створенню єдиного інформаційного простору в компанії.

3. Комплексний підхід до вирішення питань документаційного забезпечення, що дозволяє створювати повнофункціональні системи.

4. Використання складних промислових інструментів для впровадження систем, що гарантує короткі терміни. впровадження, легкість модифікації та розвитку системи і ряд інших переваг.

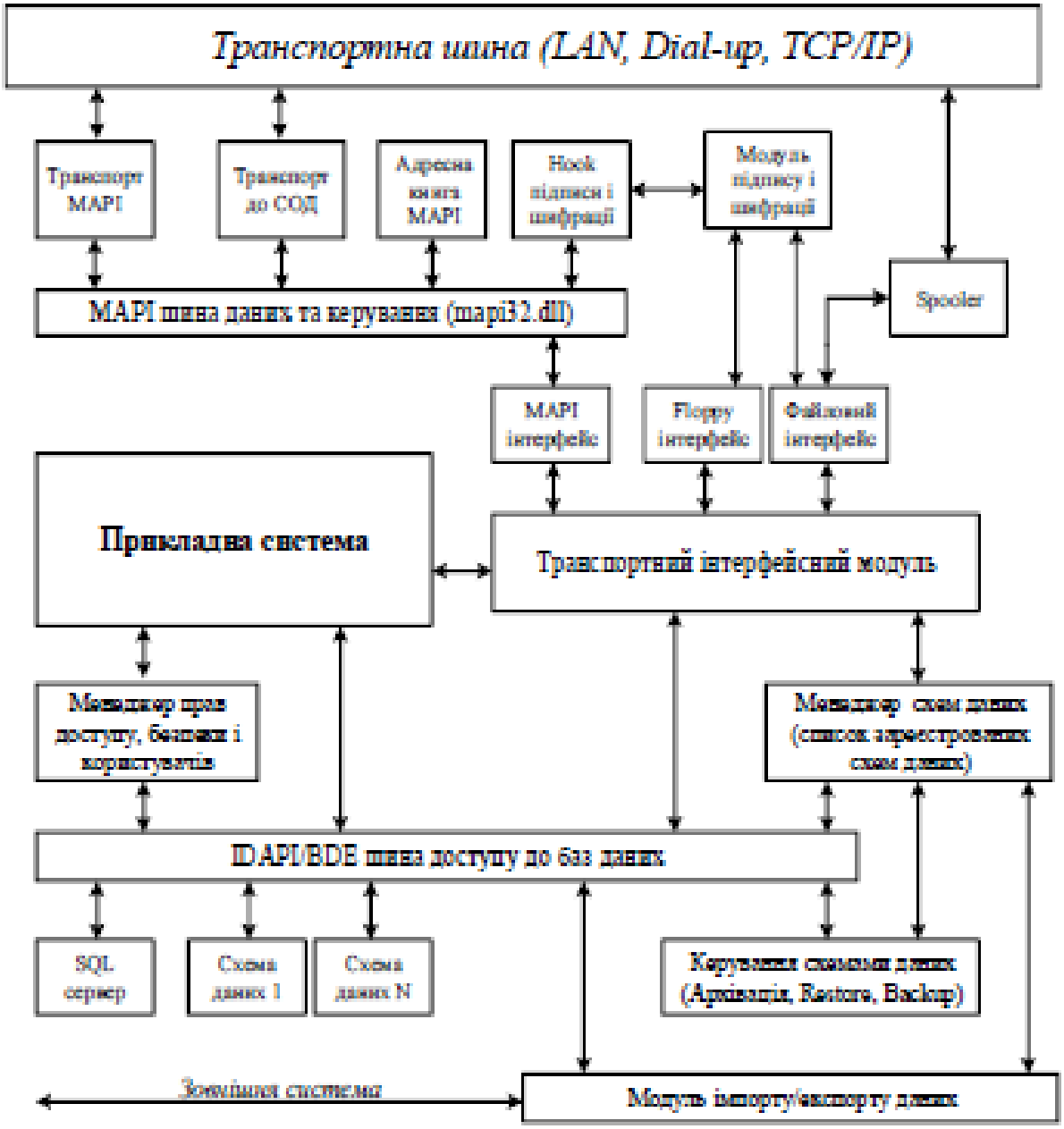


Рисунок 1.2. Схема архітектури типової системи електронного документообігу

EMC Documentum

EMC Documentum – це платформа управління контентом, що охоплює всю компанію. Інформація, яка є контентною або неструктурованою, виражається в різних формах: текстові документи, інженерні креслення,

XML-документи, відскановані паперові документи, аудіо- та відеофайли, а також інші типи та формати файлів. EMC Documentum спрощує створення контенту за допомогою популярних настільних інструментів та простих у

використанні шаблонів. Він також отримує та агрегує попередньо розроблений контент з різних джерел.

EMC Documentum підвищує інтелект контенту, використовуючи категоризацію та метадані, що підвищує ефективність пошуку та вилучення. EMC Documentum автоматизує процес перевірки, прийняття та затвердження контенту, який визначено користувачем з точки зору бізнес-правил, визначених у функціях управління робочим процесом та життєвим циклом. (Функціональна архітектура системи EMC Documentum обговорюється в Додатку А).

Атрибути та обов'язки системи:

Незважаючи на те, що управління корпоративним контентом використовується в багатьох дисциплінах, фундаментальна мета ECM однакова в усіх його аспектах: використовувати корпоративні знаннєві ресурси для отримання конкурентної переваги. Незалежно від сфери застосування ECM-технологій: веб-сайт для клієнтів, корпоративний портал, додаток для управління ланцюгом поставок або система обробки кредитних заявок, неструктурований контент є або ключем до підвищення ефективності бізнесу, або причиною відсутності прибутку, або вузьким місцем, яке перешкоджає його досягненню. Очевидно, що локальні рішення, що існують у вигляді відділів, не зможуть впоратися зі зростаючою популярністю корпоративного контенту. Організації, які виключно використовують ці рішення, мають ізольовані, нездатні взаємодіяти зі сховищами контенту, що серйозно погіршує обмін інформацією. Правильний вибір – це рішення корпоративного рівня, навіть якщо ви починаєте з його впровадження лише в одному відділі. Щоб прийняти правильне рішення, ви повинні знати про основні функції, які повинна мати ECM-система. Вони забезпечують необхідну підтримку або основу для рішення для управління контентом – основи. Без них система управління контентом не матиме необхідної функціональності для створення надійного та релевантного контенту для клієнтів, партнерів, постачальників та співробітників сьогодні, а також для задоволення їхніх зростаючих вимог у

майбутньому. Управління корпоративним контентом – це термін, що охоплює комбінацію технологій, що вирішують такі основні проблеми:

Управління документами (DocumentManagement). • Управління веб-контентом (WebContentManagement).

• Управління активами з оцифруванням (AssetManagement with Digitization).

• Партнерство (Collaboration). • Фотографування документів (Document Photography).

Управління звітами (ReportManagement). • Архівування контенту (Content Archiving).

Адміністрування записів (records Administration).

Архівування електронної пошти (E-mailArchiving). Управління бізнес-процесами (BPMS).

• Поєднання з внутрішніми додатками (інтегровано в підприємство).

Інтеграція корпоративного контенту. Електронне розкриття інформації.

Відповідність. Завдання, які виконала система.

Функціональні рішення – це поєднання продуктів та послуг, що надають рішення для різних функціональних аспектів діяльності організації. Функціональні рішення можуть використовувати одну або декілька технологій для управління контентом. Функціональні рішення поділяються на три основні класи:

Управління організаційною документацією. Управління технічними документами.

Управління фінансовими документами.

Обов'язки, які найчастіше виконуються сьогодні за допомогою системи: • Управління офісом та зберігання. Рішення пропонує функціональність, яка задовольняє

Допомога з управлінням документами в контексті електронного управління документами.

Незважаючи на складність вимог до документів для організації праці з документами, система готова їх виконувати та гарантувати їх досягнення.

• Контрольовані дії. Різні нормативні акти продиктували набір вимог до цього рішення, яке, з одного боку, гарантує дотримання нормативних актів, а за допомогою технічних та організаційних методів забезпечує, що інспекційні органи визнають це з часом.

• Управління дебетом та кредитом. Автоматизує трудомісткий та переважно ручний процес виставлення рахунків, перевірки та складання рахунків. Рішення дозволяє здійснювати інтелектуальне, високопродуктивне сканування, автоматизовану та пов'язану обробку документів, а також мати можливість доступу до документів з інтерфейсу ERP-системи.

Управління контрактами. Рішення сприяє більш ефективному управлінню життєвим циклом контракту та пов'язаними з ним документами шляхом централізації зберігання, захисту інформації та контролю доступу, а також автоматизації бізнес-процесів створення, затвердження та виконання контрактів.

Технічні креслення та документація.

Рішення базується на сховищі контенту, яке керує всіма типами технічного контенту, включаючи креслення, схеми, таблиці та специфікації. Його метою є створення технічної документації, корисної з різних причин, з визначеним шаблоном доступу та потенціалом для географічно розподілених користувачів.

Управління проектами. Рішення використовується для регулювання проектів та програм у різних дисциплінах. Воно спрощує планування та управління проектами, підтримує взаємодію членів проектної команди в безпечному проектному просторі та автоматизує створення документів, що стосуються проектів.

Управління якістю. Рішення базується на управлінні життєвим циклом стандартних операційних процедур, автоматизації процесів розробки цих процедур, додаванні функцій, поширенні змін та скасуванні цих процедур.

Включає функцію, яка повідомляє про зміни, та журнал аудитів, що гарантує знайомство.

Переваги системи

Одним з найважливіших активів бізнесу є інформація в різних формах, яка представляє знання та інтелектуальну власність організації, накопичені з часом. Ця інформація, включаючи специфікації продукту, маркетингові матеріали, веб-сторінки, дані про обслуговування клієнтів, контракти з постачальниками, електронні листи, фотографії тощо, часто називається корпоративним контентом і являє собою значне зобов'язання щодо інтелектуальної власності, часу та грошей.

П'ять переваг рішень EMC для управління контентом та архівування включають:

Відповідність нормативним вимогам. Продукти EMC можуть допомогти вам досягти нормативних та державних цілей і стандартів, визначених урядом, регуляторними органами або внутрішніми політиками.

Ефективність. Продукти EMC сприяють операційній ефективності завдяки автоматизованим процесам та забезпеченню дотримання бізнес-правил.

Продуктивність. Продукти EMC підвищують ефективність як окремих осіб, так і цілих команд, полегшуючи доступ до корпоративного контенту та його організацію.

Архівування. Продукти EMC сприяють досягненню довгострокових цілей, досягають угод про рівень обслуговування та збільшують повторне використання контенту.

Консолідація: продукти EMC знижують загальну вартість володіння (порівняно з кількома програмами від різних постачальників), створюючи єдину стандартизовану інфраструктуру, інформація зберігається в одному місці та досягається економія від масштабу.

Критерії підбору сучасних систем електронного документообігу Критерії підбору сучасних систем електронного документообігу подано в порівняльній

табл. 1.2.

Таблиця 1.2

	Критерії підбору				
	Операційна система	Система управління базами даних	Система електронної пошти	Система колективної роботи	Сервер інтеграції
Місцевий або інший орган влади з невеликим обсягом документообігу	Microsoft Windows	MSDE	Не обов'язково	Не обов'язково	Не потрібно
Місцевий орган самоврядування	Microsoft Windows Server	Microsoft SQL Server	Microsoft Exchange Server	SharePoint Team Services	Не потрібно
Орган виконавчої влади	Microsoft Windows Server з Active Directory	Microsoft SQL Server	Microsoft Exchange Server	SharePoint Portal Server та SharePoint Team Services	Microsoft BizTalk Server
Центральний орган виконавчої влади (з урахуванням географічно або територіально рознесених структурних підрозділів)	Microsoft Windows Server	Microsoft SQL Server	Microsoft Exchange Server	SharePoint Portal Server	Microsoft BizTalk Server Enterprise Edition

Складові засоби систем захисту інформації

Для Інтернету було впроваджено рекомендації Дослідницької групи IETF з питань конфіденційності та безпеки (PSRG). Ці рекомендації передбачають введення комплексної відповідності між мережевими інформаційними службами та існуючими службами та механізмами безпеки. Ця відповідність, перш за все, стосується забезпечення сумісності окремих реалізацій служб у багатопротокольному глобальному середовищі Інтернету.

Цей метод передбачає визначення вимог безпеки, пов'язаних з кожною програмою, та служб і протоколів, необхідних для досягнення цих вимог. Основною метою та перевагою цього підходу є забезпечення сумісності різних реалізацій додатків в Інтернеті, що дозволяє використовувати продукти різних компаній.

Набір інструментів безпеки (SSP) – це сукупність програмного та апаратного забезпечення, що сприяє реалізації політик безпеки.

SSP в AS класу 2 повинен мати такі функції: - брандмауер;

- систему виявлення атак (як компонент системи антивірусного захисту, систему виявлення атак на рівні мережі, систему виявлення атак на рівні вузла);

- систему виявлення вразливостей (сканер);

- інструменти обробки інформації для криптоаналізу були включені до віртуальних приватних мереж.

Відокремте повноваження користувача від консолі адміністратора.

Ми зосередимося на захисті від порушників NSD, обговоримо брандмауери, віртуальні мережі, захищені протоколом, та загальний захист.

Брандмауер або мережевий екран – це набір апаратних або програмних компонентів, які регулюють та пропускають через мережу на різних рівнях моделі OSI, дотримуючись визначених правил. Основне призначення мережевого екрана – захистити комп’ютерні мережі або окремі гілки від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їхня основна функція полягає в тому, щоб не розпізнавати (фільтрувати) пакети, які не відповідають специфікаціям, зазначеним у конфігурації.

Інші брандмауери також мають можливості трансляції адрес – можливість динамічно змінювати внутрішні адреси або порти на зовнішні адреси або порти, що використовуються поза локальною мережею.

Функції мережевих екранів

Виділення пакетів. Це одна з трьох визнаних можливостей брандмауера. У цьому випадку використовуються прості функції (майже як спеціалізований маршрутизатор), метою яких є перевірка верхньої частини заголовка кожного пакета та забезпечення правильності IP-адреси та порту. Наприклад, пакет, який надсилається в Інтернет, має локальну адресу призначення, але блокується. Ця функціональність присутня у всіх сучасних брандмауерах і характеризується високою швидкістю та відсутністю необхідності взаємодії з користувачем.

Відбір пакетів. Це друга за популярністю функція. Різниця між проксі-сервером і фільтром пакетів полягає в тому, що останній вимагає, щоб усі сеанси зв'язку проводилися через нього, а не безпосередньо. Отримавши дані, проксі-сервер передає їх на потрібний комп'ютер у внутрішній мережі, а отримавши відповідь, він передає їх на потрібний комп'ютер у зовнішній мережі. Як загальновідомо, продуктивність не така висока, як при фільтрації пакетів, але все ж достатня, оскільки змінюється лише заголовок пакета. Основна перевага проксі-сервера полягає в тому, що він замінює реальні адреси ваших комп'ютерів своїми власними. Це виключає можливість цільового доступу до конкретного комп'ютера в підмережі.

Сервер, який застосовує проксі. Це третя роль. Цей тип проксі-сервера вирізняється тим, що він знає протоколи, пов'язані з передачею даних. Гарними прикладами цього типу серверів є поштові сервери. Проксі-сервер додатків може розпізнавати користувачів і покладатися на IP-адресу лише в деяких випадках, це можливо через передачу вірусів та іншого шкідливого програмного забезпечення. Зазвичай це вимагає додаткової обчислювальної потужності, а в більшості випадків вимагає значної реструктуризації робочих станцій, що призводить до втрати прозорості роботи брандмауера.

Буферизація даних. Це не є традиційною функцією брандмауерів, але зараз її використовують багато популярних додатків. Концепція полягає в тому, що всі дані проходять через брандмауер, він може зберігати найпопулярнішу інформацію, а коли до неї згодом звертаються, вона видається з кешу.

Статистика та сповіщення. Однією з унікальних властивостей брандмауера є зберігання історії кожного мережевого підключення, а також розсилка повідомлень про атаки на мережу або комп'ютер. Історія підключень допомагає правильно налаштувати брандмауер для запобігання комп'ютерним атакам, дозволяючи при цьому авторизованим користувачам отримувати доступ до комп'ютера.

Керування. Для персональних брандмауерів основною властивістю є простота їх налаштування. Брандмауери переважно контролюються з віддаленого місця (через інтерфейс на основі HTML або інший), що вимагає певн ого ступеня впевненості в надійності авторизації та каналу зв'язку.

Адміністративні заходи захисту

Неможливо належним чином захистити будь-яку комп'ютерну систему виключно за допомогою програмного чи апаратного забезпечення. Вплив цих інструментів має бути посилений адміністративними засобами захисту. Це також стосується операційної системи в цілому. Для забезпечення надійного та ефективного захисту системи недостатньо лише програмних та апаратних засобів захисту (частин КПК); також слід вживати додаткових адміністративних заходів, без яких жоден програмний чи апаратний захист не буде ефективним.

Під системою адміністрування ми розглянемо весь набір програмного забезпечення та організаційної допомоги для нагляду та контролю системи в цілому. В інших випадках система адміністрування включатиме додаткове спеціальне обладнання, таке як електронні ключі захисту.

Зі зростанням ефективності установи та збільшенням кількості електронних документів, якими керують, стає очевидною складна проблема організації інструментів адміністрування. Адміністрування SEDO саме по собі є складним і має більші труднощі зі збільшенням розміру установи, і чим різноманітніше програмне та апаратне забезпечення, що використовується в ній, тим складніше її обслуговувати. Крім того, якщо установа велика та займає значну територію або має кілька філій, які використовують комп'ютери з різними операційними системами, різними типами документів та протоколами передачі даних, тоді завдання адміністрування стає досить складним. Вибір найбільш

підходящої системи адміністрування з розширеними службами управління та аналітичними можливостями стає особливо актуальним.

Система адміністрування зазвичай виконує такі функції. Розподіл нових користувачів на нові завдання, створення для них каталогів (довідників).

Керування ресурсами та визначення пріоритету та прав доступу.

Управління конфігурацією системи, яке включає наступне: створення середовища, що підходить для нового програмного та апаратного забезпечення, підключення нового апаратного та програмного забезпечення до системи, створення виділеної мережі для корпорації, прив'язка певних завдань до певних серверів та налаштування середовища.

Адміністрування захищеної системи включає: збір даних від служб інформаційної безпеки, контроль доступу користувачів та забезпечення безпеки від зовнішніх атак.

Зменшення кількості системних помилок та збоїв, включаючи процес пошуку, виявлення, локалізації та усунення помилок у роботі системи, моніторинг роботи системи та реєстрацію аварійних ситуацій, планування режиму резервного копіювання інформації, забезпечення швидкого відновлення системи після збоїв.

Облік роботи користувачів, підсистем та завдань додатків, включаючи реєстрацію часу, витраченого на використання комп'ютера, та обсягу використаного простору, облік ліцензій на програмне забезпечення та набутих знань, все це включено до цього типу обліку.

Вимірювання продуктивності системи включає збір та аналіз роботи системи, оцінку ефективності використання системних ресурсів та визначення найважливіших компонентів. Ці компоненти потім втрачаються в продуктивності, і складаються плани щодо їх відновлення. Ці компоненти також важливі для розширення та розвитку функціональних можливостей системи.

Для виконання завдання система адміністрування повинна мати такі компоненти:

Інтерфейс адміністратора дозволяє отримати доступ до всієї інформації щодо системи, включаючи її поточний стан, конфігурацію її робочих параметрів, доступ до файлів конфігурації та файлів журналів, а також збір системної статистики.

Інтелектуальні агенти, вбудовані в кожну частину системи, включаючи систему управління, збирають інформацію безпосередньо на відповідних серверах і, за необхідності, можуть змінювати поточні параметри окремих компонентів.

Інструменти для збору інформації щодо роботи системи, ці інструменти опитують інтелектуальних агентів і передають отриману від них інформацію системному адміністратору.

Високорозвинений метод представлення інформації щодо всієї системи та її окремих компонентів.

Оскільки SEDO має як корпоративну мережу, так і численні бази знань і баз даних, адміністративна система повинна мати як можливості управління мережею, так і можливості адміністратора бази даних. Під час проектування SEDO адміністративна система повинна бути природно інтегрована в організаційну структуру SEDO та мати тісний зв'язок із системою безпеки.

Щодо адміністративних дій, спрямованих на захист ОС, визнаються такі основні типи:

Постійне спостереження за належною роботою ОС (зокрема її підсистем захисту). Для повного контролю необхідно вжити таких заходів:

- запис подій у системі;

- Управління цілісністю файлів, зокрема тих, що містять програмний код для ОС. компоненти, є особливо важливим.

- перевірка належного функціонування компонентів ОС.

Усі ці заходи неможливі без наявності спеціалізованих частин системи безпеки ОС, які виконують необхідні функції.

Організація та підтримка комплексної політики безпеки. Політика безпеки, що використовується в операційній системі, фактично відповідає за:

- користувачів, які мають дозвіл, та компоненти ОС, до яких вони мають доступ;

- які користувачі мають дозвіл на доступ та які об'єкти ОС контролює (наприклад, зовнішні носії, пристрої введення та дисковий простір);

- як користувачі ОС розпізнають себе та що вимагається від їхніх прав доступу;

- які інциденти необхідно документувати в системних журналах.

Політику безпеки необхідно часто переглядати через зміни в конфігурації ОС, налаштування встановлених програм, спроби злочинців обійти захист ОС, поточні небезпеки (епідемії шкідливих вірусів).

Інструкція для користувача. Окрім суто технічних питань щодо роботи ОС, користувачі повинні усвідомлювати необхідність дотримання протоколів безпеки під час використання ОС. Також важливим у процесі моніторингу є компонент дотримання цих протоколів.

Створення замінників. Постійне створення та підтримка копій програм і даних ОС дозволяє відновлювати ОС після збоїв та виходу з ладу компонентів системи з мінімальними втратами.

Постійний огляд змін у конфігураційних даних та політиці безпеки операційної системи. Фактично, йдеться про спостереження за розташуванням засобів безпеки.

інших компонентів операційної системи. Ця інформація є частиною технологічних знань СРР, які, безсумнівно, захищені. Зміни в цій інформації вказують ОС на те, що засоби захисту повинні змінити свою стратегію безпеки. Якщо система реєстрації подій налаштована належним чином, цей тип змін не можна пропустити. Однак, злочинець часто намагається «замести сліди», знищуючи пов’язані записи журналів технологічних змін. Як наслідок, важливо постійно відстежувати зміни в системі. Крім того, необхідно організувати метод автоматичного сповіщення адміністраторів про суттєві зміни в системі з точки зору безпеки, а також використовувати спеціальний метод зберігання даних, стійкий до пошкодження. система (наприклад, дзеркальне відображення журналів на інші комп’ютери або запис важливих подій на принтер).

1.6 Висновки по розділу

1. Перша частина кваліфікаційного завдання присвячена розпізнаванню властивостей та складності впровадження SEDO в корпоративну мережу.

2. Розкрито атрибути функціональних можливостей систем електронного документообігу.

3. Описано модель застосування та функції і обов'язки електронного підпису.

4. Описано загальну архітектуру типової системи електронного документообігу та визначено причини її прийняття.

Розділ 2
АНАЛІЗ КАНАЛІВ НЕСАНКЦІОНОВАНОГО ВИТОКУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Класифікація та розподіл інформації, що циркулює в центрі електронного документообігу корпоративної мережі

Інформація – будь-які розвідувальні дані або дані, які можуть зберігатися на фізичних носіях або відображатися електронними засобами [1]. Залежно від теми, інформація поділяється на різні типи:

– особисті дані особи;

– інформація, яка переважно базується на дослідженнях і має енциклопедичний характер;

– екологічна інформація щодо стану навколишнього середовища (екологічна інформація); – інформація щодо продукту (роботи, послуги);

– науково-технічні знання; – таксономічна інформація;

– формальні правила;

– статистичні дані; – соціологічні дані; – інші види інформації [1].

Однак для практичного застосування більш важлива класифікація інформації за порядком доступу до неї. Це відповідає цьому.

Інформація складається з: доступної та інформації з обмеженим доступом (рис. 1) [1]. Відкритість – доступною є будь-яка інформація, крім тієї, що є секретною.

За законом, інформація вважається такою, що має обмежений доступ. Основними ознаками відкритої інформації є те, що вона доступна кожному, хто бажає отримати до неї доступ, і будь-які обмеження права на отримання відкритої інформації заборонені.

Способи забезпечення доступу до відкритої інформації.

– її планове включення до офіційних письмових праць.

(бюлетені, збірники);

– її передача через загальновживані носії;

– її безпосереднє поширення серед зацікавлених сторін, включаючи державні органи та юридичні особи.

Рис. 2.1 Спосіб отримання інформації

Інформація, яка оприлюднюється публічно, вважається відкритою інформацією.

Відповідно до закону, а також секретна інформація, яка є власністю держави, або необхідність захисту цієї інформації встановлена законом [2].

Секретна інформація класифікується як вид інформації, що включає інформацію щодо оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та правоохоронної діяльності, інформація підлягає державному захисту та визнається такою. Інформація, яка вважається державною таємницею, поділяється на різні категорії.

Відповідно до Закону України "Про державну таємницю" [2].

Конфіденційна інформація – це інформація, яка належить, використовується або знищується фізичними чи юридичними особами та надається на їх запит відповідно до умов, визначених ними. Щодо інформації, що належить державі та використовується державними органами або органами місцевого самоврядування, підприємствами, установами та організаціями всіх типів, може виникнути необхідність обмеження доступу відповідно до закону – статус конфіденційності [2].

Відповідно до Закону «Про захист інформації в інформаційно-телекомунікаційних системах», під захистом у системі вважаються:

- Відкритість інформації, що є власністю держави та, згідно з визначенням Закону України «Про інформацію», пов'язана зі статистичною, правовою та соціологічною інформацією.

інформація, інформація довідкового та енциклопедичного характеру, яка використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація щодо діяльності цих органів, яка опублікована в Інтернеті, інших глобальних інформаційних мережах та системах або передається через телекомунікаційні мережі (далі – відкрита інформація).

- інформація, що є приватною та належить державі або яка підлягає захисту законом, включаючи інформацію про особу (далі - конфіденційна інформація);

Інформація, яка вважається таємною законом (або яка призначена для збереження в таємниці) [2].

Інформація повинна бути відкритою під час процесу обробки, що досягається шляхом її захисту від несанкціонованих змін, які можуть призвести до її випадкового або навмисного знищення чи модифікації. Усі користувачі повинні мати доступ до ознайомчих ресурсів, необхідних для розуміння відкритої інформації. Тільки ідентифіковані та офіційно затверджені користувачі мають право користуватися системою.

Відповідні повноваження [2] можуть змінювати або знищувати загальнодоступну інформацію.

Під час роботи з конфіденційною та секретною інформацією вкрай важливо забезпечити її захист від несанкціонованого доступу, зміни, знищення, копіювання та розповсюдження.

Заклади інформаційної діяльності несуть відповідальність за всі дії, пов'язані з обробкою інформації з обмеженим доступом. Згідно з визначенням, об'єктом інформації є будівля, приміщення, транспортний засіб або інша споруда, яка є технічною та функціональною та має обмежений доступ до інформації. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави.

Обробка IZOD на інформаційних об'єктах сприяє досягненню інформаційної безпеки, яка забезпечується за допомогою таких критеріїв:

Цілісність – це властивість інформації, яка має бути захищена від несанкціонованого знищення або зміна.

- секретність - властивість інформації, яка має бути захищена від несанкціонованого доступу.

- доступність - властивість інформації, яка має бути захищена від несанкціонованого доступу [2].

Для виконання інформаційних потреб державні органи, органи місцевого та регіонального самоврядування створюють інформаційні служби, системи, мережі, банки даних та бази даних. Процес їх створення, склад, права та обов'язки делегуються Кабінету Міністрів України або іншим державним посадовцям, а також місцевим та регіональним органам влади.

Основними видами інформаційної діяльності є отримання, використання, зберігання та поширення інформації.

Отримання інформації - це процес отримання та зберігання документованої або публічно розкритої інформації.

Інформації від громадян, юридичних осіб або держави відповідно до чинного законодавства України [1].

Використання інформації - це виконання інформаційних потреб громадян, юридичних осіб та держави. Поширення інформації - це передача, публікація та впровадження формальної або юридичної інформації, яка

документована або оголошується публічно. Це здійснюється відповідно до процедури, визначеної законом.

Зберігання інформації відповідає за підтримку належного стану інформації та пов'язаних з нею носіїв [2].

Отримання, використання, розповсюдження та зберігання документованої інформації або інформації, що публічно оголошується, здійснюється за процедурою, зазначеною в цьому Законі та інших законах щодо інформації. Крім того, можна класифікувати діяльність, що стосується інформаційного забезпечення, - отримання, оцінка, зберігання та обробка даних, пов'язаних з метою прийняття управлінських рішень. Це охоплює різноманітні види діяльності, включаючи виробництво та продаж, обслуговування та вдосконалення виробничого процесу. Інформація щодо якості продукту, вартості продукту, реклами та інших аспектів продукту охоплюється цією категорією.[2].

Будь-яка форма інформаційної діяльності (включаючи інформаційний бізнес) не може відбуватися самостійно. Її учасники (контрагенти): продавець або покупець, роботодавець або працівник, діють у певному середовищі, яке впливає на їхнє становище, і називається середовищем підприємницької діяльності (або підприємництва).

Жодне підприємство не може мати бюджету без плану підприємства. На основі розроблених бюджетів система управління спрямовує різні види підприємницької діяльності, спрямовує діяльність усіх своїх підрозділів, контролює та оцінює ефективність. На початку звітного періоду бюджет є планом, який формалізує очікувані продажі, витрати та інші фінансові операції на наступний період. Наприкінці звітного періоду бюджет функціонує як засіб вимірювання відхилення між отриманими результатами та очікуваними.

Планові значення та змінені більш масштабні види діяльності.

Якщо створення бюджетів та прогнозів базується на одному наборі вхідних даних та оцінках того, скільки доходів буде отримано, скільки коштів буде витрачено та скільки запасів буде підтримуватися, то бюджети будуть

відповідати один одному та утворювати залежну систему. Розумне використання коштів сприятиме більш ефективному використанню технологій для підвищення ефективності підприємства, його стратегії розвитку та інформаційної безпеки всього підприємства, а також його грошових активів.

2.2 Канали витоку інформації, що обробляється технічними засобами електронного документообігу корпоративної мережі

Технічний канал витоку інформації вважається сукупністю джерел інформації, ліній зв'язку (фізичних носіїв), що переносять інформаційний сигнал, сукупністю шумів, що перешкоджають передачі сигналу в лініях зв'язку, та технічними засобами захоплення інформації.

Джерелами інформації можуть бути безпосередньо людські, гучномовці звукових систем, що доповнюються друкованими паперами, радіопередавачами або іншими пристроями.

Сигнали використовуються для передачі інформації. За своєю природою сигнали можуть бути механічними, магнітними, електричними або акустичними. Тобто коливання, як правило, є електричними, магнітними, акустичними та іншими видами коливань (хвилями), інформація міститься у змінах їх параметрів.

Залежно від природи сигналу, він може поширюватися в певному фізичному середовищі. Зазвичай середовищем для поширення є повітря, рідке або тверде тіло. До них належать повітряний простір, будівельні елементи, з'єднувальні лінії та провідні речовини, ґрунт (земля). Звук пов'язаний з кожною фізичною процедурою та присутній на вході до збору інформації.

Методи перехоплення використовуються для отримання та перетворення інформації з метою її отримання.

Технічні терміни, пов'язані з прийомом, обробкою, зберіганням та передачею інформації (ТПЗІ), вважаються технічними термінами, що безпосередньо стосуються конфіденційної інформації. До них належать: електронні обчислювальні машини, автоматичні телефонні станції, що ведуть

таємні переговори, засоби оперативного контролю та гучномовці, що здійснюють таємний зв'язок.

При визначенні технічних засобів витоку інформації ТПЗІ необхідно розглядати як систему, що включає основне обладнання, кінцеві пристрої, з'єднувальні лінії, розподільчі та комутаційні пристрої, джерела живлення та системи заземлення. Інші технічні методи також називаються основним технічним методом (ОПМ).

Поряд з ТПЗІ, у приміщенні розміщуються технологічні засоби та системи, які не беруть участі в обробці персональної інформації, що є конфіденційною, а використовуються разом із ТПЗІ та знаходяться поблизу електромагнітного поля, що створюється ТПЗІ. Ці технічні методи та пристрої називаються допоміжними технічними методами та засобами (ДТЗП). До них належать: технічні методи зв'язку через відкритий телефон, гучномовці, а також системи пожежної безпеки, засоби кондиціонування повітря, електрифікації та електроприлади.

Як засіб передачі інформації, найбільше занепокоєння викликають ДТЗП, що виходять за межі обмеженої зони. Замкнена зона – це територія (або будівля, комплекс приміщень, або доступ), яка виключає необмежене перебування осіб або транспортних засобів, що не мають постійного або одноразового доступу. У зоні контролю повинні бути вжиті технічні та організаційні заходи, що запобігають витоку секретної інформації з неї.

Зона контролю визначається керівництвом організації відповідно до конкретної ситуації на місці розташування об'єкта та технічних можливостей виявлення.

Окрім з'єднувальних ліній ТЗПІ та ДТЗС, поза контрольованою зоною можуть знаходитися дроти та кабелі, які не пов'язані з системою, але проходять через простір, де встановлені технічні компоненти, а також металеві труби, що служать системами опалення, водопостачання та іншими провідними конструкціями. Такі дроти, кабелі та провідні компоненти називаються сторонніми провідниками.

Залежно від фізичної природи походження інформації, а також середовища, в якому вона поширюється та передається, технічні канали інформації можна розділити на електромагнітні, електричні, параметричні та вібраційні.

Інформаційні канали, призначені для витоку електричної енергії.

Інформація про витік електроенергії виникає через:

Генерацію електромагнітного випромінювання через лінії DTZS та зовнішні провідники, що проходять за межі зони контролю;

Успішну передачу інформаційних сигналів, призначених для кіл живлення та заземлення TZPI.

Використання вбудованих пристроїв.

Індукція електромагнітного випромінювання через елемент TZPI залежить від генерації інформаційного сигналу, а також від наявності гальванічного зв'язку між зовнішнім провідником та з'єднувальною лінією TZPI. Величина індукованих сигналів в першу чергу залежить від потужності випромінюваних сигналів, відстані до провідників та довжини загального шляху з'єднувальних ліній TZPI та зовнішніх провідників.

Випадкова антена - це антена DTZS або зовнішнього типу, яка приймає побічне випромінювання з навколишнього середовища.

Змагальні антени зазвичай зосереджені та розкидані. Випадкова антена, яка зосереджена, - це невеликий технічний пристрій.

(наприклад, телефонний апарат). Розсіяна випадкова антена

включають шнури, металеві трубки та інші механічні комунікації. Інформація, що надсилається джерелами живлення, може бути доступна.

Якщо низькочастотний підсилювач має магнітне поле, трансформатор джерела живлення матиме відповідне поле. Крім того, інформаційний сигнал може передаватися через лінію живлення в результаті збільшення середнього споживання струму з амплітудою інформаційного сигналу.

Вторгнення інформації щодо основи лінії. Окрім заземлення електроенергії, різні постачальники електроенергії, що проходять за межі контрольованої зони, мають гальванічний зв'язок із землею. До них належать

нульовий провід ланцюга живлення, екрани, що з'єднують кабелі, труби, що нагрівають та забезпечують водою, металева арматура бетону та інші компоненти. Всі ці провідники, а також заземлювальний пристрій, утворюють розгалужену систему заземлення, через яку може витікати інформація.

Можливість отримання інформації обмежена прямим підключенням до ліній, що з'єднують DTZS та зовнішні провідники, що проходять через приміщення, де встановлені TZPI, а також системою живлення та заземлення.

Захоплення інформації через вбудовані пристрої. Інформація, що обробляється в TZPI, доступна шляхом встановлення вбудованих у них електронних пристроїв моніторингу. Ці пристрої вважаються міні-реплікаторами, випромінювання яких змінюється сигналом з інформацією. Електронні пристрої перехоплення інформації, встановлені в TZPI, іноді називають апаратними закладками. Інформація, що збирається за допомогою вбудованих пристроїв, передається по радіоканалу або спочатку записується на пристрій зберігання даних, а потім передається до місця призначення.

2.3 Несанкціонований доступ до інформації, що обробляється засобами обчислювальної техніки центру електронного документообігу корпоративної мережі

Загалом, програмне забезпечення комп'ютера складається з компоненти системи такі: операційна система, мережеве програмне забезпечення та система керування базами даних (СКБД). Як наслідок, усі спроби злому комп'ютерної безпеки можна класифікувати на три категорії:

Атаки системного рівня, що діють на операційну систему;

Мережеві атаки, спрямовані на програмне забезпечення, що використовується для керування базами даних.

Захист СКБД є одним з найпростіших завдань. Це зумовлено тим, що СКБД мають певний внутрішній склад, а операції над компонентами СКБД чітко визначені. Як правило, несанкціонований доступ здійснюється шляхом

обходу захисту комп'ютерної системи на рівні операційної системи, що дозволяє отримувати доступ до файлів СКБД через операційну систему.

Однак СКБД, яка не має достатніх механізмів захисту, ймовірно, буде подолана захистом на рівні СКБД:

викрадення пароля;

моніторинг активності жорстких дисків на комп'ютері;

збір сміття (якщо система дозволяє відтворювати раніше видалені об'єкти);

зловживання владою (нерівність у програмному забезпеченні або в адмініструванні операційної системи);

відмова в обслуговуванні (мета NDS – частково або повністю блокувати операційну систему).

Насильницькі атаки на програмному рівні мережі.

Програмне забезпечення для мережевого зв'язку є найбільш вразливим, оскільки шлях, по якому воно передає дані, є вразливим.

Повідомлення часто не захищене, і будь-хто, хто може його отримати, також може це зробити.

Доступ до цього каналу, відповідно, може зупиняти повідомлення та доставляти їх власну версію.

Як результат, на програмному рівні мережевого програмування доступні такі методи:

прослуховування адреси локальної мережі; захоплення повідомлень на маршрутизаторі; створення фальшивого маршрутизатора;

впровадження повідомлень (надсилаючи повідомлення до мережі з неправильною зворотною адресою, зловмисник змінює вже встановлені з'єднання з його комп'ютером, і в результаті отримує авторизацію).

відмова в обслуговуванні (під час надсилання певного типу повідомлення до мережі комп'ютери, підключені до мережі, повністю або частково не можуть цього зробити).

Щоб пом'якшити наслідки зазначених підходів NSD, важливо максимально екранувати канали зв'язку та таким чином ускладнити передачу інформації з мережі неакредитованим користувачам.

2.4 Висновки по розділу

1. Друга частина процесу кваліфікації описує категоризацію та класифікацію інформації.

Розподіл інформації по всьому центру електронного документообігу в корпоративній мережі.

2. Було проведено дослідження методів витоку інформації через технічні засоби електронного документообігу в корпоративній мережі.

3. Було задокументовано методи, що використовуються для доступу до інформації без авторизації.

.

Розділ 3
СТРУКТУРА СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ОБ’ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Призначення, завдання та структура системи електронного документу

Цифровий документ – це електронна версія паперового документа, записана в цифровому форматі та містить всю необхідну інформацію (згідно зі статтею 5 Закону України «Про електронні документи та електронний документообіг»).

Одне з визначень документа полягає в тому, що це фізичний об'єкт, який містить інформацію у фіксованій формі, написаний у звичайному вигляді та має юридичне значення відповідно до чинного законодавства.

Необхідними реквізитами електронного документа є дані, пов'язані з ним, без цих реквізитів документ не може бути зареєстрований та не матиме юридичного значення.

Обов'язкова інформація, пов'язана з електронним документом, також включає його електронний підпис, цей підпис використовується для відрізнення автора від інших суб'єктів, залучених до управління електронними документами. Заключним компонентом створення електронного документа є додавання електронного підпису. Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законодавством. Інші види електронних підписів використовуються в управлінні електронними документами договірним шляхом.

Оригіналом електронного документа вважається цифрова версія документа, яка містить авторитетну інформацію, включаючи цифровий підпис автора. У разі надсилання електронного документа кільком одержувачам або зберігання його на кількох електронних пристроях та носіях, кожна з електронних копій вважається оригіналом електронного документа.

Якщо автор створює цифровий документ та письмову версію, ідентичні за документальною інформацією та реквізитами, кожен з документів вважається оригіналом і має однакову юридичну силу. Оригінал електронного документа повинен мати можливість продемонструвати свою автентичність та цілісність відповідно до вимог закону; у випадках, коли це передбачено законом, документ може бути представлений у візуальному форматі, що включає паперову копію.

Цифрова версія документа, підписана електронним підписом, вважається засвідченою версією документа, як це передбачено законом. Візуальне представлення письмового документа для електронної версії називається копією, це робиться відповідно до процедури, визначеної законом.

Юридична сила електронного документа не ґрунтується виключно на його електронній природі. Можливість визнати електронний документ як доказ не може ґрунтуватися виключно на концепції його електронності.

Електронні документи, які не можуть вважатися оригіналами: 1) документи, що засвідчують право на спадщину.

2) письмовий документ, який є унікальним як такий, за винятком випадків, коли існує централізоване сховище оригіналів електронних документів;

3) інші ситуації, що передбачені законом. Процес нотаріального посвідчення цивільно-правової угоди, створеної електронними засобами (електронні документи), супроводжується процедурою, передбаченою законом.

Електронні документи можуть включати декодований текст, зображення друкованих документів, зображення, згенеровані комп'ютером, аудіо- та відеофайли, що є цифровими. Фактично, це все типи інформації, що зберігаються в цифровій формі.

Електронні документи мають компонент, який вимагає обов'язкових функцій. До них належать функціональність, авторизація та реєстрація.

Функціональність є важливою для документа, це зазначено у вимогах до документа.

Передбачувані наслідки документа (включаючи наступні кроки) оцінюються в контексті існуючих соціальних зв'язків.

Для оприлюднення будь-якого документа необхідний дозвіл, оскільки фізична або юридична особа, яка бере участь у створенні документа, повинна бути уповноважена.

Реєстрація необхідна для кожного документа, оскільки визначено унікальний атрибут документа в групі документів.

Документ вважається таким, що має формальну структуру, що визначено в міжнародних стандартах (ISO, CCITT, ESMA). Були встановлені стандарти щодо проектування архітектури документів, а також передачі, доступу та маніпулювання інформацією. Зараз багато з них втратили своє значення, але все ще корисно розуміти фундаментальні принципи структури, щоб зрозуміти обґрунтування створення електронних документів. Розрізняйте логічну структуру (розділи, посилання, атрибути) та структуру представлення документа (сторінки, рядки, шрифти).

ISO 8879 – це стандарт, який визначає загальний синтаксис мов розмітки, призначених для документів, які можна узагальнити на різних платформах та в різних додатках. Опишіть технології, що використовуються для підготовки, зберігання та передачі електронних записів, наприклад, набір даних, що документує передбачуване значення документів.

SGML надає загальний формат для тегів, що описують документи (наприклад, дані, що впливають на структуру та дизайн документа, але не на його вміст. SGML дозволяє представляти інформацію не як символи на сторінці, а як об'єкти даних. Ця технологія сприяє ефективному зберіганню та повторному використанню інформації, обміну інформацією між користувачами та підтримці інформації в базі даних.

Стандарт мав на меті досягти автономії.

Від структури та представлення документа, щоб забезпечити незалежність від системи форматування; забезпечити можливість обробки документів у кількох функціях; форматувати весь документ, вибирати частини тексту, ключові слова, інформацію про назву, автора та анотації з документа.

При використанні стандартизованої мови документів із загальною розміткою SGML очікується, що текст складається з логічних компонентів, які називаються елементами та документуються в тексті за допомогою розмітки. Як правило, компонент обмежений початковим та кінцевим тегами його елемента. Вкрай важливо, щоб назви тегів та їх структурний склад не були визначені або заздалегідь визначені в стандарті SGML. Довільний текст може бути включений до стандарту через рамки стандарту. Також SGML не має чітко визначеного методу інтерпретації документів; тому в певних випадках для використання SGML необхідний прикладний процесор, який обробляє структуру та вміст документів. Як посередник зазвичай використовується процесор, який перетворює SGML на команди, специфічні для текстового процесора конкретної системи. Використання SGML є корисним:

Під час створення численних документів одного типу продуктивність підвищується.

Під час написання документів, специфічних для певного формату, дотримуються загальних принципів впровадження прийнятих стандартів.

Коли документи часто змінюються протягом тривалого періоду часу, обслуговування спрощується.

Під час роботи над документом, який містить інформацію, яку необхідно обробляти різними способами, можна використовувати весь вихідний файл без необхідності конвертувати його для певного типу обробки, наприклад, не витягувати зображення.

Під час перенесення документів в інші системи конвертація форматів документів спрощується, щоб представити різні частини документа в різних форматах.

Основа стандарту SGML:

Документація для експлуатаційних та ремонтних завдань розробляється у вигляді складних мультимедійних історій, що підтримують процеси технічного обслуговування, ремонту, усунення несправностей тощо.

Спрощується процес обміну електронними документами між компаніями або з клієнтом.

SGML сприяє поширеному методу опису документів. SGML походить від складу документа з трьох окремих компонентів.

Зміст – це фактична інформація, яка представлена в письмовій формі. Зміст включає заголовки, абзаци, списки, таблиці, графіки та аудіоконтент;

• організація (розділи, посилання, права доступу). SGML дозволяє визначити ієрархічний порядок для кожного створеного типу документа. Програми, що використовують SGML як основу, залежать від використання файлу DTD (визначення типу документа). Зміст файлу DTD:

– описує склад вмісту документа так само, як схема бази даних описує різні типи інформації, які підтримує база даних, та способи організації цієї інформації.

– надає основу для компонентів (таких як заголовки розділів та розділів, секції та абзаци), що складають документ.

– встановлює правила щодо зв'язків між компонентами, наприклад: «заголовок розділу має бути першим компонентом після початку розділу» або «кожен список має містити щонайменше два абзаци». Ці правила, перелічені в DTD, служать для сприяння послідовній логічній композиції.

– знаходиться з документом за кожної можливості. «Екземпляр документа» – це певний документ, який слідує за певним DTD.

Стилізація.

Також важливо знати, що відомий стандарт HTML є підмножиною SGML. Як результат, будь-яке програмне забезпечення, яке підтримує HTML, вважається персональною реалізацією SGML.

Ще один поширений стандарт, ISO 8613 (частини 1-6) – Архітектура офісних документів (ODA) та формат обміну (ODIF), призначений для передачі та представлення документів, що стосуються офісної роботи – форм, рахунків-фактур, транскриптів, звітів тощо.

ODA має дві основні функції. По-перше, це метод опису електронного представлення документа, включаючи всю інформацію, що міститься в ньому (текст, лінії та графіки, таблиці). Цей формальний опис архітектури документа називається його архітектурою документа. Крім того, це засіб представлення

вмісту попередньо розробленої інформації у формі, зручній для автоматизації зв'язку між текстовими процесорами, комп'ютерами, принтерами та іншою структурованою інформацією. Кодування даних ODA між цими пристроями здійснюється у послідовному форматі ODF, що є корисним для цілей комунікації. Зокрема, використовується стандартний синтаксис, що використовується в архітектурі OSI.

Формальна структура ODA. В описі документа згідно з протоколом ODA розпізнаються такі категорії структурних документів: логічна структура, склад вмісту.

Метою логічної структури є представлення будь-якої довільної форми організації інформації, яка є ієрархічною. Наприклад, категоризація документів, додавання таблиць та рисунків до тексту. Крім того, стандарт ODA не містить конкретної термінології, але натомість надає засоби для опису різних типів організації інформації.

Структура форматування використовується для опису методу розміщення документа на фізичному носії. Очевидними є такі ідеї:

кластери сторінок, пов'язані між собою та представляють різні частини документа.

окремі блоки та сторінки, розташовані на сторінках;

таблиці, графіки або тексти в блоках. Зміст – це фактичні знання про документ: текст, ілюстрації тощо. Стандарт ISO 8613 класифікує контент на три типи: символічний текст, растрова графіка та геометрична графіка. Коли це можливо, для опису контенту використовуються існуючі стандарти.

Для церемоніальних текстів це стандарт ISO 6937. Геометрична та растрова графіка походить зі стандарту ISO 8632 та пропозицій SSITT T.6.

Мета SEDO та основні обов'язки.

Управління електронними документами включає: створення документів, їх обробку, передачу, зберігання та відображення інформації, що поширюється в організації чи бізнесі, все це здійснюється через комп'ютерні мережі. Електронне управління документами зазвичай розглядається як організація

руху документів між різними частинами організації чи підприємства, а також між різними групами користувачів чи окремих осіб. У цьому випадку рух документів пов'язаний не з їх фізичним переміщенням, а з передачею прав на їх використання з конкретним повідомленням конкретних користувачів та контролем за їх виконанням.

В результаті прийнято ідею системи електронного управління документами (СЕД); ця система спрощує процес створення, управління, доступу та розповсюдження великої кількості документів у комп'ютерних мережах, а також забезпечує контроль над потоком документів в організації. Часто ці документи зберігаються у спеціальному сховищі або в ієрархії файлової системи. Поширені типи файлів, які зазвичай підтримують СЕД, включають: текстові документи, зображення, електронні таблиці, аудіо, відео та веб-документи. Загальні можливості СЕД включають: створення документів, контроль доступу, перетворення даних та їх захист. Системи електронного управління документами (СЕД) спрощують процедуру створення, управління доступом та розповсюдження великої кількості документів у комп'ютерних мережах, крім того, вони забезпечують контроль над потоком документів в організації.

СЕД призначена для автоматизації всієї процедури отримання документів як від цієї установи, так і від інших:

Основна мета СЕД полягає в спрощенні зберігання електронних документів, а також у співпраці з ними (насамперед, у пошуку документів за атрибутами, а також шляхом порівняння з іншими документами).

(за змістом). СЕД повинна автоматично відстежувати зміни в документах, терміни виконання документів, переміщення документів та контролювати всі версії та підверсії. Повноцінна СЕД повинна включати весь цикл управління діловодством в організації чи на підприємстві – від створення завдання до написання документа та його зберігання в архіві, а також забезпечувати централізоване місцезнаходження документів у будь-якому форматі, включаючи складні документи, що складаються з кількох частин. СЕД повинна об'єднувати віддалені джерела документів різних компаній в єдину систему.

Вони повинні пропонувати гнучку систему управління документами, яка є одночасно суворою та безпомилковою. У SEDO має бути впроваджено точне визначення того, як обмежується доступ користувачів до різних документів на основі їхньої спроможності, посади та призначених повноважень. Крім того, SEDO має бути адаптована до існуючого організаційного та штатного складу, а також системи управління діловодством на підприємстві, а також повинна інтегруватися з існуючими корпоративними системами.

Електронне управління документами передбачає процедуру створення, обробки, передачі та зберігання документів через комп'ютерні мережі, пов'язані зі структурою підприємства та з'єднані через корпоративні мережі.

Електронне управління документами передбачає організацію передачі документів між різними організаціями або окремими особами.

Основними користувачами SEDO є великі організації, що перебувають у державній власності, банки, великі промислові організації та всі інші організації, які мають значну кількість створених, оброблених та збережених документів.

Під час реалізації SEDO у практиці установи досягаються такі цілі:

підвищення продуктивності праці;

підвищення ефективності обробки документів;

Збільшення потужності довідково-інформаційних служб, покращення якості підготовки, обробки та відтворення документів, а також зменшення кількості непотрібних документів та комунікацій, що має на меті підвищити ефективність організації та зменшити витрати на її ведення. Основними обов'язками SEDO є:

Створення документів та їх упорядкування;

– розміщення їх у сховищі даних установи та надання користувачам способів доступу до документів в інтерактивному режимі;

Управління доступом відповідно до наданих прав доступу до даних.

Забезпечення безпеки інформації, що використовується в SEDO.

Аналіз документованих систем та практичний досвід у цій галузі свідчить про те, що до найважливіших методологічних складових створення системи електронного документообігу належать:

1. Структурування документаційного забезпечення (процес підходу).

2. Поетапне впровадження системи документообігу (перетворення середніх виконавців на достатньо хороших).

3. Повне охоплення обов'язків документаційного забезпечення та організація зберігання документації (повна автоматизація).

4. Вибір інструментів для впровадження (комплекси промислового програмного забезпечення).

3.2. Функціональна модель СЕДО

Система електронного документообігу (СЕД) використовує об'єктно-орієнтований підхід до управління документами, що означає, що будь-який документ у системі вважається об'єктом. Зокрема, електронний документ та його складові частини, такі як контент або певні деталі, також вважаються об'єктами.

Функціональна модель СЕД включає функціональні об'єкти та зв'язки між ними (рис. 3.1)

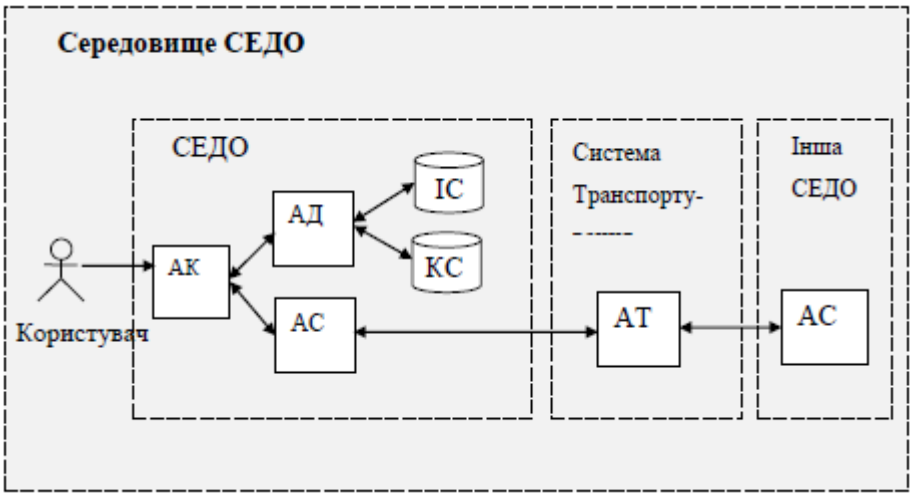


Рисунок 3.1. Функціональна модель СЕД

Функціональні об'єкти поділяються на первинні, вторинні та третинні типи. Функціональні об'єкти, які є первинними, включають СЕД та її аналог.

СЕД та користувачі складають електронне середовище для управління документами, це середовище зазвичай складається з невизначеної кількості користувачів та СЕД, які пов'язані один з одним.

Функціональні об'єкти, які є вторинними, включають агента користувача AK , агента доступу AD , інформаційні сховища (окремі IS) та колективну CS , а також агента спряження AS .

Третинними функціональними об'єктами є транспортні агенти, призначені для AT.

На концептуальному рівні об'єкти S EDO поділяються на два класи: інформаційні об'єкти та функціональні об'єкти (рис. 2.2). Функціональні об'єкти включають агентів, сховища інформації, робочі станції та сервери. Інформаційні об'єкти включають цифрові документи, запити та звіти.

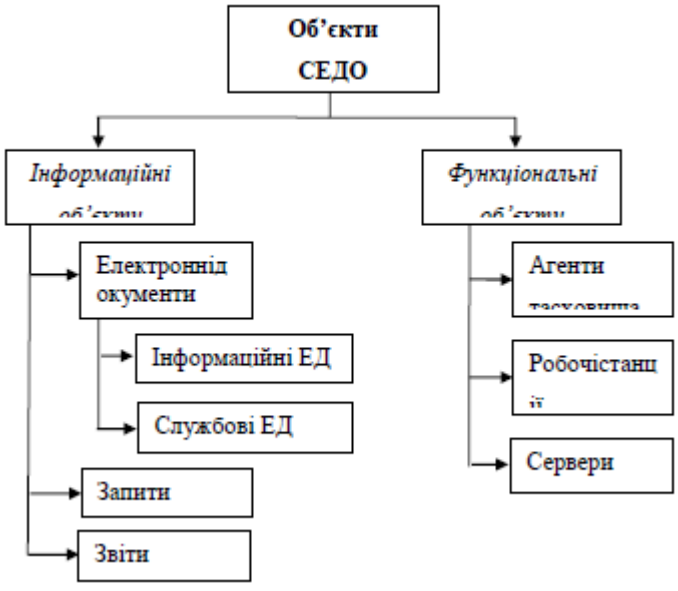


Рисунок 3.2. Інформаційні та практичні об'єкти S EDO

Операції, які автоматизовані або передбачають участь людини, є частиною життєвого циклу ЕД (рис. 2.3).

Життєвий цикл складається з кроків, які далі поділяються на процеси, а ці процеси потім далі поділяються на операції.

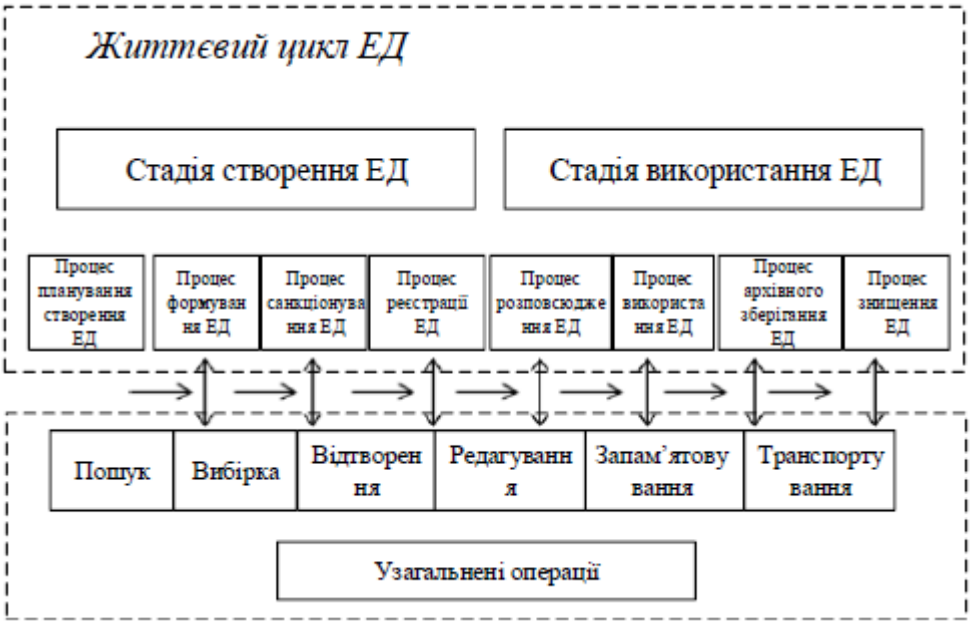


Рисунок 2.3. Життєвий цикл ЕД та комплексні операції

Опис функціональних цілей S ED O

Функціональні об'єкти, що є S ED O, включають агентів, збирачі інформації, станції та сервери.

Склад функціональних об'єктів у S ED O показано на рис. 2.4.

Процедури, що використовуються на ЕД протягом кожної фази життєвого циклу, виконуються за допомогою операцій.

Операції виконуються агентами автоматично або маніпулюються користувачем S ED O.

Агенти S ED O включають: агент користувача (U A), окремі сховища інформації, агент транспорту (TA), агент доступу (AA) та агент сполучення (CA).

Агенти користувача призначені для маніпулювання інформаційними об'єктами S ED O. U A надає послуги, які дозволяють користувачеві створювати та відтворювати інформаційні об'єкти з S ED O.

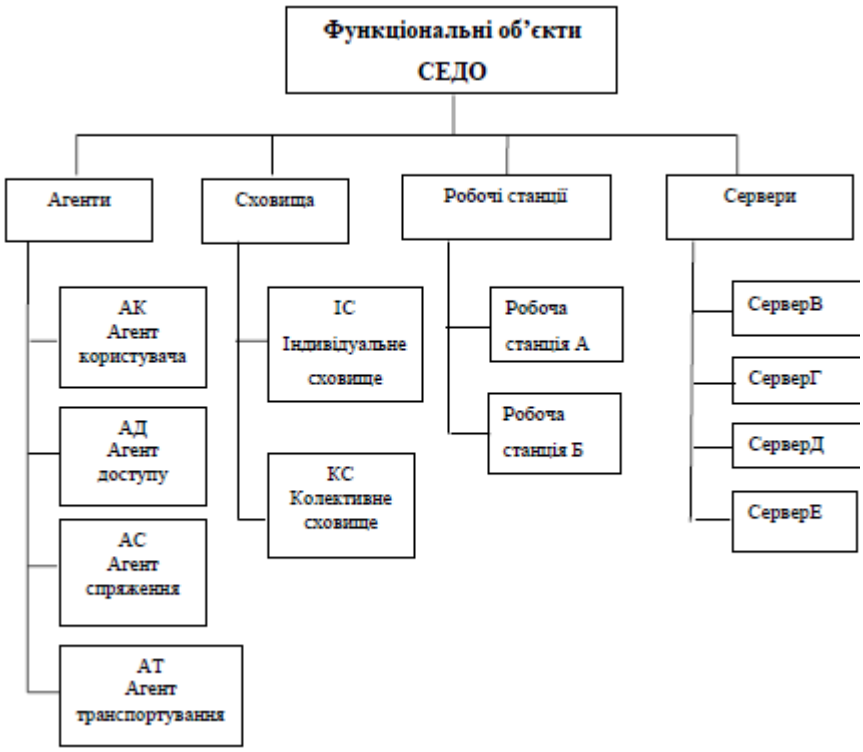


Рисунок 2.4. Функціональні об'єкти з S EDO

Операції виконуються агентами автоматично або маніпулюються користувачем S EDO.

Агенти S EDO включають: агент користувача (UA), окремі сховища інформації, агент транспорту (TA), агент доступу (AA) та агент сполучення (CA).

Агенти користувача призначені для маніпулювання інформаційними об'єктами S EDO. UA надає послуги, які дозволяють користувачеві створювати та відтворювати інформаційні об'єкти з S EDO.

Користувачам дозволено використовувати S EDO лише через UA. Взаємодія між AC та користувачем здійснюється через клавіатури, сканери, принтери, відеокамери, пристрої введення та генератори голосу тощо.

AC мають пряме або опосередковане підключення до інформаційних сховищ.

Система транспортування ED (S TED) складається з трьох функціональних об'єктів: агентів транспортування, інформаційних процесорів та комунікаційних шин. AT призначені для транспортування інформації, пов'язаної з S EDO, та з'єднання різних S EDO.

АТ сприяють маршрутизації та комутації інформаційних об'єктів, пов'язаних з S EDO. Щоб забезпечити зв'язок із зовнішнім S EDO, транспортні агенти також можуть брати участь у координації протоколів щодо транспортування (функції, що є шлюзом).

Діапазон ділових можливостей (AD) призначений для сприяння віддаленому зв'язку між парами додаткових функціональних об'єктів, таких як агенти та сховища.

Автономні системи (AS) призначені для поєднання S EDO з іншим програмним забезпеченням для управління документами. AS повинні забезпечувати документування та подання документів відповідно до правил щодо управління документами, це включатиме визначення процедури обробки інформації та її прикріплення до матеріального носія.

Електронним рішенням транспортної системи ED є центр управління документами для електронних записів.

3.3 Центр електронного документообігу

Обмін документами теоретично базується на принципі зірки, а не «кожен з кожним», як це мається на увазі в логічній структурі документа. Центри електронного документообігу (EDMC) мають можливість виконувати такі функції:

- конвертація та узгодження форматів вхідних та вихідних документів;
- підтримка адресних книг та розрахунок маршрутів доставки документів;
- гарантована доставка документів;
- додаткове архівування документів;
- ведення дерева каталогів та його синхронізація з іншими каталогами.

Також центри обміну повідомленнями можуть виконувати роль центрів сертифікації, що сприяють розвитку інфраструктури закритих та відкритих ключів, процедур автентифікації для організацій, що беруть участь в обміні.

Для інтеграції з EDMC корпоративні системи можуть бути за необхідності розширені спеціальними модулями, які взаємодіють з EDMC до конвертації форматів та обміну процедурами між EDMC.

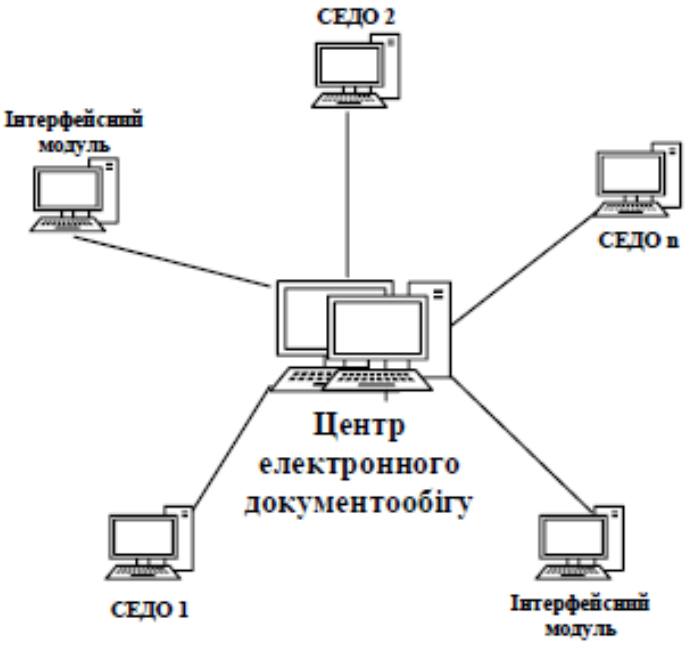


Рис. 2.5. Зв'язок з Центром електронного документообігу (EDMC)

Стандартний та формальний обмін

Одним з основних обов'язків EDMC є забезпечення послідовної передачі документів між різними системами. Найефективніший підхід полягає у створенні універсального розширюваного представлення загальних документів у XML, яке слугуватиме проміжним форматом для всіх підключених систем.

Якщо набір документів, що стосуються підключеної системи, більший, ніж потрібно в універсальному форматі, то формат можна розширити або документи можна відобразити за допомогою механізму тегів, специфічного для конкретних одержувачів.

Перетворення документів у різні формати має враховувати весь набір вхідних даних, пов'язаних з документом. Для документів, які виводяться у форматі XML,необхідно дотримуватися додаткових особливостей - можливості XMLЮ що дозволяють ховатися під "іншими" обкладинками. Інші типи

документів, такі як PowerPoint, мають обмежений набір даних. У цьому випадку можна додати додатковий файл у тому ж форматі, що й одержувач, цей файл міститиме довший або повний опис даних документа.

Окрім вимог до документів, CED повинен забезпечити передачу фактичних файлів документа. У деяких випадках формат документації може бути конвертований (наприклад, документи Microsoft Office у текстове представлення та перекодування під час експорту в системи, що працюють на базі MS DOS, або конвертація в HTML під час експорту в документ).

Забезпечення своєчасного народження дитини

Місія CED зазвичай полягає в тому, щоб сприяти передачі документа стороні, що приймає документ, та отримувати повідомлення про прийняття – квитанцію (передача документа на підпис). У цьому випадку CED може використовувати різні засоби нагадування та сповіщення, включаючи електронну пошту та інші канали.

Усі системи, пов’язані з CED, повинні мати можливість інформувати CED про те, що документ було задокументовано. Це не обов’язково автоматизовано: співробітник офісу може вручну надіслати підтвердження.

Автентифікація та секретність

Найважливішим аспектом організації обміну документами є забезпечення справжності та конфіденційності документів.

Це передбачає створення центрів сертифікації, які проводять діяльність з виробництва відкритих та закритих ключів, зберігання та сертифікації відкритих ключів учасників електронної передачі документів. Програмне забезпечення, що використовується для цього, має бути схвалене, а центр схвалення також є ліцензіатом на...

Дозвіл на проведення діяльності, що є офіційною, видається визнаним державним органом.

Поєднання ЦОД з центрами сертифікації є логічним і практичним, оскільки обидва повинні бути невід'ємними частинами інформаційної інфраструктури між одним колом учасників.

Програмні засоби, що надаються Microsoft, сприяють створенню інфраструктури центру сертифікації на основі вже існуючих модулів (криптопровайдерів), сертифікованих іншими партнерами Microsoft.

Сертифіковані версії електронних підписів повинні бути включені в системи управління документами для компаній або в інтерфейси для існуючих систем.

Архітектура системи Центру управління електронними документами.

Центри ЕД можуть бути реалізовані як єдиний національний центр або як система взаємодіючих центрів різних рівнів.

Технічна можливість створення єдиного національного ЦОД можлива, але нам здається більш доцільним другий варіант, який передбачає розробку системи взаємодіючих ЦОД, що охоплюють територіальний, відомчий та інші рівні. Важливість цього полягає у зменшенні складності адміністрування ЦОД та закритті обсягу значущих документів на "нижчих рівнях" системи.

Хоча організація підприємств зазвичай сприяє ієрархічному стилю, це пов'язано з міркуваннями безпеки та надійності, тому більш гнучка структура є більш доцільною. і може бути кілька способів досягнення документами місця призначення.

Крім того, слід впровадити технологічні та інституційні процедури для зіставлення форматів документів та довідників, а також CED різних рівнів.

Програмне забезпечення

Для організації центру обміну даними між відділами в SEDO було створено його на основі технологій Microsoft. Найбільш природним вибором є використання сервера інтеграції Microsoft BizTalk Server.

Сервер сприяє розпізнаванню та конвертації форматів документів, що надходять або відправляються з різних відділів. Ці документи генеруються різними системами та мають різне призначення. Сервер контролює розподіл документів та забезпечує їх доставку цільовому одержувачу (перевіряючи умови доставки та повторні спроби, а також повідомлення). Крім того, він

надає візуальні методи конвертації документів у різні форми та виконання бізнес-процесів.

Взаємодію між центрами документів, SEDO та інтерфейсними модулями пропонується організувати за допомогою технології веб-сервісів .NET. Технологія веб-сервісів інтегрована та підтримується всіма існуючими програмними платформами, ця технологія дозволяє легко поєднувати різні системи, що надзвичайно важливо для сучасного різноманіття систем автоматизації документообігу.

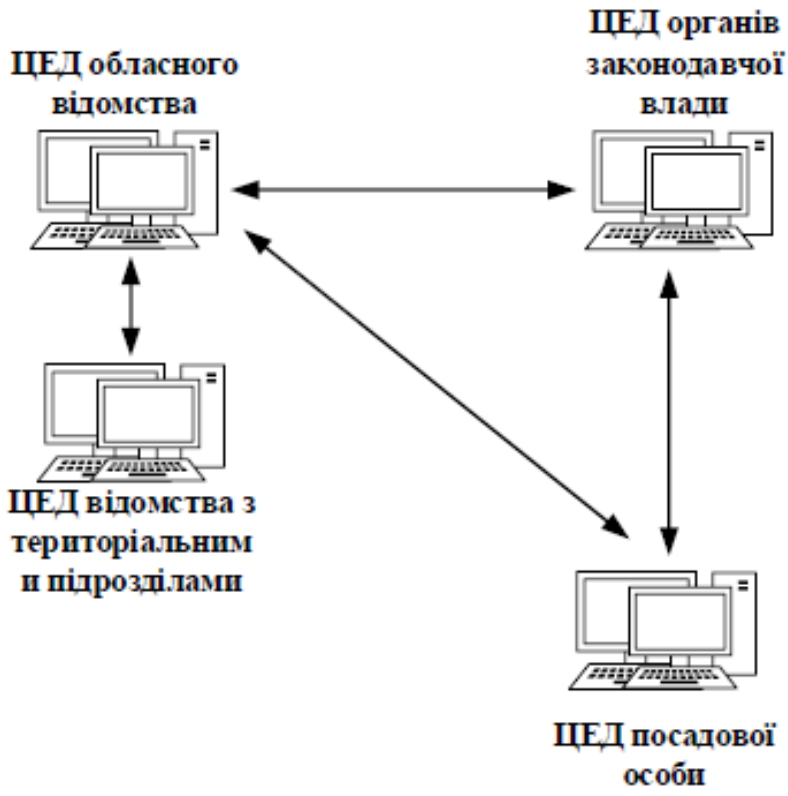


Рисунок 3.6. Ієрархія CED

Для розповсюдження документів та повідомлень найефективнішим вибором є поштовий сервер Microsoft Exchange Server.

Для використання CED без корпоративної системи або за відсутності функціональності інтерфейсних модулів можна використовувати інструменти з пакету Microsoft Office (Outlook), які можна поєднувати з модулями, що забезпечують підготовку необхідних документів, їх авторизацію та перевірку.

Як наслідок, причини впровадження електронного документообігу такі:

Зростання обсягу інформації у всьому світі;

Переваги електронного зберігання документів над паперовими численні.

Нездатність до модернізації та моральна корупція старої програми.

Необхідність автоматизації та оптимізації документообігу відділу очевидна.

Нижче наведено причини, чому необхідно збільшити швидкість обробки документів, а також створення архіву цифрових версій документів:

зростання обсягу інформації у світі;

переваги електронного зберігання документів над фізичним;

застарілість старої системи та несправність нової програми;

необхідність автоматизації та оптимізації управління документами у відділі;

необхідність збільшення швидкості обробки документів; створення цифрового архіву електронних версій документів.

3.4 Висновки по розділу

1. У третій частині роботи було проведено дослідження задань та структура та організація системи електронного документообігу.

2. Було продемонстровано функціональну модель S ED O. Було встановлено обов'язки, організацію та процедуру створення електронних документів.

3. Було розкрито склад та обов'язки центру електронного документообігу.

ВИСНОВКИ

У процесі підготовки кваліфікаційного завдання було визначено такі обов'язки:

- проведено дослідження каналів незаконного обміну інформацією через корпоративну мережу власника інформації.

- вивчено фундаментальні принципи систем електронного документообігу в корпоративних інформаційних мережах;

- досліджено напрямки дослідження та внесено пропозиції щодо вдосконалення системи кібернетичної безпеки центру електронного документообігу конфіденційної інформації корпоративної мережі.

1. У першій частині кваліфікаційного завдання описується класифікація та розподіл інформації щодо потоку документів у центральній частині корпоративної мережі. Було проведено дослідження каналів поширення інформації, що використовуються технічними засобами передачі електронних документів у корпоративній мережі.

Було проведено дослідження процедур несанкціонованого доступу до інформації, що обробляється комп'ютерним обладнанням у центрі електронного документообігу корпоративної мережі.

2. У другій частині кваліфікаційного процесу було проведено дослідження завдання та структури системи електронного документообігу. Наведено функціональний опис S ED O. Встановлено обов'язки, структуру та порядок функціонування системи електронного документообігу.

3. У третій частині кваліфікаційного завдання описано атрибути інтеграції S ED O в корпоративну мережу. Розкрито атрибути функціональних можливостей систем електронного документообігу. Описано модель застосування та пояснено обов'язки електронного підпису. Описано загальну архітектуру типової системи електронного документообігу та визначено причини її прийняття.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009 – 608 с.

3. Матвієнко О., Цивін М. Основи організації електронного документообігу: Навчальний посібник.– К.:Центр учбової літератури, 2008.– 112с.

4. Тарнавький Ю.А., Системи електронного документообігу. – К.: ІПК ДСЗУ, 2007 – 37 с.

5. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009 – 608 с.

6. Хорев А.А. Техническая защита информации. – М.: НПЦ «Аналитика», 2008– 272 с.

7. Закон України"Про електронні документи й електронний документообіг" від 22.05.2003 р. № 851-IV

8.Закон України «Про електронний цифровий підпис» від 22.05.2003

9. Асеєв Г.Г. Електронний документообіг: підр. для студ. – Х.: ХДАК, 000. – 470 с

10. Малюк А.А., Пазизин С.В., Погожин Н.С.Введение в защиту информации в автоматизированных системах. - М: Горячая линия-Телеком, 2004. - 147 с.

11. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003 – 504 с.

12. Антонюк А.О. Основи захисту інформації в автоматизованих системах. – К.: Видавничий дім «Києво-Могилянська академія», 2003. – 244 с.

13. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1453-2004-%EF

14. URL: http://www.morepc.ru/security/sec270303.html

15. URL:http://www.star-force.ru/upload/iblock/73f/T_Comm_june.pdf 16. URL:http://www.microsoft.com/Ukraine/Government/Newsletters/DocFlow

16. Матвієнко О., Цивін М. Основи організації електронного документообігу : навчальний посібник. Київ: Центр учбової літератури, 2008. 112 с. duikt.edu.ua

17. Плескач В. Л., Броварець О. О., Гарко І. І. Інформаційні системи електронного документообігу : навчальний посібник. Київ: Київський університет, 2020. 301 с. ISBN 978-966-933-114-4. irbis-nbuv.gov.ua

18. Шебаніна О. В., Клочан В. П., Клочан І. В. та ін. Електронний документообіг : конспект лекцій. Миколаїв, 2021. dspace.mnau.edu.ua

19. Копняк К. В. Електронний документообіг : опорний конспект лекцій. Вінниця: Видавничо-редакційний відділ ВТЕІ КНТЕУ, 2018. 63 с. dspace.mnau.edu.ua

20. Матвійчук-Юдіна О. В. Впровадження сучасних інформаційних систем документообігу у вищих навчальних закладах. 2014. ena.lpnu.ua

21. Київський національний університет будівництва і архітектури (КНУБА). Комп'ютерне документознавство (змістовний модуль: *«Типова система електронного документообігу. Функціональна архітектура…»*): робоча програма/силабус, 2023–2024 н. р. knuba.edu.ua

22. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. Видання офіційне. Київ: Держспоживстандарт України, 2005. vn.court.gov.ua

23. ДСТУ 3719-8-98. Інформаційні технології. Електронний документообіг. Архітектура службових документів (ODA) та обмінний формат. Частина 8… (ISO 8613-8:1989). Будстандарт Online

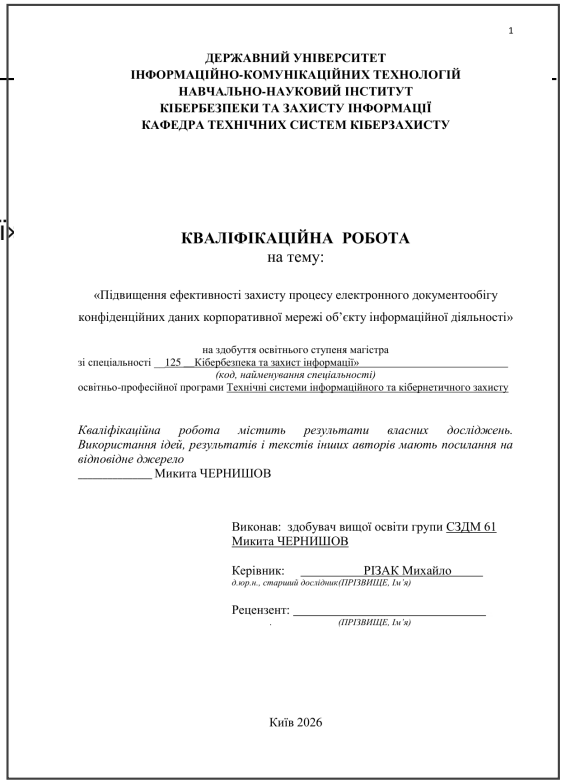
24. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003 № 851-IV (поточна редакція — від 31.12.2023). Законодательство Украины

25. Постанова Кабінету Міністрів України “Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади” від 28.10.2004 № 1453. Законодательство Украины

ДОДАТОК А

Підвищення ефективності захисту процесу електронного документообігу

- Магістерська робота
- Здобувач: Микита Чернишов
- Спеціальність 125 «Кібербезпека та захист інформації»
- Київ, 2026



1

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Підвищення ефективності захисту процесу електронного документообігу конфіденційних даних корпоративної мережі об'єкту інформаційної діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Микита ЧЕРНИШОВ

Виконав: здобувач вищої освіти групи СЗДМ 61
Микита ЧЕРНИШОВ

Керівник: _____РІЗАК Михайло_____
д.юр.н., старший дослідник(ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

Актуальність теми

- Електронний документообіг корпоративної мережі обробляє конфіденційні дані.
- Основні ризики: несанкціонований доступ, модифікація, копіювання та витік інформації.
- Потрібне підвищення ефективності криптографічного захисту процесів обробки даних.

Мета, об’єкт і предмет дослідження

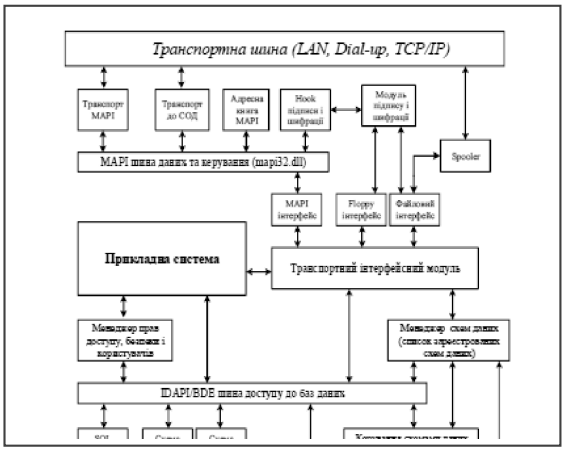
- Мета: підвищення ефективності системи криптографічного захисту процесів обробки конфіденційних даних корпоративної мережі.
- Об’єкт: процес захисту інформації на об’єкті інформаційної діяльності.
- Предмет: система кібернетичного захисту центру електронного документообігу конфіденційних даних.

Завдання магістерської роботи

- Проаналізувати принципи побудови та можливості систем електронного документообігу.
- Провести огляд каналів несанкціонованого витоку інформації через корпоративну мережу.
- Розробити рекомендації щодо удосконалення криптографічного захисту електронного документообігу.

Система електронного документообігу

- СЕДО забезпечує створення, реєстрацію, зберігання, маршрутизацію, контроль версій та доступ до електронних документів.
- Ключові компоненти: сховище документів, сховище атрибутів, повнотекстовий пошук, маршрутизація, контроль доступу.



Функціональні можливості СЕДО

- Масштабованість, розподіленість, модульність та відкритість інтерфейсів.
- Підтримка маршрутизації, workflow-процесів, версійнос аналітичної звітності та інтеграції з іншими системами
- Засоби контролю доступу та криптографічного захисту бути інтегровані в бізнес-процеси.

повідомлень про атаки на мережу або комп'ютер. Історія підключень допомага правильно налаштувати брандмауер для запобігання комп'ютерним атакам дозволяючи при цьому авторизованим користувачам отримувати доступ до комп'ютера.

Керування. Для персональних брандмауерів основною властивістю простота їх налаштування. Брандмауери переважно контролюються віддаленого місця (через інтерфейс на основі HTML або інший), що вимагає пев ого ступеня впевненості в надійності авторизації та каналу зв'язку.

Адміністративні заходи захисту

Неможливо належним чином захистити будь-яку комп'ютерну систем виключно за допомогою програмного чи апаратного забезпечення. Вплив ци інструментів має бути посилений адміністративними засобами захисту. Це також стосується операційної системи в цілому. Для забезпечення надійного т ефективного захисту системи недостатньо лише програмних та апаратни засобів захисту (частин КПК); також слід вживати додаткових адміністративни заходів, без яких жоден програмний чи апаратний захист не буде ефективним.

Під системою адміністрування ми розглянемо весь набір програмного забезпечення та організаційної допомоги для нагляду та контролю системи цілому. В інших випадках система адміністрування включатиме додатков спеціальне обладнання, таке як електронні ключі захисту.

Зі зростанням ефективності установи та збільшенням кількост електронних документів, якими керують, стає очевидною складна проблем організації інструментів адміністрування. Адміністрування SEDO саме по собі складним і має більші труднощі зі збільшенням розміру установи, і чи різноманітніше програмне та апаратне забезпечення, що використовується в ній тим складніше її обслуговувати. Крім того, якщо установа велика та займа

Електронний цифровий підпис

- ЕЦП підтверджує автора електронного документа та цілісність даних.
- Підпис формується закритим ключем і перевіряється відкритим ключем.
- Використання сертифікатів ключів забезпечує юридичну значущість електронних документів.

Кібернетичний захист корпоративної мережі

- Базові механізми: автентифікація, авторизація, журналювання, шифрування, контроль доступу, міжмережевий екран.
- Захист має будуватися як багаторівнева система: робочі станції, сервери, мережеві канали, сервіси та дані.
- Особлива увага приділяється безпечному з’єднанню «клієнт-сервер».

Архітектура типової СЕДО

- Типова архітектура включає підсистеми управління документами, електронного архіву, workflow, публікаці адміністрування та захисту.
- Системи класу EMC Documentum забезпечують центра управління корпоративним контентом.

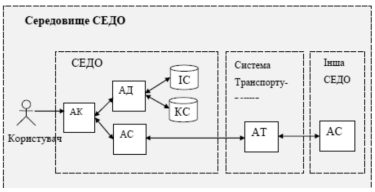
електронного документообігу належать:

1. Структурування документаційного забезпечення (процес підходу).
2. Поетапне впровадження системи документообігу (перетворення середніх виконавців на достатньо хороших).
3. Повне охоплення обов'язків документаційного забезпечення та організація зберігання документації (повна автоматизація).
4. Вибір інструментів для впровадження (комплекси промислового програмного забезпечення).

3.2. Функціональна модель СЕДО

Система електронного документообігу (СЕД) використовує об'єктно орієнтований підхід до управління документами, що означає, що будь-який документ у системі вважається об'єктом. Зокрема, електронний документ та його складові частини, такі як контент або певні деталі, також вважаються об'єктами.

Функціональна модель СЕД включає функціональні об'єкти та зв'язки між ними (рис. 3.1)



Канали витоку інформації

- Технічний канал витоку формується джерелом сигналу, середовищем поширення та засобом перехоплення.
- Основні групи каналів: електромагнітні, електричні, акустичні, параметричні, вібраційні, матеріальні.
- Канали витоку необхідно враховувати під час побудов криптографічного та технічного захисту.

При визначенні технічних засобів витоку інформації ТПЗІ необхідно розглядати як систему, що включає основне обладнання, кінцеві пристрої з'єднувальні лінії, розподільчі та комутаційні пристрої, джерела живлення та системи заземлення. Інші технічні методи також називаються основним технічним методом (ОПМ).

Поряд з ТПЗІ, у приміщенні розміщуються технологічні засоби та системи, які не беруть участі в обробці персональної інформації, що конфіденційною, а використовуються разом із ТПЗІ та знаходяться поблизу електромагнітного поля, що створюється ТПЗІ. Ці технічні методи та пристро називаються допоміжними технічними методами та засобами (ДТЗП). До них належать: технічні методи зв'язку через відкритий телефон, гучномовці, а також системи пожежної безпеки, засоби кондиціонування повітря, електрифікації та електроприлади.

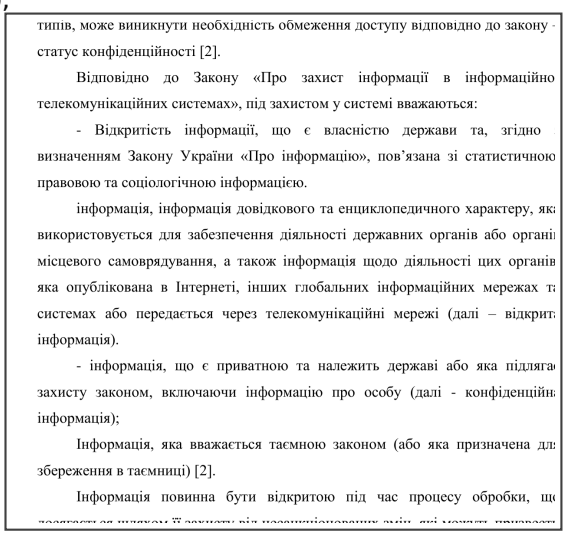
Як засіб передачі інформації, найбільше занепокоєння викликають ДТЗП що виходять за межі обмеженої зони. Замкнена зона – це територія (або будівля, комплекс приміщень, або доступ), яка виключає необмежене перебування осіб або транспортних засобів, що не мають постійного або одноразового доступу. У зоні контролю повинні бути вжиті технічні та організаційні заходи, що запобігають витоку секретної інформації з неї.

Зона контролю визначається керівництвом організації відповідно до конкретної ситуації на місці розташування об'єкта та технічних можливостей виявлення.

Окрім з'єднувальних ліній ТЗПІ та ДТЗП, поза контрольованої зони

Класифікація інформації та режим доступу

- Інформація в корпоративній мережі поділяється на відкриту та інформацію з обмеженим доступом.
- Для конфіденційних даних необхідні механізми захисту від ознайомлення, копіювання, модифікації та знищення.
- Режим доступу визначає вимоги до криптографічного, організаційного і технічного захисту.



типів, може виникнути необхідність обмеження доступу відповідно до закону - статус конфіденційності [2].

Відповідно до Закону «Про захист інформації в інформаційно телекомунікаційних системах», під захистом у системі вважаються:

- Відкритість інформації, що є власністю держави та, згідно визначенням Закону України «Про інформацію», пов'язана зі статистичною правовою та соціологічною інформацією.

інформація, інформація довідкового та енциклопедичного характеру, яка використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація щодо діяльності цих органів яка опублікована в Інтернеті, інших глобальних інформаційних мережах та системах або передається через телекомунікаційні мережі (далі – відкрита інформація).

- інформація, що є приватною та належить державі або яка підлягає захисту законом, включаючи інформацію про особу (далі - конфіденційна інформація);

Інформація, яка вважається таємною законом (або яка призначена для збереження в таємниці) [2].

Інформація повинна бути відкритою під час процесу обробки, що

Несанкціонований доступ до даних

- Загрози включають порушення конфіденційності, цілісності та доступності документів.
- Найбільш небезпечні дії: підбір паролів, компрометація ключів, несанкціоноване копіювання, перехоплення трафіку, зміна документів.
- Протидія має поєднувати криптографічний захист, контроль доступу і моніторинг подій.

Удосконалення криптографічного захисту

- Використання інфраструктури відкритих ключів для керування сертифікатами.
- Шифрування каналів передачі та вибіркове шифрування інформаційних полів документів.
- Регламентація життєвого циклу ключів: генерація, зберігання, використання, відкликання та знищення.

Практичні рекомендації

- Запровадити рольову модель доступу до документів і атрибутів.
- Забезпечити обов’язкове використання ЕЦП для юридично значущих документів.
- Організувати журналювання дій користувачів і регулярний аудит подій безпеки.
- Поєднати криптографічний захист із сегментацією мережі та резервним копіюванням.

Очікуваний ефект

- Підвищення стійкості СЕДО до несанкціонованого доступу.
- Зменшення ризику порушення цілісності та конфіденційності електронних документів.
- Підвищення контрольованості процесів обробки конфіденційних даних у корпоративній мережі.

Висновки

- Проаналізовано принципи побудови систем електронного документообігу.
- Визначено основні канали несанкціонованого витоку інформації у корпоративній мережі.
- Запропоновано напрями удосконалення криптографічного захисту процесів електронного документообігу.