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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення системи захисту центру електронного документообігу корпоративної мережі від несанкціонованого доступу до конфіденційних даних»

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
_____ Олександр ПАНЧУК

Виконав: здобувач вищої освіти групи СЗДМ 61
Олександр ПАНЧУК

Керівник: АВЕРІЧЕВ Ігорь
к.е.н (ПРІЗВИЩЕ, Ім'я)

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

Панчуку Олександру Юрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Удосконалення системи захисту центру електронного документообігу корпоративної мережі від несанкціонованого доступу до конфіденційних даних»
керівник кваліфікаційної роботи АВЕРІЧЕВ Ігорь, к.е.н.
(ПРІЗВИЩЕ Ім'я. науковий ступінь. вчене звання)
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. Провести огляд каналів несанкціонованого витоку інформації через корпоративну мережу об'єкта інформаційної діяльності;
4.2. Здійснити аналіз принципи побудови та можливостей систем електронного документообігу інформації в корпоративних мережах об'єкту інформаційної діяльності;
4.3. Дослідити напрямки та розробити рекомендації щодо удосконалення системи кібернетичного захисту центру 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 _____ Олександр ПАНЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Ігорь АВЕРІЧЕВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

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 16 найменувань і займає 2 сторінки.

Метою кваліфікаційної роботи є удосконалення системи кібернетичного захисту центру електронного документообігу конфіденційних даних корпоративної мережі.

В кваліфікаційній роботі проведено огляд каналів несанкціонованого витоку інформації через корпоративну мережу об'єкта інформаційної діяльності. Проведено аналіз принципів побудови та можливостей систем електронного документообігу інформації в корпоративних мережах об'єкту інформаційної діяльності. Досліджено напрямки та запропоновано рекомендації щодо удосконалення системи кібернетичного захисту центру 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, СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБОРОТА, 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 76 pages, has 9 figures, 2 tables. The list of sources used contains 16 items and takes up 2 pages.

The purpose of the qualification work is to improve the cybernetic protection system of the center of electronic document flow of confidential data of the corporate network.

The qualification work reviews the channels of unauthorized information leakage through the corporate network of the object of information activity. The principles of construction and capabilities of electronic document flow systems in corporate networks of the object of information activity are analyzed. Directions are investigated and recommendations are proposed for improving the system of cybernetic protection of the center 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: DUIKT Research and Development Center. – 2025. P.43-44. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: OBJECT OF INFORMATION ACTIVITY, INFORMATION WITH LIMITED ACCESS, ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, 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 удосконалення системи кібернетичного захисту центру електронного документообігу конфіденційних даних корпоративної мережі.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– 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;

– досліджено напрямки та запропоновано рекомендації щодо удосконалення системи кібернетичного захисту центру 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
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 можна архівувати на фізичних носіях або відображати електронними засобами [1].

Залежно від теми, інформація поділяється на різні типи:

– особисті дані особи;

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

– інформація про стан навколишнього середовища (екологічна інформація);

– відомості про продукт (роботу, процес);

– науково-технічні знання;

– податкові відомості;

– формальні правила;

– статистичні дані,

– соціальна інформація про соціологію.

Інші види знань [1].

Однак на практиці розподіл праці...

інформація, до якої здійснюється доступ у порядку її найважливішого значення. Далі йде інформація, яка є або загальнодоступною, або має обмежений доступ. 1) [1].

Відкритість – будь-яка інформація доступна, за винятком тієї, яка обмежена законодавством, це називається відкритістю. Основними атрибутами

відкритої інформації є те, що вона доступна кожному, хто бажає отримати до неї доступ, і будь-які обмеження права на отримання відкритої інформації заборонені.

Як забезпечити доступ кожного до відкритої інформації.

– систематичне поширення її в офіційних письмових виданнях (бюлетенях, збірниках);

– її передача через загальновживані засоби масової інформації;

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

Рис.1.1 Режим доступу до інформації

ІзОД – це інформація, що вважається державною таємницею, або інша персональна інформація, яка має зберігатися в таємниці згідно із законом, а також інформація, що вважається конфіденційною згідно із законом.

Секретна інформація – це вид інформації, що включає інформацію щодо оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та правоохоронної діяльності, яка вважається таємною згідно із законом і підлягає захисту як державна таємниця. Інформація, що вважається державною таємницею, поділяється на класи відповідно до Закону України «Про державну таємницю» [2].

Конфіденційна інформація – це інформація, яка перебуває у власності, використовується або знищується фізичними або юридичними особами та запитується ними відповідно до умов, визначених ними. Інформація, що перебуває у власності держави та використовується державними органами або органами місцевого самоврядування, підприємствами, установами та організаціями всіх типів, для її збереження може бути встановлено обмежений доступ, який є законним, цей доступ є конфіденційним і не може бути використаний для інших цілей, ніж ті, що визначені законом.

Відповідно до Закону «Про захист інформації в інформаційно-телекомунікаційних системах», до захисту в системі належать:

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

- інформація, що має енциклопедичний характер та слугує довідником для інформації щодо діяльності органів державної влади або місцевого самоврядування, а також інформація щодо діяльності конкретних органів, яка опублікована в Інтернеті, інших глобальних інформаційних мережах або передається через телекомунікаційні мережі (далі – відкрита інформація).

- інформація, що є конфіденційною та належить державі або підлягає захисту законом, включаючи персональні дані про особу (яку також називають конфіденційною інформацією).

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

- Інформація повинна бути відкритою під час процесу обробки, це досягається шляхом захисту її 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 уповноважені користувачі можуть змінювати або знищувати загальнодоступну інформацію [2].

Під час обробки конфіденційної та секретної інформації вкрай важливо забезпечити її захист від несанкціонованого доступу, модифікації, знищення або копіювання.

Усі дії, пов'язані зі зберіганням інформації з обмеженим доступом, здійснюються в інформаційних об'єктах, призначених для цієї мети. Згідно з визначенням, об'єктом інформації є будівля, приміщення, транспортний засіб або інша технічна споруда, яка має обмежений доступ до інформації. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави.

Обробка інформації в об'єктах інформаційної діяльності сприяє забезпеченню інформаційної безпеки, яка підтримується шляхом дотримання таких критеріїв інформаційної безпеки:

Цілісність – це властивість інформації, яка повинна бути захищена від несанкціонованого знищення або модифікації.

Секретність – це властивість інформації, яка повинна бути захищена від несанкціонованого доступу.

Доступність – це властивість даних, які призначені для захисту 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 делеговані 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 отримання документованої або публічно оприлюдненої інформації відповідно до чинного законодавства України щодо інформації фізичними або юридичними особами.

Використання інформації – це виконання інформаційних потреб громадян, юридичних осіб та держави. Передача інформації – це передача документованої або оголошеної інформації, яка є загальнодоступною.

Зберігання інформації має вирішальне значення для збереження інформації та пов'язаних з нею носіїв.

Процес отримання, використання, поширення та зберігання документованої інформації здійснюється за процедурою, зазначеною в цьому законі та інших законодавчих актах щодо інформації. Крім того, можна класифікувати діяльність, що стосується інформаційного забезпечення – отримання, оцінка, зберігання та обробка даних, які створюються з метою прийняття управлінських рішень. Це охоплює різноманітні види діяльності, включаючи виробництво та продаж, обслуговування та покращення технологічності продукції, а також якість виготовленої продукції, її вартість, рекламу та інформацію про різні продукти.[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 підприємництвом).

Кожна компанія не може мати бюджету без плану підприємства. На основі розроблених бюджетів система управління керує різними видами 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 від запланованих значень, результати потім порівнюються із запланованими значеннями, і за необхідності проводяться додаткові заходи.

Якщо створення бюджетів та прогнозів базується на одному й тому ж 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. Ефективне використання коштів сприятиме більш ефективному використанню технологій для підвищення ефективності підприємства, його стратегії розвитку та інформаційної безпеки всього підприємства, а також його матеріальних активів.

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

Технічний канал витоку інформації вважається сукупністю джерел інформації, ліній зв'язку (фізичного середовища), 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 засоби, 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. Як правило, середовищем для поширення є повітря, рідке або тверде тіло. До них належать повітряний простір, будівельні конструкції, з'єднувальні лінії та інші провідні компоненти, ґрунт (рельєф

місцевості). Звук пов'язаний з кожним фізичним процесом і присутній на вході до пристроїв збору інформації.

Пристрої перехоплення інформації використовуються для прийому та перетворення сигналів з метою отримання інформації.

Технічні методи отримання, обробки, зберігання та передачі інформації (ТМП) вважаються технічними методами, які безпосередньо обробляють персональну інформацію, що є конфіденційною. До них належать: електронно-обчислювальні машини, секретні переговори через АТС, системи оперативного керівництва та аудіозв'язку, системи покращення звуку, підтримки та запису.

При визначенні технічних каналів видачі інформації ТМП 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 називають основним технічним методом (ОПМ).

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

Як засіб передачі інформації, найбільше занепокоєння викликають ДТЗС, що виходять за межі обмеженої зони. Обмежена 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 необхідно вживати технічних та інституційних заходів для створення умов, що запобігають розголошенню інформації, що є секретною. Зона контролю визначається на основі специфіки

керівництва щодо конкретного розташування об'єкта та потенційного використання технічних засобів виявлення.

Окрім з'єднувальних ліній ТЗПІ та ДТЗС, поза межами контрольованої зони 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, джерелами води та іншими струмопровідними металевими конструкціями. Такі дроти, кабелі та струмопровідні 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:

Індукцію випромінювання TZP у лінії, що з'єднують DTZS та зовнішні компоненти, що проходять за межі контрольованої зони;

Проникнення інформаційних сигналів у лінії живлення та заземлювальні кола TZPI;

Використання вбудованих пристроїв.

Індукція електромагнітного випромінювання TZPI ініціюється інформаційними сигналами, що надсилаються елементами TZPI, а також наявністю гальванічного зв'язку між зовнішнім провідником та з'єднувальними лініями TZPI. Величина індукованих сигналів залежить, перш за все, від потужності вихідних сигналів, відстані до провідників та довжини загального шляху з'єднувальних ліній TZPI та зовнішніх компонентів.

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

Змагальні антени зазвичай зосереджені та розкидані. Випадкова зосереджена антена — це невеликий технічний пристрій, який використовується

для телефонного зв'язку з людьми (наприклад, телефон). Розподілені випадкові антени включають сталеві труби, кабелі та інші механічні комунікації.

Проникнення сигналу в лінію електроживлення можливе за наявності магнітної взаємодії між низькочастотним підсилювачем та трансформатором живлення. Сигнал, що передає інформацію, також може передаватися через лінію електроживлення внаслідок того, що середнє споживання струму в кінцевих каскадах підсилювачів залежить від величини сигналу, що передає інформацію.

Проникнення інформації у фундамент. Окрім заземлення, різні постачальники електроенергії, що проходять за межі контрольованої зони, мають гальванічний зв'язок із землею. До них належать нульовий провід ланцюга електроживлення, екрани, що з'єднують кабелі, труби, що нагрівають та забезпечують водою, металева арматура бетону та інші компоненти. Всі ці провідники, а також заземлювальний пристрій, складають велику систему заземлення, яка є інформаційно щільною.

Можливість приймати інформацію 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 за допомогою вбудованих пристроїв. 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 захоплюється за допомогою вбудованих пристроїв, передається по радіоканалу або спочатку записується на пристрій зберігання даних, а потім передається до місця призначення.

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

У Технічний канал витоку інформації вважається сукупністю джерел інформації, ліній зв'язку (фізичного середовища), 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 засоби, 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. Як правило, середовищем для поширення є повітря, рідке або тверде тіло. До них належать повітряний простір, будівельні конструкції, з'єднувальні лінії та інші провідні компоненти, ґрунт (рельєф місцевості). Звук пов'язаний з кожним фізичним процесом і присутній на вході до пристроїв збору інформації.

Пристрої перехоплення інформації використовуються для прийому та перетворення сигналів з метою отримання інформації.

Технічні методи отримання, обробки, зберігання та передачі інформації (ТМП) вважаються технічними методами, які безпосередньо обробляють персональну інформацію, що є конфіденційною. До них належать: електронно-обчислювальні машини, секретні переговори через АТС, системи оперативного керівництва та аудіозв'язку, системи покращення звуку, підтримки та запису.

При визначенні технічних каналів видачі інформації ТМП 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 називають основним технічним методом (ОПМ).

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

Як засіб передачі інформації, найбільше занепокоєння викликають ДТЗС, що виходять за межі обмеженої зони. Обмежена 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 необхідно вживати технічних та інституційних заходів для створення умов, що запобігають розголошенню інформації, що є секретною. Зона контролю визначається на основі специфіки керівництва щодо конкретного розташування об'єкта та потенційного використання технічних засобів виявлення.

Окрім з'єднувальних ліній ТЗПІ та ДТЗС, поза межами контрольованої зони 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, джерелами води та іншими струмопровідними металевими конструкціями. Такі дроти, кабелі та струмопровідні 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:

Індукцію випромінювання TZP у лінії, що з'єднують DTZS та зовнішні компоненти, що проходять за межі контрольованої зони;

Проникнення інформаційних сигналів у лінії живлення та заземлювальні кола TZPI;

Використання вбудованих пристроїв.

Індукція електромагнітного випромінювання TZPI ініціюється інформаційними сигналами, що надсилаються елементами TZPI, а також наявністю гальванічного зв'язку між зовнішнім провідником та з'єднувальними лініями TZPI. Величина індукованих сигналів залежить, перш за все, від потужності вихідних сигналів, відстані до провідників та довжини загального шляху з'єднувальних ліній TZPI та зовнішніх компонентів.

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

Змагальні антени зазвичай зосереджені та розкидані. Випадкова зосереджена антена — це невеликий технічний пристрій, який використовується для телефонного зв'язку з людьми (наприклад, телефон). Розподілені випадкові антени включають сталеві труби, кабелі та інші механічні комунікації.

Проникнення сигналу в лінію електроживлення можливе за наявності магнітної взаємодії між низькочастотним підсилювачем та трансформатором живлення. Сигнал, що передає інформацію, також може передаватися через лінію електроживлення внаслідок того, що середнє споживання струму в кінцевих каскадах підсилювачів залежить від величини сигналу, що передає інформацію.

Проникнення інформації у фундамент. Окрім заземлення, різні постачальники електроенергії, що проходять за межі контрольованої зони, мають гальванічний зв'язок із землею. До них належать нульовий провід

ланцюга електроживлення, екрани, що з'єднують кабелі, труби, що нагрівають та забезпечують водою, металева арматура бетону та інші компоненти. Всі ці провідники, а також заземлювальний пристрій, складають велику систему заземлення, яка є інформаційно щільною.

Можливість приймати інформацію 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 за допомогою вбудованих пристроїв. 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 захоплюється за допомогою вбудованих пристроїв, передається по радіоканалу або спочатку записується на пристрій зберігання даних, а потім передається до місця призначення.

1.4 Висновки по розділу

1. У першій частині кваліфікаційного завдання описано класифікацію та розподіл інформації щодо потоку документів у центральній частині корпоративної мережі.

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

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

Розділ 2
СТРУКТУРА СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Призначення, завдання та структура системи електронного документу

Одне з визначень документа полягає в тому, що це матеріальний об'єкт, який містить інформацію у фіксованому форматі, розроблений відповідно до встановленого протоколу та має юридичне значення відповідно до чинного законодавства країни.

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»).

Обов'язковою інформацією, пов'язаною з електронним документом, є дані, що містяться в самому електронному документі. Без цієї інформації документ не може бути використаний для бухгалтерського обліку та не має юридичного значення.

Обов'язковою інформацією, пов'язаною з електронним документом, також є 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 типи електронних підписів використовуються в управлінні електронними документами договірним шляхом.

Оригіналом електронного документа вважається цифрова версія документа, яка містить авторитетну інформацію, включаючи цифровий підпис автора. Під час надсилання електронного документа кільком одержувачам або

зберігання його на кількох електронних 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 законодавства; 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 юридичні документи, які не можуть вважатися такими:

1) документи, що засвідчують правонаступництво;

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

3) інші ситуації, що охоплюються законом. Процес нотаріального посвідчення цивільно-правової угоди, створеної електронними засобами (електронні документи), супроводжується процедурою, визначеною 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 необхідним компонентом документа, її метою є визначення очікуваного впливу документа (включаючи наступні кроки, які

необхідно вжити) на одержувачів документа в рамках існуючих соціальних відносин, пов'язаних з документом, після його отримання та розуміння його змісту.

Для розголошення документа необхідний дозвіл, ця інформація визначається фізичною або юридичною особою, яка наразі відповідає за його створення.

Реєстрація необхідна для характеристик документа, ця характеристика є унікальною та ідентифікує документ в цілому порівняно з іншими документами.

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, набору даних, що документують 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 обробляти інформацію, яка не представлена сторінкою, а натомість як об'єкти даних. Ця технологія дозволяє ефективно зберігати та використовувати інформацію, обмінюватися нею між колегами та зберігати інформацію в базі даних.

Стандарт мав на меті досягти таких цілей: відокремити структуру документа від його представлення; забезпечити незалежність документа від формату; надати можливість обробляти документи з кількома функціями:

форматувати весь документ, вибирати фрагменти тексту, ключові слова, інформацію про назву, автора та анотації з документа.

Під час використання стандартизованої загальної мови розмітки документів SGML очікується, що текст складається з логічних компонентів, які називаються елементами та документуються в тексті за допомогою розмітки. Як правило, компонент обмежений початковими та кінцевими 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 у стандарт через рамки... стандарт. Також у SGML відсутній чітко визначений метод інтерпретації документів; тому в певних випадках для використання SGML необхідний прикладний процесор, який обробляє структуру та вміст документів. Як процесор прикладних знань зазвичай використовується інструмент перетворення SGML у розмітку. Використання SGML є корисним:

Під час створення численних документів одного типу продуктивність зростає.

Під час написання документів, що вимагають певного формату, зберігається загальна практика впровадження прийнятих стандартів.

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

Під час роботи над документом, що містить інформацію, яку необхідно обробляти різними способами, можна використовувати лише вихідний файл як засіб обробки інформації та не потрібно спеціально перетворювати її на зображення, наприклад, не витягувати зображення.

Під час перенесення документів в інші системи спрощується перетворення частин документів, що полегшує представлення різних частин 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.

Процес обміну електронними документами між компаніями або Зв'язок з клієнтом спрощується.

SGML пропагує поширений метод 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 - визначення типу документа). Зміст файлу DTD:

– описує склад вмісту документа, подібно до схеми бази даних; описує типи інформації, яку підтримує база даних, та зв'язки між полями.

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

– визначає правила зв'язків між компонентами, такі як «хаос має бути вирішений у першому абзаці кожного списку» або «списки повинні мати щонайменше два абзаци». Ці правила, перелічені в DTD, служать для сприяти послідовній логічній композиції.

– знаходиться з документом за кожної можливості. «Екземпляр документа» – це певний документ, який дотримується певного файлу 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.

Інший поширений стандарт ISO 8613 (частини 1-6) – Архітектура офісних документів (ODA) та Формат обміну (ODIF) призначений для передачі та

представлення документів, що стосуються управління офісом – 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 корисно для комунікаційних цілей. Зокрема, він дотримується стандартного синтаксису, що використовується в архітектурі OSI.

Формальна структура ODA. Згідно з протоколом ODA, в описі документа розпізнаються такі категорії структурних документів: логічна структура, склад контенту.

Мета логічної структури полягає в представленні 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.

Формат структури використовується для опису способу 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 рисунки, розташовані в блоках.

Контент – це фактичні знання про документ: слова, рисунки тощо. ISO 8613 класифікує контент на три типи: символічний текст, растрова графіка та геометрична графіка. Якщо 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 її основні обов'язки.

Електронне управління документами включає: створення документів, їх обробку, передачу, зберігання та відображення інформації, що циркулює в організації чи на підприємстві, все це робиться за допомогою комп'ютерних мереж. Зазвичай, електронне управління документами вважається переміщенням документів між відділами організації чи підприємства, групами спільних користувачів або окремими користувачами. І навпаки, переміщення документів не обов'язково передбачає фізичне переміщення документів, а радше передачу прав на використання документів з конкретним повідомленням їх цільових користувачів та контролем над їх виконанням.

В результаті прийнято ідею системи електронного управління документами (СЕД); ця система полегшує 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. Типи файлів, які зазвичай мають SEDO: текстові документи, зображення, електронні таблиці, аудіо, відео та веб-документи. Загальні можливості SEDO: створення документів, доступ до документів, конвертація даних та захист даних. Системи електронного документообігу (СЕД) спрощують процес створення, управління доступом та розповсюдження великих обсягів документів у комп'ютерних мережах, а також забезпечують контроль над потоком документів в організації.

SEDO мав на меті автоматизувати всю процедуру роботи з документами, створеними в цьому місці або отриманими з іншого місця:

Основна мета SEDO — полегшити зберігання електронних документів, а також брати участь у їх (головним чином) пошуку за атрибутом або вмістом. SEDO повинен автоматично відстежувати розвиток документів, мати терміни завершення документів, мати систему переміщення документів та контролювати

всі версії та підверсії документів. Комплексна система управління документами (SEDO) повинна включати весь цикл управління офісом в організації чи на підприємстві – від створення завдання до написання документа, зберігання його в архіві та забезпечення централізованого зберігання документів у будь-якому форматі, включаючи складні документи, що складаються з кількох частин. SEDO повинна об'єднати різнорідні потоки документів, що стосуються територіально віддалених корпорацій, в єдину систему. Вони повинні забезпечити гнучку систему управління документами, яка є одночасно суворою та ліберальною у визначенні маршрутів. SEDO повинна визначати межі доступу користувачів до різних документів за їхньою кваліфікацією, посадою та призначеними повноваженнями. Крім того, SEDO повинна бути розроблена відповідно до існуючої штатної та організаційної структури компанії та управління офісним простором, все це має бути включено в існуючу корпоративну систему.

Електронне управління документами передбачає процедуру створення, обробки, надсилання 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 відділами або окремими особами всередині організації або між організаціями.

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 виконання SEDO у практиці установи досягаються такі цілі:

підвищення продуктивності праці;

підвищення ефективності обробки документів;

покращення можливостей довідково-інформаційних служб;

підвищення якості підготовки, обробки та відтворення документів;

зменшення кількості непотрібних файлів та непотрібних електронних листів;

покращення здатності організації регулювати рух та виконання документів.

Основними обов'язками SEDO є:

Створення документів та класифікація документів;

– їх завантаження до сховища даних установи та надання користувачам способів доступу до документів в інтерактивному режимі;

- управління правами доступу відповідно до авторизації.

- конвертація даних;

– запобігання знищенню інформації 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. Розробка документаційного забезпечення (процедурний підхід).

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

3. Повне охоплення обов'язків щодо документації та організації її зберігання (повна автоматизація).

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

2.2. Функціональна модель СЕДО

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

Функціональна модель СЕД включає функціональні об'єкти та їх зв'язки (рис. 2.1).

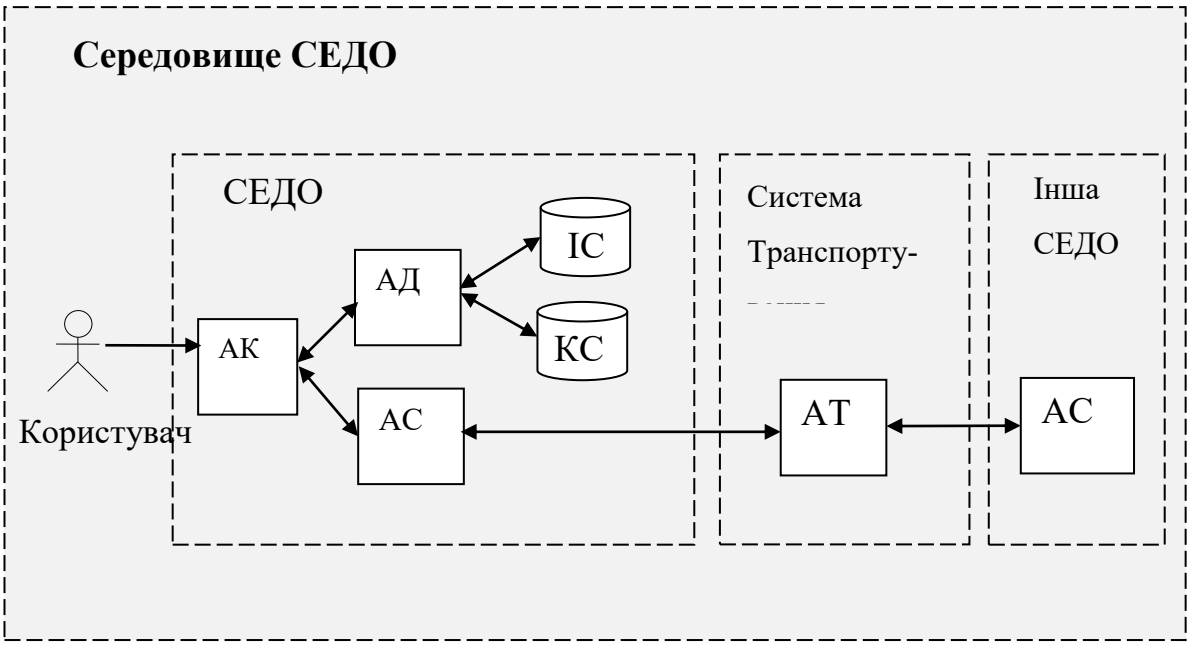


Рисунок 2.1. Функціональна модель СЕДО

Функціональні об'єкти поділяються на первинні, вторинні та третинні типи.

До первинних функціональних об'єктів належать SEDO та його користувачі. SEDO та середовище користувача складається з електронних документів, які зазвичай мають невизначену кількість пов'язаних користувачів та SEDO.

До вторинних функціональних об'єктів належать агент користувача AK, агент доступу AD, сховища інформації (окремі IS) та колективна CS, агент сполучення AS.

До третинних функціональних об'єктів належать транспортні сутності, такі як AT.

На концептуальному рівні об'єкти SEDO 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.

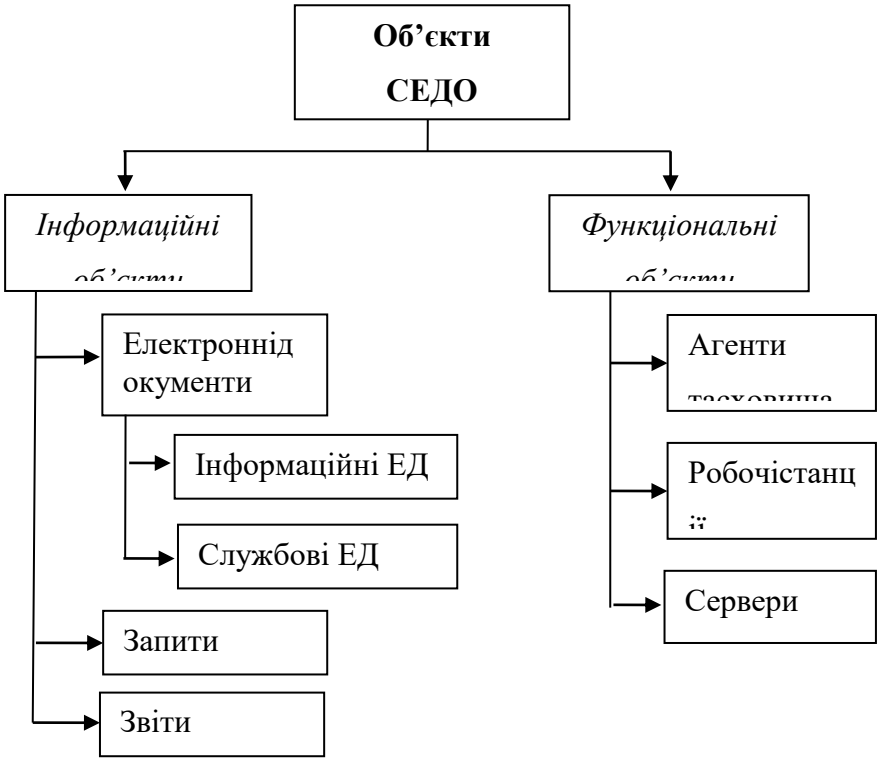


Рисунок 2.2. Інформаційні та функціональні об'єкти СЕДО

Автоматизовані або за участю людини операції 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.

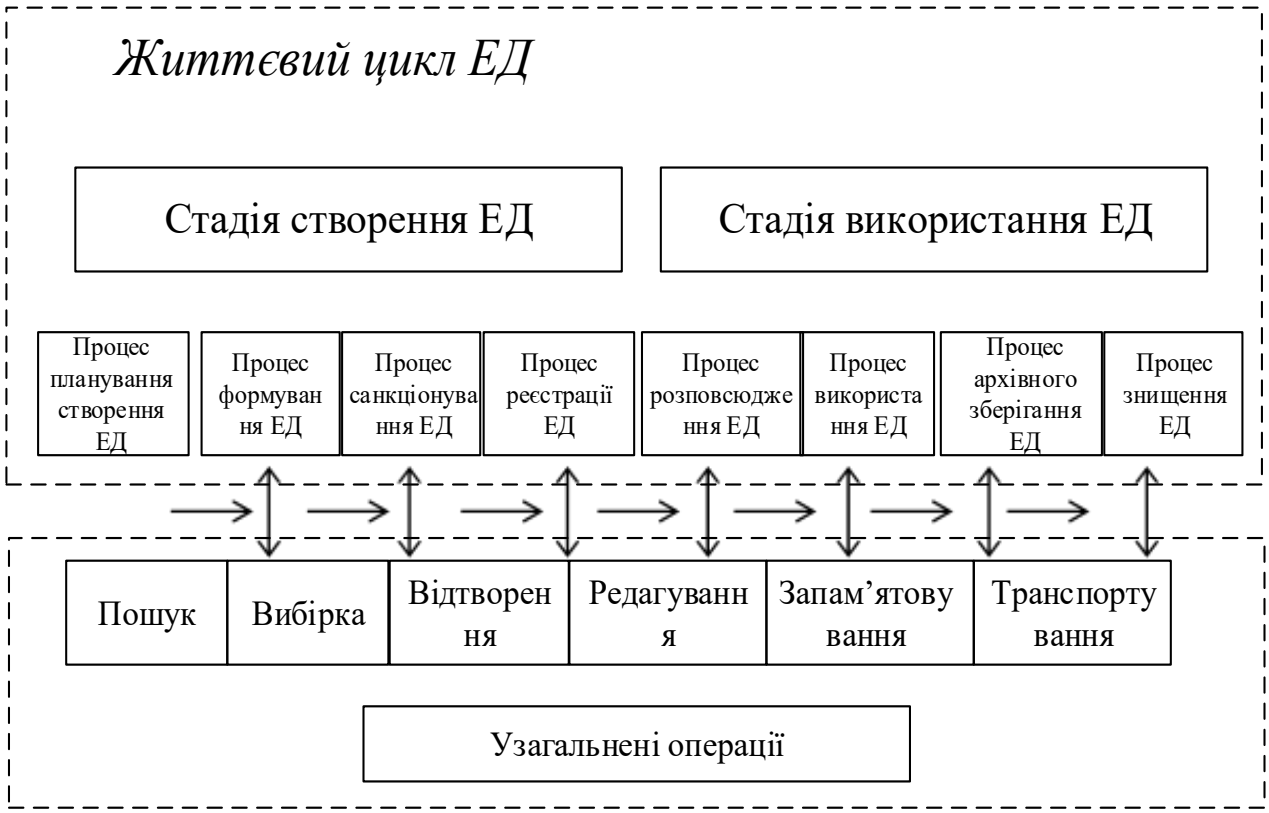


Рисунок 2.3. Життєвий цикл ЕД та узагальнені операції

Описовий опис функціональних атрибутів SEDO.

Функціональні об'єкти SEDO включають агентів, збирачів інформації, станції та сервери.

Склад функціональних об'єктів у SEDO показано на рис. 2.4.

Процедури, що використовуються на ED на кожному етапі життєвого циклу, виконуються за допомогою операцій.

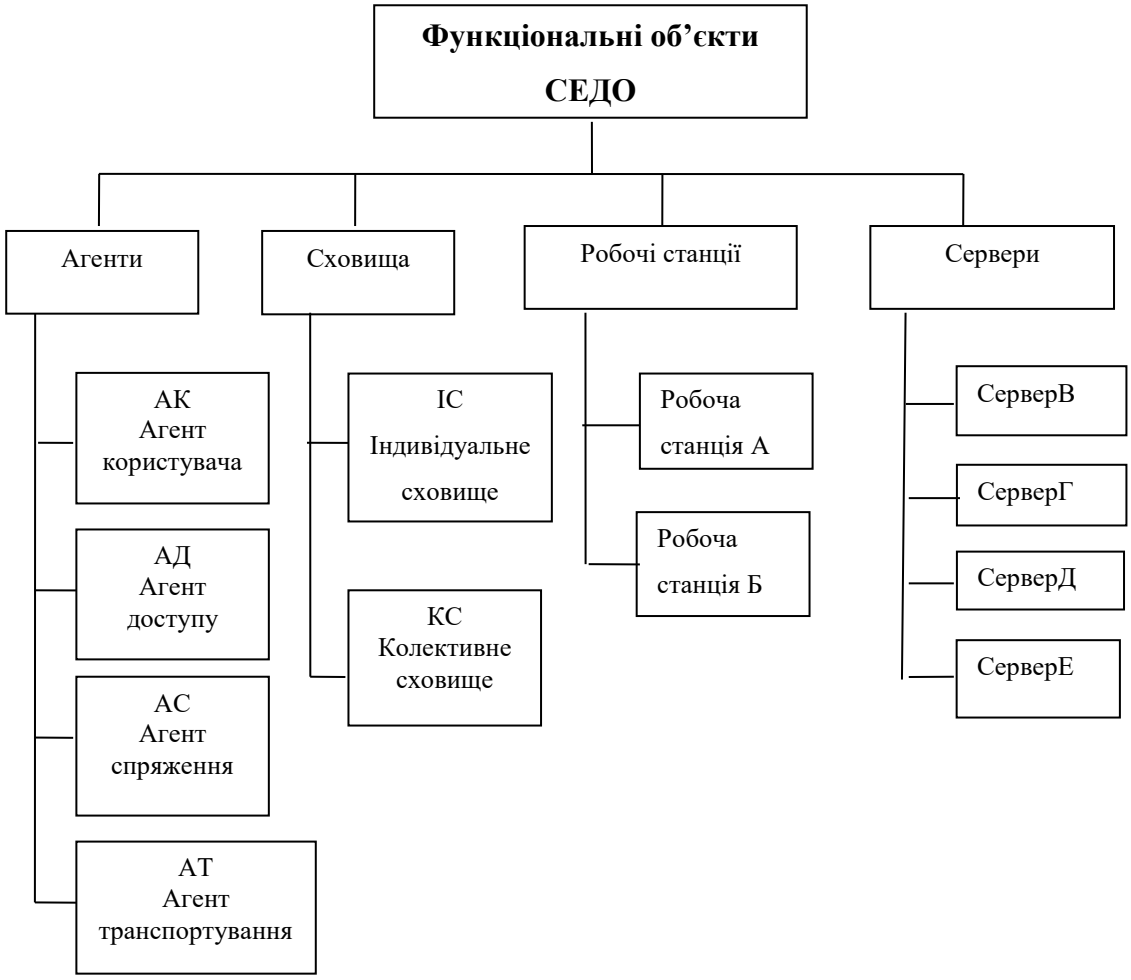


Рисунок 2.4. Функціональні об’єкти СЕДО

Операції виконуються агентами автоматично або під контролем SEDO.

Агенти SEDO включають: агента користувача (UA), окремі сховища інформації, агента транспортування (TA), агента доступу (AA) та пари (AC).

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

Користувачам дозволено використовувати SEDO лише через UAA. Взаємодія між UAA та користувачем здійснюється за допомогою клавіатур, сканерів, принтерів, відеокамер, генераторів голосу тощо.

UAA може прямо або опосередковано зв'язуватися з джерелами інформації.

Система транспортування ED (EDS) складається з трьох функціональних

об'єктів: агентів транспортування, інформаційних процесорів та комунікаційних шин. UAA призначені для транспортування інформаційних об'єктів SEDO та з'єднання кількох SEDO.

UAA сприяють маршрутизації та комутації інформації SEDO. Щоб забезпечити зв'язок із зовнішнім SEDO, агенти транспортування також можуть сприяти службам, які координують транспортування ED (функції, що з'єднують).

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

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

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

2.4 Центр електронного документообігу

Обмін документами теоретично базується на зірковій системі, а не на системі «кожен з кожним». EDM є основою цього принципу. EDM може виконувати всі наступні функції:

- конвертація та узгодження форматів вхідних та вихідних документів;
- допомога у вирішенні проблем та розрахунку 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 EDM корпоративні системи можуть бути доповнені спеціальними модулями, що конвертують формати та процедури обміну з EDM.

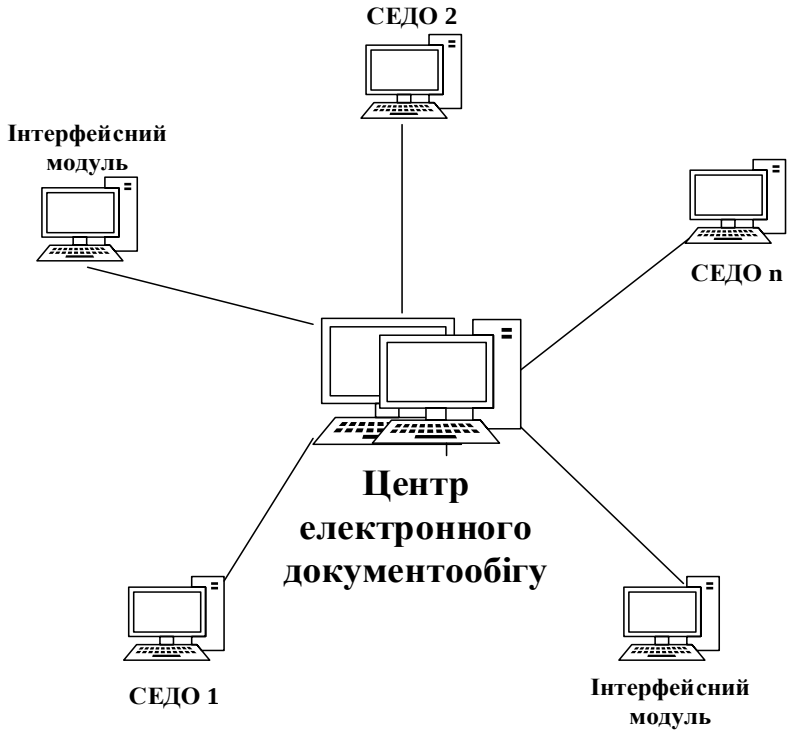


Рисунок 2.5. Взаємодія з Центром електронного документообігу

Формати та стандарти обміну.

Одним з основних обов'язків CED є забезпечення послідовної передачі документів між різними системами. Найефективнішим підходом є створення універсального розширюваного представлення загальних документів у XML, яке використовується як проміжний варіант між системами.

Якщо набір документів, що стосуються підключеної системи, більший, ніж зазначено в універсальному форматі, то можлива можливість розширення або відображення цих деталей за допомогою тегів.

Перетворення документів у форми повинно зберігати весь набір інформації, пов'язаної з вхідними документами. Для документів, що виводяться

у форматі XML, необхідно зберігати додаткову інформацію – властивості XML дозволяють ігнорувати «сторонню» інформацію. Інші типи документів, такі як PowerPoint, мають склад деталей, який можна обмежити. У цьому випадку може бути передано додатковий файл у форматі, запитуваному одержувачем, з довгим або повним документом.

Окрім вимог до документації, CED повинен забезпечити передачу самих документів. 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 сам сертифікаційний центр повинен мати ліцензію на відповідну діяльність визнаним державним органом.

Поєднання ЦОД з сертифікаційними центрами 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 сертифікаційного центру, яка базується на вже існуючих модулях (криптопровайдерах), 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 управління електронними документами 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, через проблеми безпеки та надійності доцільніша гнучкіша структура, де документ може мати кілька шляхів досягнення 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 перетворенню 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 має візуальні інструменти, які перетворюють документи з одного формату в інший, а також процеси, що проектують бізнес.

Взаємодію між центрами документів, SEDO та інтерфейсними модулями пропонується організувати за допомогою технології веб-сервісів .NET. Технологія веб-сервісів інтегрована та впроваджена на всіх існуючих програмних платформах, ця технологія сприяє інтеграції різнорідних систем, що має вирішальне значення для різноманітності систем обробки документів, що існують наразі.

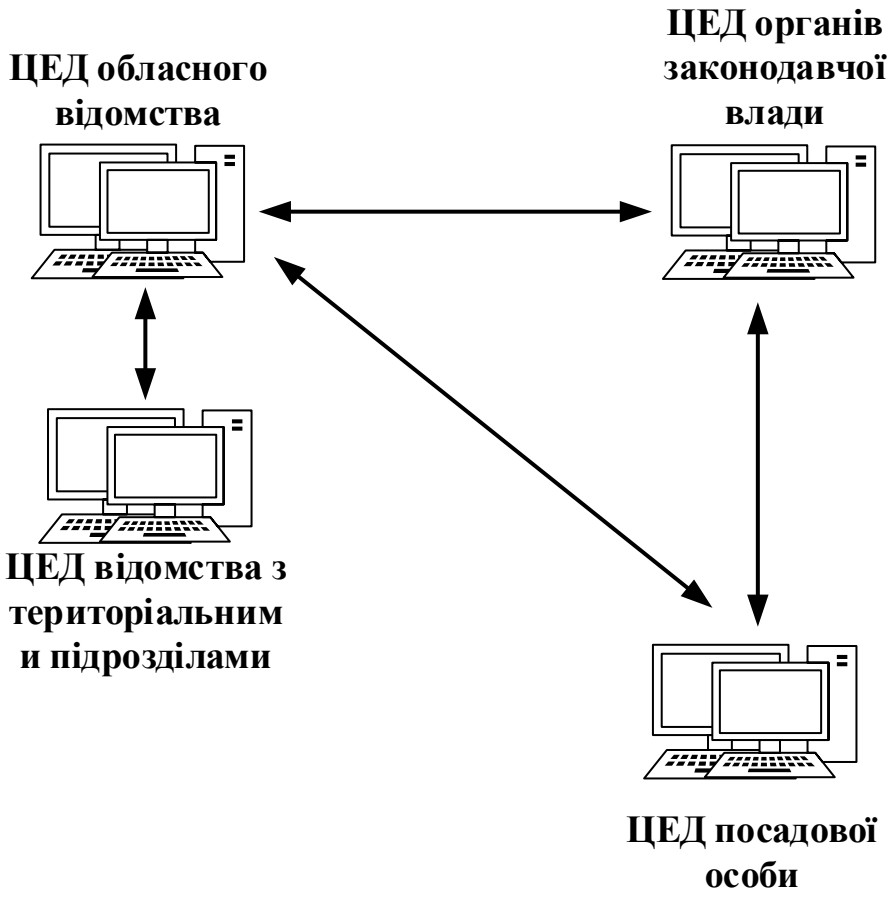


Рисунок 2.6. Ієрархія ЦЕД

Для надсилання документів та повідомлень найефективнішим вибором є

поштовий сервер Microsoft Exchange Server.

Для використання CED без корпоративної системи або з відсутністю функціональності в інтерфейсі модулів можна використовувати інструменти з пакету Microsoft Office (Outlook), які можна поєднувати з модулями, що підготовлюють необхідні документи, 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 роботи відділу документообігу очевидна.

• необхідність підвищення швидкості обробки документів;

• створення цифрового архіву електронних версій документів.

2.4 Висновки по розділу

1. У другій частині процесу кваліфікації було проведено дослідження завдання та структури системи електронного документообігу.

2. Було продемонстровано функціональну модель SEDO. Було встановлено місію, структуру та процедуру функціонування центру електронного документообігу.

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

Розділ 3
УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ЦЕНТРУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ КОНФІДЕНЦІЙНИХ ДАНИХ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Особливості впровадження СЕДО в корпоративну мережу

У SEDO поєднується кілька технологій для збору, індексації, зберігання, пошуку та перегляду електронних документів. У більшості SEDO 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. 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 SEDO). У кількох SEDO додаткова ємність сховища реалізується шляхом організації посилань між документами (ці посилання можна графічно редагувати та встановлювати).

Будь-який документ у SEDO присвоюється певному набору атрибутів (наприклад, його назва, автор документа, час створення тощо). Набір атрибутів може змінюватися між різними типами документів (в одному типі документа атрибути залишаються незмінними). 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 графа. Коли документ додається до SEDO, вибирається необхідний шаблон і заповнюється картка (вводяться значення атрибутів). Після надсилання форми картка пов'язується з самим документом.

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. Сховища атрибутів документів (картки);

2. Сховища документів;

3. Служби повнотекстового пошуку.

Репозиторій документів зазвичай є сховищем вмісту 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 практика збереження документів, а також атрибутів у базі даних стала більш популярною. Цей метод має свої переваги та недоліки. Перевагою є значне підвищення безпеки доступу до документів, а головним недоліком — низька ефективність роботи з документами, що 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 те, що в ній зберігалося.

Компоненти SEDO, що беруть участь у переміщенні документів, часто називають компонентами маршрутизації документів. Зазвичай для опису маршрутизації документів використовуються слова «вільний» та «жорсткий». За допомогою «вільної» маршрутизації будь-який учасник потоку документів може змінити поточний маршрут потоку документів (або створити новий маршрут). За допомогою «жорсткої» маршрутизації потік документів обмежений, і користувачам не дозволяється змінювати маршрут. Однак за допомогою «жорсткої» маршрутизації логічні процеси можуть виконуватися, коли маршрут змінюється, коли виконуються будь-які попередньо встановлені умови (наприклад, надсилання документа керівництву, коли певний користувач перевищує свій авторизований діапазон).

У SEDO використовуються надійні методи забезпечення живлення та доступу до документів. Зазвичай за їх допомогою розпізнаються такі типи доступу:

- повний контроль над процесом написання;

- можливість змінювати, але не знищувати написаний документ;

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

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

- можливість читати документ, але не змінювати його.

- 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 (особливо якщо його потрібно розділити на різні екземпляри), дуже корисною функцією SEDO є можливість використання різних 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 нову версію на його основі. Після того, як він передав свій чернетку документа наступній особі, він передав версію документа третьому користувачеві, який створив третю версію. Через визначений проміжок часу, коли автор першого чернетки ознайомився з коментарями та пропозиціями, перший виконавець вирішує завершити початковий 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 є найбільш релевантною, або за часом створення, або за важливістю для документа). Під час організації групового проекту над документами можливість додавання до них нотаток є корисною. Оскільки іноді неможливо надати користувачам можливість вносити будь-які зміни до

документа під час процесу затвердження, вони можуть натомість використовувати анотацію документа. 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 графічної демонстрації недоліків зображення.

3.2 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 невідповідністю форматів 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;
- різні типи документів, які обробляє система.
- масштабованість;
- максимальну кількість користувачів;

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

• можливість роботи за схемою «вільно», без необхідності дотримуватися суворого режиму.

• методи);

• 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 клієнта – все це особливості цього процесу.

Методи регулювання доступу та захисту від криптоаналізу.

Системи, що використовують передові інструменти підвищення продуктивності (ППП)

Важливо розуміти кілька найпоширеніших визначень робочого процесу, щоб зрозуміти цю концепцію:

Завдання, яке виконується без будь-якого врахування порядку чи послідовності одним або кількома членами команди 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 цілей (Коаліція управління робочим процесом).

Усі ці визначення стосуються бізнес-процесів, інформації та персоналу.

Технологія робочих процесів включає:

– автоматизовану технологію робочих процесів;

– процес автоматичного виконання бізнес-процесів;

– моделювання процесів підприємства;

– контроль за всіма співробітниками компанії, як внутрішніми, так і зовнішніми.

Технологія робочих процесів походить від такої фундаментальної 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 розглянутого бізнес-процесу (наприклад, перевірка правильності складання документа, внесення змін до документа).

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

Кожен клас систем робочих процесів вирішує щонайменше три питання:

– опис бізнес-процесу;

– контроль виконання бізнес-процесу;

– контроль виконання бізнес-процесу.

Процес виконання робочих процесів включає:

– моніторинг умов переходу між операціями;

– передачу документів між учасниками;

- інформування користувача про те, що йому потрібно зробити.

Таблиця4.1**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

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.

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;

- система ведення електронного досьє, ведення паперового досьє та забезпечення доступу до його інформації.

- кластер передових виконавчих функцій;

- комплекс з кількох проектних документів, призначених для переміщення різними маршрутами;

- комплекс передачі даних;

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

- сукупність програмних інструментів, що використовуються для ведення як нормативної, так і довідкової інформації.

- кластер державних установ;

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 діловодством одержувача.

Інтерфейс між вами та SEDO дозволяє вам досягти цього:

- Ергономіка взаємодії користувача з SEDO;

- Взаємодія між користувачами та програмними компонентами SEDO на основі прозорого та інтуїтивно зрозумілого діалогового вікна, яке використовує значки функцій, режимів та операцій;

- 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).

У SEDO може бути використана система управління базами даних, яка гарантує зберігання інформації в різних форматах, включаючи текстовий, візуальний або мультимедійний, та забезпечує доступ до інформаційних ресурсів через кількох запланованих користувачів з достатньою підтримкою продуктивності при їх підключенні.

3.3 Електронний цифровий підпис

Закон України «Про електронні підписи», прийнятий у травні 2005 року, зосереджується на регулюванні взаємодій, пов’язаних з використанням одного конкретного типу електронного підпису: електронного цифрового підпису. Закон України «Про електронні цифрові підписи» («Відомості Верховної Ради» (ВВР), 2003, № 36, стор. 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 набору електронних даних, цей набір потім додається або об’єднується з вихідним набором, що дозволяє

автентифікувати підпис та ідентифікувати підписувача. Електронний цифровий підпис використовує закритий ключ для обробки та перевірки відкритого ключа. Унікальною характеристикою ЕЦП є використання криптографічних протоколів захисту інформації.

Електронний цифровий підпис – це програмний інструмент, програмно-апаратний або апаратний пристрій, який створює ключі, володіє та/або перевіряє електронний цифровий підпис.

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

Під час використання та передачі електронних документів через телекомунікаційні засоби особливо важливо подбати про безпеку інформації. Звичайний електронний документ, який не захищений від змін або несанкціонованого доступу, не вважається захищеним документом. Електронний цифровий документ захищається за допомогою цифрового підпису.

Електронний цифровий підпис – це інформація, яка вноситься до файлу даних його творцем і яка захищає файл від зміни без дозволу та ідентифікує підписувача.

Електронний цифровий підпис використовується для забезпечення документування дій фізичних та юридичних осіб за допомогою електронних документів. Його використовують фізичні особи та юридичні організації, які мають електронні документи, для ідентифікації підписанта та перевірки легітимності даних в електронній формі.

Цифровий підпис, здійснений 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 використовувалася потужніша пара ключів, яка була дійсною під час застосування електронного цифрового підпису.

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

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

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

У випадках, коли необхідно засвідчити легітимність підпису на документах та відповідність копій документів оригіналу, до електронного документа додається цифровий підпис офіційної особи, призначеної для цієї мети.

Процес використання електронного цифрового підпису для державних установ, органів місцевого самоврядування, установ та компаній регулюється Кабінетом Міністрів України.

Процес використання електронного цифрового підпису у фінансових операціях регулюється Національним банком України.

Закриті та відкриті ключі

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

Закритий ключ – це унікальний рядок символів довжиною 264 біти, цей рядок призначений для використання під час створення ЕЦП в електронних документах. 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 є унікальним та 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 (підписант) завжди зберігає свій секретний ключ, і ніхто не може законно 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 цієї процедури дані, що підлягають підписуванню, та закритий ключ підписувача вводяться у відповідні програми. Програма генерує з інформації за допомогою секретного ключа унікальний блок даних фіксованого розміру (власний ЕЦП), ці дані дійсні лише для цього секретного ключа та введеної інформації. Тобто, ЕЦП – це цифровий підпис 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. Справжність електронного цифрового підпису (ЕЦП) отриманого документа перевіряється одержувачем за допомогою відкритого ключа підписувача (відправника).

Для виконання цієї процедури необхідно отримати відкритий ключ відправника (наприклад, з каталогу), а також захищений документ (тобто дані документа та дані ЕЦП). Програмний модуль, що відповідає підпису, перевіряє, чи дійсно цифровий підпис пов'язаний з документом та відкритим ключем. Якщо до документа або відкритого ключа було внесено зміни, перевірка матиме негативний результат.

Для повноцінної 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 цього створюються спеціальні каталоги захисту ключів, які ведуться спеціальними організаціями – центрами сертифікації ключів (ЦСК). Відкритий ключ має бути затверджений ЦСК.

3.4 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 моделлю клієнт/сервер 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 рівнями взаємодії в мережі здійснюється відповідно до рекомендацій ISO/OSI.

Розподіл мережевих сервісів з метою захисту, на основі спеціалізованого протоколу для додатків, здійснюється в рамках:

- Створення облікових записів у базі даних обмеженого доступу;

- Конфігурація 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).

- Протокол розширеної автентифікації, що використовує відкриту криптологію;

- Діагностика та документування стану захищених ресурсних об'єктів.

Для мінімізації втрат якості роботи програм використовується потоковий принцип. У рамках цього принципу розпізнаються 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 запропонованим механізмом, який включає можливість захисту інформації від усіх загроз у множині, класифікація яких базується на можливості їх видалення. Це приклади помилок та закладок у програмному забезпеченні, а також загроз, які не повністю усунені, пов'язані з необхідністю доступу до інформації (доступ не можна заборонити, як наслідок, неможливо усунути ці загрози). Багаторівневий захист передбачає використання додаткових технічних можливостей зі специфічними вимогами щодо проектування системи.

З кількома рівнями захисту в корпоративних комунікаціях дотримуються таких тенденцій:

- Створення методів захисту робочих станцій та серверів, пов'язаних з корпоративною мережею, насамперед щодо платформи, на якій вони підтримуються - 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.

Досить складно забезпечити ефективний захист окремих комп'ютерів внутрішньої мережі, тому ефективніше захищати всю мережу в цілому. Щоб запобігти доступу зовнішнього світу до компонентів внутрішньої мережі, використовується архітектура брандмауера. Брандмауер - це композиція 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, включаючи бар'єри або екрани, що запобігають передачі певних типів трафіку та каналів. Шлюз – це машина або серія машин, що виконує послуги, що компенсують наслідки обробки.

3.5 Архітектура типової системи електронного документообігу та її відповідне обґрунтування.

Сучасні системи електронного документообігу: EMC Documentum, LanDocs System, "megapolis", "optima" та "farbroc".

Давайте обговоримо 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. Підсистема, призначена для ведення облікової та аналітичної інформації, – це набір програмних застосунків, які надають користувачам інструменти для створення документів, інтерактивний аналіз інформації та автоматизована оцінка діяльності корпорації. Основними обов'язками цієї підсистеми є: введення та ведення нормативно-інформаційних даних - класифікаторів, платіжних документів, актів тощо; створення та редагування первинних документів клієнта, 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 Access, яке підключено до SQL Server. Підсистема складається з наступних компонентів:

Допоміжні: "Нормативно-інформаційні документи", "Документи приймання та випуску", "Висновки експертів", "Платежі", "Контроль доступу"?

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

2. Підсистема, призначена для ведення електронного сховища документів та сприяння потоку документів. Вона складається з Сервера управління документами (DMS) та компонента бізнес-процедур, який поєднаний з ним (компонент потоку). Основними функціями цієї підсистеми є: автоматизація бізнес-процесів щодо координації документів; автоматизоване введення сканованих зображень документів у систему та організація роботи з ними; зберігання документів у системі, включаючи договірні та директивні документи.

3. Електронні публікації – це компонент системи публікації інформації на веб-сайті комп'ютерної літератури. Ця підсистема включає веб-сервер та CGI-програму, яка взаємодіє з банками даних через FTP. Основними обов'язками підсистеми є: оновлення та підтримка інформації на WWW-сервері; забезпечення доступу до інформації через Інтернет та Інтранет; автентифікація користувачів та надання доступу до їхньої інформації; організація способу доступу до інформації та її пошуку; також вона автентифікація користувачів.

4. Підсистема адміністрування та налаштування реалізована за допомогою стандартних функцій адміністрування Windows XP або інших версій MS Windows, створення правил їх використання та відповідної операційної документації.

Система реалізована в архітектурі локальної мережі, що базується на серверах під управлінням Windows 2008 та має клієнтів, що працюють під управлінням тієї ж системи. Програми працюють за протоколом "клієнт-сервер". Користувацький застосунок реалізовано як окремий клієнтський застосунок, розташований на файловому сервері та доступний клієнтським станціям.

Серверна частина. У випадку типового мережевого протоколу використовується TCP/IP, що полегшує взаємодію комп'ютерів з веб-сервером (Інтранет/Інтернет). Електронне архівування та управління документами здійснюється за допомогою DMS DOCS Open у поєднанні з компонентом організації бізнес-процедур WorkRoute та компонентом сканованих зображень документів Deltalmage. Створення документів, введення та адміністрування нормативної та іншої інформації, аналіз окремих документів та напрямків діяльності, статистичне обстеження діяльності корпорації в цілому та підготовка звітів реалізуються унікальним користувацьким застосунком, що базується на 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 застосунків.

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. Конфігурація клієнтів централізована системним адміністратором.

Використання сучасних методів проектування під час розробки технічних вимог до програмних продуктів дозволяє розподілити загальну функціональність у модулі, які можна використовувати 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 або за моделлю клієнт-сервер, або використовують електронну

пошту для передачі документів або для повної реплікації бази даних компонентів системи.

Наприклад, система електронного документообігу (СЕД) включає поштові скриньки клієнтів, які сприяють організованому розподілу документів між різними системами. СЕД 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. Ці інтерфейси також називаються IDAPI, що є інтегрованим інтерфейсом програмування баз даних, IBDE, що є інтегрованим механізмом баз даних Borland, та іншими. 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 взаємодії між програмою та поштою використовується інтерфейс MAPI від Microsoft, що дозволяє використовувати будь-яку електронну пошту (та пов'язаний з нею криптографічний захист), що підтримує MAPI.

Якщо користувач не може використовувати MAPI, доступна альтернатива – використання Spooler (спулер, програма, яка буферизує дані), яка має відкритий інтерфейс, сумісний з системами електронної пошти.

Як результат, 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.

В результаті короткого обговорення основних методологічних аспектів створення корпоративної системи електронного документообігу можна виділити основні методологічні принципи, які застосовувалися під час впровадження цієї

системи (електронні публікації, системи підтримки клієнтів, системи електронного 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 управління документацією, що підтримує всі перелічені вище завдання, дає змогу створювати повнофункціональні системи.

4. Використання промислових інструментів, таких як комплекси, для впровадження систем, що гарантує короткі терміни, легкість модифікації та розширення системи, а також низку інших переваг.

Рисунок 3.2. Схема архітектури типової системи електронного документообігу

EMC Documentum

EMC Documentum – це платформа для керування контентом, призначена для всього підприємства. Контент, або неструктурована інформація, представлений у різних формах: текстові документи, інженерні креслення, XML-документи, скановані паперові документи, аудіо- та відеофайли, а також безліч інших типів і форматів файлів. EMC Documentum спрощує створення контенту за допомогою популярних інструментів для робочого столу та простих

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

EMC Documentum використовує таксономію, метадані та категоризацію для підвищення інтелекту контенту, що досягається завдяки ефективнішим процесам 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 структури, не здатні 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 інфраструктуру або основу для рішення для управління контентом – фундаментальні компоненти. 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 поєднання технологій, що вирішують такі основні проблеми:

Управління документами (DocumentManagement).

• Управління веб-контентом (WebContentManagement).

• Управління активами з оцифруванням (AssetManagement with Digitization).

• Партнерство (Collaboration).

Створення зображень документів – це процес фотографування документів та їх зберігання на комп'ютері.

Управління звітами (ReportManagement).

• Архівування контенту (Content Archiving).

Адміністрування записів (records Administration).

Архівування електронної пошти (E-mailArchiving).

Управління бізнес-процесами (BPMS).

• Інтеграція підприємств та додатків (Enterprise-Application Integrations).

Інтеграція корпоративного контенту (enterprise content integration).

Електронне розкриття інформації (eDiscovery).

Впровадження нормативних вимог (Compliance).

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 кілька технологій для управління контентом. Функціональні рішення поділяються на три основні класи:

Управління організаційною документацією.

Управління технічними документами.

Управління фінансовими документами.

Завдання, які зазвичай виконуються сьогодні за допомогою системи:

• Адміністрування та зберігання документів. Рішення забезпечує функціональність, яка полегшує документальну підтримку управління в електронному управлінні документами.

Незважаючи на складність вимог до документів для організації праці з документами, система готова їх виконати 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-фактур. Рішення дозволяє інтелектуальне, високопродуктивне сканування, автоматизовану та пов'язану обробку документів, а також має можливість доступу до документів з інтерфейсу ERP-системи.

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

Технічні креслення та документація.

Рішення базується на сховищі контенту, яке керує всіма типами технічного контенту, включаючи креслення, схеми, таблиці, 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. Цю інформацію, включаючи специфікації продукту, маркетингові ресурси, веб-сторінки, дані про обслуговування клієнтів, контракти з постачальниками, електронні листи, фотографії тощо, часто називають корпоративним контентом і є результатом значних інвестицій в інтелектуальну власність, час і гроші. П'ять переваг рішень EMC для управління контентом та архівування включають:

Відповідність нормативним вимогам. Продукти EMC можуть допомогти вам досягти нормативних та урядових 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, угод про рівень обслуговування та покращують повторне використання контенту.

• Консолідація. Продукти EMC знижують загальну вартість володіння (порівняно з кількома програмами від різних постачальників), створюючи єдину стандартизовану інфраструктуру, яка не має ізольованого зберігання інформації та досягає економії масштабу.

Категорії документів, що підходять для сучасних систем електронного управління документами.

Критерії вибору сучасних систем електронного документообігу розглянуто в порівняльній таблиці.3.2.

Таблиця 3.2.

¶	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 набір програмного та апаратного забезпечення, що сприяє реалізації політик безпеки.

SSP в AS класу 2 повинен мати такі характеристики:

- бар'єр безпеки;

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

- система виявлення вразливостей (сканер);

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

Інструменти розділення повноважень користувачів;

- Консоль 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 заданих правил. Основне призначення мережевого екрана – запобігти доступу до комп’ютерів або окремих вузлів без авторизації. 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 брандмауера

• Вибір 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 до Інтернету, має локальну адресу призначення, але блокується. Ця функціональність присутня у всіх сучасних брандмауерах і характеризується високою швидкістю та відсутністю необхідності взаємодії з користувачем.

Фільтр 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 інформацію, проксі-сервер надсилає її від свого імені, а отримавши відповідь, пересилає її на потрібний комп'ютер у внутрішній мережі. Як загальновідомо, продуктивність не така висока, як під час видалення пакетів, але все ж достатня, оскільки змінюється лише заголовок пакета. Основною перевагою проксі-сервера є те, що він замінює реальні адреси ваших комп'ютерів своїми власними. Це виключає можливість цільового призначення конкретного комп'ютера в підмережі.

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

Буферизація даних. Це не є традиційною функцією брандмауерів, але зараз її використовують багато популярних програм. Концепція полягає в тому, що всі дані проходять через брандмауер, який може зберігати найпопулярнішу інформацію, а під час подальшого доступу до неї він видає її зі свого кешу.

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

Керування. Для персональних брандмауерів основним атрибутом є простота їх налаштування. Адміністрування брандмауерів переважно віддалене (за допомогою HTML-інтерфейс на основі або інший), це вимагає впевненості в надійності каналів авторизації та 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:

Створення каталогів (довідників) для нових користувачів, надання їм ресурсів та організація пріоритетів і прав доступу.

• налаштування системи, що включає встановлення параметрів середовища, додавання нового програмного та апаратного забезпечення до системи, налаштування топології корпоративної мережі, прив'язку певних завдань до відповідних системних серверів та налаштування системи для виробничого процесу.

Управління безпечним функціонуванням системи включає збір даних від служб інформаційної безпеки, контроль доступу користувачів та забезпечення безпеки від зовнішніх атак.

• Усунення помилок та збоїв, що включає пошук, розпізнавання, локалізацію та виправлення помилок у системі, моніторинг роботи системи та реєстрацію надзвичайних ситуацій, планування режиму резервного копіювання інформації, забезпечення швидкого відновлення системи після збоїв.

• Облік зусиль користувачів, підсистем та компонентів програми, що включає реєстрацію та облік використання обчислювальних ресурсів (витрачений час, операційний та дисковий простір), а також використання ліцензованого програмного забезпечення та платних баз даних і знань.

Вимірювання продуктивності системи включає збір та аналіз статистики щодо функціональності системи, оцінку ефективності використання ресурсів системи, розпізнавання найвищих елементів, втрат продуктивності та планування відновлення цих елементів, стратегічне планування щодо розширення системи та розвитку її можливостей.

Для виконання завдання система адміністрування повинна мати такі компоненти:

Інтерфейс системного адміністратора, який надає інформацію про стан системи, її операційну конфігурацію, доступ до файлів конфігурації та файлів журналів, що стосуються збору 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 та 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 навички 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 компонентів ОС, є особливо важливим.

- тестування компонентів ОС для забезпечення належної роботи.

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

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

- користувачів, які мають дозволи, 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 потрібно 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).

Інструкції для користувачів. 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.

Резервні копії. Постійне створення та підтримка резервних копій програм і даних ОС дозволяє мінімізувати збитки, спричинені збоями та відмовою компонентів системи.

Постійний моніторинг змін у конфігураційних даних та політиці безпеки операційної системи. Фактично, ми обговорюємо моніторинг засобів безпеки та інших компонентів ОС. 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 підсистема реєстрації подій налаштована належним чином, ці зміни в системі не залишаться непоміченими. Однак зловмисник, який змінює технологічну інформацію, зазвичай намагається «замести свій слід», знищуючи пов'язані записи журналу реєстрації. Як наслідок, важливо постійно моніторити зміни в системі. Крім того, необхідний метод автоматичного повідомлення адміністраторів про критичні зміни безпеки в системі та зберігання даних реєстрації, стійкий до пошкодження конкретної системи (наприклад, дзеркальне відображення журналу критичних подій на інші комп'ютери або друк записів найважливіших подій на принтері).

3.6 Висновки по розділу

1. У третій частині кваліфікаційного завдання описано атрибути використання SEDO в корпоративній мережі.

2. Розкрито атрибути функціональних можливостей систем електронного

3. Описано модель застосування та пояснено обов'язки електронного підпису.

4. Подано архітектуру типової системи електронного документообігу та визначено критерії обґрунтування її побудови та складу.

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 SEDO. Встановлено обов'язки, структуру та порядок функціонування системи електронного документообігу.

3. У третій частині кваліфікаційного завдання описано атрибути інтеграції SEDO 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

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 документоо-бігу: 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 №852-IV

9. Асеєв Г.Г. Електронний документообіг: підр. для студ. – Х.: ХДАК, 2000. – 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

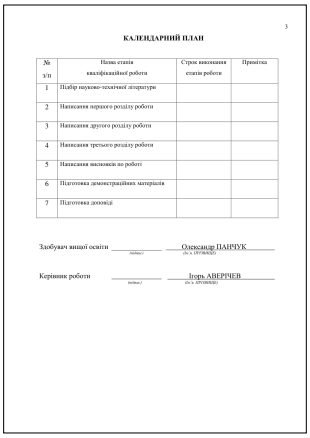
15. URL:http://www.star-force.ru/upload/iblock/73f/T_Comm_june.pdf

16. URL:http://www.microsoft.com/Ukraine/Government/Newsletters/DocFlow

ДОДАТОК А

Удосконалення системи захисту центру електронного документообігу корпоративної мережі

- Магістерська робота: Олександр ПАНЧУК
- Спеціальність 125 «Кібербезпека та захист інформації»
- Фокус: електронний документообіг, конфіденційні дані, корпоративна мережа, захист від НСД



3

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 _____ Олександр ПАНЧУК
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ Ігорь АВЕРЧЄВ
(підпис) (ім'я, ПРІЗВИЩЕ)

Актуальність дослідження

- Об’єкти інформаційної діяльності обробляють значні обсяги інформації з обмеженим доступом.
- Центр електронного документообігу є критичним вузлом корпоративної мережі.
- Порушення цілісності, конфіденційності або доступності документів створює організаційні, правові та репутаційні ризики.

Мета, об’єкт і предмет роботи

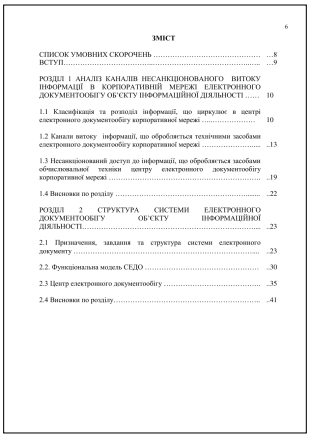
- Мета: удосконалення системи кібернетичного захисту центру електронного документообігу конфіденційних даних корпоративної мережі.
- Об’єкт: процес захисту інформації на об’єкті інформаційної діяльності.
- Предмет: система кібернетичного захисту центру електронного документообігу корпоративної мережі.

Основні завдання дослідження

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

Структура магістерської роботи

- Розділ 1 - канали несанкціонованого витоку інформації в корпоративній мережі СЕДО.
- Розділ 2 - структура системи електронного документообігу об’єкта інформаційної діяльності.
- Розділ 3 - удосконалення системи кібернетичного захисту центру електронного документообігу.

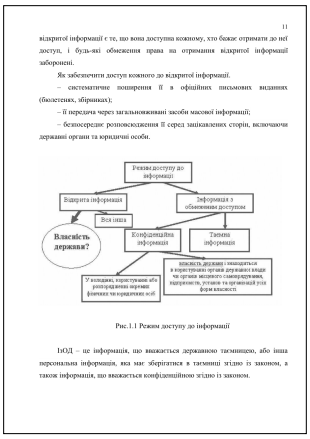


6

ЗМІСТ

Інформація з обмеженим доступом у СЕДО

- У центрі електронного документообігу циркулюють відкриті дані, конфіденційна інформація та службові документи.
- Ключові властивості захисту: конфіденційність, цілісність, доступність та контрольованість операцій.
- Режим доступу має бути формалізований через ролі, права користувачів та журналювання дій.



11

відкритої інформації є те, що вона доступна кожному, хто бажає отримати до неї доступ, і будь-які обмеження права на отримання відкритої інформації заборонені.

Як забезпечити доступ кожного до відкритої інформації.

– систематичне поширення її в офіційних письмових виданнях (бюлетенях, збірниках);

– її передача через загальноприйняті засоби масової інформації;

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

Рис.1.1 Режим доступу до інформації

ІнОД – це інформація, що вважається державною таємницею, або інша персональна інформація, яка має зберігатися в таємниці згідно із законом, а також інформація, що вважається конфіденційною згідно із законом.

Канали несанкціонованого витоку інформації

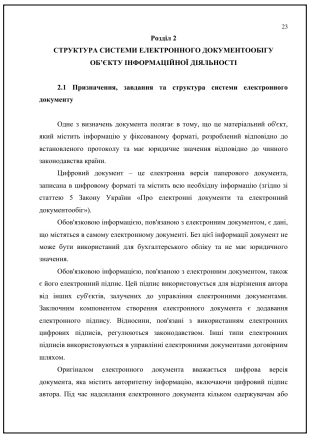
- Технічні канали виникають під час обробки, передавання, зберігання та відображення даних.
- Небезпечними є електромагнітні, електричні, параметричні, вібраційні та мережеві канали.
- Захист потребує поєднання технічних, програмних і режимно-організаційних заходів.

Несанкціонований доступ у корпоративній мережі

- Основні сценарії: компрометація облікових записів, доступ до службових каталогів, зміна або копіювання документів.
- Порушення можуть здійснюватися зовнішнім порушником або інсайдером.
- Пріоритетним є обмеження доступу до критичних ресурсів та контроль усіх дій із документами.

Система електронного документообігу

- СЕДО забезпечує створення, реєстрацію, маршрутизацію, погодження, підписання, зберігання та пошук документів.
- Електронний документ має реквізити, автора, електронний підпис і визначену юридичну силу.
- Централізація документообігу підвищує керованість, але концентрує ризики безпеки.



23

Розділ 2

СТРУКТУРА СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Призначення, завдання та структура системи електронного документу

Одне з визначень документа полягає в тому, що це матеріальний об'єкт, який містить інформацію у фіксованому форматі, розроблений відповідно до встановленого протоколу та має юридичне значення відповідно до чинного законодавства країни.

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»).

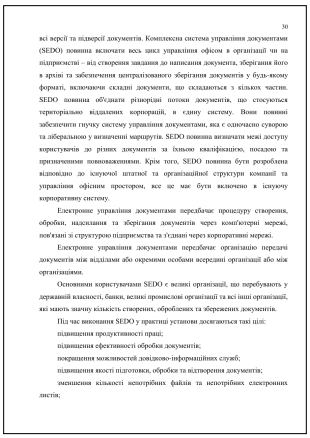
Обов'язковою інформацією, пов'язаною з електронним документом, є дані, що містяться в самому електронному документі. Без цієї інформації документ не може бути використаний для бухгалтерського обліку та не має юридичного значення.

Обов'язковою інформацією, пов'язаною з електронним документом, також є його електронний підпис. Цей підпис використовується для відділення 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 типи електронних підписів використовуються в управлінні електронними документами договірним шляхом.

Оригіналом електронного документа вважається цифрова версія документа, яка містить авторитетну інформацію, включаючи цифровий підпис автора. Під час надсилання електронного документа кільком одержувачам або

Функціональна модель СЕДО

- Функціональна модель описує взаємодію користувачів, документів, маршрутів погодження, архіву та засобів контролю.
- Критичні функції: автентифікація, розмежування доступу, контроль версій, протоколювання, резервне копіювання.
- Модель має підтримувати захист як на рівні документа, так і на рівні мережевої інфраструктури.



30

всі версії та підверсії документів. Комплексна система управління документами (SEDO) повинна включати весь цикл управління офісом в організації чи на підприємстві – від створення завдання до написання документа, зберігання його в архіві та забезпечення централізованого зберігання документів у будь-якому форматі, включаючи складні документи, що складаються з кількох частин. SEDO повинна об'єднати різнорідні потоки документів, що стосуються територіально віддалених корпорацій, в єдину систему. Вони повинні забезпечити гнучку систему управління документами, яка є одночасно суворою та зберігальною у визначені маршрутів. SEDO повинна визначати межі доступу користувачів до різних документів за їхньою кваліфікацією, посадою та призначеними повноваженнями. Крім того, SEDO повинна бути розроблена відповідно до існуючої штатної та організаційної структури компанії та управління офісним простором, все це має бути включено в існуючу корпоративну систему.

Електронне управління документами передбачає процедуру створення, обробки, надсилання 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 відділами або окремими особами всередині організації або між організаціями.

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 виконання SEDO у практиці установи досягаються такі цілі:

підвищення продуктивності праці;

підвищення ефективності обробки документів;

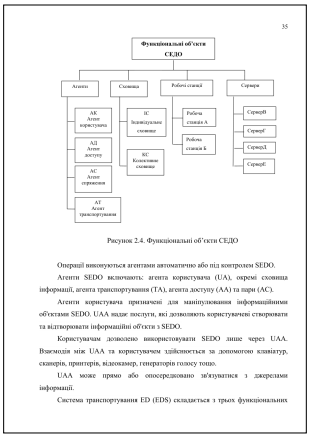
покращення можливостей довідково-інформаційних служб;

підвищення якості підготовки, обробки та відтворення документів;

зменшення кількості непотрібних файлів та непотрібних електронних листів;

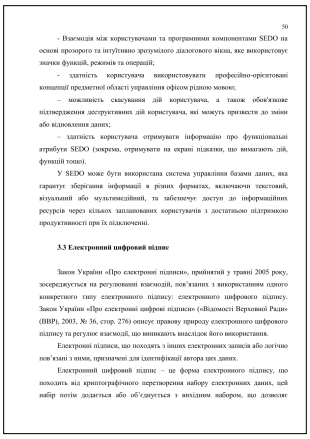
Центр електронного документообігу

- Центр СЕДО виконує роль вузла обробки документів і координує обмін даними в корпоративній мережі.
- У центрі накопичуються конфіденційні дані, тому він потребує підвищеного рівня адміністрування та моніторингу.
- Захисні механізми мають охоплювати сервери, робочі місця, канали зв’язку та сховища даних.



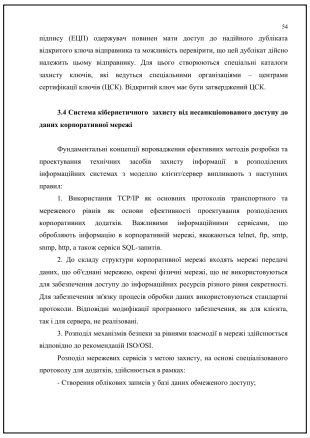
Електронний цифровий підпис

- ЕЦП підтверджує авторство документа та забезпечує контроль його цілісності.
- Підписування документів має супроводжуватися перевіркою сертифікатів і прав підписанта.
- Використання ЕЦП знижує ризик підроблення, несанкціонованої зміни та заперечення авторства.



Система кібернетичного захисту СЕДО

- Базові рівні: ідентифікація користувачів, автентифікація, авторизація, шифрування, резервне копіювання та аудит.
- Засоби захисту мають охоплювати серверний сегмент, клієнтські робочі місця, мережеві шлюзи та канали передавання.
- Ціль - зменшити ймовірність НСД та підвищити стійкість системи до інцидентів.



54

підпису (ЕЦП) одержувач повинен мати доступ до надійного дубліката відкритого ключа відправника та можливість перевірити, що цей дублікат дійсно належить цьому відправнику. Для цього створюються спеціальні каталоги захисту ключів, які ведуться спеціальними організаціями — центрами сертифікації ключів (ЦСК). Відкритий ключ має бути затверджений ЦСК.

3.4 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 моделлю клієнт/сервер 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.

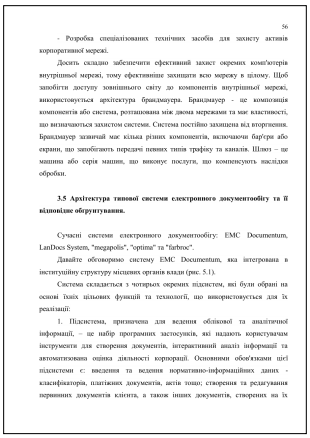
3. Розподіл механізмів безпеки за рівнями взаємодії в мережі здійснюється відповідно до рекомендацій ISO/OSI.

Розподіл мережевих сервісів з метою захисту, на основі спеціалізованого протоколу для додатків, здійснюється в рамках:

- Створення облікових записів у базі даних обмеженого доступу;

Архітектура захищеної СЕДО

- Раціональна архітектура передбачає сегментацію мережі, окремі зони доступу та контроль трафіку між ними.
- Для захисту застосовуються міжмережеві екрани, антивірусний контроль, DLP/журналювання, резервування та моніторинг.
- Критеріями обґрунтування є функціональність, надійність, масштабованість, вартість та відповідність вимогам захисту.



56

- Розробка спеціалізованих технічних засобів для захисту активів корпоративної мережі.

Досить складно забезпечити ефективний захист окремих комп'ютерів внутрішньої мережі, тому ефективніше захищати всю мережу в цілому. Щоб запобігти доступу зовнішнього світу до компонентів внутрішньої мережі, використовується архітектура брандмауера. Брандмауер - це композиція 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, включаючи бар'єри або екрани, що запобігають передачі певних типів трафіку та каналів. Шлюз – це машина або серія машин, що виконує послуги, що компенсують наслідки обробки.

3.5 Архітектура типової системи електронного документообігу та її відповідне обґрунтування.

Сучасні системи електронного документообігу: EMC Documentum, LanDocs System, "megapolis", "optima" та "farbroc".

Давайте обговоримо 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. Підсистема, призначена для ведення облікової та аналітичної інформації, – це набір програмних застосунків, які надають користувачам інструменти для створення документів, інтерактивний аналіз інформації та автоматизовано оцінка діяльності корпорації. Основними обов'язками цієї підсистеми є: введення та ведення нормативно-інформаційних даних - класифікаторів, платіжних документів, актів тощо; створення та редагування первинних документів клієнта, а також інших документів, створених на їх

Практичні рекомендації

- Впровадити рольову модель доступу до документів та регламент регулярного перегляду прав.
- Застосувати захищені канали зв’язку, резервне копіювання, контроль цілісності та централізований журнал подій.
- Організувати аудит дій користувачів, перевірку ЕЦП, антивірусний контроль і навчання персоналу.

Висновки

- Проаналізовано канали несанкціонованого витоку інформації в корпоративній мережі електронного документообігу.
- Розглянуто структуру та функціональні можливості системи електронного документообігу ОІД.
- Запропоновано напрями удосконалення системи кібернетичного захисту центру СЕДО конфіденційних даних.