Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Острівного Данііла Андрійовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***Методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
Спеціальний	ст. викл. Мєшков В.І.			
Економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

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

спеціальності ***125 Кібербезпека***

спеціалізації[1]

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

на тему ***методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***система електронного документообігу ІТС комерційного підприємства***

Предмет досліджень ***методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства***

Мета ***підвищення рівня захищеності системи електронного документообігу комерційного підприємства***

Вихідні дані для проведення роботи ***результати досліджень при проходженні виробничої та переддипломної практики***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***розробці політики безпеки для системи електронного документообігу ІТС комерційного підприємства***

Практична цінність ***полягає в наданні рекомендацій щодо забезпечення достатнього рівня захищеності системи електронного документообігу комерційного підприємства***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

ЗУ «Про Інформацію», ЗУ « Про захист персональних даних», ЗУ « Про електроні довірчі послуги», ЗУ «Про захист інформації в інформаційно-комунікаційних системах»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

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

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***досягається завдяки впровадження системи захисту СЕД ІТС комерційного підприємства, що дає змогу знизити затрати на відновлення системи після можливої атаки чи поломки на вузлах ІТС***

Соціальний ефект ***досягається завдяки впровадження рекомендацій для користувачів системи, адміністратора безпеки***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Острівний Д.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 143 с., 4 рис., 15 табл., 4 додатки, 62 джерел.

Об’єкт дослідження: система електронного документообігу ІТС комерційного підприємства.

Предмет досліджень: методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства.

Мета магістерської дипломної роботи: підвищення рівня захищеності системи електронного документообігу комерційного підприємства.

В першому розділі магістерської дипломної роботи були розкриті основні поняття електронного документообігу, визначені переваги, що отримає організація від застосування СЕД та особливості впровадження такої системи. Також були визначені основні складові частини СЕД, їх особливості. Окремо були розглянуті суб’єкти системи електронного документообігу.

У другому розділі дипломної роботи була проведена класифікація інформації, що циркулює на типовому комерційному підприємстві, виконаний аналіз інформаційних потоків, наданий перелік найбільш суттєвих загроз інформаційній безпеці підприємства. Досліджені наявні СЕД за розробленими критеріями, а також методи та моделі безпеки інформації в системах електронного документообігу. Реалізований стандартний функціональний профіль захищеності 3.КЦД.1 для СЕД підприємства.

Наукова новизна полягає у розробці політики безпеки для системи електронного документообігу ІТС комерційного підприємства.

СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ, АНАЛІЗ ЗАГРОЗ, БЕЗПЕКА ІНФОРМАЦІЇ, МОДЕЛІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ.

РЕФЕРАТ

Пояснительная записка: 143 с., 4 рис., 15 табл., 4 приложений, 62 источников.

Объект исследования: система электронного документооборота ИТС коммерческого предприятия.

Предмет исследований: методы и модели обеспечения безопасности информации в системах электронного документооборота коммерческого предприятия.

Цель магистерской дипломной работы: повышение уровня защищенности системы электронного документооборота коммерческого предприятия.

В первом разделе магистерской дипломной работы были раскрыты основные понятия электронного документооборота, определены преимущества, получит организация от применения СЭД и особенности внедрения такой системы. Также были определены основные составные части СЭД, их особенности. Отдельно были рассмотрены субъекты системы электронного документооборота.

Во второй главе дипломной работы была проведена классификация информации, циркулирующей на типичном коммерческом предприятии, выполненный анализ информационных потоков, предоставленный перечень наиболее существенных угроз информационной безопасности предприятия. Исследованы имеющиеся СЭД по разработанным критериям, а также методы и модели безопасности информации в системах электронного документооборота. Реализован стандартный функциональный профиль защищенности 3.КЦД.1 для СЭД предприятия.

Научная новизна заключается в разработке политики безопасности для системы электронного документооборота ИТС коммерческого предприятия.

СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА, АНАЛИЗА УГРОЗ, БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

ABSTRACT

Explanatory note: 143 p., 4 fig., 15 tab., 4 application, 62 sources.

Object of research: the system of electronic document circulation of ITS commercial enterprise.

Subject of research: methods and models of information security in electronic document management systems of a commercial enterprise.

The purpose of the master's thesis: to increase the level of security of the electronic document management system of the commercial enterprise.

In the first section of the master's thesis, the basic concepts of electronic document circulation were disclosed, the advantages that the organization will receive from the use of EDMS and the peculiarities of the introduction of such a system. Also, the main components of the EDMS, their features were determined. Separately, subjects of the electronic document management system were considered.

In the second section of the thesis there was a classification of information circulating on a typical commercial enterprise, an analysis of information flows was carried out, a list of the most significant threats to the information security of the enterprise was provided. Existing EDMS have been studied based on the criteria developed, as well as methods and models of information security in electronic document management systems. A standard functional security profile has been implemented. 3.CIA.1 for Enterprise EDMS.

The scientific novelty consists in developing a security policy for the electronic document management system of the ITS commercial enterprise.

ELECTRONIC DOCUMENT SECURITY SYSTEM, ANALYSIS OF THREAT, SAFETY OF INFORMATION, MODELS FOR SAFETY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС — автоматизована система;
АСД — автоматизована система документообігу;
АЦСК — акредитований центр сертифікації ключів;
БД — база даних;
ВЧ — високочастотні (нав’язування);
ГАІС — глобальна автоматизована інформаційна система;
Д — доступність;
ЕД — електронний документ;
ЖЦ — життєвий цикл;
ЗЦ — засвідчувальний центр;
ІзОД — інформація з обмеженим доступом;
ІС — інформаційна система;
ІТ — інформаційні технології;
ІТС — інформаційно-телекомунікаційна система;
К — конфіденційність;
КАІС — корпоративна автоматизована інформаційна система;
КЗ — контрольована зона;
КІС — корпоративна інформаційна система;
КО — контролюючий орган;
КСЕД — корпоративна система електронного документообігу;
ЛОМ — локальна обчислювальна мережа;
МІП — модель інформаційних потоків;
НСД — несанкціонований доступ;
ОА — об'єкт автоматизації;
ОІД — об’єкт інформаційної діяльності;

ОО — об'єктно-орієнтований;

ООБД — об'єктно-орієнтована база даних;

ПЕМВН — побічні електромагнітні випромінювання та наводки;

ПЗ — програмне забезпечення;

ПК — персональний комп’ютер;

ППЗ — прикладні програмні засоби;

САД — система автоматизації документообігу;

САДП — системи автоматизації ділових процесів;

СЕД — система електронного документообігу;

СІП — схема інформаційних потоків;

СКБД — система керування базами даних;

СКД — система керування документами;

СКЗІ — система керування захистом інформації;

ТОВ — товариство з обмеженою відповідальністю;

Ц — цілісність;

ЦЗО — центральний засвідчувальний орган;

ЦСК — центр сертифікації ключів;

HSM — Hierarchical Storage Management;

OLAP — On-Line Analytical Processing;

UML — уніфікована мова моделювання.

ЗМІСТ

с.

ВСТУП

Системи електронного документообігу (СЕД) можуть сприяти створенню нової організаційної культури в компаніях, зробивши роботу працівників з документами легшою і продуктивнішою. СЕД дають змогу працювати не тільки над виконанням внутрішніх завдань, а й спільними зусиллями вирішувати широкий спектр проблем. Основні функції СЕД забезпечують перехід на якісно новий рівень організації бізнес-процесів корпорацій.

Автоматизація діловодних процесів є обов'язковою умовою раціональної організації діловодства в компаніях та її філіях, засобом підвищення ефективності та здешевлення управлінської діяльності. Можна відзначити, що автоматизація використовується на всіх етапах діловодного процесу: підготовка документів, їх копіювання, оперативне зберігання і транспортування, контроль за виконанням тощо.

Програмно-технічні засоби автоматизації діловодних процесів сумісні та передбачають їх об'єднання в єдину корпоративну обчислювальну мережу. З метою інтегрування документального середовища в єдиний інформаційний простір, а також оптимізації завантаження технічних засобів та запобігання їх простою використовують обчислювальні інформаційні мережі та технологію «клієнт-сервер». Комплекс програмно-технічних засобів підсистеми діловодства та контролю забезпечує збирання, опрацювання та передавання інформації в електронному вигляді, сумісному з інформаційними системами державних органів. Керівництво відповідає за ефективність та дотримання посадовими особами правил використання засобів автоматизованого опрацювання інформації, а також за знання посадовими особами правил користування програмно-технічними засобами в межах їхніх службових обов'язків.

Під час одночасної роботи із документом відразу декількох користувачів (особливо якщо його необхідно погоджувати в різних інстанціях) дуже зручною функцією СЕД є використання версій і підверсій документа. Припустимо,

виконавець створив першу версію документа і передав її на розгляд наступному користувачеві. Другий користувач змінив документ і створив на його основі вже нову версію. Потім він передав свою версію документа третьому користувачеві в наступну інстанцію, що створив уже третю версію. Через певний час, ознайомившись із зауваженнями і виправленнями, перший виконавець документа вирішує доопрацювати вихідну версію і на її основі створює підверсію першої версії документа. Перевагою СЕД є реалізована в них можливість автоматичного відстеження версій і підверсій документів (користувачі завжди можуть визначити, який документ є найактуальнішим за версією або часом його створення).

СЕД також виконує функцію захисту даних, оскільки загрозу інформації становлять злочинні дії різного роду, такі як шахрайство, шпигунство, саботаж, вандалізм, незаконне знищення або спотворення документів, недотримання законодавчих і нормативних вимог до діловодства і документообігу, особливо до термінів зберігання і порядку знищення документів, – внаслідок чого можливі штрафи, програш цивільних позовів, і навіть кримінальне переслідування, ненавмисне розкриття персональної інформації й інформації, захищеної як інтелектуальна власність, а також різного роду катастрофічні явища – як природні, так і зумовлені діяльністю людини.

Застосування СЕД в організаціях усіх форм власності є необхідною умовою коректної роботи всієї системи. Тому обґрунтування вибору певного виду та побудова моделі безпеки системи електронного документообігу на сьогоднішній день є актуальною задачею.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Основні поняття документообігу

У загальнодержавних стандартах термін «документообіг» означає контрольований рух готових документів як всередині організації, так і за її межами. Електронний документообіг охоплює ще й стадії підготовки документів і вільний обмін інформацією у комп’ютерних мережах.

У світі існують два основних типи документів – паперові та – електронні. Паперові документи породжують електронні (наприклад, сканування документа), і навпаки, електронні – паперові документи (наприклад, процес друку документа).

Відповідно до статті 5 Закону України «Про електронні документи та електронний документообіг» Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Обов’язковим реквізитом електронного документа є обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили. [21]

Електронний підпис є обов’язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб’єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа. Відносини, пов’язані з використанням електронних цифрових підписів, регулюються законом. Використання інших видів електронних підписів в електронному документообігу здійснюється суб’єктами електронного документообігу на договірних засадах. [22]

Оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним цифровим підписом автора. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Це може бути текст або електронна форма Microsoft Word, таблиця Excel, повідомлення у форматі електронної пошти. Файли документів можуть бути неструктурованими (звичайні текстові документи) або структурованими. Останні містять елементи структури, що надає зовнішнім додаткам можливість їх розпізнання (форми Word, електронні таблиці, документи у форматі XML). Ще одним різновидом даної групи документів є файли збірних («складених») документів, наприклад файли Binder Microsoft Office.

Електронна копія електронного документа засвідчується у порядку, встановленому законом. Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Система електронного документообігу (СЕД) повинна підтримувати роботу з усіма типами документів, забезпечуючи прозору навігацію користувачів по всьому доступному інформаційному простору і, за необхідності, безболісно підключати до системи інші типи документів, визначаючи при цьому регламент їхньої обробки. Основним принципом організації систем роботи з ЕД є принцип «інформаційної парасольки» – працювати з усіма типами документів, що пов'язані з життєдіяльністю підприємства.

Життєвий цикл документа (ЖЦ) – це існування документа від моменту його створення до моменту його знищення. [1-63]

Життєвий цикл документа складається з двох основних стадій.

1 Стадія розробки документа, яка включає:

– власне розробку самого документа;

– оформлення документа (реєстрація);

– затвердження документа.

Якщо документ перебуває в стадії розробки, він вважається неопублікованим, і права на документ визначаються правами доступу конкретного користувача.

2 Стадія опублікованого документа, яка включає:

– активний доступ;

– архівацію і розархівацію (короткострокове збереження, довгострокове збереження);

– знищення документа.

Коли документ переходить з першої на другу стадію, він стає опублікованим, і права на документ залишаються тільки одні – доступ на читання. Прикладом опублікованого документа може бути шаблон стандартного бланка підприємства. Крім права доступу на читання, можуть існувати права на переведення опублікованого документа в стадію розробки. Залежно від конкретної стадії життєвого циклу документа архіви підрозділяються на такі типи:

– статичні архіви документів – системи, що мають справу тільки з опублікованими документами;

– динамічні архіви документів – системи, що мають справу як з опублікованими документами, так і з тими, що знаходяться в розробці.

1.2 Переваги використання системи електронного документообігу

За даними Forrester Research, 38% компаній зі списку Fortune 500 вважають що придбання сучасної СЕД є критично важливим для успішного ведення їхнього бізнесу. Відповідно до думки галузевих аналітиків (таких думок, що відрізняються у визначених моментах одна від одної, існує досить

велика кількість) користь для корпоративних користувачів при впровадженні СЕД досить значуща. Наприклад, за даними Siemens Business Services, при використанні СЕД:

– Продуктивність праці персоналу збільшується на 20-25%;

– Вартість архівного збереження електронних документів зменшується на 80%, що нижче в порівнянні із вартістю збереження паперових архівів.

Прийнято також вважати, що при впровадженні СЕД здобуваються тактичні і стратегічні вигоди. Тактичні вигоди визначаються скороченням витрат при впровадженні СЕД, зв'язаним із: звільненням фізичного місця для збереження документів; зменшенням витрат на копіювання і доставку документів у паперовому вигляді; зниженням витрат на персонал і устаткування та ін. До стратегічного відносяться переваги, зв'язані з підвищенням ефективності роботи підприємства або організації. До таких переваг можна віднести: поява можливості колективної роботи над документами (що неможливо при паперовому діловодстві); Значне прискорення пошуку і вибірки документів (по різних атрибутах); підвищення безпеки інформації за рахунок того, що робота в СЕД з незареєстрованної робочої станції неможлива, а кожному користувачеві СЕД призначаються свої повноваження доступу до інформації; підвищення схоронності документів і зручності їхнього збереження, тому що вони зберігаються в електронному виді на сервері; поліпшення контролю за виконанням документів. [1-63]

1.3 Перехід до електронного документообігу на підприємстві

Документ, як будь-яка річ, що приносить прибуток і допомагає в бізнесі, так само потребує і витрат. Як відомо, підвищувати прибуток можна шляхом зниження витрат.

Визначимо переваги електронних документів, які полягають у можливості:

1 Обслуговувати клієнта краще.

Мета будь-якої організації – обслуговувати краще своїх клієнтів. Упровадження систем електронного документообігу дозволяє виконувати цю задачу більш ефективно. При роботі з ЕД час пошуку документа, а отже й час реакції на запит, набагато менший, ніж при роботі з паперовими документами. Клієнт одержує відповідь швидше, ніж раніше, і, природно, задоволений набагато більше;

2 Управляти інформацією більш ефективно.

Керування життєво важливими документами, збереженими в електронному вигляді, радикально поліпшується.

Працівник може:

– одержувати доступ до документів швидше;

– не губити документи;

– перейти до засобів правильного зберігання документів;

– збирати, опрацьовувати документи у більшій кількості, ніж раніше, і приймати рішення швидше і точніше;

3 Захищати документи краще.

Технологія дозволяє зберігати ключову інформацію на оптичних або магнітних носіях.

Відразу дає значні переваги, а саме, забезпечує:

– захист від втрати або ушкодження. Втрата всієї або частини інформації для підприємства може загрожувати значними наслідками, аж до банкрутства і повного припинення діяльності. З папером усе набагато складніше, ніж з електронними носіями інформації. Папір схильний до багатьох «хвороб», а саме – старіння, небезпеки нагрівання і вогню. Крім того, дуже важко зробити копію всього архіву паперових документів на випадок непередбачуваних обставин. Це викликано, по-перше, високою вартістю збереження, по-друге, високою вартістю і тривалим часом копіювання документів. У випадку з електронними носіями усе навпаки. Компактність, швидкість і дешевина копіювання дозволяють робити і зберігати стільки копій інформації, скільки потрібно для забезпечення надійності бізнесу;

– захист від несанкціонованого доступу. Електронні носії дозволяють зберегти більше інформації в меншому обсязі. Отже менший обсяг дешевше захищати. Крім того, електронна інформація легше обробляється, процес криптозахисту інформації можна автоматизувати і виконувати швидше і дешевше.

4 Підвищити продуктивність праці.

Праця будь-якого співробітника має дві основні складові – продуктивну і забезпечувальну діяльність. Залежно від категорії працівника і виду діяльності співвідношення цих складових різне, але при будь-якому розкладі частка забезпечувальної діяльності залишається чималою. [1-63]

Операції з паперовими й електронними документами відносяться до забезпечувальної діяльності, і, отже, скорочуючи час на ці операції, ми скорочуємо частку цієї діяльності, звільняючи час для продуктивної праці. Крім продуктивності праці окремої людини, перехід до електронних документів радикально підвищує продуктивність праці робочих груп (при цьому перехід до обробки електронних документів ні в якому разі не варто розглядати як самоціль). Робота з електронними документами разом з мережевими технологіями дозволяє одночасно багатьом користувачам із робочої групи одержувати доступ до документів, що досить проблематично і дорого при роботі з паперовими документами. А якщо організація у своїй діяльності використовує такі технології, як workflow і groupware, то це надає можливість взаємодії співробітників всередині всіх її підрозділів, що дозволяє уникнути дублювання функцій і задач і, отже, ще знизити витрати;

5 Зменшувати витрати:

– на обробку паперу. При роботі з електронними документами немає потреби робити паперові копії документів для того, щоб вони стали доступні кільком співробітникам організації одночасно. Крім того, це зменшує необхідність наймати на роботу кур’єрів для збору і доставки документів, що забезпечують інфраструктуру передачі інформації між співробітниками;

– на устаткування. Сканер, факс-плата, програмне забезпечення можуть коштувати менше, ніж високопродуктивне копіювальне і факс-устаткування;

– на підтримку процесу обробки. Збереження документів в електронному вигляді може знизити потребу в таких предметах, як скріпки, степлери, папки і шафи для паперів;

– на збереження. Звільнення реальної, фізичної площі, необхідної для зберігання документів, забезпечення необхідних умов для зберігання паперових документів, створення копій документів тощо. [1-63]

Однак можна виділити труднощі трьох рівнів при переході на безпаперову технологію роботи з документами:

а) технічна неготовність організацій для роботи з електронними документами (що може виражатися як у тривіальній проблемі відсутності комп'ютера на столах у співробітників, так і в тому, що в організації немає необхідних програмно-апаратних засобів для переходу документів з однієї форми представлення до іншої – від паперового до електронного – через відсутність сканера);

б) технологічна недопустимість переходу окремих категорій конфіденційних документів в електронний вид (служби безпеки вимагають, щоб такого роду документи передавалися під розпис через довірену особу або кур'єра). Не можна випускати з поля зору і таку обставину, як відсутність у багатьох високопоставлених співробітників (керівна ланка) вільного часу для постійного спілкування з комп'ютером, що призводить до процедури переводу документа з електронного виду в паперовий (через друк) або навпаки (шляхом сканування) і створення, наприклад, версій документа;

в) законодавча неврегульованість електронного документообігу. Навіть, якщо в межах окремо взятої компанії або організації вирішили перейти до безпаперової роботи з документами, компанія все одно не зможе існувати ізольовано – між нею і зовнішнім світом постійно циркулюють різноманітного роду документи. Виникає необхідність законодавчого вирішення питання, що власне слід розуміти під електронним документом і який його вид може мати

юридичну силу (питання, пов’язані з достовірністю документів, що пересилаються, достовірністю підписів посадових осіб тощо).

1.4 Очікувані результати впровадження

Забезпечення більш ефективного керування документами за рахунок автоматичного контролю виконання, прозорості діяльності організації на всіх рівнях.

Підтримка ефективного накопичення, керування і доступу до інформації і знань. Забезпечення кадрової гнучкості за рахунок більшої формалізації діяльності кожного співробітника і можливості збереження всієї передісторії його діяльності.

Усунення дублювання і багаторазового перетворення інформації.

Забезпечення чіткої авторизації доступу до комерційної інформації, за рахунок чого підвищується персональна відповідальність співробітників за виконані дії строго в рамках наданих повноважень.

Протоколювання діяльності підприємства в цілому (внутрішні службові розслідування, аналіз діяльності підрозділів, виявлення «гарячих точок» у діяльності).

Оптимізація бізнес-процесів і автоматизація механізму їхнього виконання і контролю.

Виключення або максимально можливе скорочення обороту паперових документів на підприємстві. Економія ресурсів за рахунок скорочення витрат на керування потоками документів в організації.

Виключення необхідності чи істотне спрощення і здешевлення збереження паперових документів за рахунок наявності оперативного електронного архіву.

Єдиний інформаційний простір.

Рішення з автоматизації діловодства та контролю виконання документів надає можливість територіально розгалуженому підприємству «Головне підприємство – Районні управління» функціонувати в єдиному інформаційному

просторі. Це забезпечується створенням в підприємстві актуальної центральної бази даних, яка оперативно оновлюється інформацією з баз даних управлінь. Кожен документ чи об`єкт вводиться в систему один раз і після збереження стає доступним всім іншим підсистемам.

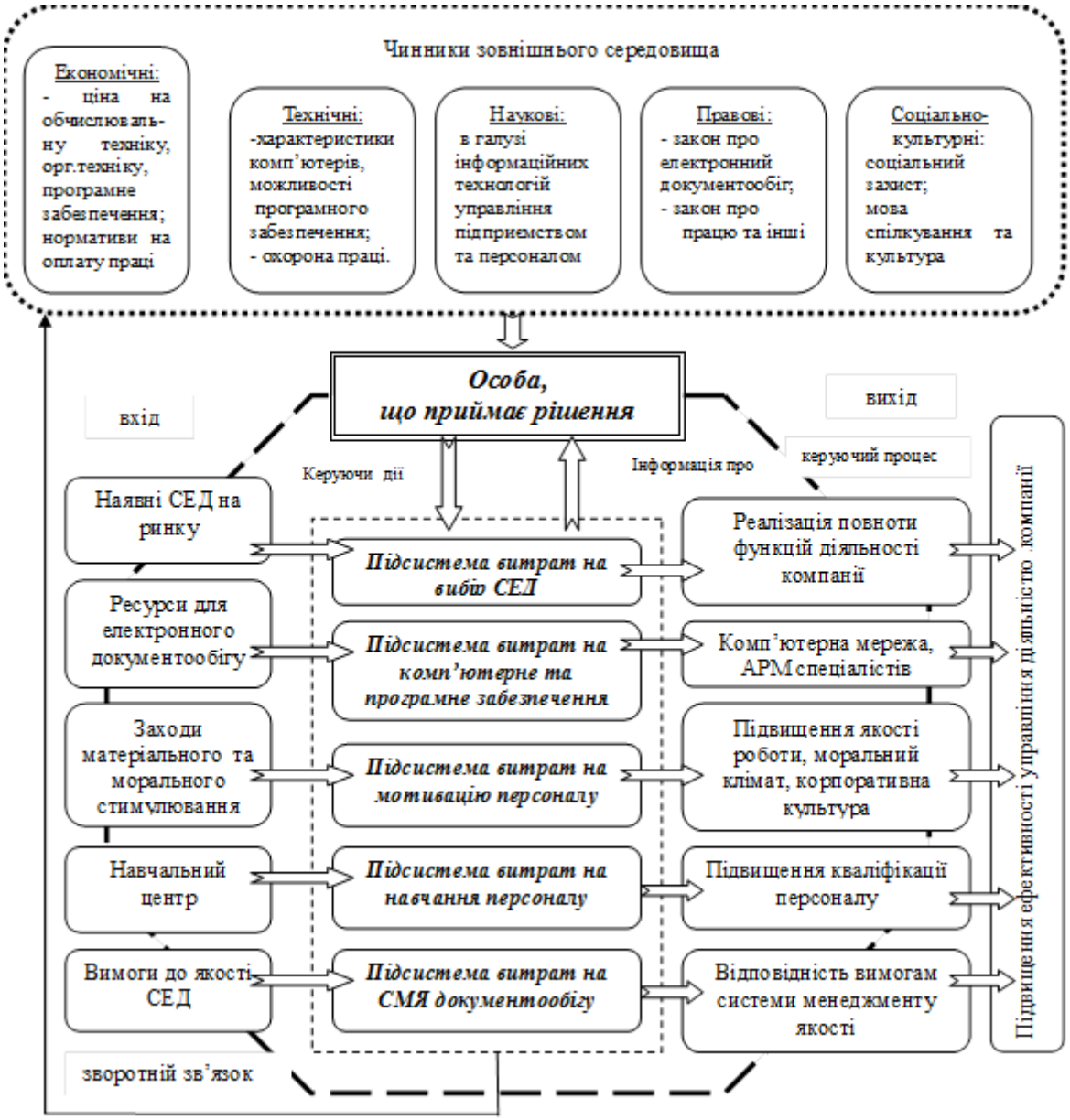

Рисунок 1.1 – Система управління витратами на організацію електронного документообігу

Створення електронного архіву.

Створення довготривалого збереження документів та управління електронним архівом, враховуючи процедури списання, та знищення документів. Створення надійного єдиного сховища для документів і знань, до

якого працівники та клієнти фірми мали б зручний доступ звідусіль та у будь-який час. Забезпечення атрибутивного та повнотекстового пошуку. Можливість настроювати кожним користувачем індивідуально результати пошуку. Забезпечення миттєвого доступу до інформації із різних репозиторіїв за допомогою єдиного запиту. Одне запитання "прозоро" адресується до сховищ документів Word/Excel/PowerPoint, файлових систем, Microsoft Exchange, Lotus Notes, SQL-баз даних та Internet/Intranet, повністю зберігаючи при цьому розмежування прав доступу. [1-63]

1.5 Складові частини системи електронного документообігу

Система електронного документообігу (СЕД) – одна з найважливіших складових інформаційної системи, яка відповідає за управління вводом документів у систему, збереження, пошук, маршрутизацію, обробку документів, збір і аналіз інформації про поточний стан виконання ділових і адміністративних процедур. [1-63]

Сучасна інтегрована система керування електронними документами повинна підтримувати механізми автоматизації комплексу таких задач:

– аналіз організації бізнес-процесів і супутнього документообігу;

– збір, зберігання, пошук і перегляд документів;

– маршрутизація й обробка документів, керування бізнес-процесами і правилами проходження документів.

Складовими частинами системи, що працює з документами, є:

1 Системи керування документами;

2 Системи автоматизації діловодства;

3 Архіви документів;

4 Системи створення документів і системи обробки документів;

5 Системи керування вартістю зберігання документів;

6 Системи маршрутизації документів;

7 Системи комплексної автоматизації виробничих процесів (бізнес-процесів);

8 Системи підтримки прийняття рішень.

Кожна підсистема має набір специфічних для неї функцій. При цьому окремі підсистеми тісно взаємодіють між собою. Поділ системи документообігу на підсистеми носить в деякій мірі «академічний» характер. У реальній практиці програмні продукти досить умовно можна віднести до тієї або іншої групи в наведеній класифікації. Як правило, системи реалізують лише частину функцій, при цьому продукт одного класу може містити в собі частину функцій систем іншого класу. Тому побудова системи електронного документообігу з існуючих на ринку продуктів потребує не тільки чіткого розуміння кінцевої задачі, але й відмінного знання ринку програмного забезпечення.

1.5.1 Система керування документами

Система керування документами – ядро системи роботи з документами. Її основними задачами є:

– забезпечення реєстрації інформації, що надходить (заповнення необхідних атрибутів документа);

– організація зберігання документів;

– підтримка пристроїв зберігання даних різних типів (від швидких магнітних дисків до стримерів, у тому числі підтримка роботи зі знімними носіями);

– підтримка міграції документів між пристроями зберігання в залежності від зміни активності обігу інформації. Виділяються два види міграції документів: міграція документів, що настроюється користувачем, і автоматична. Технологія автоматичної міграції документів називається Hierarchical Storage Management, а продукти, які її підтримують – HSM продуктами;

– автоматичні операції з документами (копіювання, відновлення, знищення);

– організація індексування документів для подальшого їх швидкого пошуку.

– підтримка індексів різноманітних типів. Виділяють два основних типи. Атрибутивний індекс, коли документу присвоюється набір текстових, цифрових та інших значень. Ці значення потім зберігаються в базах даних, і подальший пошук документа здійснюється за цими значеннями. Іншим широко застосовуваним типом індексування документа є побудова повнотекстового індексу за змістом (слова, фрази) документа;

– аудит і забезпечення безпеки документів. Під цим розуміють контроль доступу до документа і протоколювання всіх подій, пов’язаних із документом.

Контроль доступу – це дозвіл або заборона виконання, залежно від повноважень користувача, що ввійшов у систему, таких операцій як: перегляд документа, копіювання документа, знищення документа, редагування документа, керування доступом до документа. [1-63]

Система керування документами повинна дозволяти розраховувати вартість використання документа. Природно, що вартість документа вимірюється не в грошовому вираженні, а в часовому. Дана функція важлива не тільки для аналізу діяльності підприємства і конкретних співробітників, але і для виставляння рахунків на оплату клієнтам. Окремо слід відзначити можливість використання спеціалізованих апаратно-програмних модулів криптозахисту даних, що надають додатковий сервіс щодо захисту документів (електронний підпис, шифрування); інтеграція з додатками обробки документа. Існує множина додатків, що породжують документи. Якщо в організації встановлений корпоративний стандарт на використовувані додатки, то їх число обмежується десятком, якщо ж немає, то подібна задача значно ускладнюється. Виділяють два типи додатків, із якими може відбуватися інтеграція:

– додатки, що зберігають результати своєї роботи у файлах власного формату;

– додатки, що готують і виводять результати тільки на друк.

Виходячи з типів додатків, випливають два типи інтеграції:

– інтеграція на рівні операцій із файлами;

– інтеграція на рівні виводу на друк.

Як окремий вид інтеграції можна виділити інтеграцію з електронною поштою і факс-системами як найбільш поширеними механізмами передачі інформації; організація колективної роботи з документами. Як уже відзначалося раніше, організація колективної роботи з електронним документом дає серйозний виграш у продуктивності праці всього підприємства. Спільний доступ до електронного документа є основою для цього; організація розподілених сховищ документів. В умовах застосування системи керування документообігом часто виникає питання про підтримку розподіленого в просторі сховища. Під вимогою розподіленості розуміємо:

– доступ віддалених користувачів до сховища документів у режимі on-line або ж у режимі off-line – коли було б логічним використовувати електронну пошту для відпрацьовування механізмів замовлення-доставки документів;

– взаємодію декількох сховищ і одночасний доступ користувачів до інформації, розташованої в різних архівах.

Такого роду взаємодія може бути побудована на двох основних принципах:

– взаємне тиражування сховищ;

– технологія розподіленого доступу.

1.5.2 Системи автоматизації діловодства

Функції автоматизації діловодства в тому або іншому виді представлені в будь-якій системі автоматизації документообігу. У функції систем автоматизації діловодства не входить зберігання і переміщення документів в організації. В їх функції входить фіксація документів у спеціальній БД, що виражається в заповненні спеціальної картки документа. Вміст картки документа може варіюватися в залежності від сформованої в організації ситуації. Структура документів, зафіксованих у базах даних, спирається на так звану номенклатуру справ, наявну, як правило, у кожній організації, а технологія обліку й обробки документів спирається на сформульоване в даній організації «Положення про діловодство». Документи зберігаються в

паперовому вигляді, у спеціальному архіві, але в базах даних відображається їх поточне місце розташування і статус, включаючи атрибути контролю виконання. Зазвичай в системах діловодства розрізняють вхідні і вихідні документи, нормативно-розпорядчі документи, документи колегіальних органів управління, інформаційно-довідкові та інші види документів. Документи, що знаходяться на контролі виконання, підрозділяються за виконавцями, статусом виконання, термінами виконання тощо. Кожен документ у системі являє собою запис у базу даних, що характеризується набором значень атрибутів картки. Крім обліку і пошуку документів у базах даних, система повинна забезпечувати генерацію звітів, що дозволяють одержати відомості про виконання документів та іншої зведеної інформації. [1-63]

Для розробки додатків, що виконують функції автоматизації діловодства, найбільш придатними є стандартні інструменти, які використовують для розробки автоматизованих робочих місць, від настільних баз даних до систем на базі різноманітних SQL серверів. Проте в тому випадку, якщо автоматизація документообігу не закінчиться даним кроком, то можна подумати і про інші інструменти, що забезпечують більш послідовний розвиток системи. Так, наприклад, при переході до електронного сховища документів база даних системи діловодства повинна містити посилання на відповідні об’єкти електронного архіву, при використанні електронних засобів маршрутизації документів система повинна забезпечувати можливість розсилання документів на робочі місця користувачів, визначення поточного місця розташування документа тощо.

1.5.3 Архіви документів

Архіви документів – це те місце, де власне зберігається електронний документ. При цьому може зберігатися або вигляд документа, або його зміст, або і те й інше. Крім власне зберігання документів, архів повинен забезпечувати навігацію по ієрархії документів і їх пошук.

На відміну від пошуку за атрибутами документів, що був і в системах попереднього класу, архіви документів повинні забезпечувати повнотекстовий пошук за вмістом текстових фрагментів у документі. В принципі, пошуковий механізм повинен мати деякий інтелект, тобто забезпечувати пошук близьких граматичних конструкцій, а також пошук близьких за змістом слів.

На відміну від систем попереднього класу, в архівах зберігаються самі документи, і тому система повинна забезпечувати розмежування прав доступу до документів. Користувач може ідентифікуватися або за допомогою мережевого імені, або за допомогою спеціального імені і пароля, визначеного в системі керування архівом. Крім поділу прав доступу на рівні користувачів, система повинна забезпечувати виділення груп користувачів або ролей. Такою функцією архіву документів є забезпечення можливості групової роботи з документами, що знаходяться в стадії створення. При цьому використовується функція блокувань документів або Check-In/Check-Out контроль. Вона полягає в тому, що коли один із користувачів системи починає редагувати документ, останній блокується для доступу інших користувачів доти, поки з ним не закінчиться робота.

Ще однією функцією архіву є підтримка контролю версій. Версії документів можуть фіксуватися або автоматично, або з ініціативи користувача. У разі потреби користувач може повернутися до однієї з попередніх версій документа.

До сервісних функцій архіву документів відносяться можливість створення резервних копій документів без припинення роботи системи, інтеграція із системами забезпечення оптимальної вартості збереження даних та ін. [1-63]

1.5.4 Системи створення документів і системи обробки документів

Однією із самостійних функцій систем документообігу є введення документів в архів. Під цим розуміється перехід від паперових документів до електронних. У найпростішому випадку ця процедура зводиться до простого

сканування. Проте, як правило, простого зберігання образу документа недостатньо. Електронний образ документа повинен мати ідентифікаційні атрибути, що дозволять ідентифікувати його у системі діловодства і в архіві документів. Ці операції проводяться вручну.

Більш складною функцією є автоматичне розпізнавання вмісту документа і формування документа, що містить його текст. Для цього призначені програми, що відносяться до класу програмного забезпечення розпізнавання тексту. Ще більш складною функцією є розпізнавання вмісту форм. При цьому програма визначає наявність записів, у тому числі й рукописних, у визначених полях бланка документа, розпізнає його вміст і автоматично заповнює значення атрибутів даного документа в системі. За необхідності значення полів бланка може вибиратися з довідника, передбаченого в системі.

1.5.5 Системи керування вартістю зберігання документів

Сьогодні застосовується два підходи до організації зберігання електронних документів. Перший полягає в тому, що тіло документа зберігається у файловій системі, другий передбачає зберігання документів у реляційній або спеціалізованій базі даних.

При зберіганні документів в архіві обсяги зберігання можуть швидко зростати і досягати значних розмір. При цьому інтенсивність звертань до документів, що знаходяться в архіві, не рівномірна. До документів, що знаходяться в роботі, звертаються достатньо часто, у той час як доступ до документів, робота з якими вже завершена, здійснюється дуже рідко. Відповідно, система може забезпечувати різну оперативність доступу до різних документів. Оскільки вартість зберігання документів в архіві, як правило, обернено пропорційна швидкості доступу, то можна скористатися вказаною закономірністю для оптимізації вартості утримання архіву. Системи керування вартістю зберігання саме і вирішують дану задачу. Забезпечуючи можливість роботи з різноманітною периферією, система забезпечує автоматичне

перенесення даних на більш «дешеві» носії у випадку, якщо доступ до них здійснюється недостатньо часто. [1-63]

1.5.6 Системи маршрутизації і контролю виконання

Однією з основних складових систем документообігу є системи маршрутизації і контролю виконання. При побудові систем маршрутизації можуть застосовуватися два основних підходи.

Перший – документо-орієнтований. Документ є основним об’єктом системи, і маршрутизується саме він, а всі інші параметри маршрутизації асоційовані саме з документом.

Другий – робото-орієнтований, і його основним об’єктом є робота. До роботи може бути прикріплений найрізноманітніший список об’єктів, у тому числі й документи. Природно, робота може існувати і без документів. Другий підхід є більш загальним. [1-63]

Будь-який процес маршрутизації документів – це рух одного документа, а не множини його копій, як це відбувається в системах електронної пошти.

1.5.6.1 Вільна маршрутизація

Виділяються два основні типи маршрутів документів:

1) послідовна маршрутизація – документ послідовно проходить виконавців один за одним;

2) паралельна маршрутизація – документ одночасно надходить усім виконавцям, а завершення маршруту відбувається, коли один або всі користувачі закінчать роботу з документом.

Системи електронної пошти. Мінімальною достатньою системою, яка забезпечує маршрутизацію документів, є система електронної пошти, що здійснює паралельне розповсюдження документів (маршрутизація відрізняється від розповсюдження або розсилання тим, що маршрутизований документ повертається в початок маршруту, наприклад, до ініціатора, а документ, що розсилається, посилається до виконавця без контролю факту повернення). За

допомогою додаткових елементів система електронної пошти може забезпечувати послідовну маршрутизацію документів. [1-63]

1.5.6.2 Вільна маршрутизація документів із контролем виконання

Контроль виконання включає:

– контроль доставки завдання – ініціатору видається інформація про те, що його завдання досягло місця призначення (виконавця);

– контроль читання завдання – ініціатору видається інформація про те, що з його завданням ознайомилися співробітники, для котрих це завдання було призначено;

– контроль виконання – ініціатору видається інформація про те, що завдання виконане;

– моніторинг завдання – ініціатор завжди може подивитися, хто і що зараз робить із його завданням;

– повідомлення про порушення термінів виконання – система документообігу може сповістити ініціатора про те, що послане ним завдання прострочене конкретним співробітником;

– історія виконання завдань;

– контроль якості виконання – означає, що якщо користувач говорить про те, що завдання виконано, це ще не означає, що воно дійсно виконано, ініціатор повинен перевірити якість виконання, підтвердити або не підтвердити виконання.

Інформація може видаватися у вигляді зміни статусу завдання у вікнах вхідних і вихідних завдань або у вигляді нового завдання, сформованого системою ініціатору, або за допомогою повідомлення по електронній пошті.

Маршрутизація документів по заздалегідь визначених маршрутах із контролем виконання (жорстка маршрутизація). Маршрути можуть бути більш складними, ніж прості послідовні або паралельні:

– комбіновані з послідовних і паралельних елементів;

– умовні, із переходами в залежності від стану тих або інших змінних маршрутів.

1.5.7 Системи комплексної автоматизації виробничих процесів (бізнес-процесів)

Розвитком систем маршрутизації документів є WorkFlow системи, або системи комплексної автоматизації організаційно-виконавчих, виробничих процесів (бізнес-процесів). На відміну від систем маршрутизації документів, об’єктом маршрутизації в них є сукупність даних, використовуваних у визначеному процесі. Більшість спеціалістів в області сучасних інформаційних технологій розглядають технологію WorkFlow як найбільш перспективну технологію керування діловими процесами. Буквальний переклад терміна workflow – потік робіт, є, безумовно, коректним граматично, але майже ніяк не розкриває його змісту. [1-63]

Більш інформативним є визначення продуктів класу WorkFlow як програмних систем, що забезпечують повну або часткову координацію виконання виробничих операцій (завдань, робіт, функцій), що складають, наприклад, структуровані бізнес-процеси підприємства.

При цьому кожна система забезпечує вирішення трьох таких задач:

– розробка опису процесу;
– керування виконанням процесу;
– інтеграція використовуваних у процесі додатків.

1.5.8 Системи підтримки прийняття рішень

Важливим моментом у функціонуванні інформаційних систем є необхідність забезпечити, крім засобів генерації даних, також і засоби їхнього аналізу. Наявні в усіх сучасних СКД і СКБД засоби побудови запитів і різноманітні механізми пошуку хоча і полегшують витяг потрібної інформації, але все ж не спроможні дати достатньо інтелектуальну її оцінку, тобто зробити узагальнення, групування, видалення надлишкових даних і підвищити

достовірність за рахунок виправлення помилок і опрацювання декількох незалежних джерел інформації (як правило, не тільки корпоративних баз даних, але і зовнішніх, розташованих, наприклад, в Internet). Проблема ця стає надзвичайно важливою у зв'язку з лавиноподібним зростанням обсягу інформації і збільшенням вимог до інфосистем щодо продуктивності – сьогодні успіх в управлінні організацією багато в чому визначається оперативністю прийняття рішень, дані для яких і надає КСЕД. У цьому випадку на допомогу старим методам приходить оперативна обробка даних (On-Line Analitical Processing, OLAP).

Сьогодні доступний цілий ряд різноманітних систем OLAP, ROLAP (реляційні OLAP), MOLAP (багатомірні OLAP) – Oracle Express, MetaCube (Informix) та ін.

СЕД сприяє підвищенню ефективності управління підприємством за рахунок: підключення до роботи в системі всіх співробітників підприємства, які працюють з документами; суворого контролю дотримання працівниками посадових обов'язків; підвищення прозорості документообігу та бізнес-процесів, прискорення інформаційних потоків. Запропоновано визначення поняття «система електронного документообігу» – як комплексу взаємопов'язаних та узгоджених автоматизованих процесів роботи з електронними документами, що включає в себе їх створення, обробку, відправлення, зберігання, використання і знищення та забезпечує контроль над їх потоками. Визначено три групи задач, які вирішуються за допомогою СЕД в управлінні підприємством: планування, облікові задачі, управління документами.

Функціональна структура СЕД включає наступні складові :

Управління и доступ до даних

1)Робота з архівами документів і обробка зображень

2)Облік,контролю і підтримка життевого циклу

3)Розширення функціональності системи електронного документообігу

4)Пошук документів і управління даними

5)Обмін документами та забеспечення безпеки

6)Моніторинг та накопичення статистики

1.6 Суб’єкти відносин у сфері послуг електронного цифрового підпису

1.6.1 Підписувач

Має право:

– вимагати скасування, блокування або поновлення свого сертифіката ключа;

– оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку

Зобов’язаний:

– зберігати особистий ключ у таємниці;

– надавати центру сертифікації ключів дані згідно з вимогами цього Закону для засвідчення чинності відкритого ключа;

– своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.

1.6.2 Центр сертифікації ключів (ЦСК)

ЦСК може бути юридична особа незалежно від форми власності або фізична особа, яка є суб’єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог цього Закону. Обслуговування фізичних та юридичних осіб здійснюється ЦСК на договірних засадах. [1-63]

Має право:

– надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів;

– отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника.

Зобов’язаний:

– забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

– забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;

– встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

– своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених Законом;

– своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

– перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

– цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

– вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

– забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

– надавати консультації з питань, пов’язаних з електронним цифровим підписом.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

1.6.3 Акредитований центр сертифікації ключів (АЦСК)

АЦСК – ЦСК, акредитований в установленому порядку.

Має право:

– надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів;

– отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Зобов’язаний:

– виконувати усі зобов’язання та вимоги, встановлені законодавством для ЦСК, та додатково зобов’язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису. [1-63]

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України.

1.6.4 Засвідчувальний центр (ЗЦ)

Кабінет Міністрів України за необхідності визначає ЗЦ центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої ЗЦ, призначені для виконання таких функцій.

ЗЦ щодо групи ЦСК, має ті ж функції і повноваження, що й центральний засвідчувальний орган стосовно ЦСК.

ЗЦ відповідає вимогам, встановленим законодавством для АЦСК.

ЗЦ реєструється, засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Положення про ЗЦ центрального органу виконавчої влади затверджується Кабінетом Міністрів України.

1.6.5 Центральний засвідчувальний орган (ЦЗО)

ЦЗО визначається Кабінетом Міністрів України.

Повноваження:

– формує і видає посилені сертифікати ключів ЗЦ і ЦСК з дотриманням вимог, встановлених Законом «Про електронні довірчі послуги»;

– блокує, скасовує та поновлює посилені сертифікати ключів ЗЦ та ЦСК у випадках, передбачених Законом;

– веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів ЗЦ та ЦСК;

– веде акредитацію ЦСК, отримує та перевіряє інформацію, необхідну для їх акредитації;

– забезпечує цілодобово доступ ЗЦ та ЦСК до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

– зберігає посилені сертифікати ключів ЗЦ та ЦСК;

– надає ЗЦ та ЦСК консультації з питань, пов’язаних з використанням електронного цифрового підпису.

ЦЗО відповідає вимогам, встановленим законодавством для АЦСК. Положення про ЦЗО затверджується Кабінетом Міністрів України.

1.6.6 Контролюючий орган (КО)

Функції КО здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації. КО перевіряє дотримання вимог Закону ЦЗО, ЗЦ та ЦСК.

У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для ЦСК, ЗЦ, КО розпорядження ЦЗО про негайне вжиття заходів, передбачених законом.

Скасування, блокування та поновлення посиленого сертифіката ключа:

АЦСК негайно скасовує сформований ним посилений сертифікат ключа у разі:

– закінчення строку чинності сертифіката ключа;

– подання заяви власника ключа або його уповноваженого представника;

– припинення діяльності юридичної особи – власника ключа;

– смерті фізичної особи – власника ключа або оголошення його померлим за рішенням суду;

– визнання власника ключа недієздатним за рішенням суду;

– надання власником ключа недостовірних даних;

– компрометації особистого ключа.

– ЦЗО негайно скасовує посилений сертифікат ключа ЦСК, ЗЦ у разі:

– припинення діяльності з надання послуг електронного цифрового підпису;

– компрометації особистого ключа.

– ЦЗО, ЗЦ, АЦСК негайно блокують посилений сертифікат ключа:

– у разі подання заяви власника ключа або його уповноваженого представника;

– за рішенням суду, що набрало законної сили;

– у разі компрометації особистого ключа.

Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції.

ЦЗО, ЗЦ, АЦСК негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Блокований посилений сертифікат ключа поновлюється:

– у разі подання заяви власника ключа або його уповноваженого представника;

– за рішенням суду, що набрало законної сили;

– у разі встановлення недостовірності даних про компрометацію особистого ключа. [1-63]

1.7 Впровадження системи електронного документообігу

Впровадження системи електронного документообігу – це насамперед автоматизація діяльності із підготовки та опрацювання електронних документів, що здійснюється підприємством.

СЕД призначена для вирішення наступних завдань:

– автоматизація таких процесів: підготовка, погодження та опрацювання (розсилка і контроль) документів, які утворюються в установі (вхідні, вихідні, внутрішні, розпорядчі службові, доповідні записки, окремі доручення, службові листи тощо);

– впровадження електронного цифрового підпису та перехід до роботи з електронними документами;

– забезпечення колективної роботи з електронними документами та їх маршрутизації;

– підвищення продуктивності праці персоналу за рахунок вивільнення робочого часу шляхом зменшення обсягів рутинних операцій (на пошук документів, підготовку звітів, тощо);

– забезпечення належного рівня виконавчої дисципліни та відповідного поточного контролю за нею;

– забезпечення інформаційно-аналітичної підтримки діяльності керівництва, якості та своєчасності прийняття управлінських рішень;

– створення єдиного сховища документів, що дозволяє поліпшити якість обробки даних та зменшення часу прийняття рішень.

Головне призначення СЕД – це організація збереження електронних документів, а також роботи з ними (зокрема , їхнього пошуку як по атрибутах, так і по змісту). У СЕД повинні автоматично відслідковуватися зміни в документах, терміни виконання документів, рух документів, а також контролюватися всі їхні версії і підверсії. Комплексна СЕД повинна охоплювати весь цикл діловодства підприємства чи організації – від постановки завдання на створення документа до його списання в архів, забезпечувати централізоване збереження документів у будь-яких форматах, у тому числі, складних композиційних документів. СЕД повинні поєднувати розрізнені потоки документів територіально віддалених підприємств у єдину систему. Вони повинні забезпечувати гнучке керування документами як за допомогою жорсткого визначення маршрутів руху, так і шляхом вільної маршрутизації документів. У СЕД повинне бути реалізоване розмежування доступу користувачів до різних документів у залежності від їхньої компетенції, займаної посади і призначених їм повноважень. Крім того, СЕД повинна настроюватися на існуючу організаційно-штатну структуру і систему діловодства підприємства, а також інтегруватися з існуючими корпоративними системами.

Інформаційне середовище (Information environment) – сукупність технічних і програмних засобів зберігання, опрацювання, передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації. [1-63]

Таблиця 1.1 – Основні види інформаційних обмінів на підприємстві

Вид інформаційного обміну	Застосування
Обмін між організацією та зовнішнім середовищем	взаємодія з громадянами, іншими органами державного управління та сторонніми організаціями з метою реалізації функцій державного управління.
Міжрівневий (вертикальний) обмін інформацією в організації	- низхідні потоки інформації, якими повідомляють підлеглим про поточні завдання, конкретні доручення, зміну пріоритетів та ін.; - висхідні потоки інформації – звіти про виконання завдань, пропозиції з удосконалення технології та ін., за допомогою яких керівництво інформують про поточні та можливі проблеми, про можливі варіанти рішень.
Горизонтальний обмін інформацією	- наради керівників суміжних підрозділів, задіяних у виконанні спільних завдань; - наради керівників підрозділів, які мають схожі виробничі завдання; - робота у межах робочих груп (управління проектом).
Неформальний обмін інформацією	- обговорення виробничих питань під час неформальних зустрічей (під час обідньої перерви, святкових заходів та ін.); - чутки, основною причиною яких є дефіцит офіційної інформації.

В діяльності будь-якої організації важливе місце займає робота з документами, які необхідно одержувати ззовні, готувати всередині організації, реєструвати, передавати працівникам, контролювати виконання, вести довідкову роботу, зберігати. Організація роботи з документами є важливою складовою частиною процесів управління і прийняття управлінських рішень, яка істотно впливає на оперативність, економічність і надійність

функціонування апарату управління установи, культуру праці управлінського персоналу і якість управління.

Організація роботи з документами (документаційне забезпечення управління) – важлива складова частина процесу управління і прийняття управлінських рішень, яка істотно впливає на оперативність та якість управління.

Параметри, що описують документообіг в організації та її структурних підрозділах і визначають необхідність впровадження системи електронного документообігу.

Для систем документообігу основними параметрами є:

– обсяг документообігу;

– швидкість руху документів;

– вартість виконання типових операцій над документами.

Таблиця 1.2 – Параметр 1. Обсяг документообігу

Показник	**Характеристика показника**	**Чинники підвищення ефективності від впровадження електронного документообігу**
Потік вхідних документів	Число документів, що надходять в організацію протягом року	Скорочення витрат на паперові документи
Потік вихідних документів	Число документів, що надсилаються організацією протягом року	Скорочення витрат на паперові документи
Обсяг внутрішнього документообігу	Число документів (наказів, розпоряджень, службових записок, заяв та ін.), які створюються в організації протягом року	Скорочення витрат на паперові документи
Рівномірність документопотоку протягом року	Типові сезонні коливання кількості вхідних документів, загальна тенденція зміни обсягів, пов’язана із збільшенням або скороченням організації, збільшенням або спадом ділової активності	Скорочення витрат на паперові документи

Продовження таблиці 1.2

Показник	**Характеристика показника**	**Чинники підвищення ефективності від впровадження електронного документообігу**
Обсяги документообігу у структурних підрозділах	Характеризується розподілом документів між структурними підрозділами	Скорочення витрат на паперові документи
Обсяги документообігу за видами документів	Характеризує витрати на обробку певного виду документів	Скорочення витрат на паперові документи
Частка контрольних документів	Відношення кількості документів, які ставлять на контроль до загальної кількості документів	Скорочення витрат на паперові документи
Середній обсяг документів	Характеризує кількість інформації, яка надсилається у окремому документі. Для документів, що надсилаються комп'ютерними мережами, обсяг вимірюється у Кб, для друкованих – кількість сторінок	Скорочення витрат на паперові документи
Середня кількість копій	Для паперових документів до впровадження множу вальної техніки – 5-6 копій (за кількістю резолюцій), із впровадженням копіювальної техніки – документ копіюється до 18 разів	Скорочення витрат на паперові документи

Таблиця 1.3 – Параметр 2. Швидкість руху документів

Показник	**Характеристика показника**	**Чинники підвищення ефективності від впровадження електронного документообігу**
Час реєстрації одного документа	Витрачається не більше однієї хвилини	Скорочення непродуктивних витрат робочого часу співробітників Прискорення інформаційних потоків

Продовження таблиці 1.3

Час передавання одного документа на виконання	Середній час, який проходить з моменту надходження документа в організацію до моменту, коли він опиняється в руках відповідального виконавця (не менше 1 дня)	Скорочення непродуктивних витрат робочого часу співробітників Прискорення інформаційних потоків Зміна корпоративної культури організації
Час пересилання документа між структурними підрозділами	У невеликих локальних організаціях – кілька хвилин. Чим більш організація, тим більше значення показника (до кількох днів для віддалених підрозділів)	Скорочення непродуктивних витрат робочого часу співробітників Прискорення інформаційних потоків Зміна корпоративної культури організації
Час пошуку документа за відомими атрибутами	При «паперовій» технології – кілька хвилин	Скорочення непродуктивних витрат робочого часу співробітників Прискорення інформаційних потоків
Час пошуку документа з невідомими атрибутами	При «паперовій» технології – кілька годин і навіть днів	Скорочення непродуктивних витрат робочого часу співробітників Прискорення інформаційних потоків Зміна корпоративної культури організації
Час підготовки і узгодження типових документів	Типові документи – проекти наказів, угод, плани роботи та ін. При оцінці показника можуть виникнути проблеми, пов’язані з доступністю та достовірністю даних. Можна оцінити, порівнюючи дату підпису відповідного документа і дату одержання першого підпису на листі узгодження	Прискорення інформаційних потоків Зміна корпоративної культури організації
Час, що витрачається на підготовку типових звітів	На підготовку звітів може витрачатись 30-40 % робочого часу	Прискорення інформаційних потоків Зміна корпоративної культури організації

Таблиця 1.4 – Параметр 3. Вартість виконання типових операцій над документами

Показник	**Характеристика показника**	**Чинники підвищення ефективності від впровадження електронного документообігу**
Вартість робочого часу співробітників	Засоби на оплату праці, оренду виробничих приміщень, податкові виплати	Скорочення непродуктивних витрат робочого часу співробітників
Вартість ресурсів	Папір, витратні матеріали, принтери, копіювальні апарати, витрати на утримання архіві, амортизаційні відрахування та ін.	Скорочення витрат на паперові документи

При виборі системи електронного документообігу організації необхідно в першу чергу визначити завдання, які будуть вирішуватись з використанням цієї системи. Після цього необхідно обрати 4-5 рішень різних виробників, які мають необхідний досвід впровадження у аналогічній сфері діяльності. Ці системи надалі підлягають аналізу. [1-63]

Виходячи із завдань діяльності організації необхідно визначити критерії для оцінювання представлених на ринку систем. У кожної організації ці критерії індивідуальні.

Наприклад, для організації, яка має віддалені філії та підрозділи, важлива підтримка територіальної розподіленості.

В якості критеріїв можуть бути такі напрями аналізу:

- функціональність;
- продуктивність і масштабованість;
- інтегрованість;
- ліцензійна політика;
- цінова політика;
- вартість масштабування;
- інструментальні засоби;
- локалізація.

1.8 Етапи переходу до електронного документообігу в організаціях

Проаналізуємо кілька характерних етапів, які може проходити організація на шляху від паперового до електронного документообігу:

1 етап (початковий) – впровадження автоматизованої системи документообігу (АСД).

В АСД функціонують первинні елементи аналітико-синтетичної обробки документа, що знаходять вираження у створенні електронної реєстраційної картки документа, що є пошуковим образом документа.

Функціональні можливості АСД не розраховані на збереження та переміщення документів в установі. їх основними завданнями є фіксація етапів проходження документів та їх поточного статусу в спеціальній базі даних, що находить відображення в заповненні спеціальної реєстраційної картки документа. База даних не містить оригіналів документів, а відображає лише їх поточне місцезнаходження та статус, включаючи атрибути контролю виконання. Крім обліку та пошуку документів в базі даних, система повинна генерувати звіти, що дозволяють отримати відомості про стан виконання документа та іншу загальну інформацію.

Автоматизація документообігу дає змогу:

– підвищити виконавську дисципліну (здійснюється за рахунок покращання контролю за виконанням документів, а саме ефективна система повідомлень та нагадувань дає можливість попереджувати всіх посадових осіб про наближення строку виконання доручення);

– легко скласти повну картину ефективності діяльності як окремих працівників, так і установи в цілому (за допомогою прикінцевих звітів та журналів);

– формувати індивідуальні маршрути документів і визначити найбільш оптимальний шлях їх руху в установі;

– зменшити час на обробку і реєстрацію, а також уникнути помилок, пов’язаних із заповненням реквізитів документа (використовуючи автоматичну генерацію номера і поточної дати, використання довідників);

– засобами системи здійснювати швидкий пошук документів та доручень (за їх змістом або будь-якою комбінацією реквізитів).

2 етап (розширений) – створення «образу» електронного документообігу.

Розширений рівень автоматизації дозволяє додавати до електронної реєстраційної картки електронне іконічне зображення документа (сканована копія), інакше кажучи, «образ документа», єдиною відмінністю якого від електронного документа є відсутність електронно-цифрового підпису (що гарантує його цілісність, достовірність і відповідно юридичну силу). Отже, рівень АСД, у якому функціонує електронний «образ документа», умовно можна назвати «образом електронного документообігу».

Створення «образу електронного документообігу» відбувається за допомогою сканування документів. Швидке отримання електронної версії документа за допомогою використання технологій сканування, розпізнання та друку документа робить легшим перехід від паперової версії документа до електронної.

3 етап (розвинений) – електронний документообіг.

Електронний документообіг забезпечує циркуляцію електронних документів, які є основою нової форми взаємодії держави та суспільства. Однак кожен документ повинен мати встановлений законодавством набір реквізитів, до яких належить, зокрема, підпис – елемент, що підтверджує авторство документа. Функцію підпису в електронному документі виконує електронно-цифровий підпис.

Наведені етапи впровадження електронного документообігу є об’єктивно зумовленими як розвитком інформаційних систем, так і готовністю установ до їх впровадження. Зважаючи на соціально-освітні та психологічні чинники, така послідовність впровадження електронного документообігу попередить нераціональне використання матеріальних ресурсів установи, пришвидшить

адаптацію працівників до роботи в нових умовах, як наслідок зросте ефективність опрацювання документів в установі.

При впровадженні систем електронного документообігу відзначають такі типові помилки:

– відсутність попереднього обстеження організації;

– розробка системи власними силами;

– відсутність попередньої (пілотної) експлуатації;

– низький рівень навчання співробітників.

Організаційні проблеми пов’язані, перш за все, з людським фактором:

– недостатньою мотивацією співробітників до роботи з новою системою;

– низький рівень комп’ютерною грамотності;

– помилкове або неповне визначення завдань, які повинна вирішувати система, при прийнятті рішень про її впровадження.

Компанії, які впроваджують системи електронного документообігу, пропонують консалтингові послуги. Підприємства вдаються до послуг консалтингових компаній з таких причин:

– нестача ресурсів (людей, часу, навичок, знань) – у період значних змін організація не має часу шукати людей з новими навичками або ж навчати своїх співробітників; консультанти ж і вирішують завдання, які постають, і передають свої знання і навички співробітникам організації;

– допомога на тимчасовій основі. Консультанти можуть залучатись для аналізу схем документообігу, інших видів аналізу і вироблення рекомендацій без відволікання від поточної діяльності співробітників організації;

– незалежний погляд «зі сторони». Перевагою консультанта є «свіжий» погляд і безпристрасність у ситуаціях, коли співробітники організації не можуть бути об’єктивними;

– навчання співробітників через консультування.

Ефективність впровадження систем електронного документообігу визначається такими чинниками:

1 Ціна. Вартість однієї ліцензії може коливатись від 1000 до 4000 грн. Покрокове впровадження системи управління документообігом дає змогу замовнику «розтягнути» у часі виплати, отже застосовується у багатьох випадках.

2 Побоювання помилитись у виборі програмного продукту. Хоча практично у кожній із систем є сховище і WorkFlow, реалізуються вони порізному і різною мірою відповідають потребам того або іншого замовника. Систему електронного документообігу можна перевірити у режимі пілотного проекту.

3 Саботаж співробітників. Систему управління електронним документообігом можна вважати тільки тоді успішно впровадженою, якщо всі користувачі охоче використовують її в повсякденній роботі.

Одним із шляхів подолання проблеми «людського фактора» при впровадженні систем електронного документообігу керівництво організації часто вважає примус співробітників до роботи із автоматизованою системою. Часто у таких «вимушених користувачів» створюються передумови до розкриття потенціалу до роботи із системою.

1.9 Висновок

В першому розділі магістерської дипломної роботи були розкриті основні поняття електронного документообігу, визначені переваги, що отримає організація від застосування СЕД та особливості впровадження такої системи. Також були визначені основні складові частини СЕД, їх особливості та вимоги до СЕД в залежності від специфіки діяльності організації.

Окремо були розглянуті суб’єкти системи електронного документообігу, а саме підписувач, центр сертифікації ключів, акредитований центр сертифікації ключів, засвідчувальний центр, центральний засвідчувальний орган, контролюючий орган та визначені їх функції в рамках СЕД.

На основі проведених досліджень вважаємо, що використання системи електронного документообігу в організації є необхідним. Для впровадження СЕД необхідно вирішити наступні задачі:

– класифікувати оброблювану інформацію та дослідити інформаційні потоки;

– провести категорювання та обстеження ОІД;

– проаналізувати існуючі СЕД на предмет відповідності вимогам організації та обрати конкретну систему документообігу;

– дослідити відповідність обраної СЕД вимогам нормативних документів із захисту інформації, а саме, стандартному функціональному профілю захищеності 3.КЦД.1 та надати рекомендації щодо приведення стану захисту СЕД до визначеного рівня.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Класифікація інформації, що циркулює та обробляється в автоматизованій системі організації

Згідно закону України «Про інформацію» на підприємстві циркулює: статистична інформація; адміністративна інформація (дані); масова інформація; інформація про особу, яку можна класифікувати наступним чином:

За режимом доступу:

– відкрита;

– з обмеженим доступом(за правовим режимом).

Відкрита, в свою чергу поділяється:

– відкрита, що не потребує захисту (податкові звітності, обов’язкові виплати, відомості про ліквідність підприємства, відомості про чисельність, склад працюючого персоналу, фонд заробітної плати, умови праці та наявність вільних робочих місць).

– відкриту, що потребує захисту (правила та інструкції роботи в інформаційно-обчислювальної мережі, данні розпорядчих документів, статуту, відомості з документів, що дають право власності на підприємницьку діяльність, данні з основних форм звітності фінансово-підприємницької діяльності).

До інформації з обмеженим доступом відносяться данні (конфіденційна інформація), розголошення яких може призвести до значних збитків підприємства, клієнтів. [1-62]

До конфіденційної інформації відносяться данні:

У сфері виробництва:

– інформація про зміст проектних робіт.

У сфері управління:

– о перспективних методах управління підприємством.

Планові відомості:

– розвиток підприємства;

– інвестиції підприємства;

– звіти про виконання проектних робіт.

У сфері фінансів:

– планові та фактичні показники фінансового плану;

– данні про баланс підприємства;

– майнове становище;

– бюджет, данні про оберт грошових потоків підприємства;

– банківські операції, данні про фінансові операції;

– банківські зв’язки;

– специфіка міжнародного співробітництва;

– рівень прибутків;

– боргові обов’язки;

– стан кредитів;

– розміри та умови банківських кредитів;

– джерела кредитування.

Про партнерів:

– коло клієнтів;

– комерційні зв’язки;

– данні про клієнтів;

– данні про договори та умови їх виконання;

Про співробітників:

– домашня адреса, телефони, паспорті данні, ідентифікаційний код та інша особиста інформація;

– стан здоров’я.

Проаналізувавши інформацію, що циркулює на підприємстві та його відділах, можна визначити основні види інформації, що є найбільш важливою та при порушенні властивостей цієї інформації, підприємство (клієнти) можуть зазнати найбільших збитків (таблиця 2.1, рисунок 2.1).

Класифікація найбільш важливої інформації підприємства:

– данні про клієнтів;

– данні про договори та умови їх виконання;

– інформація про зміст проектних робіт;

– звіти про виконання проектних робіт;

– особиста інформація та персональні данні співробітників.

Видами оброблення інформації в системі можуть бути:

– обговорення;

– оброблення в АС;

– оброблення технічними засобами (крім тих, що входять до складу АС);

– збереження на різних носіях в пасивному стані (постійно чи тимчасово).

Носії інформації:

– акустичні поля;

– електромагнітні поля радіодіапазону;

– електричні сигнали в струмопровідних комунікаціях;

– електромагнітні поля в інфрачервоній, видимій та ультрафіолетовій частині спектра;

– матеріально-речові носії: папір, фото, магнітні та оптичні носії, використаний матеріал, тощо;

– до того ж одним з носіїв інформації є людина.

Таблиця 2.1 – Класифікація інформації згідно відділів підприємства, що її обробляє

Види інформації	**Склад**	**Структура обробки інформації**
Фінансова	Первинні документи, звіт про господарську діяльність,бухгалтерські звітності, квитанції, договори	Бухгалтерія, адміністративні підрозділи
Адміністративна	Фінансові звітності, Внутрішні та зовнішні розпорядження, регламентуючі діяльність організації, статут, облік часу працівників	Бухгалтерія, адміністративні підрозділи
Статистична	Первинні та вторинні документи, бухгалтерські звітності, статистичні данні	Бухгалтерія, адміністративні підрозділи
Інформації про кадри	Дані про працівників підприємства (персональні дані про особу, інформація про сім’ю)	Відділ кадрів, бухгалтерія
Інформації про замовників	Договори, фінансова інформація	Керівники проектних відділів, бухгалтерія

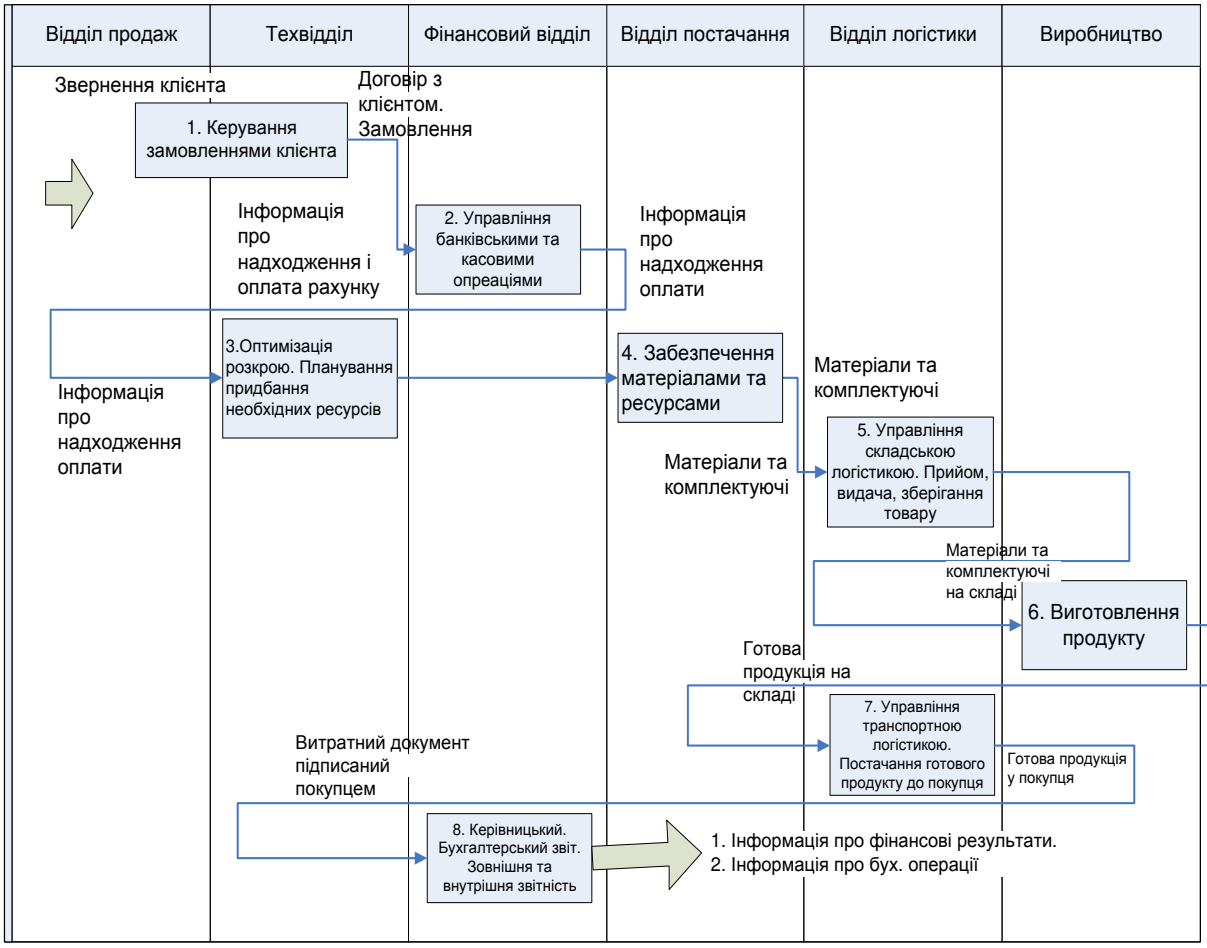

Рисунок 2.1 – Виробничий процес. Інформаційні потоки

2.2 Об’єкт інформаційної діяльності комерційне підприємство

Загальна характеристика ОІД

Об’єктом інформаційної діяльності являється комерційне підприємство.

Це виробниче підприємство.

Вид діяльності: виробництво залізорудних окатишів, науково-дослідна діяльність в цій галузі.

Послуги, що надаються: виробництво та експорт залізорудних окатишів в межах країни та за кордон.

Підприємство розташоване на приватній території.

Найвищий ступінь обмеження доступу до інформації, що циркулює на об’єкті: конфіденційна.

Інформаційне середовище

Документальна (письмова) інформація, що потребує захисту, зберігається та оброблюється на Підприємстві в межах виділеного приміщення та зберігається у сейфі керівника відділу.

Інформація у електронному виді, що потребує захисту, оброблюється та зберігається у АС класу 3.

Всі робочі станції та виробниче обладнання об'єднані в інформаційну мережу з сервером. Вся інформація яка оброблюється на робочих станціях та виробничому обладнанні зберігається на сервері. Робочі станції та виробниче обладнання підключено до мережі через мережеві комутатори. До серверу підключено модем, за допомогою якого мається можливість виходу до глобальної мережі Internet.

Види інформації яка циркулює в ІТС підприємства:

– відкрита (загальнодоступна) інформація;

– інформація з обмеженим доступом (персональні данні, комерційна таємниця).

Перелік інформації з обмеженим доступом:

1 Договірна інформація (договори з постачальниками, замовниками, транспортними компаніями тощо).

2 Бухгалтерські документи (документи бухгалтерської звітності).

3 Фінансова інформація (плани фінансових затрат та інше).

4 Економічна інформація (економічні показники, розрахунки, стратегічні ходи тощо).

5 Касова документація (накладні, касові ордери).

6 Прайсова інформація.

7 Проектні документи (розроблювані проекти тощо).

8 Бізнес плани, ідеї.

9 Складська інформація (залишки на складах тощо).

10 Графічна інформація (схеми, макети, ескізи, креслення тощо).

11 Банківські реквізити.

12 Нормативні документи та посилання.

13 Довідкова інформація.

14 Технічна інформація.

15 Внутрішні документи (розпорядження, накази, посадові інструкції тощо).

16 Експлуатаційна інформація.

Порушення властивостей інформації класифікували за трьома критеріями (таблиця 2.2):

– порушення конфіденційності (К0-К4);

– порушення цілісності (Ц0-Ц4);

– порушення доступності (Д0-Д4).

Пояснення критеріїв:

К0 – розголошення інформації призводить до припинення роботи підприємства, або дуже великих збитків.

К1 – розголошення призводить до значних збитків, якщо не буде вжито заходів.

К2 – розголошення призведуть до деяких збитків, що може призвести до перебоїв в роботі.

К3 – підприємство зазнає незначних збитків.

К4 – може принести малозначний збиток в рідкісних випадках.

Ц0 – призводить до неправильної роботи підприємства в цілому, або значної її частини і наслідки зміни незворотні.

Ц1 – несанкціоновані зміни, призводять до неправильної роботи підприємства через деякий час, якщо не буде вжито заходів. Наслідки незворотні.

Ц2 – несанкціоновані зміни призводять до збоїв в роботі підприємства, можуть призвести до не стабільної роботи.

Ц3 – несанкціоновані зміни призводять до зміни показників на негативні, незначна нестабільність підприємства.

Ц4 – несанкціоноване зміни не нанесуть збитків підприємству.

Д0 – в разі порушення доступності підприємство зазнає сильних збитків. Має можливість припинити свою діяльність.

Д1 – в разі порушення підприємство зазнає значної нестабільності в роботі.

Д2 –в разі порушення підприємство зазнає незначних перебоїв в роботі, які не призведуть до значних змін.

Д3 – в разі порушення робочий процес підприємства не зазнає великого збитку, можливі незначні перебої в роботі.

Д4 – в разі порушення підприємство не зазнає перебоїв в роботі та збитків, але втрачену інформацію потрібно буде поновити.

Таблиця 2.2 – Аналіз можливого негативного впливу на функціонування підприємства при порушенні властивостей інформації

Тип інформації з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
Договірна інформація	К1	Ц2	Д3
Бухгалтерські документи	К2	Ц2	Д2
Фінансова інформація	К2	Ц2	Д2
Економічна інформація	К2	Ц2	Д2
Банківські реквізити	К4	Ц0	Д3
Касова документація	К3	Ц2	Д3
Прайсова інформація	К3	Ц2	Д3
Проектні документи	К1	Ц1	Д1
Графічна інформація	К3	Ц1	Д2
Нормативні документи	К1	Ц2	Д1
Довідникова інформація	К4	Ц3	Д3
Бізнес плани, ідеї	К3	Ц2	Д3

Продовження таблиці 2.2

Тип інформації з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
Складська інформація	К3	Ц3	Д4
Технічна інформація	К3	Ц2	Д2
Внутрішні документи	К2	Ц1	Д1
Експлуатаційна інформація	К3	Ц2	Д2

Інформаційні потоки на ОІД

Інформаційний обмін в ІС реалізується по каналам зв’язку, розташованих в рамках КЗ, та каналами зв’язку, котрі виходять за рамки КЗ. Канали зв’язку котрі виходять за межі КЗ представляють собою загально доступні канали зв’язку.

Канали зв’язку, розташовані в рамках КЗ, представляють собою:

– Канали зв’язку між ПК користувачів построєні з використанням комутаційного обладнання.

– Канал зв’язку, організований на використанні зйомник носіїв інформації для передачі даних між ПК користувачів, та передачі друкованої інформації.

Опис інформаційних потоків підприємства: вся інформація оброблюється робочими станціями та виробничим обладнанням, які входять до складу ІТС комерційного підприємства, передається по каналам зв’язку на сервер де зберігається. Всі працівники, котрі працюють за ПК та виробничим обладнанням на початку роботи повинні встановити з’єднання з сервером, за допомогою власних ідентифікаційних даних, та завантажити початкову інформацію для роботи.

Загрози безпеці інформації

Для безпеки інформації, що обробляється та зберігається в межах підприемства,визначені такі види потенційних загроз технічного та антропогенного характеру:

– витоку прямими акустичними, віброакустичними, лазерними акустичними, акустоелектричним каналами; каналами ПЕМВН, ВЧ–нав’язування;

– за рахунок впровадження та використання закладних пристроїв для підслуховування;

– оптичний (візуальний) канал витоку інформації.

2.4 Побудова моделі захисту інформації

2.4.1 Побудова узагальненої моделі захисту інформації

Проектування будь-якої системи слід починати з побудови моделі. В даному випадку побудова системи захисту інформації відбуватиметься в узагальненому вигляді, отже, і структуру блоків моделі функціонування системи захисту інформації визначимо узагальнено.

Узагальнена модель процесів захисту інформації складається з десяти елементів, кожний з яких, у свою чергу, є також моделлю (складною структурою взаємозв’язаних і взаємодіючих елементів) певних процесів:

– модель процесів функціонування АС;

– модель використання ресурсів АС;

– модель впливу зовнішнього середовища;

– модель визначення значень керованих параметрів;

– модель визначення значень некерованих, але таких, що піддаються дії параметрів;

– модель розподілу засобів поточного управління;

– модель розподілу засобів дії;

– модель розподілу ресурсів управління;

– модель розподілу ресурсів дії;

– модель розподілу ресурсів, що виділяються на ЗІ.

2.4.2 Системна класифікація загроз АС

На другому етапі проектування системи захисту інформації слід визначити класифікацію можливих загроз по різних критеріях оцінки. [1-62]

Види загроз:

- порушення фізичної цілісності: знищення (спотворення);
- порушення логічної структури: спотворення структури;
- порушення змісту: несанкціонована модифікація;
- порушення конфіденційності: несанкціоноване отримання;
- порушення права власності: привласнення чужого права.

Природа походження загроз:

- випадкова: відмова, збої, помилки, стихійні лиха, побічні впливи;
- навмисна: зловмисні дії людей.

Передумови появи загроз:

- об’єктивні:

кількісна недостатність елементів системи;

якісна недостатність елементів системи;

- суб’єктивні:

промислове шпигунство;

кримінальні елементи;

недобросовісні співробітники.

Джерела загроз:

- люди: сторонні особи, користувачі, персонал;
- технічні пристрої: реєстрації, передачі, зберігання, переробки, видачі;
- моделі, алгоритми,програми: загального призначення, прикладні, допоміжні технологічні схеми обробки: ручні, інтерактивні, внутрішньомашинні, мережеві;
- зовнішнє середовище: стан атмосфери, побічні шуми, побічні сигнали.

2.4.3 Визначення змісту показників уразливості

На даному етапі слід проаналізувати можливі дестабілізуючі дії на кожен вид захисту інформації (таблиця 2.4). При цьому дестабілізуючі дії можна розділити на випадкові та зловмисні, які можуть створити як співробітники організації, так і зловмисники. [1-62]

Таблиця 2.3 – Опис дестабілізуючих дій за видами захисту інформації

Вид захисту інформації	Вид дестабілізуючої дії	
	Випадковий	Зловмисний
Попередження знищення або спотворення	Вірогідність того, що під впливом випадкових чинників інформація буде спотворена або знищена. Математичне очікування об’єму знищеної або спотвореної інформації.	Вірогідність того, що зловмисникові вдасться знищити або спотворити інформацію. Математичне очікування об’єму знищеної або спотвореної інформації.
Попередження несанкціонованої модифікації	Вірогідність того, що під впливом випадкових чинників інформація буде модифікована при збереженні синтаксичних характеристик. Математичне очікування об’єму модифікованої інформації.	Вірогідність того, що зловмисникові вдасться модифікувати інформацію при збереженні синтаксичних характеристик. Математичне очікування об’єму модифікованої інформації.
Попередження несанкціонованого отримання	Вірогідність того, що під впливом випадкових чинників інформація, що захищається, буде отримана особами або процесами, що не мають на це повноважень. Математичне очікування об’єму несанкціоновано отриманої інформації.	Вірогідність того, що зловмисникові вдасться отримати (викрасти) інформацію, що захищається. Математичне очікування об’єму інформації, що викрадається.

Продовження таблиці 2.3

Вид захисту інформації	Вид дестабілізуючої дії	
	Випадковий	Зловмисний
Попередження несанкціонованого розмноження (копіювання)	Випадкове несанкціоноване розмноження (копіювання) інформації в корисливих цілях є маловірогідним.	Вірогідність того, що зловмисникові вдасться несанкціоновано зняти копію з інформації, що захищається, без залишення слідів зловмисних дій. Математичне очікування об'єму несанкціоновано скопійованої інформації. Математичне очікування числа несанкціоновано знятих копій.

2.4.4 Визначення чинників, що впливають на необхідний рівень захисту *(таблиця 2.4).*

Таблиця 2.4 – Класифікація чинників, що впливають на необхідний рівень захисту

Чинник	Класифікація
Характер оброблюваної інформації	o Конфіденційність (дуже висока, висока, середня, невисока) o Об'єм (дуже великий, великий, середній, малий) o Інтенсивність обробки (дуже висока, висока, середня, низька)
Організація роботи АС	o Загальна постановка справи (хороша, середня, слабка, дуже погана) o Укомплектованість кадрами (повна, середня, слабка, дуже слабка) o Рівень підготовки і виховання кадрів (високий, середній, низький, дуже низький) o Рівень дисципліни (високий, середній, низький, дуже, низький)

Продовження таблиці 2.4

Чинник	Класифікація
Архітектура АС	○ Геометричні розміри (дуже великі, великі, середні, незначні) ○ Територіальна розподіленість (дуже велика, велика, середня, незначна) ○ Структурованість компонентів (повна, достатньо висока, часткова, повністю відсутній)
Технологія обробки інформації	○ Структурованість інформації (повна, достатньо висока, часткова, повністю відсутній) ○ Масштаб обробки (дуже великий, великий, середній, незначний) ○ Стабільність інформації (регулярна, достатньо впорядкована, частково стабільна, відсутній) ○ Доступність інформації (загальнодоступна, з незначними обмеженнями, з істотними обмеженнями, з регулярним доступом)
Умови функціонування АС	○ Розташування в населеному пункті (дуже незручне, значні труднощі, певні труднощі, хороше) ○ Розташування на території об’єкту (хаотично розкидане, розкидане, розподілене, компактне) ○ Облаштованість (дуже погана, погана, середня, хороша)

2.4.5 Системна модель захисту інформаційних технологій

На основі принципів системного аналізу: цілісності, ієрархічності, багатоаспектності пропонується системна модель захисту даних в інформаційних технологіях. Принцип цілісності передбачає інтеграцію (об’єднання) частин цілого і проявляється в появі нових властивостей (ознак, параметрів, характеристик, фізичних величин) цілого, які відсутні у його частинах. Принцип ієрархічності надає можливість точно виділити істотні властивості і взаємозв’язки складного об’єкта, що забезпечує докладний опис його властивостей за рахунок використання апріорних знань про внутрішню

будову об’єкта. Принцип багатоаспектності вимагає розгляду об’єкта з різних точок зору з урахуванням взаємозв’язків виявлених аспектів. В основу такої моделі покладено концепцію захисту даних: об’єкт – загроза – захист – управління. [1-62]

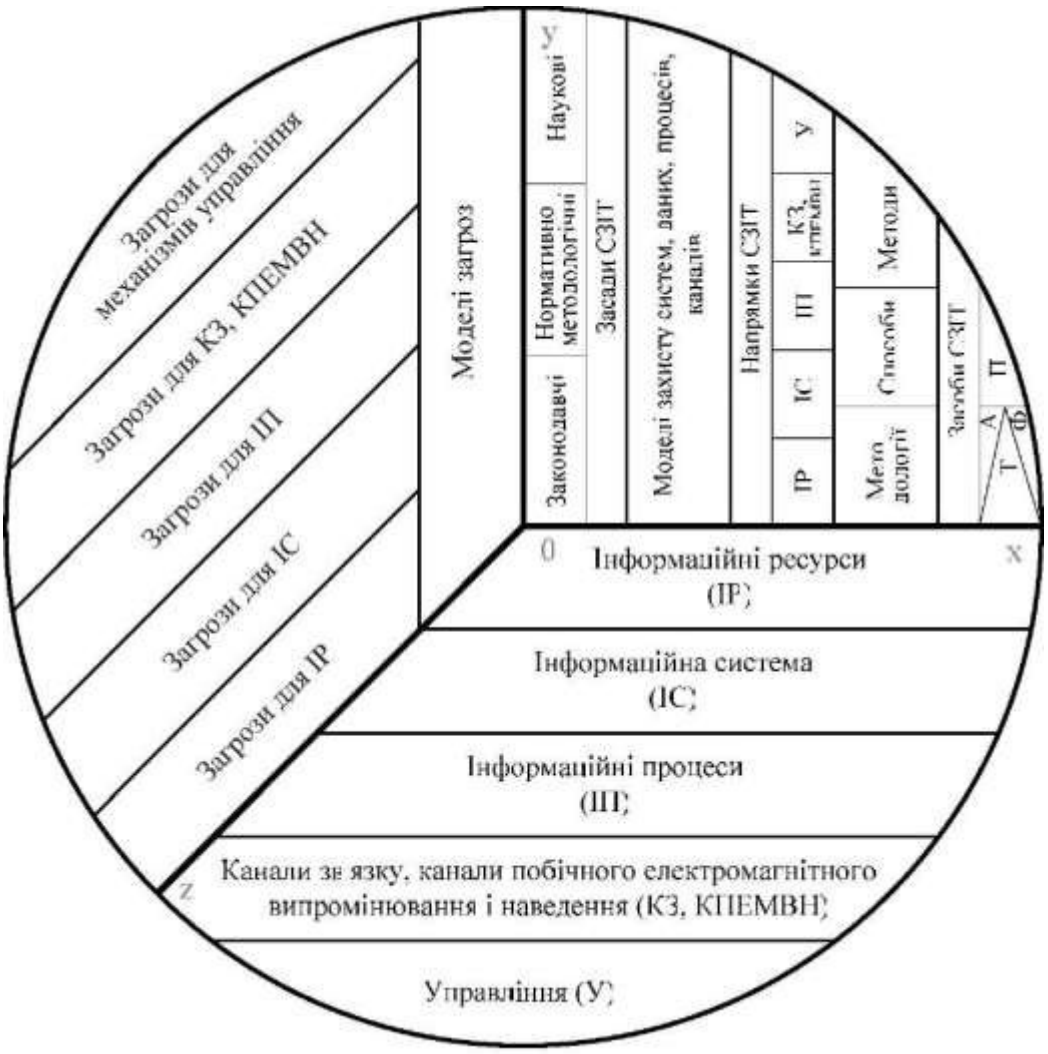

Рисунок 2.2 – Системна модель захисту інформаційних технологій

Системна модель захисту ІТ представлена у вигляді тривимірного простору *x-y-m,* охопленого сферою (рисунок 2.2). У площині *x-m* знаходяться об’єкти захисту: інформаційні ресурси, інформаційні системи, інформаційні процеси, канали зв’язку та канали побічного електромагнітного випромінювання і наведення, елементи управління. У площині *y-m* представлені

рівні моделей загроз адекватно до об’єктів захисту. У площині *x-y* представлена система захисту інформаційних технологій (СЗІТ) адекватно до об’єктів захисту та моделей загроз. Стратегічна структура СЗІТ така: засади – законодавчі, нормативно-методологічні, наукові; моделі захисту; напрямки; методології, способи, методи; засоби СЗІТ – технічні (апаратні, фізичні), програмні. Подання об’єкта захисту – інформаційних технологій п’ятьма взаємозв’язаними підсистемами дає змогу формувати моделі загроз для цих підсистем та відповідні моделі їх захисту на законодавчій, нормативній та науковій основах, не порушуючи концепції об’єкт – загроза – захист – управління для відповідного класу ІТ.

Комплексний захист ІТ від НСД до інформації та від її витоку можливими каналами здійснюється на основі структури взаємозв’язку і взаємодії всіх компонентів на рівнях: методологічного, апаратного-фізичного (технічного), програмного, комунікаційного, управлінського забезпечення (таблиця 2.6).

2.4.6 Проектування системи ЗІ

Послідовність і зміст проектування.

1 Обґрунтування вимог до захисту і аналіз умов захисту.

2 Визначення функцій захисту.

3 Обґрунтування переліку задач захисту, що підлягають вирішенню.

Таблиця 2.5 – Управління захистом інформації

Методи управління	Класифікація та опис методів
Планування	Короткострокове: аналіз планів обробки інформації; аналіз умов ЗІ; оцінка уразливості; визначення потреб в СЗ; оцінка можливостей механізмів захисту; розподіл СЗ; формування графіка використання СЗ; оцінка ефективності використання СЗ.
	Середньострокове: аналіз виконання робіт в АС; прогнозування умов ЗІ; визначення вимог до ЗІ; аналізСЗ і ресурсів захисту; визначення завдань на ЗІ в найближчий інтервал та подальші інтервали; розподіл СЗ і ресурсів захисту.

Продовження таблиці 2.5

Методи управління	Класифікація та опис методів
	Довгострокове: аналіз структур і технологічних схем функціонування АС; аналіз очікуваного функціонального використання АС; визначення вимог до ЗІ; оцінка ресурсів захисту; оцінка арсеналу СЗІ; обгрунтування функціонування СЗІ; розробка програм розвитку СЗ; оцінка очікуваної ефективності захисту.
Оперативно-диспетчерське управління	Короткострокове: регулярне використання СЗ; збір, обробка і реєстрація оперативної інформації; розпізнавання ситуації; ухвалення рішень на втручання у функціонування СЗІ; реалізація рішень; аналіз і прогнозування розвитку ситуації; розробка пропозицій по коректуванню планів захисту.
Календарно-планове керівництво	Короткострокове: поточна оцінка стану ЗІ; оцінка вимог до захисту; оцінка впливу на захист зміни умов функціонування АС; коректування планів захисту; розробка пропозицій по вдосконаленню планування захисту.
	Середньострокове: аналіз відповідності фактичного і необхідного рівнів захисту; аналіз зміни вимог до захисту; аналіз зміни умов функціонування АС; коректування планів захисту; розробка пропозицій по вдосконаленню механізмів і розвитку СЗ.
	Довгострокове: аналіз рівня забезпечення ЗІ; аналіз функціонування механізмів захисту; розробка пропозицій по вдосконаленню структури функціонування АС; організація впровадження СЗ; вдосконалення механізмів захисту.
Забезпечення повсякденної діяльності	Короткострокове: збір інформації; базова обробка інформації і формування початкових даних; видача інформації.
	Середньострокове: аналітико-синтетична обробка даних; формування масиву регламентних даних; видача інформації.

4 Вибір засобів, необхідних для вирішення завдань захисту.

5 Оцінка очікуваної ефективності вибраних механізмів захисту.

6 Обґрунтування структури і технологічних схем функціонування системи захисту.

7 Техніко-економічна оцінка проекту.

8 Рішення організаційно-правових питань ЗІ.

2.4.7 Моделі безпеки

Розглянемо формальні моделі безпеки. Вони є основним інструментом докази відповідності системи захисту автоматизованої системи заданої політики безпеки. [1-62]

2.4.7.1 Модель Харрісона, Руззо, Ульмана

Модель Харрісона, Руззо, Ульмана реалізує дискреційну політику безпеки.

Ідея – використання таблиці, яка відображає правила розмежування доступу, так званої матриці доступу.

Рядки матриці доступу відповідають суб'єктам, а стовпці – суб'єктам і об'єктам. В осередках матриці міститися права доступу суб'єктів до об'єктів.

Призначення моделі – модель дозволяє встановити кожному суб'єкту системи індивідуальні дозволи доступу до кожного об'єкту системи і є легко реалізовується.

2.4.7.2 Модель Take Grant

Модель Take Grant реалізує дискреційну політику безпеки.

Ідея – представлення системи у вигляді спрямованого графа, в якому вершини є суб'єкти або об'єкти системи. Спрямовані дуги на графі означають права, які один об'єкт має по відношенню до іншого. Безліч прав, крім звичайних прав доступу, містить два права take (t) і grant (g), що змінюють матрицю доступу.

Призначення моделі: модель забезпечує безліч правил переписування графа (за допомогою прав take і grant), що дозволяють вивчати зміни графа внаслідок передачі прав та зміни стану системи. Зміна стану системи виконується з використанням наступних правил переписування графа.

Правило take. Дане правило може бути записано як «суб'єкт бере-яке право по відношенню до об'єкта іншого суб'єкта».

Правило grant. Дане правило може бути записано як «суб'єкт дає будь-яке право по відношенню до об'єкта іншого суб'єкта».

Правило create. Дане правило може бути записано як «суб’єкт створює вершину графа з будь-яким правом по відношенню до об’єкта іншого суб’єкта».

Правило remove. Дане правило може бути записано як «суб’єкт видаляє будь-яке право для іншого суб’єкта».

2.4.7.3 Модель Белла-Лападула

Модель Белла-Лападула реалізує мандатну політику безпеки.

Ідея – визначення для кожного суб’єкта ступеня довіри та для кожного об’єкта рівня секретності; дозвіл доступу суб’єктів тільки до тих об’єктів, які мають рівень доступу не більший, ніж ступінь довіри даного суб’єкта. Сукупність лінійно впорядкованих рівнів секретності утворює класифікацію.

Прикладом класифікації може бути наступне безліч рівнів секретності: «Загальнодоступний», «Для службового користування», «Секретний», «Цілком таємно».

Рівень секретності об’єкта – ієрархічний атрибут, який визначає його цінність чи важливість, може враховувати його вразливість.

Ступінь довіри – рівень секретності суб’єкта.

Чим вище ступінь довіри суб’єкта, тим до більш секретної інформації він має доступ. Чим вище секретність об’єкта, тим більше секретна інформація зберігатися в ньому.

Ідеї, що лежать в моделі Белла і Лападула, беруть походження з «паперового світу». Белл і Лападула перенесли модель безпеки, прийняту при роботі з документами. Вони виявили, що для запобігання витоку інформації до неуповноваженою суб’єктам, суб’єктам з низькими рівнями секретності не дозволяється читати інформацію з об’єктів з високими рівнями секретності.

Белл і Лападула зробили додаткове спостереження при побудові своєї моделі: суб’єктам не дозволяється розміщувати інформацію або записувати її в об’єкти, що мають більш низький рівень секретності. Наприклад, коли «Цілком секретний» документ поміщається в «некласифікованих» відро для сміття, може статися витік інформації.

Принципи моделі Белла і Лападула: «немає читання вгору» – суб’єкт з рівнем секретності може читати інформацію з об’єкта з рівнем секретності, тільки якщо суб’єкт переважає над об’єктом; «немає запису вниз» – суб’єкт з рівнем секретності 1 може писати інформацію в об’єкт з рівнем секретності 1, тільки якщо об’єкт переважає над суб’єктом.

Проблеми моделі Белла і Лападула

1) Операція читання «зверху вниз» призводить до протіканню інформації від читаного об’єкта до запиту доступу на читання об’єкту. Даний потік є безпечним, тому що суб’єкт з високим рівнем секретності має доступ на читання до об’єкта з низьким рівнем секретності. Проте в розподіленої конфігурації читання ініціюється запитом від одного компонента до іншого. Такий запит утворює потік інформації в невірному напрямі (запис в об’єкт з меншим рівнем секретності). Таким чином, віддалене читання в розподілених системах може статися, тільки якщо йому передує операція запису вниз, що є порушенням правил моделі Белла і Лападула.

Рішення проблеми – впровадження в систему додаткових засобів обробки віддалених запитів для забезпечення того, щоб потік інформації від високорівневого суб’єкта до низкорівневому об’єкту був обмежений запитом на доступ.

2) Якщо в деякому стані секретний суб’єкт захотів прочитати абсолютно секретний об’єкт, то доти, поки система задовольняє моделі Белла і Лападула, здійснити це буде неможливо, але ніщо в моделі не запобігає систему від «декласифікацію» об’єкта від зовсім секретного до секретного. Рішення проблеми – введення в систему правила сильного спокою, яке свідчить, що рівні секретності суб’єктів і об’єктів ніколи не змінюються в ході системної операції. Очевидним недоліком такої реалізації в системі є втрата гнучкості при виконанні операцій.

2.4.7.4 Модель «Китайської стіни»

Модель побудована на динамічній зміні прав доступу.

Політика безпеки «Китайської стіни» може бути представлена як кодекс, що вживається фахівцями з аналізу ринку. Такий спеціаліст не може радити корпорації, якщо він має «внутрішні дані» про корпорації конкурентів, а може працювати тільки зі загальнодоступною ринковою інформацією.

Основою політики «Китайської стіни» є твердження про те, що суб'єкт може отримати доступ до інформації, що не входить у конфлікт з будь-якою інформацією, до якої він мав доступ до цього. При цьому спочатку суб'єкт може отримати доступ до будь-якого інформаційного ресурсу за своїм вибором. Визначаються класи конфліктів інтересів, що включають в себе деякі інформаційні ресурси. Якщо суб'єкт отримав доступ до одного з цих ресурсів, то йому забороняється доступ до ресурсів, що входять до той же конфлікт інтересів.

2.4.7.5 Модель ролей

Модель ролей – модель контролю доступу, що базується на ролях – не ставитися ні до мандатної, ні до дискреційної політики безпеки, тому що в моделі використовуються абстракції більш високого рівня. Так в моделі контролю доступу, що базуються на ролях використовуються такі поняття:

- користувач – співробітник організації;
- роль – список виконуваних в системі функцій;
- суб'єкт – активна сутність системи;
- операція – деяка дія, для виконання якої потрібні права доступу до одного чи декількох захищених об'єктів.

Звичайно модель ролей (модель контролю доступу, що базується на ролях) реалізується на рівні додатків, а не на рівні операційної системи. Труднощі підтримки на рівні операційної системи полягає в практичній неможливості виявлення досить загальних базових конструкцій, незалежних від області застосування і легко реалізованих.

Моделі безпеки інформації

I) Моделі розмежування доступом

1) Ймовірністні моделі:

- Ігрова модель;
- Модель з повним перекриттям.

2) Інформаційні

3) Побудовані за принципом надання прав:

- Матриця доступу;
- Модель Харрісона-Руззо;
- Модель Take-Grand;
- Модель АДЕПТ-50;
- Модель Хартсона.

3.1) Мандатна модель

- Модель Белла-ла Падула.

3.2) Рольова модель

II) Моделі контролю цілісності:

- Модель Біба;
- Модель Кларка Вільсона.

III) Моделі забезпечення доступності

- Мандатна модель;
- Модель Міллена.

2.4.8 Модель порушника

Порушники бувають внутрішніми і зовнішніми.

Серед внутрішніх порушників в першу чергу можна виділити:

– безпосередніх користувачів і операторів інформаційної системи, в тому числі керівників різних рівнів;

– адміністраторів обчислювальних мереж та інформаційної безпеки;

– прикладних і системних програмістів;

– співробітників служби безпеки;

– технічний персонал з обслуговування будівель і обчислювальної техніки, від прибиральниці до сервісного інженера;

– допоміжний персонал і тимчасових працівників.

Серед причин, що спонукають співробітників до неправомірних дій, можна вказати наступні:

– безвідповідальність;

– помилки користувачів і адміністраторів;

– демонстрацію своєї переваги (самоствердження);

– «боротьбу з системою»;

– корисливі інтереси користувачів системи;

– недоліки використовуваних інформаційних технологій.

Групу зовнішніх порушників можуть становити:

– клієнти;

– запрошені відвідувачі;

– представники конкуруючих організацій;

– співробітники органів відомчого нагляду і управління;

– порушники пропускного режиму;

– спостерігачі за межами території, що охороняється.

Крім цього класифікацію можна проводити за такими параметрами.

Використовувані методи і засоби:

– збір інформації і даних;

– пасивні засоби перехоплення;

– використання коштів, що входять в інформаційну систему або систему її захисту, і їх недоліків;

– активне відстеження модифікацій існуючих засобів обробки інформації, підключення нових засобів, використання спеціалізованих утиліт, впровадження програмних закладок і «чорних ходів» в систему, підключення до каналів передачі даних.

Рівень знань порушника щодо організації інформаційної структури:

– типові знання про методи побудови обчислювальних систем, мережевих протоколів, використання стандартного набору програм;

– високий рівень знань мережевих технологій, досвід роботи зі спеціалізованими програмними продуктами і утилітами;

– високі знання в області програмування, системного проектування та експлуатації обчислювальних систем;

– володіння відомостями про засоби і механізми захисту атакується системи;

– порушник був розробником або брав участь в реалізації системи забезпечення інформаційної безпеки.

Час інформаційного впливу:

– в момент обробки інформації;

– в момент передачі даних;

– в процесі зберігання даних (з огляду на робочий і неробочий стану системи).

За місцем здійснення впливу:

– віддалено з використанням перехоплення інформації, що передається по каналах передачі даних, або без її використання;

– доступ на територію, що охороняється;

– безпосередній фізичний контакт з обчислювальною технікою, при цьому можна виділити: доступ до робочих станцій, доступ до серверів підприємства, доступ до систем адміністрування, контролю та управління інформаційною

системою, доступ до програм управління системи забезпечення інформаційної безпеки.

У таблиці 2.6 наведені модель порушників інформаційної безпеки і їх порівняльна характеристика.

Таблиця 2.6

Характеристика	Хакер	Група хакерів	Конкуренти	Держструктури, спецпідрозділи
Обчислювальна потужність технічних засобів	Персональний комп'ютер	Використання чужих обчислювальних мереж	Потужні обчислювальні мережі	Необмежена обчислювальна потужність
Доступ до інтернету, тип каналів доступу	Модем або виділена лінія	Використання чужих каналів з високою пропускною здатністю	Власні канали з високою пропускною здатністю	Самостійний контроль над маршрутизацією трафіку в Інтернеті
Фінансові можливості	Сильно обмежені	Обмежені	Великі можливості	практично необмежені
Рівень знань в області IT	Невисокий	Високий	Високий	Высокий, розробники стандартів
Використовувані технології	Готові програми, відомі уразливості	Пошук нових вразливостей, виготовлення шкідливих програм	Сучасні методи проникнення в інформаційні системи і впливу на потоки даних в ній	Докладні знання інформаційних технологій: можливі уразливості і недоліки
Знання про побудову системи захисту об'єкта	Недостатні знання про побудову інформаційної системи	Можуть докладати зусиль для отримання уявлення про принципи функціонування системи захисту	Можуть докладати зусиль для отримання уявлення про принципи функціонування системи захисту, впроваджувати свого представника в службу безпеки	У процесі сертифікації системи представники держорганів можуть отримувати досить повну інформацію про її побудові
Переслідувані цілі	Експеримент	Внесення спотворень в роботу системи	Блокування функціонування системи, підрив іміджу, розорення	Непередбачувані

Продовження таблиці 2.6

Характеристика	Хакер	Группа хакерів	Конкуренти	Держструктури, спецпідрозділи
Характер дій	Прихований	Прихований	Прихований або відкритий демонстративний	Може не обтяжувати себе приховуванням своїх дій
Глибина проникнення	Найчастіше зупиняється після першого успішного впливу	До моменту досягнення поставленої мети або появи серйозної перешкоди	До переможного кінця	Нічого не здатне їх зупинити

2.5 Завдання компанії, які можуть вирішувати сучасні електронні системи

1 У великих компаніях під час упровадження нових методологій виконання стандартів якості часто виникають проблеми, що пов’язані з глобальним розподілом та функціональною ізоляцією різних операцій.

2 Всі публічні компанії повинні підтверджувати достовірність своєї фінансової звітності та її відповідність стандартам. За невідповідність нормам чи сфальсифіковані дані передбачено штрафи.

3 Бізнес багатьох компаній побудований навколо складних бізнес-програм, які часто об’єднують взаємопов’язані і взаємозалежні проекти. Для таких програм необхідним є стратегічне управління, грамотне впровадження ресурсів, а також можливість їх ефективного перерозподілу між програмами.

4 Практично у всіх сферах діяльності для злиття компаній чи купівлі однієї компанії іншою необхідна ретельна підготовка до підписання угоди та інтеграції діяльності структур, що об’єднуються. Серйозними проблемами для будь-якої компанії, яка ставить за мету об’єднати зусилля і потенціал корпорацій, є віддаленість працівників, неоднорідність систем, що використовують підрозділи компанії для розв’язання різних задач, відмінність у ділових процесах тощо.

5 Всі компанії, які надають професійні послуги, тим чи іншим способом завжди співпрацюють із замовниками. Це потребує наявності можливості

контролю фінансового становища і відстеження бюджету, збереження основних ідей і цілей, розподіл доступу до інформації.

Основні задачі, які стоять перед компанією щодо організації її потоків документів:

1 Забезпечення ефективнішого управління, прозорість діяльності організації в загально важливих питаннях та захист інформації, яка доступна обмеженому колу осіб.

2 Підтримка системи контролю якості та відповідність міжнародним нормам.

3 Підтримка ефективного накопичення, управління і доступу до інформації. Забезпечення кадрової гнучкості за рахунок великої формалізації діяльності кожного працівника і можливість збереження всієї історії його діяльності.

4 Створення протоколів діяльності корпорації загалом (аналіз діяльності підрозділів, внутрішні службові розслідування).

5 Оптимізація бізнес-процесів і автоматизація механізму їх виконання і контролю.

6 Економія ресурсів за рахунок ефективного управління потоками документів у компанії.

2.6 Програмні системи автоматизації діловодства і документообігу

Спектр сучасних систем автоматизації діловодства і документообігу досить різноманітний щодо їх функціональності та технологічного рівня. Дамо коротку характеристику програмних продуктів.

Система Docs електронного документообігу ECM класу пропонує повнофункціональні механізми управління документами та моделювання бізнес-процесів (створення, погодження, підписання, зберігання, доархівне та архівне зберігання). Можливість підписати документ електронним цифровим підписом

(ЕЦП) для більш ніж 19 центрів сертифікації ключів (ЦСК), що сертифіковані і акредитовані в Україні.

Система Optima-WorkFlow («Оптима») - програмна платформа для створення систем управління документами (електронного документообігу) в державних і комерційних організаціях будь-якого масштабу. Забезпечує комплексну автоматизацію процесів обробки документів і дозволяє перейти до безпаперової технології роботи з електронними документами. Платформа Optima-WorkFlow - це відкрита, web-орієнтована архітектура, функціональність, застосування найсучасніших технологій і промислових стандартів, інтеграція з лідируючими IT-рішеннями, візуальні засоби налаштування і адаптації системи.

Система ТЕЗА - це сучасна і надійна система електронного документообігу. Вона є зручним інструментом контролю виконавської дисципліни та сприяє підвищенню керованості та контрольованості організації, дозволяючи скласти об'єктивне уявлення про стан справ всередині компанії, навести порядок в потоках корпоративної інформації.

Система Work Expeditor (Compag) забезпечує швидку та ефективну організацію колективної роботи і автоматизація бізнес-процесів, захист інформації на рівні полів даних, аудит всіх видів операцій, цілісність транзакцій і документів, автоматичний контроль версій документів, підтримка жорсткої та вільної, а також послідовної та паралельної маршрутизації, контроль виконання та розсилку повідомлень, прозору інтеграцію з Outlook, можливість швидкої розробки замовлень на базі стандартних інтерфейсів Microsoft, потужний графічний редактор карт ділових процесів.

Система «Босс-Референт» розроблена на основі Lotus Notes, виконує централізоване зберігання, пошук, пересилку складних документів будь-яких форматів та розмежування доступу до них.

Система «Е1Євфрат» працює в середовищі Windows і забезпечує комплексну автоматизацію діловодства, включаючи реєстрацію, контроль

виконання, організацію та обслуговування електронного архіву документів, отриманих із різних джерел. Передбачає пошук тексту за вмістом документа та за реквізитами, морфологічний аналіз документів, підтримку широкого спектру графічних форматів. Наявні робочі столи – «Секретаріат», «Бухгалтерія», «Відділ кадрів», «Страховакомпанія», «Домашня база Євфрат». Підтримуються додаткові можливості: утиліти для тестування БД, її ущільнення, архівування, функції фільтрування інформації.

Система «Дело» («Електронні офісні системи»). Основа продукту – поняття предметної області діловодства, взяті з нормативних документів, інформаційна та функціональна моделі діловодства, побудовані з урахуванням міжнародних стандартів структурного аналізу і проектування систем з використанням сучасних CASE-технологій. Розроблений Web-орієнтований варіант системи для розподіленої роботи з документами в Internet.

Система «LanDocs» (АО «Ланит») – дворівневий комплекс ПЗ,призначений для автоматизації функцій реєстрації та заповнення облікових карток документів, розсилки документів, завдань, доручень, забезпечує контроль стану документів, версій, створення звітів, запис в архів.

Система DIRECTUM – управління корпоративним контентом (Enterprise Content Management), дозволяє побудувати повноцінну систему електронного документообігу вашого підприємства. Архітектура заснована на власній надійної предметно-орієнтованої платформі. Інструмент розробки IS-Builder відкриває можливості для швидкого налаштування, високою масштабованості, легкої адаптації системи під потреби конкретного клієнта, під його бізнес-процеси і завдання силами IT-фахівців замовника, без залучення вендора.

Таблиця 2.7 – Порівняння систем електронного документообігу

	DIRECTUM	**LanDocs**	**Optima WorkFlow**	**Босс-референт**	**ДЕЛО**
Серверна ОС	Microsoft Windows Server 2008/ 2008 R2/ 2012/ 2012 R2/ 2016,Linux	MS Windows Server 2000 – 2016	Windows Server 2008, Windows Vista,7, Linux	MS Windows Server 2000 – 2016, RedHat Linux, CentOS, SuSE, AIX	Windows 2008 R2 SP1 Server, Windows 2012 R2 Server, Windows 2016 Server.
Клієнтська ОС	Windows 7/8/8.1/10 Windows Server /2008 R2/2012/2012R2/2016	Vista/Windows 7 / 8 /10	Microsoft Windows 7 / 8 / 10	Windows (2000-2016), Linux, MacOS	Windows 7, Windows 8, Windows 8.1, Windows 10.
СКБД. Платфо-рма	Microsoft SQL Server 2008/ 2008 R2/2012 / 2014/2017 Standard/Enterprise Edition/Business Intelligence	MS SQL Server 2005-2017	Microsoft SQL Server,Oracle Database	Oracle, PostgreSQL, MS SQL 2005-2008, MySQL 5, MS Access, FireBird, Interbase, Informix, Apache Cassandra	MS SQL Server 2008 R2 SP3, MS SQL Server 2012 SP3, MS SQL Server 2014 SP1, MS SQL Server 2016 SP1, Oracle 10g, Oracle 11g Oracle 12c
Підтримка кількох БД (розподілених відділень)	+	+	+	+	+
Можливість інтеграції	SAP, Microsoft Dynamics AX Microsoft Navision Axapta, 1C Microsoft Office, Apache OpenOffice, Libre Office Microsoft Outlook	ABBYY Recognition, ABBYY FlexiCapture	Microsoft SharePoint Server	1C, MS Office, MS Share Point	1C, MS Office, VentaFax & Voice
API	+	+	+	+	+
Демоверсія/ демодоступ	Демодоступ	Демодоступ	Демодоступ	Демодоступ	Демоверсия
Вартість ліцензії на 20 користувачів	115400 грн.	70500 грн.	62900 грн.	81400 грн.	108250 грн.
Діловодство	+	+	+	+	+
Загальний документообіг	+	+	+	+	+
Управління діяльність діловодства	+	+	–	+	–
Електронний архів	+	+	+	+	+
Управління проектами	+	+	+	+	+

Враховуючи те, що придбання кожної із вищезгаданих систем пов’язане з вагомими витратами та подальшою адаптацією для конкретних потреб, необхідно виконати детальний аналіз підприємницької діяльності та обрати з урахуванням підходів та технологій найбільш конкурентоспроможну охарактеризовану систему такого класу (таблиця 2.7).

У результаті аналізу для систем електронного документообігу виділено такі критерії порівняння: документообіг, автоматизація ділових процесів (workflow), сховище документів, адміністрування і безпека. Оскільки управління конфіденційною інформацією вимагає надійного захисту, то основним критерієм для вибору СЕД будуть показники адміністрування та безпеки.

Критерій “безпека” є найважливішим чинником в оцінюванні і порівнянні таких можливостей, як розподілення прав та ролі користувачів, використання надійної криптосистеми, здійснення реєстрації за паролем, відносна безпека порівняно з іншими системами.

Критерій “сховище документів” є наступним важливим критерієм оцінювання, який характеризує ефективність використання даних, їх збереження, пошуку, доступу.

Критерій “діловодство” – це можливості роботи з електронними документами як з паперовими, тобто створення документів, реєстрація, накладання резолюцій, можливість колективної роботи та контроль за функціонуванням документів.

Загальні параметри СЕД – критерій загальної оцінки та характеристики СЕД: гнучкість, технічні засоби, придатність програмного забезпечення і простота використання, можливість розвитку системи та інтеграції.

Таблиця 2.8 – Аналіз функціональних можливостей СЕД

Функціональні можливості	Directum	PayDox	БОСС-Референт	Дело
Підтримка різних способів аутентифікації	+	+	+	+
Призначення прав користувачам	+	+	+	-
Призначення прав групам користувачів	+	-	+	+
Підтримка користувацьких ролей	-	+	+	-
Розмежування прав доступу до об'єктів системи	+	-	+	+
Розмежування прав доступу на рівні операцій до об'єктів	-	+	+	+
Видача прав на час виконання дій	+	-	+	+
Наявність жорстких маршрутів	-	+	-	+
Шифрування даних системи	+	+	+	-
Шифрування даних при передачі	-	+	+	+
Протоколювання дій користувача	+	-	+	+
Засоби моніторингу подій у системі	+	+	+	+
Використання ЕЦП	+	+	+	+
Застосування сертифікованих засобів криптозахисту	+	-	+	+
Блокування документа редагованого іншим співробітником	+	+	+	-
Наявність програмних засобів контролю цілісності документів	+	+	+	+
Організація резервного копіювання бази даних	+	+	+	+

Враховуючи загальні показники, організуємо управління корпоративною конфіденційною документацією. Засоби та методи забезпечення інформаційної безпеки докорінно залежать від того, які технічні та програмні засоби використовуються як базові під час побудови системи, яка її загальна структура. Навіть якщо корпорація є територіально розподіленою, сегменти різних рівнів

мають аналогічну структуру і функціональність. Для їх побудови застосовують технічні засоби одного рівня, але різної потужності. Оскільки завдання забезпечення інформаційної безпеки є пріоритетними, то необхідно враховувати безліч чинників, зокрема психологічний.

Як основну прикладну систему на сервері слід використовувати СЕД Documentum. Особливістю побудови захищеної системи є використання термінальних технологій. Використовуючи архітектуру побудови рішення, основану на застосуванні в якості робочих місць користувача апаратних "тонких клієнтів" або терміналів, можна знизити загрози з боку працівників.

Термінальне рішення з погляду захисту інформації має переваги: позбавляє користувачів багатьох можливостей, які породжують загрози інформаційній безпеці, або не передбачені функціональними обов'язками працівника. Працюючи за терміналом, не можна скопіювати на дискету чи флеш-пам'ять інформацію, не можна встановити на робоче місце шкідливе або заборонене для використання програмне забезпечення. Доступ до такого термінала користувач може одержати, ввівши ім'я користувача і пароль або вставивши зчитувач, який наявний в терміналі, пластикову картку з персональною ідентифікаційною інформацією. Отримати доступ до системи може тільки власник смарт-карти.

Отже, розв'язано частину задачі запобігання несанкціонованому доступу до системи. Але відомі випадки, коли за такої надійної системи зловмиснику вдалось отримати доступ до закритої для нього системи. Тому використання мандатного доступу і мітки безпеки як підсилення механізму захисту інформації дає змогу вирішити безліч проблем.

Використання інших організаційних засобів інформаційної безпеки в СЕД, таких як розподілення прав доступу користувачів до обмежених ресурсів, які доступні відповідно до посади/привілеї, підсилює систему безпеки. Організація забезпечення контролю доступу до периферійних пристроїв, наприклад,

можливість організації обов’язкової перевірки мітки документа, який передається на друк, з міткою принтера – дає змогу гарантувати, що конфіденційні документи будуть видрукувані тільки на довірених принтерах. Засобом запобігання несанкціонованому доступу до серверів і комп’ютерів системи є використання електронних замків. Вони забезпечують розмежування і контроль доступу до серверів і їх апаратних ресурсів, а також контроль цілісності програмного середовища і мають необхідні сертифікати. [1-62]

Головне – це забезпечення надійного захисту документів протягом усього життєвого циклу, а також можливість координації системи у напрямі специфічних завдань та вимог підприємства.

Важливими для підприємства є такі функціональні можливості: можливість територіально розподіленої СЕД (оскільки будь-яка компанія націлена на розвиток, що часто пов’язано із розростанням масштабів, поширюючись на інші країни), інтеграція (часто виникають такі ситуації, які потребують використання додаткових можливостей інших систем і/або програмних продуктів); захищеність інформації (охоплює доступ, розмежування прав користувачів, шифрування даних, запобігання витоку цінної інформації); ефективне використання баз даних (пов’язане зі збереженням, пошуком, зберіганням даних, можливістю збереження історії документів); управління документами (можливість колективної роботи, накладання резолюцій, контролювання виконання доручень).

2.7 Особливості збереження документів

СЕД працюють, переважно, на базі розподіленої архітектури і використовують різноманітні комбінації технологій збору, індексування, збереження, пошуку і перегляду електронних документів. У більшості СЕД реалізована ієрархічна система збереження документів (за принципом "шафа /папка"). Кожен документ міститься в папці, що, у свою чергу, знаходиться на

полиці і т.д. Кількість рівнів вкладення при збереженні документів не обмежений. Той самий документ може входити до складу декількох папок і полиць за рахунок застосування механізму посилань (вихідний документ у цьому випадку залишається незмінним і зберігається на місці, визначеному адміністратором СЕД). У ряді СЕД реалізовані ще більш могутні можливості збереження за рахунок організації зв'язків між документами (ці зв'язки можна встановлювати і редагувати в графічному виді).

Будь-якому документові в СЕД властивий певний набір атрибутів (наприклад, його назва, автор документа, час його створення й ін.). Набір атрибутів може змінюватися від одного типу документа до іншого (у межах одного типу документів він зберігається незмінним). У СЕД атрибути документа зберігаються в реляційній базі даних. Для кожного типу документів за допомогою візуальних засобів створюється шаблон картки, де в зрозумілому графічному вигляді представлені найменування атрибутів документа. При введенні документа в СЕД береться необхідний шаблон і заповнюється картка (заносяться значення атрибутів). Після заповнення картка виявляється зв'язаною із самим документом. [1-62]

Деякі галузеві аналітики навіть вважають, що СЕД цілком можуть стати основою корпоративної інформаційної системи підприємства чи організації. СЕД працюють, переважно, на базі розподіленої архітектури і використовують різноманітні комбінації технологій збору, індексування, збереження, пошуку і перегляду електронних документів. У більшості випадків, серверна частина СЕД складається з наступних логічних компонентів (які можуть розташовуватися як на одному, так і на декількох серверах):

1 Сховища атрибутів документів (карток);

2 Сховища документів;

3 Сервісів повнотекстової індексації.

Під сховищем документів звичайно розуміється сховище вмісту документів. Сховище атрибутів і сховище документів часто поєднують під загальною назвою "архів документів". Слід зазначити, що великими перевагами СЕД є збереження документів у вихідному форматі й автоматичне розпізнавання безлічі форматів файлів.

Останнім часом все більшу популярність здобуває збереження документів разом з атрибутами в базі даних. Такий підхід має свої переваги і недоліки. Перевагою є значне підвищення безпеки доступу до документів, а основним недоліком – низька ефективність роботи з документами при великому обсязі збереженої інформації. При даному підході також потрібне використання могутніх серверів з великими обсягами оперативної пам’яті і жорстких дисків. Крім того, у випадку збою бази даних відновити документи, що зберігалися в ній, буде дуже непросто.

2.8 Особливості маршрутизації документів

Модулі СЕД, що відповідають за документообіг, прийнято називати модулями маршрутизації документів. У загальному випадку використовуються поняття динамічна і статична маршрутизації документів. При динамічній маршрутизації будь-який користувач, що бере участь у документообігу, може за своїм розсудом змінити існуючий маршрут проходження документів (або задати новий маршрут). При статичній маршрутизації маршрути проходження документів строго регламентовані, і користувачі не мають права їх змінювати. Однак при статичній маршрутизації можуть оброблятися логічні операції, коли маршрут змінюється при виконанні яких-небудь заздалегідь заданих умов (наприклад, відправленню документа керівництву при перевищенні конкретним користувачем своїх посадових повноважень).

2.9 Розмежування доступу

У СЕД реалізовані такі методи безпеки, як надійні засоби розмежування повноважень і контролю за доступом до документів. У більшості випадків з їхньою допомогою визначаються наступні види доступу (набір повноважень, що задаються, залежить від конкретної СЕД):

– повний контроль над документом;

– право редагувати, але не знищувати документ;

– право створювати нові версії документа, але не редагувати його;

– право анотувати документ, але не редагувати його і не створювати нові версії;

– право читати документ, але не редагувати його;

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

– повна відсутність прав доступу до документа (під час роботи із СЕД кожна дія користувача протоколюється, і, таким чином, вся історія його роботи з документами може бути легко проконтрольована).

2.10 Відстеження версій і підверсій документів

При одночасній роботі із документом відразу декількох користувачів (особливо, якщо його необхідно погоджувати в різних інстанціях) дуже зручною функцією СЕД є використання версій і підверсій документа. Припустимо, виконавець створив першу версію документа і передав її на розгляд наступному користувачеві. Другий користувач змінив документ і створив на його основі вже нову версію. Потім він передав свою версію документа в наступну інстанцію третьому користувачеві, що створив уже третю версію. Через певний час, ознайомившись із зауваженнями і виправленнями, перший виконавець документа вирішує допрацювати вихідну версію і на її основі створює підверсію першої версії документа. Перевагою СЕД є реалізована в них можливість

автоматичного відстеження версій і підверсій документів (користувачі завжди можуть визначити, яка саме версія документа є найбільш актуальною один по одному або часові їхнього створення). [1-62]

2.11 Анотування документів

При організації групової роботи над документами досить корисна можливість їхнього анотування. Тому що в деяких випадках користувачі позбавлені права на внесення яких-небудь змін у документ у процесі його узгодження, то вони можуть скористатися з можливості його анотування. У більшості СЕД анотування реалізується за рахунок включення в картку документа атрибута для анотації і передачі користувачам прав на редагування такого поля картки. Але таке рішення не завжди прийнятне (особливо при анотуванні графічного документа). У зв’язку з цим, у деяких СЕД існує так називана функція "червоного олівця", за допомогою якої можна графічно вказати недоліки на самому зображенні. [1-62]

2.12 Забезпечення достовірності документів

Сьогодні основним і практично єдиним пропонованих на ринку методом для забезпечення достовірності документа є використання електронно-цифрового підпису (ЕЦП). Основний принцип роботи ЕЦП заснований на технологіях шифрування з асиметричним ключем. Тобто ключі для шифрування і дешифрування даних різні. Є «закритий» ключ, який дозволяє зашифрувати інформацію, і є «відкритий» ключ, за допомогою якого можна цю інформацію розшифрувати, але з його допомогою неможливо «зашифрувати» цю інформацію. Таким чином, власник «підпису» повинен володіти «закритим» ключем і не допускати його передачу іншим особам, а «відкритий» ключ може поширюватися публічно для перевірки автентичності підпису, отриманого за допомогою «закритого» ключа. [1-62]

Для наочності ЕЦП можна представити як дані, отримані в результаті спеціального криптографічного перетворення тексту електронного документа. Воно здійснюється за допомогою так званого «закритого ключа »- унікальної послідовності символів, відомої тільки відправнику електронного документа. Ці «дані» передаються разом з текстом електронного документа його одержувачу, який може перевірити ЕЦП, використовуючи так званий «відкритий ключ» відправника – також унікальну, але загальнодоступну послідовність символів, однозначно пов’язану з «закритим ключем» відправника. Успішна перевірка ЕЦП показує, що електронний документ підписаний саме тим, від кого він виходить, і що він не був модифікований після накладення ЕЦП.

Таким чином, підписати електронний документ з використанням ЕЦП може тільки володар «закритого ключа», а перевірити наявність ЕЦП – будь-який учасник електронного документообігу, який отримав «відкритий ключ», відповідний «закритому ключу» відправника. Підтвердження належності «відкритих ключів» конкретним особам здійснює засвідчувальний центр – спеціальна організація або сторона, якій довіряють всі учасники інформаційного обміну.

Протоколювання дій користувачів – важливий метод захисту електронного документообігу. Його правильна реалізація в системі дозволить відстежити всі неправомірні дії і знайти винуватця, а при оперативному втручанні навіть припинити спробу неправомірних або завдають шкоди дій. Така можливість обов’язково має бути присутня в самій СЕД. Крім того, додатково можна скористатися рішеннями сторонніх розробників і партнерів, чиї продукти інтегровані з СЕД. Говорячи про партнерські рішеннях, перш за все мова йде про СУБД і сховищах даних, будь-який подібний продукт великих розробників, таких як Microsoft або Oracle, наділений цими коштами. Також не варто забувати про можливості операційних систем з протоколювання дій користувачів і рішеннях сторонніх розробників у цій області.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно тверезо оцінювати можливі загрози і ризики СЕД і величину можливих втрат від реалізованих загроз. Як вже говорилося, захисту СЕД не зводиться лише до захисту документів і розмежування доступу до них. Залишаються питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв; захисту мережевої середовища, в якій функціонує система, захист каналів передачі даних і мережевого устаткування, можливо виділення СЕД в особливий сегмент мережі. Комплекс організаційних заходів грають роль на кожному рівні захисту, але їм, на жаль, часто нехтують. Але ж тут і інструктаж, і підготовка звичайного персоналу до роботи з конфіденційною інформацією. Погана організація може звести до нуля всі технічні заходи, наскільки досконалі вони б не були.

2.13 Обґрунтування вибору системи електронного документообігу

На основі проведених досліджень та аналізу наявних СЕД на відповідність сформульованим критеріям оцінки вважаємо доцільним використання на підприємстві системи «Босс-Референт», що розроблена на основі Lotus Notes, що виконує централізоване зберігання, пошук, пересилку складних документів будь-яких форматів та розмежування доступу до них. Як система керування документообігом є складовою АСУП – «БОСС».

Ця СЕД може працювати на великій кількості операційних систем, підтримує web-клієнт (це дуже важливо для користувачів, що повинні мати доступ до СЕД з будь-якого комп'ютера без спеціального ПЗ), підтримує роботу з розподіленими відділеннями, має великі можливості інтеграції з прикладними програмами. Недоліком є вартість продукту, але, беручи за увагу розміри та обсяг діяльності підприємства, цей недолік не є критичним.

«Босс-Референт» має модульну архітектуру. Модулі, що входять до складу системи, являють собою взаємопов'язані бази даних, що працюють в середовищі Lotus Notes / Domino. Ці бази можна розділити на три групи.

2.13.1 Функціональні модулі

Призначені для обробки управлінської інформації та прийняття рішень. [1-62]

2.13.1.1 Модуль «Канцелярія»

Забезпечує повний цикл роботи організації з вхідними та вихідними документами. Дозволяє здійснювати контроль, облік і реєстрацію кореспонденції.

Функціональні можливості бази даних «Канцелярія»:

1 Введення електронних документів. При цьому можуть використовуватися шаблони, готові документи, створені в інших додатках (Microsoft Word, Excel, PowerPoint і т.д.), відсканованої образи паперових оригіналів.

2 Реєстрація кореспонденції з автоматичною або напівавтоматичною нумерацією.

3 Резервування номерів для вихідних документів.

4 Відправлення документів на розгляд і виконання, списання в справу.

5 Створення доручень по документах.

6 Друк контрольних карток (у тому числі за шаблонами, підготовленим в Microsoft Word) і карток резолюцій.

7 Ведення декількох канцелярій з можливістю пересилання документів з однієї канцелярії в іншу.

8 Пошук документів за різними параметрами, заданим користувачем. Якщо система включає кілька баз даних «Канцелярія», то пошук може вестися як по всіх базах даних, так і по кожній окремо.

Після того, як робота з документами завершується, вони переміщаються в модуль «Архів Канцелярії», при цьому доступні гнучке налаштування автоматичного архівування і пошук документів по всіх модулях, включаючи архівні.

2.13.1.2 Модуль «Прийняття рішень»

Призначений для автоматизації бізнес-процесів, які реалізуються в системі у вигляді «Процесів прийняття рішень», формуються з двох обов'язкових елементів: картки документа і маршруту руху документа. У постачання системи входять перед налаштовані «процеси прийняття рішення» для типових документів (договорів, організаційно-розпорядчих документів, проектів вихідних документів, службових записок, заявок). Процеси для спеціалізованих документів (наприклад, кредитних заявок) можуть бути швидко настроєні додатково.

Функціональні можливості бази даних «Прийняття рішень»:

1 Створення та збереження документів / проектів документів. При цьому можуть використовуватися шаблони, готові документи, створені в інших додатках (Microsoft Word, Excel, PowerPoint і т.д.), відсканові образи паперових оригіналів.

2 Обробка документів відповідно визначеним процесам, які можуть включати такі стадії, як підготовка, узгодження, візування, підписання, затвердження документів.

3 Контроль руху документів.

4 Автоматична та ручна реєстрація документів.

5 Резервування номерів для договорів, проектів вихідних і організаційно-розпорядчих документів.

6 Підтримка роботи з листами ознайомлення і списками розсилки.

7 Формування доручень за документами та контроль їх виконання.

8 Створення окремих модулів для кожного типу документів (наприклад, модуль «Прийняття рішень за договорами», модуль «Прийняття рішень з організаційно розпорядчих документів», і т.д.).

9 Пошук документів за різними параметрами, заданим користувачем. Якщо система включає кілька баз даних «Прийняття рішень», то пошук може вестися як по всіх базах даних, так і по кожній окремо.

Після того, як робота з документами завершується, вони переміщаються в модуль «Архів Прийняття рішень», при цьому доступні гнучка настройка автоматичного архівування і пошук документів по всіх модулях, включаючи архівні.

2.13.1.3 Модуль «Доручення»

Дозволяє в масштабах всієї організації ставити завдання співробітникам за допомогою створення доручень по документах або незалежних доручень і відстежувати їх виконання. Надає можливість формувати пов’язані доручення, що утворюють «дерево» доручень, і контролювати їх виконання.

Доручення можуть видавати керівники всіх рівнів. Виконавці можуть зберігати звіти про виконану роботу в модулі «Доручення». Модуль тісно пов’язаний з іншими базами системи («Прийняття рішень», «Канцелярія»). Доручення можуть створюватися як у самій базі даних «Доручення», так і в інших модулях системи («Прийняття рішень», «Канцелярія»), при цьому всі доручення зберігаються у модулі «Доручення».

Функціональні можливості БД Доручення:

1 Підготовка проекту доручення.

2 Відображення в системі відомостей про хід виконання доручення.

3 Автоматичне сповіщення про закінчення терміну виконання доручення та про виконання доручення.

4 Зміна терміну виконання доручення та відповідального виконавця доручення.

5 Повернення доручення на доопрацювання.

6 Затвердження результатів виконання доручень.

2.13.1.4 Модуль «Довідник організації»

Призначений для зберігання і поновлення даних про структуру і співробітників підприємства. У базі даних міститься інформація про підрозділи

та філії, які входять до складу організації, їх взаємна підпорядкованість, а також про співробітників організації, в тому числі інформація щодо суміщення посад, делегування повноважень і ролям з обробки документів (який стверджує, узгоджувальний, і т.п .).

Функціональні можливості бази даних «Довідник організації»:

1 Введення і зберігання інформації про структуру організації у вигляді ієрархічного дерева. У разі, якщо структура організації включає самостійні підрозділи (філії), можливе ведення загального довідника для всієї компанії або окремих «Довідників організації» для кожного підрозділу.

2 Зберігання службових та особистих даних по кожному співробітнику (ПІБ, посада, номери телефонів, та ін.)

3 Створення списків розсилки.

4 Оформлення сумісництва, перекладу співробітника в інший підрозділ, звільнення та поновлення на посаді.

5 Призначення ролей з обробки документів для користувачів системи.

6 Налаштування механізму делегування повноважень для передачі в разі потреби прав на роботу в системі іншим співробітникам – окремо для основної та сумісництвом посади (проекту).

7 Підтримка загальносистемних налаштувань: зберігання ліцензійного ключа, реєстрація користувачів та їх груп, підтримка роботи з декількома канцеляріями.

2.13.1.5 Модуль «Зовнішні адресати»

Призначений для зберігання даних про організації-контрагентах (замовниках, партнерів, клієнтів) та їх представників. Тут може зберігатися найрізноманітніша інформація – від банківських реквізитів організації до мобільного телефону її представника.

У системі дані з модуля «Зовнішні адресати» використовуються скрізь, де потрібно вказувати контрагентів, наприклад, при роботі з договорами, вхідними та вихідними документами, і т.д.

2.13.1.6 Модуль «Словники»

Призначений для створення та зберігання списків ключових слів, використовуваних для заповнення полів введення в картках баз даних системи. Використовується більшістю модулів системи в якості довідника словникових значень. Додавання нових записів і редагування старих здійснюється адміністраторами або спеціально виділеними працівниками.

2.13.1.7 Модуль «Комутатор»

Є центральною базою, за допомогою якої відбувається налаштування програми. У ній міститься технологічна інформація про розташування інших баз даних системи «Босс-Референт» на серверах. База даних «Комутатор» призначена для вирішення наступних завдань:

1 Навігація користувачів – модуль забезпечує навігацію по базах даних, виступає єдиною точкою входу в систему для користувачів.

2 Комутація модулів системи – встановлює зв’язки між базами даних системи і зі словниково-довідковими модулями.

3 Конфігурація робочих місць користувачів.

Функціональні можливості бази даних «Комутатор»:

1 Навігація по базах даних системи.

2 Реєстрація баз даних певної конфігурації.

3 Прив’язка робочої станції до бази даних «Комутатор».

4 Додавання в робочий простір користувача значка бази даних.

5 Оновлення структури баз даних програми.

6 Відкриття баз даних.

7 Перенесення програми на інший сервер.

8 Перейменування баз даних.

9 Видалення з бази даних «Комутатор» посилання на бази даних.

10 Налаштування адрес баз даних системи.

11 Категоризація бази даних.

12 Синхронізація баз даних «Комутатор» в кластері Lotus Domino.

2.13.1.8 Модуль «Кабінет»

Призначений для інформування користувачів про їхні завдання: сюди доставляються всі службові повідомлення системи «Босс-Референт». База даних доступна всім користувачам, при цьому кожен користувач отримує тільки адресовані йому повідомлення. Система дозволяє дублювати повідомлення, що приходять в «Кабінет», в поштову скриньку користувача.

Функціональні можливості бази даних «Кабінет»:

1 Збереження повідомлень з посиланнями на документи.

2 Відстеження поточних завдань користувача.

2.13.1.9 Модуль «Пошук»

Допоміжний модуль, що дозволяє проводити пошук по набору атрибутів карток документів баз даних «Канцелярія», «Прийняття рішень», і їх архівів.

2.13.1.10 Модуль «Реєстратор»

Містить набір програмних лічильників, генеруючих реєстраційні номери документів. Дозволяє гнучко налаштовувати різні формати нумератора відповідно до прийнятого в організації порядку формування реєстраційних номерів для документів різного типу. Крім «лічильника», формат може містити різні параметри, наприклад: ПІБ підписанта, дата реєстрації, роздільники, індекс справи, і т.п. Для одного нумератора можна створити кілька форматів.

2.13.2 Архівні модулі

Призначені для зберігання архівних документів з модулів «Канцелярія», «Доручення», «Прийняття рішень», і яке до них відноситься модулів «Електронні образи». Для кожного модуля створюється окрема архівна база даних. Документи, передані в архів з модулів «Канцелярія» і «Прийняття рішень», отримують статус «У справу», статус доручень не змінюється.

2.13.2.1 Модуль «Налаштування Прийняття рішень»

Допоміжний модуль, застосовуваний для створення типових процесів, відповідно до яких будуть оброблятися документи в базі даних «Прийняття рішень». У картці типового процесу задаються стадії і етапи обробки документів, налаштування значень полів документів за замовчуванням, співробітники, що беруть участь в обробці, а також співробітники, що мають право на створення документів.

2.13.2.2 Модуль «Протокол»

Використовується для протоколювання дій користувачів при роботі з документами в системі «Босс-Референт». Інформація з БД Протокол призначена тільки для перегляду і використовується службою, відповідальною за інформаційну безпеку.

2.13.2.3 Модуль «Транспорт»

Відноситься до технологічних сервісів і являє собою допоміжний модуль, який застосовується для обміну документами між серверами. У цій базі даних формуються запити, транспортні документи і повідомлення про проходження по маршруту транспортних документів.

2.13.2.4 Модуль «Шаблони»

Зберігає шаблони типових документів, стандартних форм і бланків, типових резолюцій, а також шаблони проміжних форм, що створюються в Microsoft Word і використовуються для друку документів різних баз даних.

2.13.2.5 Модуль «Електронні образи»

Допоміжний модуль, який застосовується для зберігання електронних образів документів окремо від самих документів модулів «Канцелярія», «Прийняття рішень» і «Доручення», а також їх архівів. Для кожного модуля створюється окрема база даних «Електронні образи».

2.13.3 Організація роботи в розподіленої середовищі

Для роботи в розподіленої середовищі система використовує всі переваги платформи Lotus Domino, а також власний транспортний механізм.

2.13.3.1 Транспортний механізм «Босс-Референт»

Щоб користувач, що розташовується на віддаленому сервері (наприклад, у філії організації) міг працювати з документами, які створені на сервері центрального офісу, ці документи треба доставити на його сервер. Разом з документом віддаються всі файли вкладення, пов’язані документи, доручення. При реплікації (фактично копіюванні змісту модулів системи) можуть виникати ситуації, коли, наприклад, доручення співробітник філії вже отримав, а документ, за яким воно видане, ще не прийшов на сервер філії.

Щоб не допускати таких ситуацій, «Босс-Референт» використовує власний транспортний механізм – дані передаються безпосередньо через сокетні з’єднання XML-пакетом. Коли система розуміє, що необхідно передати документи на інший сервер, в модулі «Транспорт» створюється «заявка» на транспортування і формується пакет документів і даних. Він стискається і пересилається на інший сервер. Після того, як пакет цілком отриманий, система

підтверджує його отримання. Тільки після цього пакет розпаковується, документи направляються у відповідні бази, а користувач отримує відповідні повідомлення в модуль «Кабінет».

Механізм реплікації в Бос-референт застосовується тільки для синхронізації довідкових та словникових даних.

2.13.4 Сервер Lotus Domino

Система електронного документообігу «Босс-Референт» побудована на платформі IBM Lotus Notes / Domino, і використовує в роботі Lotus Domino Server.

Сервер Domino є основою інфраструктури для спільної роботи співробітників підприємства і платформою для додатків, що реалізують різноманітні бізнес-функції. Створення системи електронного документообігу на платформі Lotus Notes / Domino, дає можливість використовувати відразу всі основні компоненти, які об’єднує в собі унікальна технологія Domino:

- засоби електронної пошти;
- документоорієнтовані бази даних;
- засоби розробки додатків;
- систему реплікації баз даних;
- методи захисту інформації;
- кошти календарного планування;
- Інтернет / Інтранет, веб-технології;
- засоби інтеграції з додатками сторонніх розробників.

Domino працює під управлінням різних серверних операційних систем, включаючи Windows, Linux. Єдиний інформаційний простір територіально розподіленої організації часто підтримується декількома серверами. Найбільш оптимальною схемою організації серверів в такому випадку є топологія

«багаторівневої зірки». На рисунку 2.4 розглянемо модель інформаційної безпеки ІКС з обраної СЕД. [1-62]

2.14 Приведення інформаційної безпеки СЕД «Босс-Референт» до визначеного стану

Комерційне підприемство– це велика георгафічно розподілена організація, захист інформації в якій є важливим та актуальним завданням. Тому особливу увагу слід придиліти безпеці обраної системи електронного документообігу. Для цього проаналізуємо відповідність СЕД вимогам стандартного функціонального профілю захищеності 3.КЦД.1.

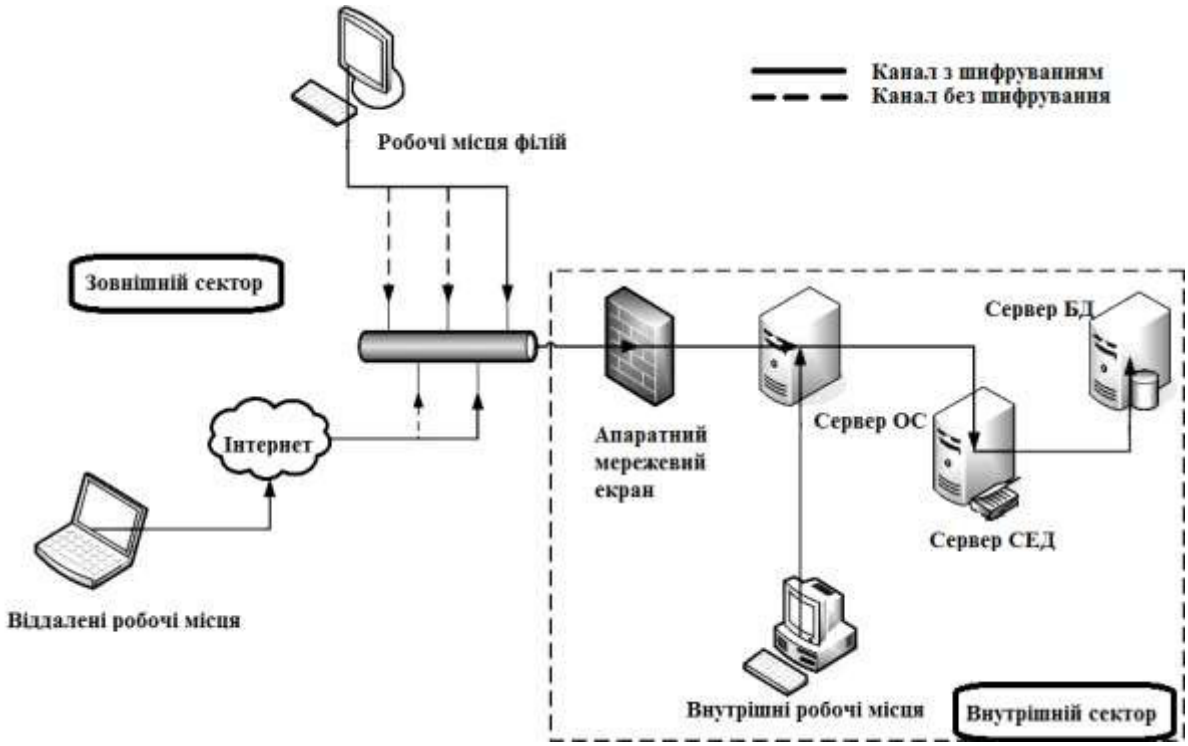

Рисунок 2.3 – Модель інформаційної безпеки ІКС з СЕД «Босс-Референт»

Це стандартний функціональний профіль захищеності від НСД в комп’ютерних системах, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Обрання цього профілю є доцільним, бо на ОІД

присутня інформація з обмеженим доступом, для якої необхідно забезпечити всі базові властивості інформації.

Сукупність вимог до сервісів безпеки описується стандартним функціональним профілем безпеки (згідно з рекомендаціями НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»):

3.КЦД.1 = { КД-2, КО-1, КВ-1,
ЦД-1, ЦО-1, ЦВ-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }.

Обраний профіль захищеності 3.КЦД.1 включає наступні вимоги:

КД-2 – базова довірча конфіденційність;

КО-1 – повторне використання об’єктів;

КВ-1 – мінімальна конфіденційність при обміні;

ЦД-1 – мінімальна довірча цілісність;

ЦО-1 – обмежений відкат;

ЦВ-1 – мінімальна цілісність при обміні;

ДР-1 – квоти;

ДВ-1 – ручне відновлення;

НР-2 – захищений журнал;

НИ-2 – одиночна ідентифікація і автентифікація;

НК-1 – однонаправлений достовірний канал;

НО-2 – розподіл обов’язків адміністраторів;

НЦ-2 – КЗЗ з гарантованою цілісністю;

НТ-2 – самотестування при старті;

НВ-1 – автентифікація вузла.

Проаналізуємо, чи всі функціональні послуги безпеки стандартного профілю реалізовані в СЕД підприємства (таблиця 2.8).

Послуга КД-2 реалізується службою каталогів (Active Directory) серверною ОС Windows, з якою працює СЕД, і передбачає, що атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково існує можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації

Послуга КО-1 частково реалізована, тому що після завершення роботи користувач повинен вимкнути або перезавантажити комп'ютер, якщо зробити це неможливо, треба використовувати спеціальне ПЗ для декількаразового перезапису оперативної пам'яті комп'ютера. Зазвичай, достатнім вважається трьохразовий перезапис випадковими даними.

Послуга КВ-1 реалізується за допомогою програмного шифрування файлів перед їх передачею каналами зв'язку або прозорого шифрування файлів перед їх записуванням на диск за допомогою вбудованих в ОС криптоалгоритмів (ПЗ BitLocker, що використовує надійні криптоалгоритми для прозорого шифрування даних, що вбудоване як в серверну, так в клієнтські ОС Windows).

Послуга ЦД-1 реалізується в системі за допомогою розмежування прав доступу (групові політики) в ОС Windows та окремо права доступу встановлює СЕД. Існує можливість розмежування доступу для груп користувачів.

Послуга ЦО-1 реалізується за допомогою стандартної утиліти Microsoft Windows, що дозволяє відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу, також СЕД «Босс-Референт» дозволяє певну множину операцій над документом та зберігає всі його попередні версії.

Послуга ЦВ-1 реалізується за рахунок використання контрольних сум, хеш-функцій та цифрового підпису, що присутні в ОС та СЕД. КЗЗ забезпечує

можливість виявлення порушення цілісності інформації, що міститься в об’єкті, який передається.

Послуга ДР-1 реалізується наданням адміністратором квот користувачам (дискового простору, оперативної пам’яті, ресурсів процесора та інше) стандартними засобами серверної ОС та засобами СЕД.

Відновлення системи (послуга ДВ-1) проходить за допомогою засобів ОС і забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування. СЕД підтримує відновлення системи завдяки зберіганню всіх попередній версій документів, тобто, цінна інформаційна з великою ймовірністю втрачена не буде.

Таблиця 2.9 – Аналіз реалізації профілю захищеності

Послуги	Метод реалізації
КД-2	Серверна ОС Windows
КВ-1	Серверна та клієнтська ОС Windows
КО-1	Частково реалізована клієнтською ОС Windows, для повної реалізації необхідне ПЗ для перезапису оперативної пам’яті
ЦД-1	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
ЦО-1	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
ЦВ-1	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
ДР-1	Серверна ОС Windows та СЕД "Босс-Референт"
ДВ-1	Серверна ОС Windows та СЕД "Босс-Референт"
НР-2	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
НИ-2	Серверна ОС Windows
НК-1	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
НО-2	Серверна та клієнтська ОС Windows, СЕД "Босс-Референт"
НЦ-2	Серверна та клієнтська ОС Windows
НТ-2	Реалізована частково, тому що самотестування КЗЗ здійснюється при старті системи за допомогою процедури POST, для тестування на запит потрібно використати спеціальне ПЗ
НВ-1	Серверна та клієнтська ОС Windows

Для реалізації послуги НР-2 використовується журнал реєстрації Windows та СЕД, що протоколює все значимі події безпеки, а також всі основні дії користувача в системі.

Для реалізації послуги НИ-2 використовується служба каталогів ОС (протоколи NTLMv4 або Kerberos, більш надійний другий протокол).

Реалізація послуги НК-1 передбачає використання протоколу SSL 3.0 або TLS1.0 та ЕЦП (наприклад, ECDSA), які присутні в ОС та СЕД.

Для реалізації послуги НО-2 необхідне виділення ролей адміністратора системи та адміністратора безпеки, що можливо зробити як засобами ОС, так і СЕД.

Послуга НЦ-2 реалізована за допомогою підтримки КЗЗ власного домену виконання завдяки засобам розмежування доступу ОС.

Послуга НТ-2 реалізована частково, тому що самотестування КЗЗ здійснюється при старті системи за допомогою процедури POST (Poweronself-test.

Для реалізації послуги НВ-1 необхідне використання протоколу автентифікації Kerberos, що наявний в ОС Windows.

Тобто, за наявності клієнтської та серверної операційних систем Windows, на яких працює СЕД "Босс-Референт", маємо лише дві частково нереалізовані послуги – КО-2 та НТ-2, умови їх реалізації наведені в таблиці 2.8.

2.15 Політика безпеки

Передмова

Відповідно до концепції інформаційної безпеки комерційного підприємства, система електронного документообігу, як частина інформаційної інфраструктури віднесена до інформаційних і комунікаційних систем.

Головною метою, на досягнення якої спрямовані всі положення політики, є надійне забезпечення інформаційної безпеки підприємства і, як наслідок, недопущення нанесення матеріального, фізичного, морального чи іншої шкоди підприємству в результаті проектно-технологічної та інформаційної діяльності.

Політика інформаційної безпеки є планом високого рівня, в якому описуються цілі і завдання заходів у сфері безпеки. Політика описує безпеку в узагальнених термінах, без специфічних деталей і не оперує способами реалізації.

Перш ніж приступати до розробки керівних документів, необхідно визначити глобальні цілі політики підприємства та створити концепцію.

Призначення політики інформаційної безпеки:

– збереження конфіденційності критичних інформаційних ресурсів;

– стійке функціонування системи електронного документообігу

– забезпечення безперервності доступу до інформаційних ресурсів підприємства для підтримки бізнес діяльності;

– цілісність і автентичність інформації, що зберігається і оброблюваної в СЕД і передається по каналах зв'язку

– підвищення обізнаності користувачів в області ризиків, пов’язаних з інформаційними ресурсами підприємства;

– визначення міри відповідальності і обов’язків співробітників по забезпеченню інформаційної безпеки на підприємстві.

– забезпечення конфіденційності інформації, що зберігається, обробляється на засобах обчислювальної техніки і передається по каналах зв'язку

Призначення документа політики безпеки

Політика встановлює структуру захисту інформації з обмеженим доступом, сфери відповідальності користувачів та адміністраторів, мети, завдання і функції користувачів та адміністраторів.

Метою діяльності по забезпеченню інформаційної безпеки є зниження загроз інформаційній безпеці до прийнятного рівня.

Основні завдання діяльності по забезпеченню інформаційної безпеки:

– виявлення потенційних загроз інформаційній безпеці;

– захист від втручання сторонніх осіб в процес функціонування СЕД;

– розмежування доступу зареєстрованих користувачів до інформації апаратними, програмними та криптографічними засобами захисту, які використовуються в СЕД;

– періодичний контроль коректності дій користувачів системи шляхом аналізу вмісту цих журналів фахівцями інформаційної безпеки;

– реєстрація дій користувачів при використанні ресурсів СЕД в системних журналах;

– контроль цілісності використовуваних програмних засобів, а також захист системи від впровадження шкідливих кодів, включаючи комп'ютерні віруси;

– забезпечення аутентифікації користувачів, що беруть участь в інформаційному обміні;

– запобігання інцидентам інформаційної безпеки;

– створення умов для мінімізації та локалізації завданих збитків неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу і ліквідації наслідків порушення безпеки інформації;

Перегляд Політики проводиться на регулярній основі не рідше

одного разу на рік.

Цей документ призначений для використання користувачами і адміністраторами в рамках.

Терміни та визначення політики безпеки

Електронний документообіг - сукупність процесів створення, обробки, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту отримання таких документів.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Автоматизована система (далі АС) – організаційно-технічна система, що реалізує інформаційну технологію і об’єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

Інформаційна система (далі ІС) – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

Інформація з обмеженим доступом – конфіденційна, таємна та службова інформація.

Політика безпеки інформації – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Безпека інформації – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Захист інформації в АС – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Користувач – фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

Несанкціонований доступ до інформації; НСД до інформації – доступ до інформації, здійснюваний з порушенням ПРД.

Розмежування доступу – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

Адміністратор безпеки – адміністратор, відповідальний за дотримання політики безпеки.

Порушник – користувач, який здійснює несанкціонований доступ до інформації.

Втрата інформації – неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

Комп'ютерний вірус – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

Модель загроз – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Модель порушника – абстрактний формалізований або неформалізований опис порушника.

Ризик – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Автентифікація – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Пароль – секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

Призначення та правова основа документа політики безпеки

Політика інформаційної безпеки комерційного підприємства визначає систему поглядів на проблему забезпечення безпеки інформації і є систематизованим викладом цілей і завдань захисту, як одне або декілька правил, процедур, практичних прийомів і керівних принципів в області інформаційної безпеки, якими необхідно керуватися в своїй діяльності, а також основних принципів побудови, організаційних, технологічних і процедурних аспектів забезпечення безпеки інформації.

Політика враховує сучасний стан і найближчі перспективи розвитку інформаційних технологій на комерційному підприємстві, цілі, завдання і правові основи їх експлуатації, режими функціонування, а також містить аналіз

загроз безпеці для об’єктів і суб’єктів інформаційних стосунків комерційного підприємства.

Вимоги політики безпеки поширюються на всю інформацію і ресурси обробки інформації компанії. Дотримання Політики обов’язкове для всіх співробітників, як постійних, так і тимчасових. У договорах з третіми особами, одержуючими доступ до інформації компанії, має бути обумовлений обов’язок третьої особи по дотриманню вимог Політики.

Дана політика безпеки розроблена на базі нормативних документів:

– Закон України «Про інформацію» від 02.10.1992 № 2657-XII;

– Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (1994, N 31, ст.286);

– Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV

– Закон України «Про електронні довірчі послуги» від 22.05.2003 № 852-IV

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

– НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

– НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

– НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

– ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

Правила політики безпеки контролю доступу до приміщень організації

1 Правила для будівлі в цілому:

– на підприємстві має бути встановлена система відеоспостереження;

– система відеоспостереження повинна охоплювати як зовнішній периметр, так і внутрішні приміщення будівлі;

– система відеоспостереження за внутрішніми приміщеннями може охоплювати лише коридор і важливі приміщення (серверна);

– можливість потрапити до будівлі, минувши КПП, має бути повністю відсутня;

– при винесенні технічних засобів, що належать підприємству, необхідно надати дозвіл на КПП;

– всі приміщення мають бути обладнані засобами пожежогасіння.

2 Правила для всіх приміщень тих, що мають засоби обробки інформації:

– необхідне забезпечення стабілізованим живленням кожного компонента інформаційної системи;

– необхідні резервні джерела живлення для устаткування;

– робочі місця повинні розташовуватися відповідно до санітарних норм (не менше 4,5м^2 виробничої площі).

Правила політики безпеки для апаратних засобів

Апаратні засоби є частиною ІТС що оброблюють інформацію. Збереження належної якісної роботи – одне з пріоритетних завдань політики безпеки

підприємства.

– кожен апаратний засіб підлягає інвентаризаційному обліку, відповідно документам;

– необхідно скласти номенклатуру по всьому устаткуванню з вказівкою місця його розміщення;

– суворо дотримуватися правил експлуатації устаткування;

– купувати устаткування лише у надійних постачальників, що дають гарантію і що мають власні центри обслуговування в межах локації підприємства;

– ремонтувати апаратне забезпечення лише у організацій, що мають ліцензію на роботу з засобами захисту інформації;

– при заміні устаткування або ремонті, переконатися, що конфіденційні дані видалені з носія, маючи відповідну копію з цими даними;

– регулярно проводити діагностику апаратних засобів.

Правила політики безпеки при роботі з програмним забезпеченням

Програмне забезпечення впливає на швидкість і якість обробки даних. Також тип ПЗ залежить від типу оброблювальної інформації. Слід уважно вибирати ПЗ для підприємства. Не дотримання цього правила може привести до втрати даних, зайвим витратам на встановлення нового ПЗ, втрати інформації.

– програмне забезпечення, використовуване на підприємстві, а також документація, що поставляється з ним, мають бути враховані;

– на ПК повинно встановлюватися ліцензійне ПЗ, або ПЗ, яке не порушує авторських прав;

– при установці ПЗ необхідно враховувати політику інформаційної безпеки підприємства;

– встановлення устаткування повинна виробляти спеціально вивчена людина;

– перед встановленням ПЗ повинно бути протестовано;

– перед початком використання ПЗ, співробітників необхідно навчити правильному використанню;

– кожен користувач повинен знати, відповідно до договору, які права інтелектуальної власності він може порушити;

– стежити за оновленнями і встановлювати їх (виконується відповідальними за це особами);

– використовувати програмний засіб може особа, що має на це права;

– по можливості забезпечити оптимальні умови для роботи устаткування;

– захист програмних засобів ведеться як від помилок програм, так і від помилок користувача.

Правила політики безпеки при резервуванні даних і системи

Необхідно регулярно створювати і тестувати резервні копії даних і ПЗ.

Необхідно забезпечити відповідне обладнання для резервного копіювання СЕД, що гарантує відновлення всієї необхідної інформації і ПЗ після відмови носіїв інформації або аварії. Необхідно мати в розпорядженні не менше двократного фізичного запасу протестованих носіїв.

При копіюванні даних слід враховувати наступні фактори:

Власниками ресурсів СЕД бути визначений, а керівництвом затверджено склад інформації, що підлягає резервному і страховому копіюванню;

Повинні складатися точні і повні звіти встановленої форми зі створення резервних копій, повинні документуватися процедури відновлення інформації;

Обсяг резервного копіювання (наприклад, повне або вибіркове резервне копіювання) і періодичність його виконання повинні відповідати виробничим вимогам організації, вимогам безпеки залученої в копіювання інформації та критичність цієї інформації для продовження роботи організації;

Резервні копії СЕД повинні зберігатися в віддаленому місці, на відстані, достатньому для запобігання будь-якої шкоди внаслідок стихійного лиха або аварії на основній території організації, причому категорично забороняється зберігання носія безпосередньо в пристрої запису / читання;

Резервна копія даних СЕД, винесена на віддалене зберігання, повинна мати рівень фізичного захисту і захисту від впливу навколишнього середовища, що відповідає стандартам, що застосовуються на основній території; засоби управління, які застосовуються для носіїв інформації на основній території, повинні діяти і на території, на якій зберігаються резервні копії;

Носії резервних копій інформації повинні регулярно перевірятися, щоб гарантувати їх надійність на той випадок, якщо ними необхідно буде скористатися в надзвичайних обставинах, залишковий ресурс служби повинен бути не менше 30 відсотків від повного;

Повинні регулярно тестуватися і перевірятися робочі і аварійні режими процедури відновлення інформації, щоб гарантувати їх ефективність і можливість завершення в терміни, відведені для відпрацювання процедур відновлення робочих даних;

В ситуаціях, в яких важливе збереження конфіденційності, резервні копії повинні бути захищені шифруванням.

При наявності технічних можливостей процеси відновлення і резервного копіювання інформації можуть бути автоматизовані. При цьому такі автоматизовані рішення повинні бути в достатній мірі вивірені, протестовані і відпрацьовані до введення їх в промислову експлуатацію.

Правила політики безпеки звернення з носіями інформації

Всі операції і процеси, що виконуються з носіями інформації, повинні гарантувати недопущення фактів несанкціонованого розкриття, зміни, видалення або руйнування ресурсів або відмову в доступі.

Всі операції і процеси, що виконуються з носіями інформації, повинні контролюватися. Носії як речовий ресурс повинні бути фізично захищені.

Повинні бути розроблені та реалізовані відповідні процедури роботи для захисту від несанкціонованого розкриття, зміни, видалення та знищення комп'ютерних носіїв інформації, даних введення - виведення, системної документації.

Правила політики безпеки з управління доступом

Розділення повноважень і можливостей співробітників допомагає уникнути несанкціонованого доступу до різної інформації у СЕД. Сучасні методи допомагають це зробити фізично. При здобутті даних спочатку потрібно пройти реєстрацію з позитивною ідентифікацією у СЕД.

З метою забезпечення інформаційної безпеки ІС, а також визначення зони відповідальності та компетентності кожного користувача ІС використовується процедура призначення і підтримки рівнів доступу і ролей СЕД. Відповідальність за вибір пари «рівень доступу - роль» несе керівник підрозділу користувача.

При призначенні рівня доступу і ролей, зазначеним в заявці, адміністратор зобов'язаний здійснювати контроль їх сумісності і несуперечності: доступ до об'єктів і перелік дозволених дій над ними на рівні доступу і права ролі повинні бути приведені до взаємної відповідності

– для кожної посади мають бути визначені повноваження, і доступна лише та інформація, яка йому необхідна, повинен вестися облік даних, які отримав працівник;

– ключі від приміщень видаються особам, що мають права доступу, при цьому заноситься відповідний запис в журнал;

– кількість символів в паролі має бути не менше ніж вісім, бути таким, що діє протягом 90 днів після останньої зміни;

– пароль повинен періодично мінятися для всіх співробітників підприємства. Використання старих паролів не дозволяється;

– дані про логіни і паролі повинні зберігатися централізовано;

– передача логіна або пароля іншій особі заборонена;

– одночасне використання одного логіна на декількох станціях неможливе;

– при звільненні користувача, його обліковий запис видаляється;

– при введенні пароля в програмних засобах або передачі його через ЛВС, пароль не повинен відображуватися в явному вигляді;

– створити правило обмеження числа сеансів. Після закінчення заданого проміжку часу – автоматичний вихід з системи. Для деяких непередбачених ситуацій передбачити можливість збільшення часу знаходження в системі;

– при установці нових програмних засобів слід отримати право на це, відповідне правилам безпеки.

Правила політики безпеки використання антивірусної системи

Антивіруси – потужна зброя зі шкідливими програмами. Вони завжди мають бути активними, щоб у будь-який момент захистити програму/мережу/дані від атаки. Будь-які порушення ходу роботи антивіруса можуть привести до зараження машини і знищення інформації.

– на всіх призначених для користувача системах ще до того, як вони будуть підключені до мережі, слід встановити програмне забезпечення для захисту від вірусів;

– користувачі повинні сприяти оновленню цього програмного забезпечення, а також не повинні відключати ці засоби;

– користувачі не повинні відключати антивірусне програмне забезпечення при запуску завантаженого з мережі Інтернет в систему користувача програмного забезпечення;

– користувачі, які завантажують будь-які дані або програми із зовнішнього носія, повинні перед завантаженням сканувати цей носій на предмет наявності на ньому вірусів;

– всі системи, підключені до мережі організації, повинні піддаватися періодичній загальній перевірці на шкідливі програми. Перевірки повинні проходити не рідше за один раз в місяць.

Правила політики безпеки зовнішнього доступу

Мережа Інтернет – одна з невід'ємних частин нашого життя. Використання Інтернету надає безліч переваг але є і недоліки. Величезній

загрозі піддається підприємство при використанні Інтернету. Варто захищати ПЗ СЕД додатковими модулями для запобігання вторгненню, атаці, просочуванню інформації.

– проводити регулярне обслуговування для підтримки порядку в загальнодоступних даних;

– системні адміністратори несуть відповідальність за процедури обслуговування серверів, що надають інформацію або послуги користувачам Інтернет;

– користувачі, що мають доступ до Інтернет, повинні заздалегідь пройти програму навчання, де буде роз'яснена політика компанії у сфері безпеки і відповідальність користувачів за представлення компанії в світовій мережі;

– користувачі не повинні пересилати жодної інформації, яка може завдати збитку репутації організації або їх особистої;

– користувачі можуть завантажувати програмне забезпечення Інтернет, яке допоможе їм виконувати свої функції в організації тільки після узгодження з системним адміністратором;

– підприємство повинно зберегти за собою право блокування доступу до всіх сайтів, які вважаються неприйнятними, а також робити реєстраційні записи про відвідані сайтів всіма користувачами, на підставі яких у будь-який час можна провести аудиторську перевірку;

– адміністратор безпеки повинен розробити архітектуру системи електронної пошти так, щоб забезпечити належну доставку повідомлень як усередині організації, так і в Інтернет. Використання посередницьких програм допускається;

– підприємство повинно зберігати і архівувати всі повідомлення електронної пошти, які проходять через її сервер. Архів повинен зберігатися на включеному в мережу пристрої, що запам'ятовує;

– адміністратори повинні переносити повідомлення, що архівуються, на автономний пристрій, що запам'ятовує, кожні шість місяців, видаляючи ці

повідомлення з оперативних пристроїв, що запам’ятовують. Після закінчення терміну придатності даних, інформація повністю стирається з носіїв без можливості відновлення;

– підприємство має право сканувати вміст кожного повідомлення електронної пошти, яке проходить через її сервери, на основі заздалегідь встановлених критеріїв. Якщо повідомлення не відповідає критеріям, то воно не повинне доставлятися користувачеві;

– розмір повідомлень електронної пошти, що відправляються і отримуваних користувачами, в цілому, не повинен перевищувати встановленого ліміту. Всі останні випадки обговорюються з адміністратором;

– правило обміну конфіденційною інформацією включає розпорядження шифрувати повідомлення перед їх пересилкою і "підписувати" їх цифровими підписами;

– користувачі не повинні брати участь в розсилці шкідливих послань, що пересилаються по ланцюжку, містять погрози.

Відповідальність за дотримання положень Політики безпеки

Категорично заборонена будь-яка поведінка, яка несприятливо відбивається на роботі інших осіб в системах і мережах підприємства, або яка може нашкодити іншим особам.

Керівництво залишає за собою право досліджувати дані, що зберігаються на всіх комп’ютерах і в мережевих системах, за допомогою засобів фізичного дослідження і електронного моніторингу. Якщо в зібраній інформації виявлені факти порушення правил інформаційної безпеки або закону, то підприємство може використовувати ці дані для дисциплінарних стягнень або правових санкцій.

Керівництво має право розірвати контракти і договори з підрядчиками і іншими зовнішніми користувачами, якщо вони порушують розпорядження правив або демонструють поведінку, яка заважає нормальній роботі мережі і комп’ютерних систем підприємства.

Контроль за дотриманням положень Політики безпеки

Поточний контроль дотримання Політики здійснює адміністратор безпеки. Контроль здійснюється шляхом проведення моніторингу і менеджменту інцидентів інформаційної безпеки організації, за результатами оцінки інформаційної безпеки, а також в рамках інших контрольних заходів.

Політика оговорює відповідальність за дотримання положень відповідної Політики. Обумовлює контроль за дотримання положень відповідної Політики.

Політика безпеки підприємства розвивається і іншими документами підприємства, та пристосовується до вимог чинного законодавства.

Політику доповнено інструкціями для користувачів інформаційної системи.

До Політики додаються інструкції:

– адміністратора безпеки, що визначає обов'язки, права і відповідальність адміністратора інформаційної безпеки;

– користувача інформаційної системи, що визначає загальні функції, права і обов'язки користувача при обробки даних на ПК, що входять до складу ІТС.

Посадова інструкція адміністратора безпеки

Загальні положення

Інструкція визначає функції, права і обов'язки адміністратора безпеки інформації по питаннях забезпечення інформаційної безпеки при роботі з інформаційною системою та СЕД.

Адміністратор безпеки інформації призначається з числа співробітників і забезпечує правильність використання і нормальне функціонування встановлених систем захисту інформації від НСД, резервне копіювання інформації, оновлення антивірусних баз, робить періодичний аналіз захищеності.

Інструкція є доповненням до нормативних документів, що діють, з питань забезпечення безпеки інформації з обмеженим доступом, і не виключає обов'язкового виконання їх вимог.

Основні функції адміністратора безпеки інформації:

– Контроль за виконанням вимог нормативних документів, що діють, в питаннях забезпечення захисту інформації з обмеженим доступом, що оброблюється в інформаційній системі;

– Ведення журналу реєстрації користувачів;

– Складання списку персоналу організації, що має право доступу до сервера із зазначенням характеру виконуваних робіт.

– Для аутентифікації в СЕД, користувачам, створення унікальних ідентифікаційних файлів (ID-файли)

– Своєчасне оновлення копій ID-файлів

– Створення і тестування резервних копій даних і ПЗ

– налаштування і супровід в процесі експлуатації системи управління доступом в інформацій системи обробки інформації з обмеженим доступом;

– контроль доступу осіб в приміщення, де встановлені АС відповідно до списку співробітників, допущених до роботи на АС;

– контроль за своєчасним проведенням зміни паролів для доступу до АС користувачами відповідних АС;

– Технічне обслуговування та супровід програмно-технічних засобів і комплексів засобів автоматизації СЕД

– Щомісячне опублікування нововведень в області захисту, нових стандартів, а також контроль над виконанням планів безперервної роботи і відновлення (при необхідності) і за зберіганням резервних копій.

– Реалізація і зміна засобів захисту даних, контроль над станом захисту, набір даних, посилення захисту в разі потреби

Адміністратор безпеки інформації має право:

– брати участь в аналізі ситуацій, що стосуються функціонування засобів захисту інформації і розслідування фактів несанкціонованого доступу;

– Реєструвати користувача в ІС з наданням йому доступу до інформаційних ресурсів;

– Одноосібного доступу без супроводу;

– вимагати припинення обробки інформації з обмеженим доступом в разі порушення встановленого порядку робіт або порушення функціонування засобів і систем захисту інформації.

Посадова інструкція користувача ІТС

Загальні положення:

– користувач ІТС здійснює обробку даних;

– для аутентифікації в СЕД користувачам Адміністратором створюються унікальні ідентифікаційні файли (ID-файли);

– користувач в обов'язковому порядку повинен бути ознайомлений з призначенням і властивостями ID-файлів;

– користувач несе персональну відповідальність за збереження і конфіденційність наданої йому ID-файлу;

– користувачем є кожен співробітник, що бере участь в рамках своїх функціональних обов’язків в процесах обробки даних.

– користувач несе персональну відповідальність за свої дії;

– користувач в своїй роботі керується інструкцією користувача, політикою інформаційної безпеки;

– методичне керівництво роботою користувача здійснюється адміністратором безпеки;

– користувач при виконанні своїх обов'язків має право використовувати ресурси ІС в повному обсязі у відповідність до встановлених рівнем доступу і правами;

– користувач має право перевіряти вміст свого облікового запису.

Посадові обов’язки:

– виконувати вимоги та інструкції пов’язані з забезпеченням інформаційної безпеки;

– виконувати вимоги парольної політики;

– виконувати вимоги політики безпеки зовнішнього доступу;

– звертатися з питань безпеки інформації до адміністратора безпеки, повідомляти про випадки, що можуть порушувати інформаційну безпеку.

– користувач зобов'язаний забезпечити конфіденційність і збереження логіна і пароля. При компрометації своїх реєстраційних даних користувач повинен негайно сповістити про це безпосереднього керівника (співробітника ІБ, адміністратора ІС);

– користувач зобов'язаний повідомляти про всі стали йому відомі факти компрометації паролів інших співробітників в службу ІБ;

– при звільненні з організації, перехід в інший підрозділ або будь-якому іншому подію, при якому змінилася вищевказана інформація, користувач (керівник користувача) зобов'язаний повідомити про це адміністратора ІС.

– для видалення / зміни свого облікового запису користувач зобов'язаний подати Заявку адміністратор на підставі цієї заявки ІС зобов'язаний знищити / змінити обліковий запис користувача в системі, внести відповідний запис до журналу реєстрації користувачів і повідомити про це підрозділу, відповідального за інформаційну безпеку

Користувачам забороняється:

– розголошувати інформацію, що захищається, третім особам;

– копіювати інформацію, що захищається, зовнішні носії без дозволу свого керівника або адміністратора безпеки;

– самостійно встановлювати, тиражувати, або модифікувати програмне забезпечення і апаратне забезпечення, змінювати встановлений алгоритм функціонування технічних і програмних засобів;

– заборонено підключати до робочої станції інформаційної мережі особисті зовнішні носії і мобільні пристрої;

– відключати засоби захисту інформації;

– користувач не має права працювати під чужими логіном і / або паролем. У разі, якщо керівництво пропонує користувачеві працювати в таких умовах, користувач має право вимагати письмового вказівки (наказу) керівництва, узгодженого зі службою ІБ, і не приступати до роботи до отримання такого вказівки (наказу);

– виконувати процедури не пов’язані зі службовими обов’язками.

2.16 Висновок

В спеціальній частині магістерської дипломної роботи була проведена класифікація інформації, що циркулює на підприємстві, виконаний аналіз інформаційних потоків, наданий перелік найбільш суттєвих загроз інформаційній безпеці підприємства. Були розглянуті особливості та основні принципи побудови узагальненої моделі захисту інформації.

Досліджені наявні системи електронного документообігу за розробленими критеріями. За результатами досліджень обрана СЕД "Босс-Референт".

Для забезпечення захисту СЕД від НСД прийняте рішення реалізувати для СЕД підприємства стандартний функціональний профіль захищеності 3.КЦД.1. Аналіз реалізації послуг безпеки, що входять до профілю, показав, що за наявності клієнтської та серверної операційних систем Windows, на яких працює СЕД "Босс-Референт", маємо лише дві частково нереалізовані послуги – КО-2 та НТ-2. Наведені методи та способи їх реалізації.

Для регулювання управління, захисту і розподілу комерційної інформації на підприємстві на якому використовується СЕД, була розроблена політика безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

На комерційному підприємстві при забезпеченні захисту інформації в СЕД необхідно враховувати час який треба витрати на проектування, розробку, впровадження та підтримку розроблюваної підсистеми. Якщо під час виконання одного з етапів проекту будуть допущені помилки, це призведе до виникнення додаткового часу який знадобиться для виявлення помилок та подальшого їх усування. Відповідно до цього необхідно додатково витратити кошти на оплату праці працівників, штрафів, які виникають при зміні термінів виконання роботи, що зазначені в договорах і т. ін.

Економічно доцільним буде вважатися, якщо витрати на забезпечення підтримки працездатності комплексної системи проектування, розробку, впровадження та підтримку розроблюваної системи не будуть перевищувати збиток при реалізації можливої загрози при поломках обладнання. Тому для обґрунтування економічної доцільності розробки та впровадження комплексної системи необхідно розрахувати збитки від реалізації можливих загроз і порівняти їх з витратами на забезпечення підтримки працездатності системи.

3.1 Розрахунок витрат на закупівлю системи

Таблиця 3.1 – Розрахунок витрат на програмне забезпечення

Компонент	Вартість компоненту, грн.	Необхідна кількість компонентів, шт.	Загальна вартість, грн.
1	2	3	4
Система електронного документообігу «БОСС-референт»	81 400,00	1	81 400,00

Продовження таблиці 3.1

1	2	3	4
ОС Microsoft Windows 10	2300,00	15	34 500,00
Серверна Windows Server Standard 2016	13 300,00	1	13 300,00
Антивірусне ПО avast! Pro Antivirus	360,00	16	5760,00

Витрати на придбання необхідних програмних компонентів складають:

$$Кпр = 81\ 400 + 34\ 500 + 13\ 300 + 5\ 760 = 134\ 960\ грн.$$

Таблиця 3.2 – Розрахунок витрат на апаратне забезпечення

Компонент	Вартість компоненту, грн.	Необхідна кількість компонентів, шт.	Загальна вартість, грн.
Маршрутизатор «Cisco 861 Ethernet Router CISCO861-K9»	5 740,00	1	5 740,00

Таким чином, капітальні витрати на організацію комплексної системи, складатимуться із витрат на закупівлю програмних та апаратних засобів:

$$К = 134\ 960 + 5\ 740 = 140\ 700\ грн.$$

3.2 Розрахунок експлуатаційних витрат

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

Отже, річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$C = C_в + C_к , \quad тис. грн. \tag{3.1}$$

Витрати на відновлення й модернізацію системи інформаційної безпеки (визначено за даними організації) $С_в$ = 1000 грн.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$C_к = С_н + C_а + C_з + C_{єв} + C_е + C_{ел} + C_о + C_{тос}, грн.$$

Річний фонд амортизаційних відрахувань складається з амортизації основних фондів та амортизації нематеріальних активів.

Амортизація основних фондів (апаратних засобів) :

$$Са_{оф} = (Ф_п – Л)/100 * Н_а, \tag{3.2}$$

де $Ф_п$ – вартість апаратних засобів;

$Н_а$ – норма амортизації, $Н_а$=1/Т;

Л – ліквідаційна вартість;

Для апаратних засобів Т=5р, отже $Н_а$=1/5 * 100 = 20,

$$Са_{оф} = (5\ 740\text{-}0)/100 * 20 = 1\ 148 грн.$$

Амортизація нематеріальних активів (програмних засобів):

Для програмних засобів Т=6р, отже $Н_а$=1/6 * 100 = 16,7

$$Са_{на} = (134\ 960\text{-}0)/100 * 16,7 = 22\ 538 грн.$$

$$С_а = Са_{оф} + Са_{на} = 1\ 148 + 22\ 538 = 23\ 686 грн.$$

Річний фонд заробітної плати з податком на ЄСВ інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки:

ЄСВ=22%

$$С_з = 5500*12+14520=80\ 520 грн.$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е , \ грн, \quad (3.3)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

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

$$Р= 16*350 \ Вт/год. = 5\ 600 \ Вт/год. = 5,6 \ кВт/год$$

$$С_{ел} = 5,6*2\ 080*1=11\ 648 \ грн.$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування (визначено за даними організації) $С_о = 0$ *грн.*

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо (визначено за даними організації) $С_н$=*0 грн*

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%). $С_{тос} = 1407$ *грн.*

Отже, $С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_о + С_{тос}$, *грн.*

$$С_к = 23\ 686+80\ 520+1000+11\ 648+1407=118\ 261$$

$$С = С_в + С_к = 1000 + 103\ 741= 119\ 261 грн.$$

3.3 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично не можливо. Природно, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

– Час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 2 год;

– Час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 1 год;

– Час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 1 год;

– Заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць),Z_0 = 5500 грн.;

– Заробітна плата співробітників, Z_c (грн. в місяць), Z_c = 6000 грн.;

– Кількість обслуговуючого персоналу, N_0, $N_0 = 2$;

– Число співробітників, N_c, $N_c = 20$;

– Дохід , O (грн. на рік), $O = 40\ 800\ 000$ грн.;

– Число зламаного обладнання, I, $I = 1$;

– Число поломок на рік, n, $n = 4$.

Вартість втрат від зниження продуктивності співробітників несправного обладнання:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.} \qquad (3.4)$$

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (20 * 6\ 000 / 160) * 2 = 1500{,}00\ грн.$$

Вартість відновлення зламаного обладнання:

$$П_в = П_{ви} + П_{пв}\ ,\ грн. \qquad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації,

$П_{пв}$ – вартість відновлення обладнання.

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

*$П_{ви}$ = (20 * 6 000 / 160) * 1 = 750,00 грн.*

*$П_{пв}$ = (2 * 5 500 / 160) * 1 = 68,75 грн.*

Підставивши отримані результати в загальну формулу отримаємо:

$П_в$ = 750,00 + 68,75 = 818,75 грн.

Втрачена вигода від простою зламаного обладнання становить:

$$U = П_п + П_в + V, \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \quad (3.9)$$

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

*V = (40 800 000 / 2 080) * (2 + 1 + 1) = 78 461,55 грн.*

U = 1500,00 + 818,75 + 78 461,55 = 80 780,30 грн.

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе:

$$B = \sum_i \sum_n U \quad (3.10)$$

*B = 4 * 1 * 34 810,10 = 323 121,20 грн.*

3.4 Загальний ефект від впровадження системи

Загальний ефект від впровадження системи захисту інформації в СЄД визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \quad (3.11)$$

де B– загальний збиток від поломки обладнання на вузлі або сегменті корпоративної мережі, тис. грн;

R – очікувана імовірність поломки на вузлі або сегменті корпоративної мережі, частки одиниці;

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

Таким чином, загальний ефект від впровадження становить:

$$E = 323\ 121{,}20 * 0{,}6 - 119\ 261 = 74\ 611 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності системи

Оцінка економічної ефективності системи, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) та терміну окупності капітальних інвестицій T_o

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.12)$$

де E – загальний ефект від впровадження системи захисту, грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Підставивши відповідні значення, маємо:

$$ROSI = 74\ 611 / 140\ 700 = 0.53$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (N_{деп} - N_{інф}) / 100, \quad (3.13)$$

де $N_{деп}$ – річна депозитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Підставивши відповідні значення, маємо:

$$ROSI > (18 - 13.7) / 100,$$

$$0,53 > 0,043.$$

Отже, проект є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 140\ 700 / 89\ 121 = 1 / 0,53 = 2 \text{ роки.}$$

3.6 Висновок

Розрахувавши збитки від реалізації несправностей які можуть виникнути на комерційному підприємстві, які склали *323 121,20* грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи *С = 119 261 грн* грн., *К = 140 700* грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом (*ROSI = 0,53*), термін окупності

системи безпеки становить *2* роки. Та для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

В першому розділі магістерської дипломної роботи були розкриті основні поняття електронного документообігу, визначені переваги, що отримає організація від застосування СЕД та особливості впровадження такої системи. Також були визначені основні складові частини СЕД, їх особливості та вимоги до СЕД в залежності від специфіки діяльності організації.

Окремо були розглянуті суб’єкти системи електронного документообігу, а саме підписувач, центр сертифікації ключів, акредитований центр сертифікації ключів, засвідчувальний центр, центральний засвідчувальний орган, контролюючий орган та визначені їх функції в рамках СЕД.

На основі проведених досліджень було прийняте рішення, що використання системи електронного документообігу на підприємстві є необхідним та доцільним.

В спеціальній частині дипломної роботи була проведена класифікація інформації, що циркулює на підприємстві, виконаний аналіз інформаційних потоків, наданий перелік найбільш суттєвих загроз інформаційній безпеці підприємства, проаналізовані методи та моделі безпеки інформації.

Досліджені наявні системи електронного документообігу за розробленими критеріями. За результатами досліджень обрана СЕД "Босс-Референт".

Для забезпечення захисту СЕД від НСД прийняте рішення реалізувати для СЕД підприємства стандартний функціональний профіль захищеності 3.КЦД.1. Аналіз реалізації послуг безпеки, що входять до профілю, показав, що за наявності клієнтської та серверної операційних систем Windows, на яких працює СЕД "Босс-Референт", маємо лише дві частково нереалізовані послуги. Наведені методи та способи їх реалізації.

Для регулювання управління, захисту і розподілу комерційної інформації на підприємстві на якому використовується СЕД, була розроблена політика безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1 Глинський А. Мировой рынок систем электронного документооборота [Электронный ресурс]. – Режим доступу: http://citforum.ru/consulting/ docflow/market/article1.8.200222.html.

2 Електронний документообіг [Електронний ресурс]. – Режим доступу: http://www.viaduk.com/viaduk/web5ua.nsf/0/ACC6E5C6C0A30BD9C225726F0051E265

3 Саттон Д.Д. Корпоративный документооборот. Принципы, технологии, методология внедрения [Текст]: Азбук, 2002. – 446 с.

4 Послуги. державним службовцям. Інструкціїї з діловодства. Електронний документообіг [Електронний ресурс]. – Режим доступу: http://www.carpathia.gov.ua/ua/publication/content/1615.htm

5 Асеев Г. Г. Электронный документооборот [Текст]: Учебник для вузов. – К.: Кондор, 2007. – 500 с.

6 Соболь С. Ю. Понятие и сущность информационной безопасности и ее место в системе обеспечения информационной безопасности // Научно-техническая информация. Сер.1. – 2003. – № 11. – С.10–15

7 Сапков В. В. Информационные технологии и компьютеризация делопроизводства [Текст]: Учебное пособие, 2008. – 288 с.

8 Жеребенкова А. В. Документооборот на предприятиях [Текст]: Вершина, 2005. – 384 с. 9.

9 Клименко С. В. Электронные документы в корпоративных сетях / С.В. Клименко, И.В. Крохин, В.М. Кущ и др. // Инженер. энцикл.: Технологии электрон. коммуникаций. – М.: Эко-Трендз, 1999. – 270 с.

10 Асєєв Г. Методологія корпоративного документообігу: схеми і вимоги до них // Вісник Книжкової палати, № 3, Березень, 2006, Київ.

11 Пахчанян А. Рынок ПО: Обзор систем электронного документооборота / А. Пахчанян, Д. Романов [Электронный ресурс]. – Режим доступу: http://www.cnews.ru/reviews/index.shtml?2002/05/17/140012

12 Задорожна Н. Т. Кероване проектування документообігу в управлінських інформаційних системах: дис. канд. фіз.-мат. наук: 01.05.03 / НАН України; Інститут кібернетики ім. В.М. Глушкова. – К., 2004.

13 Круковский М.Ю. Критерии эффективности систем электронного доку-ментооборота// Системи підтримки прийняття рішень. Теорія і практика – 2005. – С. 107с – 111с.

14 Электронные офисные системы [Электронный ресурс].-Спосіб доступу: URL: http://eos.ru

15 Aladdin – защита информации, информационная безопасность, аутентификация [Електронний ресурс] http:// URL http://www.aladdin.ru/

16 Бобылева М. П. Эффективный документооборот: от традиционного к электронному. – М.: изд-во МЭИ, 2004. — 172 с.

17 Пікульський В., Дубова С. Автоматизація документообігу в органах державного управління: етапи впровадження// Вісник Книжкової палати. - 2006. - № 2. - С. 33 - 35.

18 Видання. Основні види. Терміни та визначення: ДСТУ 3017-97.- К.: Держстандарт України, 1995. - 345 с.

19 Примірна інструкція з діловодства в місцевих органах виконавчої влади. – К.: Знання, 2000. – 94с.

20 Про електронний цифровий підпис: Закон України// Вісник Держ. комітету архівів України. - 2003. - Вип. 2 (14). - С. 23-32.

21 Про електронні документи та електронний документообіг: Закон України// Вісник Держ. комітету архівів України. - 2003. - Вип. 2 (14). - С. 15-22.

22 Про інформацію: Закон України// Відомості Верховної Ради України. - 2001.- № 11.- С. 25-27.

23 Про підприємництво: Закон України від 07.02.91// Відомості Верховної Ради України. - 1999.- № 8.- С. 43.

24 Про підприємства в Україні: Закон України// Відомості Верховної Ради України. - 1999.- №16.

25 Акопянц А. ЕЦП - год в законе/ А. Акопянц// Компьютер. - 2003. - № 7. - С. 57-61.

26 Андреев В. Этот многообразный мир документооборота/ В. Андреев. – М., 2003. – С. 24-26.

27 Андреев В. Человек и документ в информационную епоху/ В. Андреев. – М., 2003. – С. 14-17.

28 Афанасьев А. Частные реализации систем документооборота/ А.Афанасьев// Открытые системы. - 1997. - № 1. - С. 32-36.

29 Баласанян В. Автоматизация делопроизводства и документооборота: введение в проблему/ В. Баласанян// Рынок ценных бумаг. - 1998. - № 16. - С. 25-27.

30 Бибик С.П. та ін. Універсальний довідник-практикум з ділових паперів. - К.: Довіра. - 1997.

31 Вендров А.М. Case-технологии. Современние методи и средства проектирования информационних систем. - М.: «Argus-soft Co», 1999.

32 Вендров А.М. Один из подходов к выбору средств проектирования баз данных и приложений // «СУБД». - 1995. № 3.

33 Гавердовский А. Концепция построения систем автоматизации документооборота. - М.: «Открытие системи», 1997, № 01.

34 Глущик С.В., Дияк О.В., Шевчук С.В. Сучасні ділові папери. -К., 2001.

35 Давидова З.Н., Рыбаков А.Е. Делопроизводство. - Минск,1999. - 288с.

36 Делопроизводство. Инструкции. Типовіе положення. - Сборник нормативніх документов. - Харьков: Конус, 2003. - 160 с.

37 Діденко А.Н. Сучасне діловодство. - К.: Либідь, 1998.

38 Золотих И. Обзор компьютерных систем автоматизации делопроизводства и документооборота // Информационные технологи. - 1997. - № 2.

39 Іванова Т.В., Піддубна Л.П. Муніципальне діловодство. -К.: Либідь, 2003.

40 Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. - М: Госс-тандарт СССР, 1991, 143 с.

41 Кирсанова М.В., Аксенов Ю.М. Курс делопроизводства: Документационное обеспечение управления. - М.: Инфра-М, Новосибирск, - 1997.

42 Корж А.В. Юридичне документування. - К.: Ін-т держави і права, 2001.

43 Колесников С. Управленческий консалтинг. Современные технологии для работи со структурами организации // http//www.geocities.com/WallStreet/2907/text_ec/Idef.htm.

44 Кудрявцев В.А. и др. Организация работы с документами:(Учебник). М.: Инфра-М, 1999.

45 Кузнецов С.Л. Компьютеризация делопроизводства без проблем. - К.: А.Л.Д., 1997.

46 Кушнаренко Н.Н. Документоведение. - К.: Знання , КОО,2001. - 400 с.

47 Лисенко Н.А., Сербиновский Б.Ю., Цветкова С.Н. Документирование управленческой деятельности на предприятии: делопроизводство и корреспонденция. - Ростов на Дону: Изд. Центр«МарТ», 2002. - 272 с.

48 Новоженов Ю.В. Обьектно-ориентированние технологи разработки сложних программных систем. - М.: Аргуссофт компа-ни, 1996.

49 Организация роботы с документами. - М.: Инфра-М, 1998.

50 Павлов В. Інтегровані рішення для керування паперовим та електронним документообігом підприємства // Інформаційні системи - стратегічний фактор розвитку підприємства: матеріали конференції Київ, 21-24 березня 2000 р. - К., 2000.

51 Павлюк Л.В. Справочник по деловодству, архивному делу и основам работы на компьютере. - М.: ИТД, 1999.

52 Паламар Л.М., Кацавець Г.М. Українське ділове мовлення:Навч. посіб. - К.: Либідь, 1997. - 297 с.

53 Палеха Ю.І. Управлінське документування: Навч. посіб: У2-х частинах. Ч. 1. Організація загального діловодства. - К.: Вид-воЄвроп. ун-ту, 2003. - 383 с.

54 Палеха Ю.І. Управлінське документування: Навч. посіб: У2-х частинах. Організація кадрового діловодства. - К.: 2002. - 230 с.

55 Печинков Т.В., Печинкова А.В. Документационное обеспечение деятельности организации: Новий стандарт. ГОСТ р.30-97. -М.: Тандем, 1999.

56 Пашутинський Є.К. Діловодство кадрової служби: Кадрипідприємства. К.: КНТ, 2006. - 272 с.

57 Погиба Л.Г., Грибінченко Т.О., Баган М.П. Складення ділових паперів. - Практикум. - К.: Либідь, 2002. - 240 с.

58 Сапун А. Краткий путеводитель по системам электронного документооборота // Компьютерное обозрение. - 2000. - № 18-19,17-23 мая.

59 Составление и оформление служебных документов. - М.:ЗАО Интел.Сигма, - 1999.

60 Стенюков М.В. и др. Делопроизводство на малом предприятии. Документи по личному составу. - М.: Приор, 1999.

61 Старцев О. Трудовий контракт: особливості застосування //Консультант. - 1999. - № 29 (192).

62 Шевчук С.В. Українське ділове мовлення. - К., 1998.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	4	
4	А4	Вступ	2	
5	А4	1 Розділ	37	
6	А4	2 Розділ	72	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:

Методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства

студента групи 125м-17-1

Остривного Данііла Андрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 143 сторінках та містить 4 рисунків, 15 таблиць, 62 джерела та 4 додатка.

Актуальність теми полягає у необхідності розробки рекомендацій щодо забезпечення безпеки інформації в системі електронного документообігу комерційного підприємства.

Зміст та структура дипломного проекту дозволяють розкрити поставлену тему повністю.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі розкриті основні поняття електронного документообігу, визначені переваги, що отримає організація від застосування СЕД та особливості впровадження такої системи. Також були визначені основні складові частини СЕД, їх особливості. Окремо були розглянуті суб’єкти системи електронного документообігу. У спеціальній частині дипломної роботи була проведена класифікація інформації, що циркулює на підприємстві, виконаний аналіз інформаційних потоків, наданий перелік найбільш суттєвих загроз інформаційній безпеці підприємства. Досліджені наявні СЕД за розробленими критеріями, а також методи та моделі безпеки інформації в системах електронного документообігу. Розроблена політики безпеки для використання на комерційному підприємстві на якому застосовується СЕД.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Острівний Данііл Андрійович заслуговує на оцінку «_____».

Керівник дипломної роботи,
д.т.н., проф. кафедри БІТ В.І. Корнієнко

Керівник спеціальної частини
ст. викл. кафедри БІТ В.І. Мєшков