**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
“14” червня 2022 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

**дипломної роботи**
***бакалавра***
(назва освітнього ступеня)

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)

**спеціальність** 125 Кібербезпека
(код і назва спеціальності)

**освітня програма** Кібербезпека
(назва освітньої програми)

**на тему:** «Інформаійні технології управління безпекою електронного документообігу на підприємстві»

**Виконавець:** студент IV курсу, групи КБ-42

_____ **Денис ЗИМБИЦЬКИЙ**
(підпис) (прізвище ім’я)

| | **Прізвище, ініціали** | **Підпис** |
|---|---|---|
| **Керівник** | Юрій ЩЕБЛАНІН | |

| | | |
|---|---|---|
| **Нормоконтроль** | Сергій ДАКОВ | |

**Київ 2022**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

# ЗАВДАННЯ
## на виконання дипломної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньої програми)

**Студента** **КБ-42** **Зимбицькому Денису В'ячеславовичу**
(група) (прізвище ім'я по-батькові)

**Тема дипломної роботи** Інформаійні технології управління безпекою електронного документообігу на підприємстві

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол № 5 від 29.10.2021 р.

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Інформаційні технології електронного документообігу, структура підприємства, бізнес-процеси підприємства, технології забезпечення інформаційної безпеки

### 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері впровадження електронного документообігу, сучасні системи електронного документообігу, технології контролю цілісності електронного документу, програмні та програмно-апаратні засоби захисту системи електронного документообігу

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** Розроблена система захисту електронного документобігу

## 5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року.

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Денис ЗИМБИЦЬКИЙ
(підпис) (ініціали, прізвище)

## КАЛЕНДАРНИЙ ПЛАН

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.10.2021 – 30.11.2021 | *виконано* |
| 2 | Аналіз літератури | 01.12.2021 – 31.01.2022 | *виконано* |
| 3 | Електронний документообіг. Загальні відомості | 01.02.2022 – 24.02.2022 | *виконано* |
| 4 | Технології забезпечення інформаційної безпеки в системах електронного документообігу. | 25.02.2022 – 01.03.2022 | *виконано* |
| 5 | Аналіз документообігу підприємства | 02.05.2022 – 08.05.2022 | *виконано* |
| 6 | Розробка рекомендацій щодо підвищення захисту системи електронного документообігу | 09.05.2022 – 29.05.2022 | *виконано* |
| 7 | Оформлення пояснювальної записки | 30.05.2022 – 04.06.2022 | *виконано* |
| 8 | Підготовка до захисту дипломної роботи | 05.06.2022 – 13.06.2022 | *виконано* |

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Денис ЗИМБИЦЬКИЙ
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

# РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Інформаійні технології управління безпекою електронного документообігу на підприємстві» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 63 сторінки. Робота містить 4 рисунки, 3 таблиці. Список використаних джерел включає 39 джерел.

**Об'єкт дослідження** – система управління безпекою електронного документообігу на підприємстві.

**Мета роботи** – розробити системи захисту електронного документообігу на підприємстві.

**Предмет дослідження** – інформаійні технології забезпечення безпеки електронного документообігу.

Перший розділ розкриває сутність і принципи електронного документообігу, для чого необхідно впроваджувати систему електронного документообігу і з якими проблемами можна зіткнутися при його впровадженні.

У другому розділі проводиться класифікація загроз і методів захисту електронного документообігу.

У третьому розділі розглянуто варіанти удосконалення захисту електронного документообігу на підприємстві.

Результатом роботи є розроблені рекомендації щодо вдосконалення системи документообігу для Державного підприємства «Медичні закупівлі України».

**Ключові слова:** електронний документообіг, система електронного документообігу, захищений електронний документообіг, електронний підпис

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

НСД – Несанкціонований доступ
ІС – Інформаційні технології
АС – Автоматизована система
СЕД – Система електронного документообігу
ЕД – Електронний документ
ECM – Enterprise content management
ISO – International Organization for Standardization
МНІ – Машинні носії інформації
ІАЗУ – Інформаційно-аналітичне забезпечення управління
EDM – Enterprise Data Management
ОРД – Організаційно-розпорядчих документи
ІВК – Інфраструктура відкритих ключів
КЕП – Кваліфікований електронний підпис
КНЕДП – Кваліфікований надавач електронних довірчих послуг
СУБД – Система управління базами даних
ПЗ – Програмне забезпечення

# ЗМІСТ

# ВСТУП

У зв'язку зі стрімким розвитком технологій і їх повсюдним впровадженням, електронний документообіг все більше освоюється і займає найбільш високу позицію в порівнянні зі своїм паперовим аналогом. Це пов'язано з тим, що система електронного документообігу багато в чому полегшує і підвищує продуктивність підприємства, дозволяє моментально знайти необхідну вам інформацію, не вимагає багато місця в офісі на відміну від паперового архіву.

Хоча на жаль організації автоматизованого захищеного документообігу в системі інформаційної безпеки підприємства приділяється, як правило, найменша увага, хоча отримання конфіденційної інформації через прогалини в діловодстві є найбільш простим і мало витратним способом отримання інформації [1]. У зв'язку з вищесказаним актуальною на сьогоднішній день є завдання створення системи конфіденційного документообігу на підприємстві складовими частинами якої є: паперовий документообіг, електронний документообіг, системи взаємодії і сполучення паперового та електронного документообігу.

Враховуючи, що метою роботи було розробити систему захисту електронного документообігу, для її досягнення було визначено такі завдання:

- Провести аналіз документообігу підприємства
- Аналіз функціонування систем електронного документообігу
- Дослідити можливості сучасних систем електронного документообігу підприємства та їх порівняння
- Проаналізувати технології захисту систем електронного документообігу підприємства
- Розробити заходи, пов’язані із впровадженням інформаційної системи електронного документообігу
- Сформулювати цілі впровадження систем електронного документообігу
- Визначити можливі загрози та вразливості системи електронного документообігу на підприємстві

- Систематизувати і розкрити зміст засобів забезпечення інформаційної безпеки електронного документообігу
- Розробити архітектуру системи захисту електронного документообігу підприємства;
- Розробити практичні рекомендації щодо створення та управління системою захисту електронного документообігу.

# РОЗДІЛ 1
# АНАЛІЗ ВИКОРИСТАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ПІДПРИЄМСТВІ

## 1.1 Основні поняття та сутність інформаційних систем управління діяльністю

Ефективна діяльність будь-якої організації, перш за все, залежить від інформаційної забезпеченості та використання отриманої інформації в діяльності. Робота з отримання інформації про діяльність підприємства займає велику кількість часу і є, як правило, трудомісткою. Ця проблема полягає в тому, що при отриманні найбільш точної і повної інформації про діяльність компанії, керівництво при розробці і впровадженні управлінських рішень може більш ефективно використовувати отриману інформацію.

Відповідно, вирішуючи дану проблему, необхідно використовувати різні автоматизовані методи для обробки наявної інформації. При використанні автоматизованих систем і їх впровадження керівництво будь-якого підприємства отримує можливість швидкого отримання необхідної інформації про діяльність підприємства, яка забезпечить подальшу ефективність поточної діяльності і має можливість оптимізації даної діяльності [2].

Усі підприємства, як великі, і малі впроваджують інформаційні системи для отримання доступу до бізнес-знань у масштабах усієї компанії, підвищення продуктивності праці співробітників та зведення до мінімуму дублювання бізнес-процесів. Інформаційні системи можуть також дозволити бізнесу знизити вартість інформаційних технологій та звести до мінімуму ручне введення даних. Ці якості системи підприємства пропонують певні переваги, як покращена реакція до змін у навколишньому середовищі підприємства, повішена якість роботи, розширити можливості співпраці з партнерами та підвищена ефективність роботи працівників.

Роль інформаційно-комунікаційних технологій для діяльності підприємств та економік країн підкреслюється у всьому світу великою кількістю як досліджень [3].

Під інформаційною системою управління розуміють систему обробки інформації в сукупності з ресурсами організації: технічні та фінансові ресурси. Такі системи призначені для забезпечення ефективного функціонування об'єкта управління шляхом автоматизованого виконання функцій управління

Оскільки сучасні технології розвиваються незрівнянними за часу темпами, IT-фахівці та менеджери повинні працювати над тим, щоб органічно інтегрувати різні технології. Ця задача полягає не тільки в тому, щоб забезпечити передачу даних по всій системі, але і в тому, щоб результати передачі даних мали певну мета в рамках бізнесу.

Ці системи прискорюють темп повсякденної діяльності, дають можливість людям розвивати та підтримувати нові й часто корисніші стосунки, впливають на соціальні та організаційні структури, змінюють види придбаної продукції та впливають на характер роботи. Інформація та знання стали важливими економічними ресурсами. Однак з новими можливостями з’являється залежність від інформаційних систем з новими загрозами. Інтенсивні інновації в промисловості та наукові дослідження постійно розвивають нові можливості, прагнучи стримувати загрози [4].

Різні інформаційні системи, як правило, можна характеризувати за такими характеристиками: багатогранні та багатофункціональні інформаційні системи також мають вказівки на застосування – управління, автоматизація діловодства, рівень державного управління, сфера діяльності, тип процесу управління.

Функціональні інформаційні системи, які підтримують певну організаційну функцію, таку як маркетинг або виробництво, у багатьох випадках витісняються крос-функціональними системами, створеними для підтримки загальних бізнес-процесів, таких як обробка замовлень або управління персоналом. Такі системи можуть бути більш ефективними в розробці та постачанні продуктів фірми і можуть бути більш ефективні щодо результатів бізнесу.

До основних інформаційних процесів в даних системах відносяться [5-7]:

1. Рівень в інформаційній системі державного управління, до якого належить об'єкт дослідження.

2. Область або сфера в якій діє об'єкт дослідження.

3. Основні види управління та їх процеси.

4. Автоматизація та її ступінь у використанні інформаційних процес.

Розглянемо деякі якості в інформаційних системах, які враховуються при їх впровадженні та формуванні систем обробки інформації. Як правило, до них можна віднести: ефективність, надійність, стійкість. Для ефективності та правильного використання функціонування інформаційної системи є одна важлива особливість - визначення точних і чітких завдань. При розробці інформаційної системи кожен користувач висуває свої вимоги до форм і переліку звітів, аналізу потоків інформації та угруповання різних номенклатур [8].

Таким чином, вивчивши теоретичну основу інформаційних систем на підприємстві, можна зробити наступні висновки:

- інформаційна система - незамінний інструмент в сучасному бізнесі;
- все більше підприємств впроваджують інформаційні системи в свою діяльність;
- інформаційні системи управління підприємством розвиваються швидко, як і будь-які інші інформаційні технології, тому при їх впровадженні на підприємстві керівництву необхідно враховувати всі сучасні тенденції.

З одного боку, спостерігається наступна картина-інформаційні системи призводять до додаткових витрат підприємства на їх впровадження і супровід, а з іншого боку ми можемо відзначити, що значно скорочують трудові та фінансові витрати, зменшують дублювання бізнес-процесів.

## 1.2 Інформаційна система електронного документообігу та її захищеність

Інформаційна система (ІС) - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [9]. ІС надає нові вимоги до служб, які відповідальні за роботу з

документами, тобто створення, звернення, а також зберігання документів. Сучасні інформаційні технології дозволяють правильно оформити документ і дають можливості з обліку, контролю за виконанням, передачі документів по каналах зв'язку, ефективного збереження і пошуку інформації. Функції, які раніше виконувалися секретарем-діловодом тепер автоматизовані за допомогою системи електронного документообігу, що підвищує швидкість оперативного управління і прийняття рішень. Найважливішу роль для поліпшення роботи компанії складають системи електронного документообігу (СЕД) [10].

Ефективність управління компанією безпосередньо залежить від правильності організованого в ньому управління документообігом. В будь-якій компанії, в якій проводиться безперервна робота з документами, істотне місце займає питання систематизації, обробки та безпечного збереження великої кількості даних. Пересування документів являє собою не їх фізичне переміщення, а передачу прав для їх користування з інформуванням певних користувачів і контролем за їх виконання.

СЕД на підприємстві - це набагато більше, ніж проста база даних в хмарі, вона є цілим функціональним набором програмного забезпечення, яке дозволяє створювати, зберігати, індексувати, захищати, витягувати і відстежувати документацію, дані, форми та іншу інформацію. Система діє для побудови успішного бізнесу. У СЕД кожен документ (на паперовому або електронному носії) розглядається як об'єкт інформації.

Таким чином, ми можемо сказати, що система електронного документообігу - це система управління різними видами документів на підприємстві з використанням комп'ютерних програм та електронних систем зберігання даних. Вона включає в себе комплекс документів, робочий процес, сховища документів, інформаційно-пошукові системи та процеси, що використовуються для відстеження, зберігання та контролю документ.

Правовою основою електронного документообігу є закони України «Про електронні документи та електронний документообіг» та «Про електронні довірчі послуги», які встановлюють загальні вимоги до електронного документообігу в

Україні [11, 12]. Ці нормативні акти регулюють відносини, що виникають у процесі створення, відправлення, передачі, отримання, зберігання, обробки, використання та знищення електронних документів. Водночас існує низька підзаконних актів, які деталізують, зокрема, питання електронного документообігу в органах державної влади, органах місцевого самоврядування та компаніях.

Згідно з Наказом Міністерства юстиції України «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» організацієй електронного документообігу на підприємстві займаються згідно інструкцією установи, яку розробляють згідно вимог роботи з електронними документами, а також наявності технічних або програмних засобів [13].

Установи можуть використовувати одну з трьох форм реєстрації документів: щоденникову, карткову та автоматичну (за допомогою спеціальної комп’ютерної програми) [14].

Основне завдання функціонування системи документообігу полягає в систематизації всього обсягу документів на паперових і електронних носіях. Основним завданням СЕД є організація збереження електронних документів, а також робота з ними. Системи електронного документообігу можуть сприяти безпеці доступу до документам, стежити за виробленими в них змінами та контролювати всі їх модифікації. Основою процесів управління і прийняття управлінських рішень є організація роботи з документ. Процес прийняття управлінського рішення містить отримання інформації, переробку цієї інформації, підготовку, аналіз і прийняття рішення. Цей склад процесу прийняття управлінського рішення тісно пов'язаний з документаційним забезпеченням управління [15].

Зі збільшенням розміру компанії проблема ефективності документаційного забезпечення управління виявляється більш актуально. Системи документообігу, які впроваджуються в компанії, повинні вирішувати поставлені завдання [16]:

- оптимізувати бізнес-процеси та автоматизувати механізм виконання та контролю;

- забезпечувати ефективне управління за допомогою автоматичного спостереження за виконанням і прозорістю роботи всієї компанії на будь-яких рівнях;
- підтримувати систему контролю якості, яка відповідає міжнародним вимогам;
- підтримувати ефективність збору, управління та можливості доступу до інформації та даних;
- забезпечувати кадрову гнучкість за допомогою збільшення формалізації роботи всіх співробітників і можливості збереження всієї передісторії його роботи;
- оптимально скоротити оборот паперових документів в компанії;
- протоколювати роботу підприємства в цілому;
- заощадити ресурси за допомогою зменшення витрат на управління потоками інформації на підприємстві;
- значно спрощувати і здешевлювати збереження паперових документів за допомогою наявного ефективного електронного документообігу.

Враховуючи зростаючу кількість даних, зламаних у великих компаній, зберігання на паперовому носії може навіть виявитися більш безпечний. Однак є справжні переваги для перетворення файлів в цифрові дані. Досить навести кілька ключових факторів, які пояснюють необхідність переходу підприємства на СЕД [17, 18]:

- надійне резервне копіювання. найчастіше співробітники підприємства занадто пізно розуміють про важливість резервного копіювання даних, що призводить до істотних втрат, як до тимчасових, так і до фінансових. своєчасне копіювання даних же гарантує, що ваш бізнес переживе будь-яку катастрофу;
- економія простору. електронна пам'ять пропонує хорошу альтернативу шафам з нескінченними стосами паперів. система електронного документообігу зберігатиме всі необхідні бізнес-операції, фінансові записи, звітність, не займаючи додаткового простору;
- підвищена безпека і контроль. співробітники підприємства повинні забезпечувати високий ступінь захисту документів і контролю над вони. досягнення

цих цілей із застосуванням паперового документообігу є досить складним завданням. сед пропонують переміщати документи в хмарне сховище, що дозволяє встановлювати права доступу до кожного документа, чітко визначати, хто витягував які документи і коли;

- спрощена співпраця. можливість відстеження переміщення документів значно покращує внутрішнє і зовнішнє співпраця. наприклад, співробітник або керівник в змозі визначити, де знаходиться файл в процесі затвердження в будь-який момент час;
- своєчасний доступ до даних. співробітники, які працюють в головному офісі або з віддалених підрозділах можуть отримати миттєвий доступ до документації, яка їм необхідна. можливість пошук файлу або документа з їх комп'ютера значно економить час. крім того, оскільки документи тепер електронні, вони можуть бути переглянуті багатьма користувачами відразу;
- низькі витрати на архівування. управління паперовими документами та їх архівування можуть бути дуже трудомісткими і, отже, дорогими. обробка, зберігання та витяг архівних записів значно спрощуються при переміщенні документів в електронні середовища;
- підвищення ефективності управління документами. процес управління документами, який пропонують сед, передбачає величезні можливості підвищення продуктивності для персоналу підприємства. вся інформація стає доступною з персонального комп'ютера співробітник;
- можливість пошуку. можливість легко знаходити інформацію та знання з індексованого контенту дозволяє нам поліпшити прийняття рішень і скоротити кількість втраченого часу на пошук інформація;
- спрощене управління завданнями. оцифровка інформації дозволяє призначати завдання користувачам, якщо це потрібно. також доступні розширені можливості робочого процесу, які дозволяють маршрутизувати документи по всій організації, зберігаючи при цьому можливість відстежувати їх прогрес і підписуватися на повідомлення по електронною поштою про їх стан;

З усім цім не дивно, що світові проекти з розробки СЕД і систем управління корпоративним контентом (ECM) неухильно зростають, як показано на рисунку 1.1:

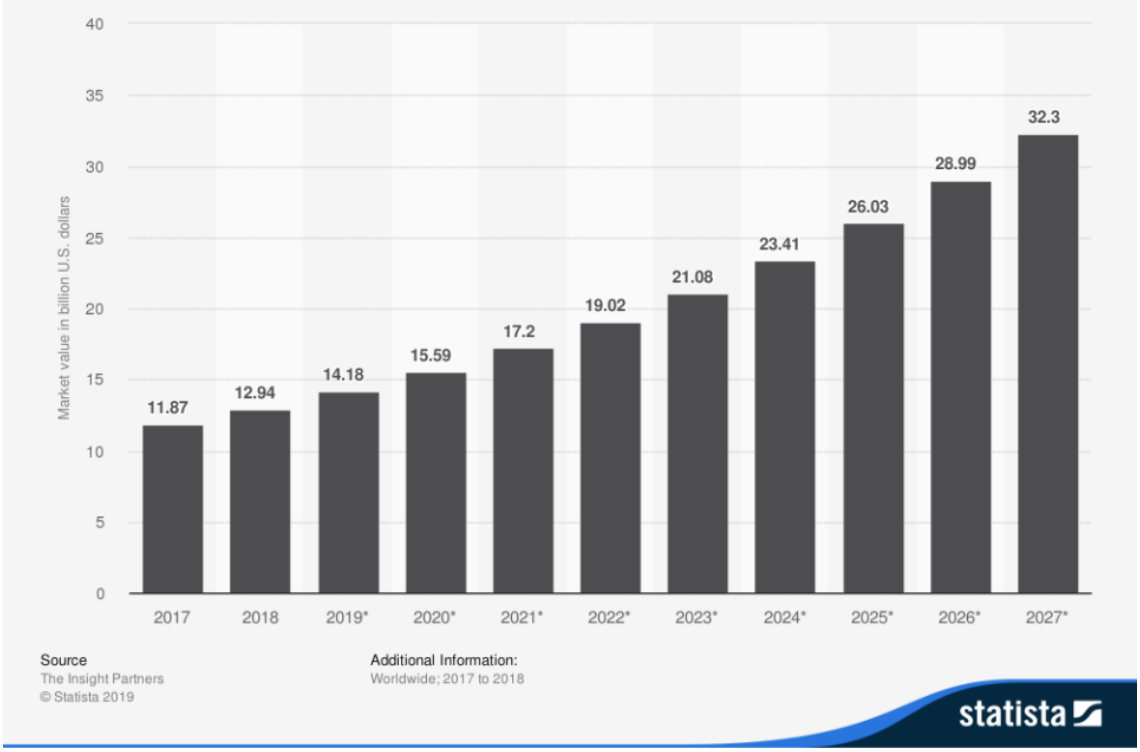


Рисунок 1.1 - Графік виручки компаній розробників СЕД (в мільйонах доларів).

Система електронного документообігу складається з декількох шарів: обладнання, системного і прикладного програмного забезпечення і даних, оброблюваних і переданих по мережі. Саме тому захист СЕД неможливо вибудувати окремо від інших ІБ-систем організації, вона повинна бути комплексною. Важливо забезпечити безпеку на всіх рівнях - від використання інструментів захисту периметра до організації інформаційної безпеки на рівні додатків, робочих станцій і мобільних пристроїв.

У зв'язку з цим необхідно передбачити заходи протидії загрозам безпеці на всіх рівнях:

- мережевому - мережеві екрани, шифрування трафіку, Засоби виявлення атак і контролю інформаційних потоків, захист віддаленого доступу і т. п.;
- серверів, робочих станцій і мобільних пристроїв – антивіруси, розмежування доступу на рівні ОС, шифрування, оновлення системного і прикладного ПЗ, контроль додатків і т. п.;

- систем управління базами даних (СУБД) і додатків-захист від атак на веб-додатки і СУБД, аутентифікація і розмежування доступу, контроль цілісності і т. п.

Крім того, слід вживати таких заходів:

- фіксувати події та керувати інцидентами інформаційної безпеки;
- контролювати дії персоналу - як рядових користувачів, так і адміністраторів систем, для чого можна використовувати організаційні заходи, методики підвищення обізнаності, технічні засоби контролю адміністраторів;
- сформувати необхідний набір організаційних заходів, розробити концепцію, правила і методики для управління інформаційною безпекою, призначити відповідальних за дотриманням вимог і розподілити їх обов'язки;
- забезпечити заходи фізичного захисту обладнання та приміщень.

Важливою особливістю захисту СЕД є розмежування прав доступу як до системного функціоналу, так і до окремих документів. При цьому системи документообігу, як правило, забезпечують захист документів тільки тоді, коли вони знаходяться на сервері СЕД і не надають необхідного набору інструментів контролю протягом усього періоду існування документальних файлів.

Таким чином, аналізуючи даний параграф випускної роботи, можна сказати, що на сьогоднішній день відмінним рішенням проблеми ефективного управління робочим процесом, координації потоків інформації, прискорення її обробки, оптимізації прийняття управлінських рішень є системи електронного документообігу. Якщо підприємство бажає відповідати сучасним тенденціям в ведення бізнесу, то керівництву необхідно розглянути перехід від паперового документообігу до електронного.

До захисту електронного документообігу необхідний комплексний підхід. Безпека СЕД не зводиться тільки до захисту документів і розмежування доступу до них — це завдання вирішується на рівні програмного забезпечення. Необхідна також підготовка персоналу, особливо IT-адміністраторів до роботи з конфіденційною інформацією. Погана організація може звести до нуля навіть найскладніші технічні способи захисту документів.

## 1.3 Етапи впровадження системи електронного документообігу підприємства

Для впровадження електронного документообігу потрібно розуміти завдання цього процесу і послідовність дій.

Для цього необхідно [19]:

- провести обстеження та аналіз існуючого документообігу в компанії;
- сформулювати завдання для підрозділів, залучених до впровадження СЕД;
- сформулювати вимоги до СЕД.

При організації системи електронного документообігу необхідно враховувати певні перешкоди [20]:

- консерватизм співробітників, низька освіта, небажання вчитися і перекваліфіковуватись. після впровадження системи електронного документообігу вони переживають за прозорість власної управлінської діяльності;
- організаційна структура постійно змінюється, а формалізація бізнес-процесів слабка;
- необхідність взаємодії із зовнішнім «паперовим» світом, особливо у випадку паралельних структур споріднених організацій чи установ, з якими вони часто співпрацюють.

Розглянемо процес впровадження електронного документообігу на підприємстві, який можна розділити на кілька етапів:

1) вивчення структури управління підприємством;
2) визначення основних бізнес-процесів;
3) вивчення, формування та складання номенклатури використовуваних документів, різних довідників і класифікаторів, а також формування інструкцій;
4) проведення системи адаптації на основі наявної інформації та отриманої в ході дослідження;
5) встановлення та введення в експлуатацію програмного забезпечення електронного документообігу;

6) налаштування системи, враховуючи проблеми, отримані в ході введення програмного забезпечення в експлуатацію;

7) навчання персоналу підприємства роботі з електронним документообігом.

Можливо, використання декількох етапів відразу або паралельно. Важливим моментом, який вимагає уваги, є використання процесу навчання персоналу підприємства програмному забезпеченню, так як від ефективності використання даного електронного документообігу залежить ефективність діяльності підприємства. Час впровадження програмного забезпечення електронного документообігу, як правило, займає від декількох тижнів до півроку, а також якщо великі компанії або галузі зі специфікою, то можливість впровадження може займати і рік.

Основні моменти при організації системи електронного документообігу, до яких можна віднести прийняття рішень про впровадження автоматизації документообігу, видання та підписання наказу про автоматизації інформаційно-аналітичного забезпечення управління (ІАЗУ), призначення відповідальної особи, терміни впровадження, терміни контролю і т. д.

Як правило, при формуванні та підписанні наказу, складається план по термінах впровадження заходів автоматизації системи ІАЗУ, в якому відображені дати початку та завершення робот з автоматизації документообігу. Далі узгодять технічне завдання з органами технічного нагляду та організаціями, які мають інтерес до одержуваної інформації протягом 15 днів. Наступним етапом йде укладення договору між сторонами, які представляють собою замовника і розробника проектування АС ІАЗУ. Далі йде саме проектування АС ІАЗУ [21].

Далі проводиться експериментальне впровадження автоматизованої системи електронного документообігу на підприємстві, а також удосконалення роботи програм з використанням зауважень та пропозицій, наявних з боку користувача або замовника. Введення в експлуатацію автоматизованої системи електронного документообігу на підприємстві, проведення заходів з навчання персоналу підприємства роботі з впроваджуваною програмою.

Навчання використанню програмного забезпечення, як правило, проводиться фахівцями відділу з персоналу, а також наявними фахівцями підрозділу, що несе відповідальність за автоматизацію документообігу, або представниками організації-розробника АС ІАЗУ.

Як правило, наявні проблеми при впровадженні системи автоматизації документообігу наступні:

- наявна потреба зміни оргструктури підприємства;
- проблема вдосконалення технології роботи з інформацією та удосконалення наявних принципів у діловодстві;
- збільшення навантаження на співробітників під час впровадження системи;
- вибір варіанту впровадження програмного забезпечення в діяльність підприємство;
- проблеми у персоналу підприємства з вивчення програмного забезпечення.

До проблем впровадження електронного документообігу слід відносити і надання електронному документу юридичної сили, взаємодія із зовнішнім і внутрішнім середовищем при взаємообміні інформацією, перехід документів з паперової форми в електронну і т. д.

Таким чином, етапи впровадження електронного документообігу супроводжуються рядом проблем, які в свою чергу не носять нерозв'язного характеру, а, навпаки, в ряді літератури висвітлені конкретні рекомендації, що дозволяють автоматизувати діловодство грамотно і з найменшими втратами. Незважаючи на існуючі труднощі, електронний документообіг знаходить все більш широке застосування саме тому що, ефект від нього вимірюється не прямою економією ресурсів, а підвищенням якості роботи організації.

Електронний документообіг повинен не тільки повністю автоматизувати діловодство в компанії, але також гарантувати можливу колективну роботу з документообігом, уніфікованого допуску або доступу до інформації, так званого – єдиного порталу.

Навіть деякі можливості сучасних систем електронного документообігу, вже мають найважливіше місце в забезпеченні суворого і правильного документообігу та діловодства, і, значно спрощують роботу всього підприємства.

Фактично електронний документообіг виглядає як "колективний органайзер" , в якому можна відстежувати сьогодення стан справ, настання термінів виконання завдань, історію роботи з документацією, статистику Виконання доручень. В результаті підприємство стає єдиним налагодженим механізмом, яким легко управляти. У сучасного керівника з'являється можливість з успіхом втілювати в життя все нові рішення. При веденні бізнесу різні види кореспонденції враховуються в декількох журналах, які зберігаються в різних місцях або навіть підрозділах організації. Для того щоб знайти конкретний документ, спочатку необхідно дізнатися, де і ким він зареєстрований, і після цього вже можна буде дізнатися, кому переданий для виконання або зберігання.

Можна відзначити, що потреби малого бізнесу стимулюють виробників IT-систем на створення різних спеціалізованих продуктів, які враховують своєрідність діяльності та особливості використання IT-системами цими суб'єктами економіки. Система електронного документообігу є одними з найпопулярніших IT- продуктів, необхідних самим різним підприємствам.

На сьогоднішній день електронний документообіг активно впроваджується в усі сфери інформаційної діяльності сучасного суспільство. Він став звичайним інструментом бізнесу, що дозволяє впорядкувати роботу з документами і налагодити проходження документів всередині приватних компаній і державних організацій.

### 1.4 Порівняльний аналіз сучасних систем електронного документообігу

Електронний документообіг в більшості випадків можна побачити у великих організаціях, на підприємствах з великим потоком даних, в будь-яких структурах, де є великий обсяг створюваних, оброблюваних і збережених документів, а також в банках.

Найбільш значущою функцією СЕД є зберігання електронних документів у структурованому вигляді та безпосередня робота з ними. В будь-якій системі головною функцією, якою є документообіг, система повинна налаштовуватися і підлаштовуватися під кожну структуру відділу та системи діловодства підприємства [22].

Основні типи систем електронного документообігу [23]:

- enterprise-centric EDM - корпоративні системи. Інфраструктура таких систем дозволяє корпоративним користувачам створювати документи, а також колективно працювати над ними і публікувати. Корпоративний системи впроваджуються як загальнокорпоративні технології, і вони не зорієнтовані на використання їх тільки в якійсь конкретній галузі. Яскравими представниками, що займаються розробкою і подальшим просуванням таких систем, є компанії Lotus, iManage, Novell, OpenText і Oracle.

- business-process EDM-системи, орієнтовані на бізнес- процес. Ці системи представлені в специфічних додатках. Основу такої системи становить концепція ECM. Системи забезпечують повний життєвий цикл роботи з документами (включаючи роботу з управлінням записами і потоками робіт, образами, управлінням вмістом та ін.). Вони зберігають і забезпечують пошук документів в оригінальних форматах, а також є можливість їх угруповання в папки. Всі EDM-системи забезпечують високий рівень реалізації репозитаріїв і бібліотечних сервісів для управління. Відомими розробниками таких систем є компанії Hummingbird, Fileneti ін.

- information management systems-портали, системи управління інформація. Такі системи займаються агрегуванням інформації, управлінням і доставкою через Internet/intranet/extranet. Прикладами таких порталів є системи Excalibur, Verity, Lotus та ін.

- content management systems-системи управління вмістом. Вони потрібні для створення вмісту, для доступу і управління вмістом, а також відповідають за доставку вмісту. Доступність інформації представляється у вигляді об'єктів

найбільш меншого розміру. Відомими компаніями систем управління вмістом є: Adobe, Vignette, Excalibur, Microsofti та ін.

- imaging systems - системи управління зображеннями / образами. Технологія працює на основі перекладу в електронну форму інформації з усіх успадкованих паперових документів. Базовий функціями систем є: пошук зображень, їх сканування, зберігання та ін.

Розглянемо ближче деякі з найбільш популярних СЕД, а саме: Megapolis.DocNet, DIRECTUM, DocsVision.

1. Megapolis.DocNet забезпечує повний цикл управління документами від їх підготовки до зберігання. Це серверне рішення, яке може бути розгорнуто на системах Windows Server, Linux або Unix. Бази даних, які підтримуються: Oracle, MS SQL Server, PostgreSQL. Можливе паралельне використання кваліфікованих електронних підписів (КЕП) українських АСЦК та КЕП RSA.

СЕД Megapolis.DocNet дозволяє впорядковувати та структурувати оцифровані дані, швидко шукати та налаштовувати синхронізовані завдання, незалежно від відстані користувача, дозволяє сканувати, ідентифікувати та зберігати документи, навіть якщо вони зберігаються на папері. Після цього оцифрування документи індексуються в базу даних і каталогізуються. Перевага Megapolis.DocNet полягає в тому, що він веб-орієнтований. Це означає, що організації не потрібно витрачати великі кошти на оновлення матеріально-технічної бази – вся робота виконується через браузер. Вся інформація може бути перенесена в хмару, що значно знижує витрати.

У 39,5% державних органів влади функціонує система електронного документообігу Megapolis [24].

2. DIRECTUM - система управління цифровими процесами і документами з елементами штучного інтелекту, в основі яких лежать технології машинного навчання і комп'ютерного зору. Система електронного документообігу DIRECTUM включає до свого складу наступні модулі:

- Управління електронними документами.

- Управління діловими процесами..

- Канцелярія.

- Управління договорами.

- Управління нарадами і засіданнями.

- Управління взаємодією з клієнтами.

- Звернення громадян та організацій.

- Управління показниками ефективності.

Базові компоненти системи включають базову серверну ліцензію системи та базові клієнтські ліцензії користувачів на базові модулі («Управління електронними документами» і «управління діловими процес») [25].

3. Система DocsVision включає в себе наступні окремо компоненти, що поставляються:

- Платформу DocsVision з вбудованими додатками, засобами настройки і розробки рішень

- Додатки-прикладні рішення, побудовані на платформі DocsVision і реалізують спеціалізовану функціональність для класу задач предметної області системи (наприклад «адміністративне діловодство» або «робоче місце керівника»

- Додаткові модулі - технологічні компоненти, які реалізують розширення інтеграційних можливостей системи (наприклад шлюзи DocsVision), а також розширюють можливості масштабування системи (наприклад модуль реплікації, або модуль архівування).

Функції системи:

- реєстрація листів, що надійшли в організацію, направлення їх до посадових осіб та контроль їх проходження;

- розробляти завдання для виконання вхідних документів та контролювати весь ланцюжок виконання, включаючи авторизацію, підлеглі та пов'язані з ними завдання;

- реєстрація та облік вихідних повідомлень, формування двосторонніх зв'язків з вхідними зв'язками;

- обробляти внутрішні записки, завдання та контролювати їх виконання;

- процес підготовки розпорядчих розпоряджень та рішень колегіального органу на основі звітів (службових записок, протоколів засідань), включаючи етапи створення, узгодження, затвердження, видання, підтвердження обізнаності та контроль за виконанням;

- ведення архіву нормативних, організаційно-розпорядчих документів, контроль прав доступу та управління життєвим циклом документів [26].

**Висновки до 1 розділу**

На підставі розглянутого теоретичного матеріалу з організації електронного документообігу на підприємстві було встановлено наступне. До впровадження СЕД, як і до будь-якої корпоративної інформаційної системі підприємства, варто підходити дуже ретельно. Неминуче враховувати потреби та можливості об'єкта впровадження, кваліфікацію співробітник. І вже після ретельного аналізу підприємства, варто підходити до вибору підходящої СЕД. Переваги електронного документообігу для сучасного підприємства безумовно очевидні. Однак присутність бар'єрів впровадження СЕД на підприємстві ніхто не скасовуючи. Керівництво повинно це враховувати при організації проекту по впровадженню СЕД на підприємство.

У цьому розділі були розглянуті теоретичні аспекти систем електронного документообігу на підприємстві. Дане вивчення дозволило зробити ряд висновків:

- інформаційні системи управління підприємством стали незамінним помічником у веденні бізнесу;
- на сьогоднішній день неможливо знайти жодне підприємство, де б не застосовувалися ІС управління;
- однією з сучасних тенденцій розвитку інформаційних систем на підприємстві є впровадження систем електронного документообігу;
- сучасні системи електронного документообігу надають широкий спектр інструментів автоматизації ведення діловодства, управління документообігом, підтримки бізнес- процес;

- перехід з паперового документообігу на електронний дає значний економічний ефект (скорочення трудових, фінансових і тимчасових витрат);
- до процесу впровадження СЕД варто підходити з усією відповідальністю, ретельно аналізуючи об'єкт впровадження, підбираючи відповідну систему

# РОЗДІЛ 2
# ТЕХНОЛОГІЇ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ПІДПРИЄМСТВІ

## 2.1 Формування вимог до забезпечення безпеки електронного документообігу

Захищеність СЕД забезпечується сукупністю програмних і технічних засобів захисту інформації. Юридичну значимість отримують лише ті електронні документи (ЕД), які задовільняють вимогам [27-29]:

1) Конфіденційністі - ЕД доступне лише повноважним користувачам;

2) цілісності - ЕД незмінне незалежно від засобів його обробки;

3) доступності – ЕД доступне в необхідній формі у певний час;

4) достовірності – ЕД в повному обсязі відображає підтверждуючи операції, діяльність або факти;

Забезпечення інформаційної безпеки електронного документообігу реалізується наступними методами захисту:

- Правовий метод, такий як сертифікація засобів захисту інформації та застосування вже сертифікованих, атестація об'єктів інформатизації за вимогами безпеки інформації;
- Організаційний - включає організацію охорони, роботу з кадрами, з документами;
- Програмно-апаратний, що включає в себе розробку програм забезпечення інформаційної безпеки, визначення порядку їх фінансування, створення системи страхування інформаційних ризиків.

Розробка СЕД повинна проводитися з урахуванням захисту від виявлених загроз і можливих інформаційних ризиків, для яких визначаються способи захисту, і на основі запропонованого показника оцінки її ефективності. При цьому враховуються вимоги, які пред'являються до створення таких систем, а саме [30]:

− Організація захисту інформації здійснюється з урахуванням системного підходу, що забезпечує оптимальне поєднання взаємопов'язаних методологічних, організаційних, програмових, апаратних та інших засобів;

− система повинна розвиватися безперервно, так як способи реалізації загроз інформації безперервно удосконалюються.

− система повинна передбачати поділ і мінімізацію повноважень по доступу до інформації, що обробляється і процедурам обробки;

− система повинна забезпечувати контроль і реєстрацію спроб НСД, містити засоби для точного встановлення ідентичності кожного користувача і проводити протоколювання дій;

− забезпечувати надійність захисту інформації і контроль за функціонуванням системи захисту.

Реалізація перерахованих вимог при створенні системи захисту інформації в СЕД сприятиме організації ефективного захищеного документообігу.

### 2.1.1 Класифікація загроз

Як правило, початковим базисом класифікації порушників в документах є їх положення щодо середовища звернення документа, тобто наявність у них прав доступу до інформації та до компонентів інформаційної системи, що дає можливість розділити порушників на два типи:

- зовнішні порушники - особи, які не мають права доступу до інформаційній системі, її окремим компонентам та загрозам, що реалізують безпеки інформації з-за меж інформаційної системи;

- внутрішні порушники - особи, які мають постійний доступ до інформаційної системи;

У практиці розробки моделей актуальних загроз і порушників безпеки відомостей конфіденційного характеру зазначена категоризація охоплює весь спектр порушників, які є джерелом потенційних загроза. Склад і зміст самих загроз визначається, в тому числі, сукупністю умов і факторів, що створюють небезпеку

несанкціонованого (навмисного або випадкового) доступу до захищуваних відомостей. Обґрунтування актуальності/неактуальності загроз супроводжується описом організаційно-технічних заходів, що дозволяють нейтралізувати такі загрози. Типова модель загроз для ІС, що мають підключення до мереж загального користування, включає в себе наступні класи загроз:

- загрози витоку інформації по технічних каналах;
- загрози несанкціонованого доступу до даних, в тому числі загрози із зовнішніх мереж.

Основні загрози ЕД представлені в таблиці 2.1.

*Таблиця 2.1*

Основні загрози електронному документообігу

| **Загроза** | **Реалізація загрози** | **Заходи захисту** | **Порушник** |
|---|---|---|---|
| 1. Загрози знищення, розкрадання апаратних засобів ІС, носіїв інформації шляхом фізичного доступу до елементам ІС | | | |
| Крадіжка носіїв інформації | Може бути здійснена:<br>- за рахунок виносу користувачами врахованих машинних носіїв інформації (МНІ);<br>- за рахунок несанкціонованого копіювання інформації на невраховані МНІ;<br>- за рахунок відправки інформації (у тому числі зображень) по мережі Інтернет за допомогою персональних комп'ютерів і смартфонів | - Фізична охорона засобів обчислювальної техніки з боку співробітників охорони та співробітників організації.<br>– Затвердження організаційно-розпорядчих документів (ОРД), регламентуючих порядок доступу в приміщення співробітників і сторонніх осіб. | Внутрішний |
| Крадіжка ключів і атрибутів доступу | | | |
| Крадіжка елементів ІС | | | |
| Виведення з ладу вузлів мережі, каналів зв'язку | Може бути здійснена за рахунок НСД порушниками в приміщення, де розташовані елементи мережевої інфраструктури та проходять канали зв'язку організації | | Внутрішний |
| Несанкціонована зміна налаштувань і відключення засобів захисту | Може бути здійснена:<br>- шляхом НСД порушниками в приміщення, де розташовані засоби захисту ІС при отриманні зазначеними користувачами прав адміністратора | - Затвердження ОРД по роботі з встановленими засобами захисту.<br>- Призначення адміністратора безпеки. | Внутрішний |

*Продовження табл. 2.1*

| **Загроза** | **Реалізація загрози** | **Заходи захисту** | **Порушник** |
|---|---|---|---|
| 2. Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок НСД із застосуванням програмно-апаратних і програмних засобів | | | |
| Загрози програмно-математичних впливів | Можуть бути здійснені:<br>– у разі деструктивного програмного впливу порушником на деякі програми або систему в цілому шляхом зміни компонентів програмної середовища;<br>– за рахунок впровадження програмних компонентів, в тому числі шкідливого програмного забезпечення (ПЗ); | – Установка ліцензійного ПЗ.<br>– Затвердження ОРД в частині організації заходів антивірусного захисту, а також про правила зберігання і видалення даних з зовнішніх/внутрішніх носіїв інформації. | Зовнішний та внутрішний |
| | – при спотворення вихідного коду прикладного й системного ПЗ;<br>– при впровадженні шкідливого коду в прикладне й системне ПЗ при використанні вразливостей вихідного коду;<br>– при відновленні некоректно видалених даних з зовнішніх/внутрішніх носіїв інформації. | - Призначення відповідальних осіб в ІС організації (адміністратора безпеки). | |
| Загроза впровадження апаратних закладок сторонніми особами, у тому числі обслуговуючим персоналом (ремонтними організаціями), після початку експлуатації ІС | Може бути здійснена:<br>– при безпосередньому доступі до ресурсів ІС шляхом впровадження апаратних закладок;<br>– при технічному обслуговуванні елементів ІС. | Затвердження ОРД, що регламентують порядок доступу в приміщення співробітників і сторонніх осіб, а також правила проведення технічного обслуговування елементів ІС, в тому числі при винесенні елементів за межі КЗ. | Зовнішний |
| Загроза можливостями внесення помилок, недекларованих можливостей, програмних закладок в ПЗ | Може бути здійснена особами (програмістами-розробниками) в процесі розробки ПЗ | - Установка ліцензійного ПЗ.<br>- Періодичне оновлення ПЗ.<br>- Призначення відповідальних осіб в ІС організації (адміністратора безпеки). | Зовнішний |

*Продовження табл. 2.1*

| **Загроза** | **Реалізація загрози** | **Заходи захисту** | **Порушник** |
|---|---|---|---|
| 3. Загрози ненавмисних дій користувачів і порушень безпеки функціонування ІС через збої в програмному забезпеченні, а також від загроз неантропогенного і стихійного характеру | | | |
| Загрози ненавмисних дій користувачів, внаслідок яких порушник отримує НСД до інформації | Може бути здійснена:<br>– за рахунок надання користувачем/адміністратором своїми ненавмисними діями (бездіяльністю) можливості зовнішньому порушнику отримання НСД до інформації в ІС | – Затвердження ОРД про необхідність дотримання конфіденційності щодо оброблюваних даних і<br>– Ознайомлення користувачів і відповідальних осіб із зазначеними ОРД | Зовнішний та внутрішний |
| Загроза компрометації реквізитів доступу (втрата ключів доступу, розголошення або крадіжка пароля тощо), НСД до аутентифікаційної інформації | Може бути здійснена:<br>– за рахунок дії людського фактора користувачів ІВ при порушенні ними парольної політики, передачі ключів доступу третім особам і т.д.).<br>– за умови успішного здійснення НСД до ділянок оперативного або постійного запам'ятовуючих пристроїв, в яких зберігається інформація для аутентифікації. | - Затвердження вимог до вибору паролів і періодичності зміни паролів (парольної політики);<br>- Проведення інструктажів про дії у випадках втрати або компрометації паролів | Внутрішний |
| Загроза ненавмисної модифікації (знищення) інформації співробітниками | Може бути здійснена:<br>– за рахунок дії людського фактора користувачів ІВ при невиконанні ними положень по роботі з захищаються відомостями конфіденційного характеру. | - Затвердження ОРД, що містять правила і порядок обробки відомостей конфіденційного характеру. | Внутрішний |
| Загроза виходу з ладу програмно-апаратних засобів | Може бути здійснена:<br>– при збоях в роботі апаратно-програмних засобів, що входять до складу ІС | – Затвердження ОРД в частині реалізації заходів з резервного копіювання баз даних, що містять відомості конфіденційного характеру.<br>– Призначення відповідальних осіб (адміністратора безпеки). | Внутрішний |

*Продовження табл. 2.1*

| Загроза | Реалізація загрози | Заходи захисту | Порушник |
|---|---|---|---|
| 4. Загрози навмисних дій внутрішніх порушників | | | |
| Загроза доступу до інформації, модифікація, знищення співробітниками, не допущеними до обробки інформації, що захищається | Може бути здійснена:<br>– внутрішнім порушником, не допущеним до обробки інформації, що захищається, але здатним тими чи іншими способами отримати інформацію обмеженого поширення | – Затвердження ОРД, що регламентують порядок доступу в приміщення співробітників і сторонніх осіб.<br>– фізична охорона засобів обчислювальної техніки з боку співробітників охорони і співробітників організації. | Внутрішний |
| Загроза розголошення інформації, модифікація, знищення | Може бути здійснена:<br>- внутрішніми порушниками, допущеними до інформації, що захищається, і переслідують | – Затвердження ОРД, що містять правила і порядок обробки відомостей | Внутрішний |
| співробітниками, допущеними до її обробки | корисливі цілі внаслідок своїх протиправних дій. | конфіденційного характеру.<br>– Отримання письмового зобов'язання про нерозголошення інформації | |
| 5. Загрози безпосереднього доступу в операційну систему (далі ОС) | | | |
| Загрози, що реалізуються в ході завантаження ОС | Може бути здійснена:<br>– при отриманні доступу в операційне середовище, порушник може скористатися як стандартними функціями операційних систем або будь-якої прикладної програми загального користування, так і спеціально створеними для виконання НСД програмами | – Затвердження ОРД, що регламентують порядок доступу в приміщення співробітників і сторонніх осіб. - цілодобова охорона приміщень ІВ; | Зовнішний та внутрішний |
| Загрози, що реалізуються після завантаження ОС і спрямовані на виконання НСД із застосуванням стандартних функцій ОС і прикладного ПЗ | Може бути здійснена:<br>– за допомогою зовнішнього носія для завантаження сторонньої операційної системи або шкідливого ПЗ | – Физическая охрана средств вычислительной техники со стороны сотрудников охраны и сотрудников организации. | Зовнішний та внутрішний |

*Продовження табл. 2.1*

| **Загроза** | **Реалізація загрози** | **Заходи захисту** | **Порушник** |
|---|---|---|---|
| 6. загрози НСД по каналах зв'язку | | | |
| Загрози, пов'язані з використанням WEB-сервісів в мережі, а також сервісів клієнт-серверної архітектури при передачі інформації по зовнішніх каналах зв'язку | Може бути здійснена:<br>– при використанні внутрішніх/зовнішніх сервісів в мережі зовнішнім порушником шляхом доступу/перехоплення/зміни HTTP cookies, зараження DNS-кеша, спотворення XML-схеми, | – Установка міжмережевого екрану<br>– Криптографічне перетворення інформації, що передається за межі КЗ по каналах зв'язку | Зовнішний |
| Загрози сканування, спрямовані на виявлення мережевих адрес робочих станцій, типу ОС, відкритих портів і служб, топології мережі, доступності вузлів використовуваних сервісів та ін. | Може бути здійснена:<br>– із застосуванням спеціального програмного забезпечення-мережевий сканер. | – Встановлення міжмережевого екрану, що дозволяє фільтрувати вхідний і вихідний трафік.<br>– Криптографічне перетворення інформації, що передається за межі КЗ по каналах зв'язку | Зовнішний |
| Загроза впровадження по мережі шкідливих програм і загроза їх негативних наслідків | Може бути здійснена:<br>- шляхом впровадження по мережі шкідливого програмного забезпечення з метою подальшого отримання НСД до ресурсів інформаційної системи, ідентифікаційної або аутентифікаційної інформації, обмеження доступу до ресурсів і сервісів та ін. | – Затвердження ОРД в частині організації заходів антивірусного захисту, а також про правила зберігання і видалення даних з зовнішніх/внутрішніх носіїв інформації.<br>– Призначення відповідальних осіб в ІС організації (адміністратора безпеки). | Зовнішний |
| Загрози перехоплення інформації | Може бути здійснена:<br>- шляхом перехоплення інформації переданої по каналах зв'язку, з метою подальшого аналізу цієї інформації та отримання НСД до сервісів ІС | – Встановлення міжмережевого екрану, що дозволяє фільтрувати вхідний і вихідний трафік.<br>– Криптографічне перетворення інформації, що | Зовнішний |
| Загроза приведення системи в стан «відмова в обслуговуванні» | Може бути здійснена:<br>– при відмові дискредитованою системою в доступі легальним користувачам при збільшенні числа мережевих з'єднань | передається за межі КЗ по каналах зв'язку | Зовнішний |

З наведеної моделі можна зробити висновок, що велика частина загроз нейтралізується на практиці впровадженням ОРД, ознайомленням з ними співробітників організації, розподілом обов'язків з організаційно-технічного забезпечення системи захисту інформації, а також установкою спеціальних програмно-технічних засобів, що пройшли оцінку відповідності вимогам щодо захисту інформація. Впровадження ОРД та проведення інструктажів направлено до значної частини на нейтралізацію «людського фактора», проте навіть якщо користувач, дотримуючись вказівок парольної політики, вірно згенерує пароль, то уникнути такої властивості пароля, як його відчужуваність від користувача, практично неможливо –він може бути загублений, забутий, вкрадений, переданий третій особі і т.д., що є найсильнішим недоліком даного типу аутентифікації.

### 2.1.2 Засоби і методи захисту електронного документообігу

Засоби і методи захисту електронного документообігу схожі із засобами захисту інформації в цілому, тому їх можна розглядати майже рівнозначними із застереженням конкретно до СЕДО підприємства.

Система захисту інформації в електронному документообігу - це раціональна сукупність напрямків, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Власник інформаційних ресурсів за цінністю інформації самостійно визначає ступінь захисту ресурсу, тип системи, необхідні способи та засоби захисту (крім відомостей, що становлять державну таємницю). Цінність інформації та необхідна надійність її захисту безпосередньо пов'язані. Важливо, що структура системи захисту повинна охоплювати не тільки електронну інформаційну систему, а й весь комплекс управління об’єктом, поєднуючи його реальні функції та виробничі підрозділи з традиційними процесами документування.

Основною особливістю цієї системи є її складність, тобто вона містить обов’язкові елементи, що охоплюють усі сфери захисту інформації. Систему захисту можна розділити на п'ять елементів.

1. Правовий захист інформації.

Правові елементи системи захисту інформації базуються на нормах інформаційного права, які обумовлюють правовідносини між підприємством і державою в системі захисту інформації, законність діяльності підприємства та його працівників. захисту [31]. Цей елемент включає:

- наявність організаційних документів підприємства, правил внутрішнього трудового розпорядку, договорів з працівниками, робочих і робочих інструкцій, положень та зобов'язань щодо захисту конфіденційної інформації;
- розробити та довести положення щодо юридичної відповідальності за розголошення конфіденційної інформації, несанкціоноване знищення чи фальсифікацію документів всім працівникам компанії, у тому числі не пов’язаним з конфіденційною інформацією;
- роз'яснення особам, які приймаються на роботу, положення про добровільність прийнятих ними на себе обмежень, пов'язаних з виконанням обов'язків щодо захисту інформації.

2. Інженерно-технічний захист інформації.

Технічні (апаратні) засоби. Це різні типи пристроїв (механічні, електромеханічні, електронні тощо) та апаратних засобів вирішення проблеми захисту інформації [32]. Вони перешкоджають доступу до інформації, в тому числі блокуючи її. Устаткування включає: генератори шуму, лінійні фільтри, радіоприймачі для сканування та багато інших пристроїв, які «блокують» потенційні шляхи витоку або дозволяють їх виявляти. Перевагами технічних засобів є їх надійність, незалежність від суб'єктивних факторів, висока стійкість до модифікацій. Недоліки - недостатня гнучкість, відносно великі розміри і вага, висока вартість.

Інженерно-технічні елементи системи захисту інформації призначені для пасивної та активної протидії засобам технічної розвідки, утворюючи межі для

захисту територій, будівель, споруд, обладнання технічними засобами. Незважаючи на високу вартість технічного захисту та безпеки, цей елемент дуже важливий для захисту інформаційних систем.

3. Організаційний захист інформації

Організаційні інструменти включають організацію та технологію (підготовка приміщень комп'ютерною технікою, прокладка кабельних систем, врахування вимог щодо обмеження доступу до неї) та організаційно-правові (національні закони та нормативні акти, які приймаються керівництвом конкретного підприємства). Перевага організаційних засобів полягає в тому, що вони дозволяють вирішувати багато різноманітних завдань, прості в реалізації, мають необмежені можливості модифікації та розвитку. Недоліками є те, що вони залежать від загальної організації роботи в конкретному підрозділі.

Організаційний захист — це регулювання виробничої діяльності та взаємовідносин виконавців на нормативній основі, що усуває або значно ускладнює привласнення конфіденційної інформації та прояв внутрішніх і зовнішніх загроз.

4. Програмно-апаратний захист інформації.

ПЗ включає процедури ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації (наприклад, тимчасових файлів), контролю тестування системи безпеки тощо [33].

Переваги програмного забезпечення - гнучкість, надійність, простота встановлення, модифікації та розробки. Недоліки - обмежені можливості мережі, використовує частину ресурсів файлових серверів і робочих станцій, дуже чутливі до випадкових або навмисних змін, можуть залежати від типу комп'ютера (їх апаратного забезпечення).

Програмно-апаратні елементи системи захисту інформації призначені для захисту цінної інформації, яка обробляється і зберігається в комп'ютерах, серверах і робочих станціях. Однак фрагменти цього захисту можуть бути використані як допоміжний засіб в інженерії та консервації тканин. Проект включає:

- незалежна програма захисту інформації та контролю рівня її безпеки;

- процедури захисту інформації, які працюють з процедурами обробки інформації;
- програми захисту інформації, що використовуються в поєднанні з технічними (апаратними) пристроями захисту інформації (переривання роботи комп'ютера у разі порушення систем доступу, видалення даних у разі несанкціонованого доступу до баз даних).

5. Криптографічний захист інформації.

Криптографічні методи захисту інформації – це спеціальні методи шифрування або іншого перетворення інформації, в результаті чого доступ до її вмісту неможливий без надання криптографічного ключа та зворотного перетворення [34]. Захист шифрування, безсумнівно, є найнадійнішим методом захисту, оскільки він захищає саму інформацію, а не доступ до неї (наприклад, зашифровані файли неможливо прочитати, навіть якщо носій викрадено). Цей спосіб захисту реалізується у вигляді програми або програмного комплексу.

Сучасна криптографія включає в себе чотири великих розділи:

- Симетрична криптосистема. Вони використовують один і той же ключ для шифрування та дешифрування.
- Криптосистема з відкритим ключем - система шифрування, при якій відкритий ключ передається по відкритому каналу.
- Електронний підпис. Система електронного підпису — це вкладення до його криптографічно перетвореного тексту, що дозволяє іншим користувачам підтвердити авторство та справжність повідомлення після отримання тексту;
- Управління ключами. Це процес обробки інформації, змістом яких є створення і розподіл ключів між користувачами.

Криптографічний елемент системи захисту інформації призначений для захисту конфіденційної інформації методами криптографії. Елемент включає:

- регулювання застосування різних криптографічних методів в ЕОМ і локальних мережах;

- формулювання умови та способів шифрування для передачі текстів документів незахищеними поштовими, телеграмними, телексними, факсимільними та електронними каналами зв'язку;
- налагоджувати використання зашифрованих засобів ведення переговорів на незахищених телефонних і радіоканалах;
- налагоджувати доступ до баз даних, файлів, електронних документів за допомогою персональних паролів, команд ідентифікації та інших методів;

На підставі аналізу загроз електронного документообігу підприємства, можна сформувати основні засоби захисту інформації та методи забезпечення інформаційної безпеки електронного документообігу (Таблиця 2.2).

*Таблиця 2.2*

Основні засоби забезпечення ІБ ЕД та їх методи

| **Засоби, забезпечення ІБ ЕД** | **Методи забезпечення ІБ ЕД** |
|---|---|
| Технічні | Використання апаратних фаєрволів |
| | Фізичне розмежування мережевого обладнання |
| | Автоматичне створення резервних копій |
| Програмні | Використання антивірусного ПЗ |
| | Логічне розмежування мережі |
| | Використання програмних засобів ідентифікації та аутентифікації користувачів |
| Організаційно-правові | Введення обліку ознайомлення співробітників з інформацією обмеженого поширення |
| | Організація обліку ключів шифрування і підпису, їх зберігання, експлуатації та знищення |
| | Надання прав доступу відповідно до посади |
| Криптографічні | Використання криптографічних засобів шифрування конфіденційної інформації |

| | |
|---|---|
| | Використання технології відкритих ключів для забезпечення автентичності та цілісності інформації |

Описані засоби і методи є загальними для будь-якої інформаційної системи електронного документообігу підприємства, і їх застосування може значно зменшити ризик реалізації загроз ЕД.

## 2.2 Технології захисту інформації в системах електронного документообігу

Перед впровадженням СЕД необхідно оцінити можливі загрози та ризики від СЕД, а також ступінь шкоди, яку можуть завдати загрози. Захист СЕД не обмежується захистом файлів і обмеженням доступу до файлів. Захист апаратного забезпечення системи, персональних комп'ютерів, принтерів та іншого обладнання, в якому працює система, є також дуже важливим. Для захисту каналів передачі даних і мережевого обладнання, СЕД можуть бути виділені в спеціальні сегменти мережі.

### 2.2.1 Аутентифікація користувачів у системі

Забезпечення безпечного доступу до даних всередині СЕД забезпечується зазвичай аутентифікацією і ідентифікацією. Під ідентифікацією, стосовно до забезпечення інформаційної безпеки СЕД, розуміють однозначне розпізнавання унікального імені суб'єкта СЕД. Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає даному суб'єкту (підтвердження автентичності суб'єкта). Таким чином, механізм ідентифікації та аутентифікації є основою для механізмів розмежування доступу. Системи ідентифікації та аутентифікації можна розділити наступним чином (рисунок 2.1).


Рисунок 2.1 - Системи ідентифікації та аутентифікації.

У біометричних системах ідентифікаційними є індивідуальні особливості людини, які в даному випадку називаються біометричними ознаками. Ідентифікація проводиться за рахунок порівняння отриманих біометричних характеристик і зберігаються в базі шаблонів. Залежно від характеристик, які при цьому використовуються, біометричні системи діляться на статичні і динамічні.

Статична біометрія грунтується на даних (шаблонах), отриманих шляхом вимірювання анатомічних особливостей людини (відбитки пальців, візерунок райдужки ока і т.д.), а динамічна — на аналізі дій людини (голос, параметри підпису, її динаміка).

До складу електронних систем ідентифікації та аутентифікації входять контактні та безконтактні смарт-карти і USB-ключі (USB-token). USB-Ключі працюють з USB-портом комп'ютера і виготовляються у вигляді брелоків (eToken).

eToken — це засіб персональної аутентифікації та зберігання даних з апаратною підтримкою цифрових сертифікатів та СЕР [36]. eTokens можуть бути виготовлені у вигляді стандартних смарт-карт або USB-ключів:

- Для підключення смарт-карт до комп’ютера потрібен сумісний пристрій зчитування смарт-карт. Його можна використовувати як засіб візуальної

ідентифікації (смарт-картки eToken PRO/SC можуть містити інформацію про свого власника та фотографію для використання службами корпоративної безпеки (ID-Badge)). Смарт-картки можуть бути виготовлені з білого пластику для подальшого друку (фотографій, персональних даних тощо) з попереднім друком, а також у вигляді наклеєних магнітних смужок або тиснених карток (з тисненими символами);

- USB-ключ - безпосередньо підключається до комп'ютера через порт USB, поєднуючи в собі функції смарт-карти і пристрої для її зчитування.

Одноразові паролі-динамічна аутентифікаційна інформація, що генерується різними способами для одноразового використання. Застосування одноразового пароля можливе лише один раз або в деяких реалізаціях протягом незначного проміжку часу.

Одноразовий пароль (OTP) практично невразливий для атаки мережевого аналізу пакетів, що є істотною перевагою перед звичайними довготривалими паролями. Навіть якщо одноразовий пароль буде перехоплений, ймовірність того, що їм зможуть скористатися, вельми сумнівна, щоб її розглядати всерйоз.

У будь-який СЕД обов'язково має бути передбачено розмежування прав доступу користувачів. Розмежування прав доступу користувачів всередині СЕД можна реалізувати по-різному. Наприклад, використовувати підсистему, створену розробником СЕД, або застосувати вже відому підсистему безпеки, яка добре себе зарекомендувала на практиці, або з'єднати обидві ці підсистеми і адаптувати під конкретну СЕД.

Однак максимальний ефект захисту конфіденційних відомостей досягається використанням криптографічних методів захисту. Можливості криптографічного захисту даних дозволяють зберегти конфіденційність документа навіть у разі його потрапляння третім особам. Однак в кожній системі захисту є пролом. Не є винятком і криптозахист. Будь криптографічний алгоритм схильний до декодування-це питання часу, сил і засобів. Шифри, які ще кілька років тому вважалися надійними, зараз вважаються небезпечними. Тому при розробці способів і методів криптографічного захисту даних потрібно співвідносити витрати на це і очікуваний ефект.

Час, сили, ресурси, витрачені на злом зашифрованої інформації, повинні у багато разів перевищувати «вартість» конфіденційних даних. При цьому треба використовувати і інші заходи захисту інформації, в тому числі організаційні, фізичні та правові. Якою б не була ефективною криптографічний захист, ніщо і ніхто не завадить зацікавленій особі прочитати вміст конфіденційного документа, халатно залишеному без нагляду, або «розшифрувати» дані, скориставшись залишеним на робочому столі ключем дескриптора.

### 2.2.2 Використання мережевих екранів

Мережевий екран - сукупність апаратних або програмних засобів, що виробляє контроль і фільтрацію проходять через нього мережевих пакетів на різних рівнях моделі OSI відповідно до встановлених правил.

Головною функцією мережевого екрану вважається забезпечення безпеки комп'ютерних мереж або окремих вузлів від неправомірного доступу. Крім того, мережеві екрани часто називають фільтрами, так як їх головна мета - не давати проходити пакетам, що не відповідають під критерії, встановлені в конфігурації.

Для протистояння несанкціонованому міжмережевому доступу брандмауер повинен розташовуватися між захищається мережею і потенційно ворожою. Організаційно екран входить до складу захищається мережі. Міжмережевий екран повинен враховувати протоколи інформаційного обміну, покладені в основу внутрішньої і зовнішньої мереж. Якщо ж такі протоколи різні, то брандмауер повинен підтримувати багатопротокольний режим.

Брандмауери керують мережевим трафіком, що проходить всередині локальної мережі, дозволяють пропускати через мережеве з'єднання, тільки авторизований трафік, контролюючи тим самим мережеву взаємодію між комп'ютерами глобальної та локальної мережі. Брандмауери дозволяють маскувати IP-адреси хостів всередині локальної мережі за допомогою операції, званої транзакцією мережевих адрес NAT (Network Address Translation).

Найбільша проблема з електронними документами полягає в тому, що вони розкидані всюди [37]. Від серверів до настільних комп'ютерів, мобільних пристроїв і так далі, в будь-якій конкретній організації буквально десятки, якщо не сотні тисяч електронних документів зберігаються по всій мережі, тому що це зручно. Люди створюють файли на своїх локальних комп'ютерах, вони можуть передавати їх на загальний сервер або навіть ділитися ними прямо зі свого жорсткого диска, щоб інші могли отримати до них доступ. Багато файлів часто копіюються на смартфони і знімні носії.

Найважливіше, що потрібно зробити для забезпечення безпеки документів, - це визначити, що і де знаходиться. Це починається з класифікації інформації і закінчується знанням того, де насправді зберігаються файли.

### 2.2.3 Технології контролю цілісності електронного документа

Для перевірки цілісності ЕД та підтвердження авторства інформації використовується КЕП, який базується на інфраструктурі відкритих ключів (ІВК). ІВК - це сукупність організаційно - технічних заходів та програмно-апаратних засобів, які необхідні при використанні технологій відкритого розподілу ключів.

Надзвичайно важливим аспектом в криптографії з відкритими ключами стає визначення того, хто з користувачів володіє яким ключем. Зазвичай ключі зберігаються в загальнодоступному довіднику, але тут присутній ризик підміни або перехоплення ким - небудь відкритого ключа користувача. Цим обумовлюється необхідність існування механізму, який буде стежити за відповідністю між користувачем і наданим їм ключем. Сертифікат відкритих ключів є одним з таких механізмів. Видається він кваліфікованим надавачем електронних довірчих послуг (КНЕДП).

Ці сертифікати є механізмами міцного зв'язку між відкритим ключем і суб'єктом, який володіє відповідним йому закритим ключем. В якості сертифіката виступає цифровий документ, що містить відкритий ключ і підписаний КЕП

КНЕДП, яким він був видан. Крім цього він містить інформацію про власника ключа.

Сертифікат відкритого ключа повинен містити: його персональний реєстраційний номер; ПІБ власника чи його псевдонім, дату його терміну дії;, відкритий ключ ЕП, назву і розташування КНЕДП. Все це дозволяє КНЕДП, який видав сертифікат, перевіряти справжність зв'язку між відкритим ключем суб'єкта і ідентифікують його відомостями.

КЕП є одним з найбільш поширених способів застосування асиметричного алгоритму шифрування. В основі КЕП лежить математичне перетворення підписуваних відомостей шляхом застосування особистого закритого ключа підписувача. При цьому необхідно дотримання деяких умов:

- КЕП неможливо створити без особистого закритого ключа;
- перевірити справжність КЕП може всякий, у кого є доступ до відповідного відкритого ключа;
- навіть найменша зміна підписуваних даних призведе до того, що підпис стане недійсним.

Процес підпису документа:

1. Будується хеш-функція, яка ідентифікує вміст документа (створюється «дайджест» документа).

2. Творець документа шифрує дані в хеш-функції власним закритим ключем.

3. Вже зашифрована функція поміщається в одне повідомлення з документом. Таким чином, КЕП – це похідна «дайджесту» і особистого закритого ключа. Цим і забезпечується її унікальність .

Алгоритм верифікації КЕП (рисунок 2.2):

- особа, яка отримала повідомлення, складає свій варіант хеш-функції підписаного документа;
- розшифровка хеш-функції в повідомленні шляхом використання відкритого ключа відправника;
- порівняння хеш - функцій.


Рисунок 2.2 - Алгоритм верифікації ЕП.

Якщо вони збігаються, то справжність і авторство документа однозначно підтверджуються. Подібно до будь-яких даних, КЕП може бути передана спільно з захищеними нею відомостями. Крім цього, КЕП дозволяє упевнитися, що дані не були жодним чином змінені при передачі. КЕП успішно застосовується разом з шифруванням. Шифрування забезпечує захист листа від чужих очей, а підпис - підтвердження особи.

Для того, щоб використовувати КЕП в будь-яких системах документообігу, необхідно:

1. Забезпечити створення ключа власника сертифіката з використанням засобів ЕП;

2. Забезпечити створення сертифіката відкритого ключа з використанням КНЕДП;

3. Забезпечити створення сертифіката електронного підпису ЕД з можливістю зазначення інформації про застосування КЕП та перевірки терміну дії сертифіката, а також мети застосування КЕП ;

4. Забезпечити верифікацію електронного підпису ЕД з можливістю перевірки терміну дії сертифіката, а також мети застосування КЕП;

5. Організувати перевірку належності сертифіката власнику

**Висновки до 2 розділу**

Захист інформації в системах документообігу є гострою потребою сучасного функціонування будь-якого бізнесу. Вибір конкретних засобів захисту залежить від цінності захищеної інформації. Тому при виборі засобу захисту необхідно оцінити і порівняти реальні збитки, завдані розкриттям або спотворенням інформації, з вартістю засобів захисту. Але в будь-якому випадку необхідно реалізувати основний, найдешевший і не менш ефективний метод – вхід до системи документообігу має здійснюватися криптографічною системою з обмеженим рівнем доступу.

Підхід до забезпечення електронного документообігу має бути комплексним. Необхідно тверезо оцінити можливі загрози та ризики для СЕД, а також ступінь шкоди, яку можуть завдати реалізовані загрози. На кожному рівні захисту діє набір організаційних заходів, але, на жаль, вони часто ігноруються. Адже рядові працівники проходять як інструктаж, так і навчання щодо роботи з конфіденційною інформацією.

Політика безпеки повинна давати гарантії того, що в СЕД забезпечується [38]:

1) відповідність рівня захисту інформації рівню її критичності;

2) рентабельність заходів із захисту інформації;

3) оцінка та перевірка інформаційної безпеки;

4) персоніфікація положень політики безпеки (щодо суб'єктів СЕД), звітність (реєстрація, аудит) для всіх критично важливих для безпеки ресурсів;

5) чіткість порядку забезпечення захисту інформації;

6) безперебійну роботу та її відновлення у разі непередбачених ситуацій тощо.

# РОЗДІЛ 3
# ЗАХОДИ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДОКУМЕНТІВ В ОРГАНІЗАЦІЇ

## 3.1 Коротка характеристика Державного підприємства "Медзакупівлі України"

Для розробки захищеного документообігу потрібно ретельно вивчити напрямок діяльності організації, так як саме від особливостей її діяльності в подальшому і буде залежати склад конфіденційних відомостей, який буде необхідно захищати.

Державне підприємство «Медичні закупівлі України» (ДП МЗУ) засновано 25 жовтня 2018 року, перебуває у державній власності та належить до сфери управління Міністерства охорони здоров'я України. Є особливо важливим підприємством для економіки, адже, відповідно до фінзвітності, вартість активів на кінець 2020 року становила понад 2 млрд грн.

Ключове завдання - сформувати прозору, ефективну, конкурентну та ощадливу до коштів платників податків систему публічних закупівель товарів медичного призначення.

Коротка характеристика ДП МЗУ наведена в таблиці 3.1.

*Таблица 3.1*

Основні дані організації

| | |
|---|---|
| Назва | ДП «Медичні закупівлі України» |
| Форма власності | Державне підприємство |
| Види діяльності | Діяльність посередників у торгівлі товарами широкого асортименту |
| Керівник | Жумаділов Арсен Куатович |
| Код ЄДРПОУ | 42574629 |
| Юридический адрес | 01601, місто Київ, вулиця Грушевського, будинок 7 |

В організації працює 87 осіб. В офісі є комп'ютери для співробітників. На всіх комп'ютерах встановлені антивіруси та індивідуальні паролі. Вікна виходять на вулицю. На вікнах встановлені жалюзі, решітки відсутні. В приміщенні встановлена сигналізація. На даному підприємстві відсутня служба безпеки.

Структурна схема організації представлена на рисунку 3.1.

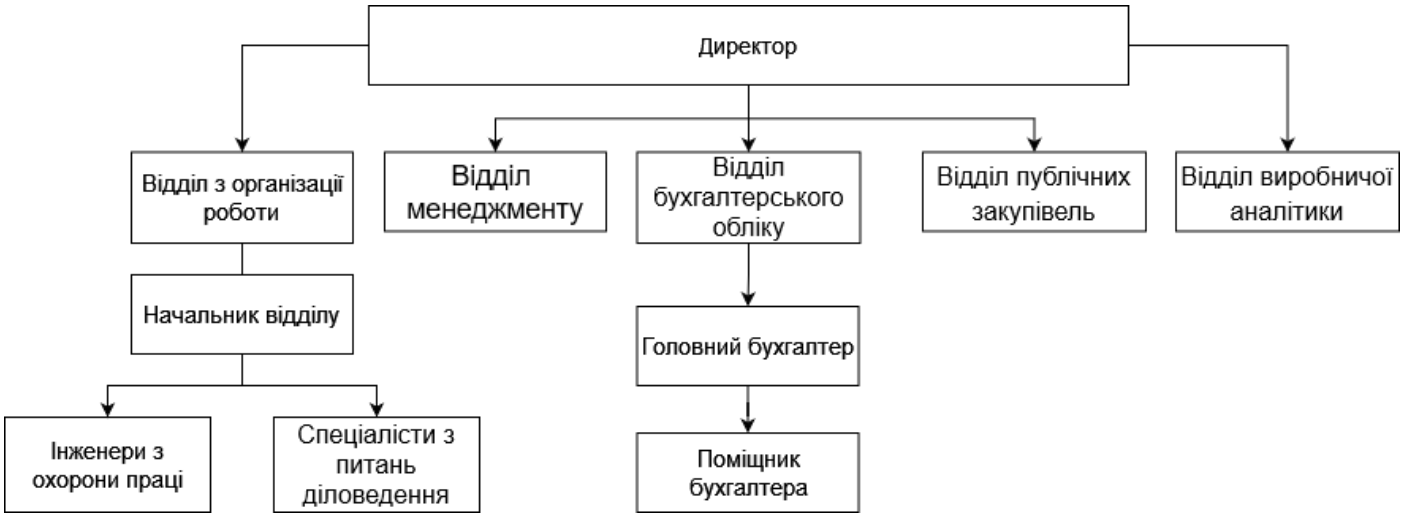


Рис. 3.1 Структурна схема ДП МЗУ

### 3.2 Характеристика оброблюваної інформації в ДП МОЗ

Найвищим грифом обмеження доступу до інформації, яка циркулює в СЕД ДП МЗУ є конфіденційна інформація.

За рівнем обмеження доступу інформація поділяється на:

1. Відкрита інформація.

2. Конфіденційна інформація.

3. Технологічна інформація.

До відкритої інформації відносяться: інформаційні ресурси загального користування – інформація, яка містить матеріали інформаційно-довідкового характеру та доступна всім користувачам СЕД (інформаційні ресурси загального користування представлені у вигляді – папок, файлів, електронних листів, Веб-сторінок, Веб-форм, електронних документів);

До конфіденційної інформації відноситься інформація, що містить персональні дані фізичних осіб;

До технологічної інформації відноситься:

- технологічна інформація щодо адміністрування СЕД;
- дані про персональні ідентифікатори засобів авторизації користувачів, паролі користувачів, їхні повноваження та права доступу, інформація журналів реєстрації дій користувачів, інформація про налаштування обладнання Системи, параметри прикладного ПЗ тощо.

Усі ці види інформації підлягають захисту в частині збереження конфіденційності, цілісності та забезпечення доступності.

### 3.3 Загальні вимоги до СЕД

Вимоги до системи електронного документообігу від організації:

- Система повинна мати можливість підключення співробітників всіх підрозділів організації (80 користувачів, що можуть використовувати різні робочі місця);
- Продуктивність не повинна знижуватись при навантаженнях;
- Система повинна забезпечувати накладання КЕП із використанням апаратно-програмних або апаратних пристроїв;
- Система повинна підтримувати розмежування прав доступу до документів організації в залежності від повноважень користувача;
- В системі повинні бути API для інтеграції з іншими системами;
- Система повинна мати повнотекстовий пошук документів. А також пошук за окремими критеріями;
- Система повинна надавати можливість додавання нових типів документів без програмування і налаштування кожного типу документа, включаючи опис маршруту його руху
- Оптимізована робота як на комп’ютері так і у мобільних пристроях.

Порівняємо декілька найбільш популярних СЕД за даними критеріями (таблиця 3.2)

*Таблиця 3.2*

Порівняння характеристик СЕД

| | Megapolis.Doc | DocsVision | DIRECTUM | Арт-Офіс | Paperless |
|---|---|---|---|---|---|
| Веб- чи десктоп-версія | І веб, і десктоп | І веб, і десктоп | Веб | Веб | Веб |
| Хмарний сервіс | Є | Є | Є | Є | Є |
| Масові дії з документами | Є | Є | Є | Є | Немає |
| Мобільний застосунок | Є | Є | Немає | Немає | Немає |
| Які види КЕП підтримує | Файловий носій, захищений носій, Mobile ID | Файловий носій, захищений носій, Mobile ID | Файловий носій, захищений носій Mobile ID | Файловий носій, захищений носій Mobile ID | Файловий носій, захищений носій, Mobile ID |
| Налаштування маршруту проходження документів | Є | Тільки в корпоративній версії | Є | Починаючи з тарифа «професійний» | Немає |
| Створення структури підприємства | Є | Тільки в корпоративній версії | Частково | Починаючи з тарифа «професійний» | Немає |
| Розподілення ролей і прав доступу до документів | Є | Тільки в корпоративній версії | Є | Починаючи з тарифа «професійний» | Немає |
| Можливість створення архіву й пошук у ньому | Є | Є | Є | Немає | Немає |
| Безкоштовний період | Базова версія, щомісяця 50 документів | Повна версія, 1 місяць, 1000 підписів | Повна версія, 10 підписів | PRO версія, 1 місяць | Повністю безкоштовний |
| Вартість | 900 грн за 1000 документів | 4200 грн за користувача (стандартна версія), 7000 грн (корпоративна) | 5000 грн за користувача | 1000 грн за 1500 документів | Повністю безкоштовний |

Виходячи з вимог до системи найбільш підходящими СЕД для підприємства будуть Megapolis.DocNet і DocsVision, оскільки вони в повному обсязі задовольняє вимогам. Але Megapolis.DocNet передбачає оплату за створені документ, а не користувачів, що для невеликого колективу компанії вигідніше.

### 3.4 Організаційно-правовий захист інформації

Організаційно-правові норми забезпечення безпеки та захисту інформації на будь-якому підприємстві відображаються в сукупності установчих та організаційних документів.

Під час аналізу в ДП МЗУ були відсутні будь-які положення або інструкції, що регламентують роботу співробітника по електронному документообігу.

#### 3.4.1 Статут підприємства

До Статуту підприємства слід додати доповнення, представлені нижче. У розділ "Права та обов'язки" вносимо наступні зміни:

1. Організація має право:

- формулювати структуру, розмір і порядок захисту конфіденційної інформації;
- пред'являти вимоги до працівників щодо захисту конфіденційної інформації;
- здійснювати контроль над дотриманням заходів забезпечення економічної безпеки та захисту конфіденційної інформації.

2. Організація повинна:

- запобігти всілякі витоку конфіденційної інформації та забезпечити економічну безпеку.
- проводити ефективний контроль виконання заходів економічної безпеки та захисту конфіденційної інформації.

Слід так само внести пункт "Конфіденційна інформація", який будить включати представлені нижче правила:

- співробітники створюють захист власної конфіденційної інформації;
- структура і розмір даних конфіденційного характеру, і процедура їх захисту формується генеральним директором.

Введення всіх цих доповнень надає адміністрації компанії можливість:

- формувати організаційні структури щодо захисту комерційної інформації або доручати ці функції відповідним посадовим особам;
- видавати нормативні та розпорядчі документи, що характеризують процедуру виділення даних, що становлять комерційну таємницю, та способи їх захисту;
- вносити правила щодо захисту комерційної таємниці в договори з усіх видів господарської діяльності (колективні та спільні з суміжниками);
- пред'являти вимоги захисту інтересів підприємства перед державними та судовими органами;
- користуватися інформацією, що належить підприємству, на шкоду співробітників компанії або ж начальника організації, для досягнення економічних цілей.

Далі повинна розробляється інструкція, яка регламентує порядок доступу співробітників до конфіденційної інформації, порядок створення, зберігання і знищення конфіденційної документів організації.

### 3.4.2 Положення про електронний документообіг

Також потрібно створити «Положення про електронний документообіг», яке встановлюватиме загальні принципи організації роботи електронної пошти та ведення баз даних у ДП МЗУ, вимоги до оформлення електронних документів, порядок їх обробки, виконання та зберігання. У ньому вказуються:

1. Вимоги, що висуваються до електронного документа:

1.1. Електронний документ має юридичну силу і тягне передбачені для даного документа правові наслідки відповідно до цього Положення.

1.2. Електронний документ містить наступні розділи:

- Реквізити організації,
- Вихідний номер документа,
- Дата реєстрації,
- Номер документа, на який здійснюється відповідь або підготовлена пропозиція,
- Кому адресовано,
- Зміст документа,
- Найменування посади керівника організації, його ініціали,
- Ініціали виконавця, який підготував документ, його контактний телефон та робочу електронну адресу.

1.3. Електронне повідомлення набуває правового статусу електронного документа за його відповідності вимогам цього Положення.

1.4. Електронний документ, що має форму, що не відповідає встановленій, як електронний документ відповідно до цього Положення не розглядається.

1.5. Електронний документ набирає чинності з моменту його отримання електронним адресатом.

Електронний документ, отриманий адресатом:

- роздруковується на паперовому носії,
- реєструється в журналі вхідних документів із зазначенням номера вхідного документа, дати отримання , за необхідності-дати кінцевого терміну виконання; дана інформація заноситься на паперовий варіант отриманого електронного документа,
- передається керівнику або замінює його посадовій особі на розгляд і подальших доручень на адресу відповідних посадових осіб організації.

2. Організація електронного документообігу

Процес електронного документообігу формується з наступних компонентів:

2.1. Призначення в ДП МЗУ відповідальних посадових осіб, що забезпечують електронний документообіг.

2.2. Відправлення та отримання електронних документів здійснюється з використанням програмних продуктів, призначених для роботи з електронною поштою. Вибір програмного продукту здійснюється організацією самостійно.

2.3. Контроль отримання адресатом відправленого електронного документа здійснюється відповідальною посадовою особою організації, провідним електронний документообіг.

2.4. Реєстрація вхідних і вихідних електронних документів, доставка виконавцям, контроль виконання.

2.5. Відправник має право відкликати відправлений електронний документ шляхом відправки одержувачу документа «Повідомлення про відкликання».

2.5.1. «Повідомлення про відкликання» є документом тієї ж категорії, що і відгукується документ.

2.5.2. «Повідомлення про відкликання» містить підставу відкликання раніше відправленого електронного документа.

3. Інформаційна безпека

3.1. Інформаційна безпека при здійсненні електронного документообігу забезпечується комплексом технічних та організаційних заходів, що реалізуються учасниками електронного документообігу та уповноваженою організацією.

3.2. До технічних заходів відносяться:

- організація та використання засобів захисту інформації в повному обсязі їх функціональних можливостей;
- забезпечення цілісності оброблюваних даних;
- забезпечення антивірусного захисту інформації.

3.3. До організаційних заходів відносяться:

- контроль виконання вимог нормативних документів, що регламентують забезпечення захисту інформації;
- визначення осіб учасників міжвідомчого електронного документообігу та уповноваженої організації, відповідальних за забезпечення інформаційної безпеки;

- встановлення порядку резервного копіювання, відновлення та архівування баз даних, що знаходяться на головному вузлі міжвідомчого електронного документообігу, а також порядку оновлення антивірусних баз;
- встановлення порядку допуску для проведення ремонтно-відновлювальних робіт програмно-технічних засобів;
- організація режимних заходів щодо приміщень, в яких розміщені вузли учасників електронного документообігу, та технічних засобів цих вузлів.

4. Зберігання електронних документів

4.1. Всі електронні документи, враховані при обміні, повинні зберігатися протягом строків, передбачених актами учасника електронного документообігу. Електронні документи повинні зберігатися в електронних архівах. Копії електронних документів, завірені в установленому порядку, можуть також зберігатися на паперових носіях.

4.2. Для виконання поточних робіт з ведення електронних архівів і контролю за ними, учасники електронного документообігу призначають відповідальних співробітників.

4.3. Якщо актами учасника електронного документообігу не передбачено інше, електронний документ зберігається в оригінальному вигляді, тобто в тому, в якому він був сформований, відправлений або отриманий, зі збереженням всіх реквізитів електронного документа, включаючи всі засвідчують електронні цифрові підписи.

4.4. Термін зберігання електронних документів відповідає терміну зберігання їх паперових аналогів.

4.5. Зберігання електронних документів супроводжується зберіганням відповідних журналів обліку, сертифікатів ключів підпису, повідомлень про доставку електронних документів, а також засобів, що забезпечують можливість роботи з електронними документами та електронними цифровими підписами.

4.6. Для сертифікатів ключів підписи оформляються та зберігаються в установленому порядку документи, що підтверджують статус сертифікатів ключів

підпису (у тому числі реєстраційні картки, довідки про відкликання та зупинення дії сертифікатів ключів підпису).

4.7. Інформація, що міститься в електронних архівах, та засоби її обробки (зберігання) підлягають захисту від несанкціонованого доступу відповідно до цих Правил.

### 3.5 Програмно-апаратні засоби захисту

З програмних способів захисту інформації в ДП МЗУ вже використовувався антивірус Dr.Web Enterprise Security Suite. Також на комп'ютерах підприємства встановлено Windows 10 корпоративна версія і включена вбудована функція BitLocker для шифрування дисків.

З апаратних засобів захисту у працівників був присутній апаратний ключ Yubico з двофакторною аутентифікацією для безпечного входу в систему.

Для підвищення безпеки в організації можна впровадити систему резервного копіювання даних і міжмережевий екран для розмежування доступа до мережі.

#### 3.5.1 Система резервного копіювання даних

На даному підприємстві оптимально буде застосувати систему резервного копіювання на сервері, де розміщена база даних СЕД, щоб можна було зробити відновлення бази даних в разі програмних або апаратних збоїв.

Для формування системи резервного копіювання скористаємося програмою Acronis True Image. Ця програма дозволяє робити резервне копіювання і аварійне відновлення даних на персональному комп'ютері, у якої безліч різних опцій резервування.

Застосування цієї програми дає можливість зменшити ймовірність загроз цілісності та доступності інформації, що знаходиться на персональному комп'ютері.

### 3.5.2 Міжмережевий екран

На сьогоднішній день в мережі Інтернет, можливо, відшукати тільки два безкоштовних повноцінних мережевих екрану - Comodo Firewall Pro і ZoneAlarm Free інші грунтовні програми такого рівня стали платними. Проте, за своїм функціоналом Comodo малоймовірно, що в чомусь поступиться подібним комерційним конкурентам. Він може застосовуватися як вдома на персональних комп'ютерах, так і в корпоративних мережах. Програма проста у використанні, тому для користувача досить базового рівня знань принципів роботи і захисту мереж. В організаціях, де часто стикаються з глобальною мережею, установка міжмережевого екрану дуже важлива.

Головні функції програми Comodo Firewall Pro:

- система правил доступу додатків до Інтернету;
- аналізатор поведінки програм;
- моніторинг доступу до файлів програм сторонніми процесами;
- засоби протидії всіляким видам вторгнень і атак , в тому-числі DDoS;
- інтеграція з центром безпеки Windows;
- економне використання системних ресурсів;
- компактний дистрибутив;
- експорт/імпорт налаштувань програми.

На підприємстві слід встановити міжмережевий екран на сервері, який в принциповій схемі локальної обчислювальної мережі організації розташований між зовнішнім і внутрішнім секторами (рисунок 3.1).

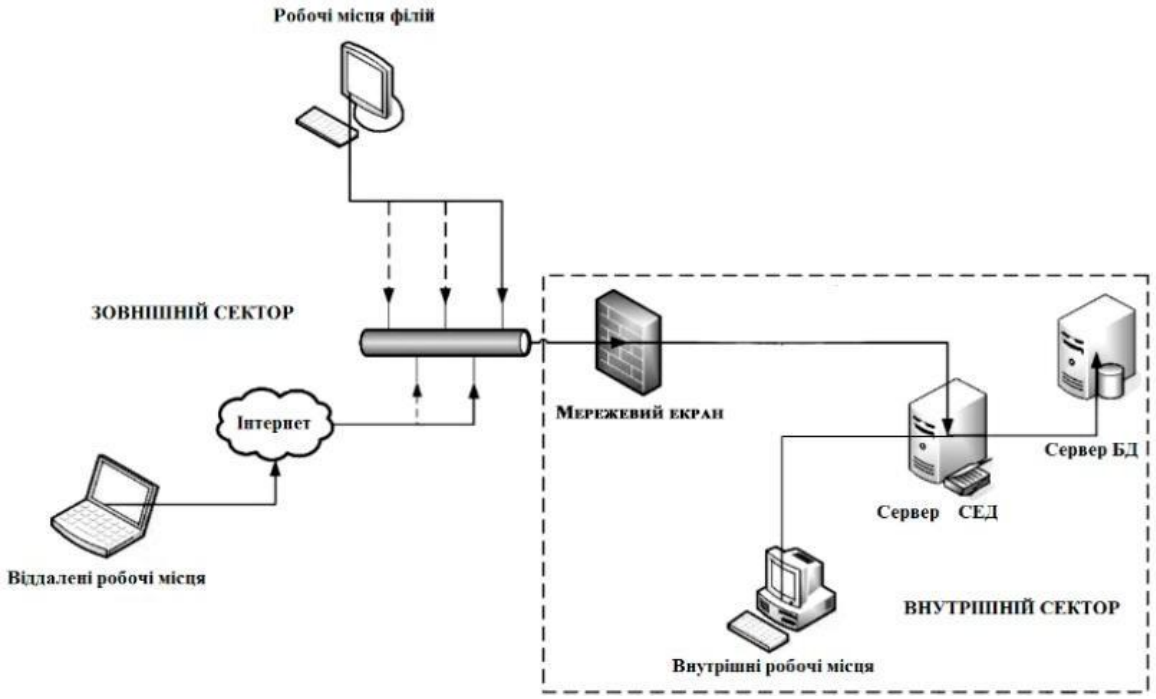


Рисунок 3.1 - схема локальної обчислювальної мережі із мережевим екраном

**Висновки до 3 розділу**

В даному розділі, використовуючи відкриті джерела, було досліджено Державне підприємство «Медичні закупівлі України», проведено структурування інформації, що захищається на об'єкті. Були розроблені проекти Положень «Про електронний документообіг», «Про конфіденційну інформацію». Запропоновано варіанти впровадження системи електронного документообігу, системи резервного копіювання даних та міжмережевого екрана.

Результатом роботи є розробка рекомендацій щодо вдосконалення рівня захисту системи електронного документообігу ДП МЗУ.

# ВИСНОВКИ

В роботі досягнуто таких науково-технічних результатів:

Дослідженням встановлено, що захист інформації в СЕД не обмежується захистом електронних документів і розподілом прав доступу. Актуальними завданнями є захист апаратного та іншого обладнання підсистеми СЕП, захист мережевого середовища, в якому працює СЕП, захист каналів передачі даних і мережевого обладнання.

Встановлено, що побудова системи електронного документообігу як документоорієнтованої інформаційної системи здійснюється на мережевій платформі: як локальних, так і розподілених комп’ютерних мережах. Безпека системи електронного документообігу повинна забезпечувати безпеку та автентичність документів, безпечний доступ та записи дій користувачів для усунення потенційних загроз інформаційній безпеці. Збереження файлу має бути гарантовано на весь термін служби файлу, а СЕД має бути здатним швидко відновлюватись у разі непередбаченої втрати чи пошкодження.

Розглянуті та проаналізовані основні загрози цілісності інформації та засоби захисту від них. Розглянуто засоби захисту інформації, проаналізовано ІТ ринок та обрано основні засоби для захисту даних.

Були розроблені нові організаційні документи Державного підприємства «Медичні закупівлі України», що регулюють роботу співробітників, пов'язаних із забезпеченням роботи електронного документообігу.

Поставлена задача була вирішена в повному обсязі, розроблені рекомендації, які при дотриманні забезпечать необхідний рівень безпеки документообігу на даному підприємстві.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конференція СЭД И ECM Day 2021 [Електроний ресурс] - Режим доступу:https://www.tadviser.ru/index.php/Конференция:Конференция_СЭД_И_ECM_Day_2021

2. Воитлева З. А. Возможности использования информационных технологий в управлении предприятием / З. А. Воитлева, Г. Ф. Нурыева // Academy. – 2017. – No 6 (21). – С. 60-61.

3. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: Підручник // С.М. Головань, В.Б. Дудикевич, В.С. Зачепило, Л.Т. Пархуць, В.О. Хорошко, Л.М. Щербак. – Львів: Видавництво Національного університету “Львівська політехніка”, 2005. – 288 с.

4. Бут К. О. Использование информационных систем в принятии управленческих решений на предприятиях / К. О. Бут – 2015. – С. 901-903.

5. Карапетян Д. Т. Экономическая значимость цифровой экономики / Д. Т. Карапетян // Научный журнал. – 2019. – No 1 (35). – С. 54-55

6. Краковський Ю. М. Захист інформації: навч. посібник для вузів / Ю. М. Краківський. - 348 с.

7. Столбов А. П. Організація електронного документообігу в охороні здоров'я / А. П. Столбов-с. 33-39

8. В.М. Фурашев . Електронне інформаційне суспільство України: погляд у сьогодення і майбутне / В.М. Фурашев, Д.В. Ланде, О.М. Григор`єв, О.В. Фурашев. // Монографія. Київ: ТОВ “Київська типографія”, 2005. – с.163.

9. Матвієнко О. Основи організації електронного документообігу : навч. посіб. / О. Матвієнко, М. Цивін. — К. : Центр учб. л-ри, 2008. — 112 с.

10. Про захист інформації в автоматизованих системах [Електронний ресурс]: Закон України від 31.05.2005 № 2594-IV – Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15

11. Комаристый Д. П. Использование информационных систем на предприятиях / Д. П. Комаристый, А. М. Агафонов, А. П. Степанчук, П. С. Коркин. – 2017. – No 2 (21). – С. 104-106.

12. Про електронні документи та електронний документообіг [Електронний ресурс]: Закон України від 22.05.2003 № 851-IV – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15

13. Про електронні довірчі послуги [Електронний ресурс]: Наказ міністерства юстицій України №1000/5 від 18.06.2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19

14. Про затвердження Правил організації діловодства та архівного зберігання документів [Електронний ресурс]: Закон України від 05.10.2017 № 2155-VIII – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0736-15

15. Герега І.Д. Проблеми захисту електронного документообігу / Всеукраїнська наукова конференція «Актуальні проблеми Кібербезпеки» // Державний Університет Телекомунікацій 2019р.

16. Владичанский Т. В. Електронний документообіг підприємств малого бізнесу / Т. В. Владичанский. – 2016. – No 5-2. – С. 246-249

17. Рыжко А. Л. Информационные системы управления производственной компанией : учеб. для академ. бакалавриата : учеб. для студ. вузов, обуч. по экон. напр. и спец. / А. Л. Рыжко, А. И. Рыбников, Н. А. Рыжко, – Нац. исслед. технол. ун-т «МИСиС». – М. : Юрайт, 2016. – 354 с.

18. Куняев Н. Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н. Н. Куняев, А. С. Демушкин, А. Г. Фабричнов. – М. : Логос, 2011. – 452 с.

19. Філіпова Л. Я. Системи управління електронним документообігом: загальні поняття термінології, організації, технології (зарубіжний досвід) / Людмила Філіпова // Вісник Книжкової палати України. — 2001. — No 4. — С. 15—18.

20. Столбов А. П. Организация электронного документооборота в здравоохранении / А. П. Столбов // Врач и информационные технологии. – 2007. – No 5. – С. 33-39.

21. Кобелев О. А. Электронная коммерция : учебное пособие / О. А. Кобелев. – 4-е. – М. : Дашков и К, 2017. – 684 с.

22. Ходак Е. Е. Внедрение систем электронного документооборота: как это происходит на практике / Е. Е. Ходак // Современные технологии делопроизводства и документооборота. 2011. – No 2. – С. 22-27.

23. Радченко С.В. Особливості систем електронного документообігу у державних органах України [Електронний ресурс]. – Режим доступу: https://archives.gov.ua/wp-content/uploads/AU_4_2013.pdf

24. Глинских А. Мировой рынок систем электронного документооборота [Электронный ресурс] : Онлайн библиотека аналитической информации «CitForum». – Режим доступа: http://citforum.ru/consulting/docflow/market/article1.8.200222.html.

25. Електронний документообіг (загальне діловодство) [Електронний ресурс]. Режим доступу: http://www.viaduk.com/viaduk/web5ua.nsf/0/ACC6E5C6C0A30BD9C225726F0051E26

26. Глинских А. Современные системы электронного документооборота [Электронный ресурс] – Режим доступа: http://www.ci.ru/inform09_01/p223edoc.htm

27. Шапошник Т.М. Правові засади електронного документообігу в органах державної влади [Текст] / Т.М. Шапошник, Ю.Л. Мохова // Держава та регіони (Серія «державне управління»). – 2018.

28. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс]: Постанова КМУ від 29.03.2006р. №373. – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

29. Концепція технічного захисту інформації в Україні [Електронний ресурс]: Постанова КМУ від 8.10.1997р. №1126. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF

30. Івахненков С.В. Інформаційні технології в організації бухгалтерського обліку: історія, теорія, перспективи / Житомир. інженерно-технологічний інститут. – Житомир: АСА, 2001. – 414 с.

31. Аскеров Т.М. Защита информации и информационная безопасность / под общ. ред. К.И. Курбакова. – 386 с.

32. Брызгалин, А. В. Свод хозяйственных договоров и документооборота предприятий с юридическим, арбитражным и налоговым к / А.В. Брызгалин, В.Р. Берник, А.Н. Головкин. - М.: Налоги и финансовое право, 2010. - 656 с.

33. Андреева, В.И. Делопроизводство. Требования к документообороту фирмы / В.И. Андреева. - М.: Бизнес-школа Интел-Синтез; Издание 2-е, перераб. и доп., 2016. – 222 с.

34. Барихин, А. Б. Делопроизводство и документооборот / А.Б. Барихин. - М.: Книжный мир, 2014. - 416 с.

35. Басаков, М. И. Документы и документооборот коммерческой организации / М.И. Басаков. - М.: Феникс, 2016. - 416 с.

36. Шелупанов А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А. Шелупанова, С. Груздева, Ю. Нахаева. — М.: Изд-во «Горячая Линия – Телеком», 2009. — 552 с.

37. Kevin Beaver, Document Security [Електронний ресурс] - Режим доступу: https://www.securityinfowatch.com/cybersecurity/information-security/article/10542069/document-security

38. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л. Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

39. Бузов Г.А. Захист від витоку інформації по технічних каналах/ Г. А. Буров, С. В. Калінін, А. В. Кондратьєв. - М.: 2013. - 416 с.