Тема 10. Організація електронного архіву. Безпека цифрового документування

1. Сутність електронного архіву: основні поняття, завдання, значення.
2. Принципи організації електронного архіву. Структура електронного архіву.
3. Технологічні рішення для архівування. Забезпечення довготривалого збереження документів.
4. Організація електронного архіву: практичні приклади.
5. Безпека цифрового документування.

1. Сутність електронного архіву: основні поняття, завдання, значення

Електронний архів – це організована система збереження електронних документів, яка забезпечує їхню цілісність, доступність, автентичність і довготривале зберігання.

Його головна мета: гарантувати, що цифрові документи залишаються читабельними, незмінними та юридично значущими протягом усього встановленого терміну зберігання.

Основні характеристики електронного архіву:

1. *Цифровий формат* – усі документи створюються, зберігаються та опрацьовуються у електронному вигляді.

2. *Структурованість* – документи впорядковані за типами, датами, проєктами, клієнтами тощо.

3. *Доступність* – швидкий пошук і перегляд документів користувачами з різними рівнями доступу.

4. *Безпека* – захист від несанкціонованого доступу, втрати або зміни даних.

5. *Юридична значущість* – електронні копії мають однакову силу з паперовими документами за умови наявності КЕП (кваліфікованого

електронного підпису).

Завдання електронного архіву:

✓ централізоване зберігання електронних документів підприємства;

✓ забезпечення швидкого пошуку та доступу до потрібних даних;

✓ контроль термінів зберігання документів відповідно до нормативів;

✓ інтеграція з бухгалтерськими, управлінськими та аналітичними системами;

✓ захист документів від втрати, знищення чи несанкціонованого редагування;

✓ збереження історії змін (audit trail).

Значення електронного архіву для бухгалтерського обліку:

- зменшення витрат часу на оформлення та пошук первинних документів;
- автоматичне підтягування документів у звітність;
- швидке надання підтверджуючих документів під час перевірок;
- мінімізація помилок і ризику втрати даних;
- підвищення прозорості облікових процесів.

Таблиця 10.1 – Відмінність електронного архіву від традиційного

Ознака	Паперовий архів	Електронний архів
Форма зберігання	Фізичні документи	Цифрові файли
Простір	Потребує приміщень	Потребує серверів або хмарного сховища
Доступ	Обмежений фізично	Дистанційний, багаторівневий
Пошук	Ручний, повільний	Автоматизований, миттєвий
Захист	Механічний, фізичний	Криптографічний, програмний
Відновлення	Складне після пошкодження	Можливе з резервних копій

Таблиця 10.2 – Відмінність між електронним архівом і базою даних

Ознака	Електронний архів	База даних
Мета	Довготривале збереження електронних документів	Збирання, обробка та аналіз змінних даних
Тип інформації	Завершені документи (накази, акти, звіти, договори)	Табличні дані, записи, числові показники

Структура	Каталоги, теги, дати, метадані, КЕП	Таблиці, поля, зв’язки між записами
Оновлення	Документи не змінюються (лише додаються нові)	Дані регулярно змінюються, оновлюються, видаляються
Доступ	За рівнями, з фіксацією історії перегляду	Динамічний, для роботи з активними даними
Інструменти	СЕД, архівні модулі (M.E.Doc, DocumentOnline, SAP ArchiveLink)	СУБД (MySQL, Oracle, SQL Server, PostgreSQL)
Юридичне значення	Документи мають правову силу	Дані — лише інформаційна складова, без юридичної ваги
Термін зберігання	Відповідно до архівних нормативів (3–75 років і більше)	Не регламентований, визначається потребами бізнесу

Отже, електронний архів – це система довготривалого зберігання документів, що вже створені, підписані й завершені в роботі. Головне завдання електронного архіву: зберегти, захистити та забезпечити доступ до документів у первісному вигляді протягом усього життєвого циклу.

База даних (БД) – це система постійної обробки, оновлення та аналізу інформації, яка змінюється в режимі реального часу. Основна мета БД: оперативна робота з даними, розрахунки, аналітика, формування звітності.

2. Принципи організації електронного архіву. Структура електронного архіву

Електронний архів ефективно виконує свої функції лише тоді, коли його побудовано на чітких принципах, що забезпечують системність, надійність, законність та доступність зберігання документів.

Основні принципи організації електронного архіву:

1. Принцип законності

Організація електронного архіву повинна відповідати:

- Закону України «Про електронні документи та електронний документообіг»,
- Закону «Національний архівний фонд та архівні установи»,

➢ Правилам організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях (Наказ Міністерства юстиції України),

➢ нормативам Держархіву та податкового законодавства.

Юридична вимога: документи, що зберігаються в електронному архіві, мають ту ж юридичну силу, що й паперові – за умови наявності КЕП і дотримання вимог цілісності.

2. Принцип системності

Архів повинен бути структурованою системою, де кожен документ має:

- ✓ логічне місце у каталозі,
- ✓ визначені метадані (дата, автор, тип документа, термін зберігання),
- ✓ зв'язок із відповідними бухгалтерськими чи управлінськими записами.

Наприклад: у бухгалтерії документи групуються за видами – договори, рахунки, акти, податкові накладні, звіти тощо.

3. Принцип доступності та контрольованості

Доступ до архіву має бути диференційований: різні користувачі бачать лише те, що їм дозволено. Ведеться журнал доступу: хто, коли і який документ відкривав або змінював. Забезпечується зручний пошук і навігація за ключовими словами, тегами, датами.

4. Принцип автентичності та цілісності

Кожен документ у архіві має залишатися незмінним від моменту підписання. Зміна навіть одного байта має фіксуватися у журналі подій. Використання електронного підпису гарантує, що документ не був підроблений. Забороняється перезапис чи «оновлення» первинних файлів – лише додавання нових версій.

5. Принцип довготривалості зберігання

Електронний архів має забезпечувати збереження документів протягом нормативних строків – іноді десятки років. Застосовуються формати, придатні

для архівування (PDF/A, XML, TIFF). Передбачено резервне копіювання і дублювання даних у хмарі чи на зовнішніх серверах. Довготривале зберігання передбачає стійкість до часу, технологій і людського фактора.

6. Принцип інтегрованості

Електронний архів не існує ізольовано, він повинен бути інтегрований з іншими інформаційними системами підприємства:

- ❖ бухгалтерським обліком (Dilovod, MASTER, SAP),
- ❖ кадровим обліком,
- ❖ управлінським документообігом.

Це дозволяє автоматично зберігати документи одразу після затвердження.

7. Принцип захисту інформації

Передбачає: шифрування даних при зберіганні та передачі; використання систем автентифікації (логіни, токени, КЕП); багаторівневі системи резервного копіювання; політику обмеження доступу до конфіденційних документів.

8. Принцип відтворюваності

Будь-який документ із архіву має бути доступним для читання, друку або передачі у разі потреби (наприклад, під час аудиту чи податкової перевірки). Важливо зберігати сумісність форматів. Забезпечити можливість міграції архіву на нові технологічні платформи.

Структура електронного архіву – це впорядкована система зберігання електронних документів, яка забезпечує їхню логічну організацію, швидкий пошук і ефективне управління життєвим циклом документів. Вона відображає, як саме документи «живуть» у цифровому середовищі – від створення до архівного зберігання.

Основні складові структури електронного архіву:

1. *Каталоги (розділи архіву)* групують документи за напрямами діяльності:

- ➤ бухгалтерія,
- ➤ кадрові документи,

➤ договори,

➤ звітність,

➤ податкові накладні тощо.

Каталоги можуть відповідати структурі підприємства (наприклад: «Фінансовий відділ → Облік → Податкова звітність»).

2. *Електронні справи (досьє)* об'єднують документи, пов'язані з однією операцією або темою:

➤ Договір №45/2024 з ТОВ «Альфа»,

➤ Перевірка ДПС за І півріччя,

➤ Закриття звітного періоду.

3. *Документи (записи архіву)* зберігаються у затвердженому вигляді з усіма реквізитами та електронними підписами; мають унікальний ідентифікатор (номер, дата, автор, тип документа).

4. *Метадані (описові дані)* – супровідна інформація, що допомагає швидко ідентифікувати документ:

- ✓ назва,
- ✓ дата створення,
- ✓ тип,
- ✓ автор/виконавець,
- ✓ термін зберігання,
- ✓ статус (чернетка, узгоджено, підписано, архівовано).

5. *Індекси і теги* використовуються для швидкого пошуку документів за ключовими словами чи темами.

Наприклад: #акт_звірки, #податковий_звіт, #договір_оренди.

6. *Журнал подій (лог доступу)* фіксує всі дії користувачів: створення, відкриття, зміни, видалення; забезпечує контроль і прозорість роботи з архівом.

Таблиця 10.3 – Логічні рівні архіву

Рівень	Характеристика	Приклад
1. Системний	Загальні налаштування архіву, права доступу, резервне копіювання	адміністратор архіву
2. Функціональний	Розподіл за підрозділами чи типами документів	бухгалтерія, кадри, юридичний відділ
3. Документний	Зберігання окремих електронних файлів і метаданих	акти, рахунки, накладні, звіти

Формати збереження документів

Для архівного зберігання використовують стандартизовані формати, які гарантують довготривале читання документів:

PDF/A – стандарт архівного збереження (виключає змінність документа);

TIFF, PNG – для зображень і сканів;

XML, CSV – для структурованих даних;

ZIP – для пакетного архівування груп документів.

3. Технологічні рішення для архівування. Забезпечення довготривалого збереження документів

Ефективна система електронного архівування спирається не тільки на нормативи, а й на *технологічну базу* – програмні комплекси, які забезпечують створення, зберігання, пошук, резервування та захист документів.

Таблиця 10.4 – Класифікація технологічних рішень

Тип рішення	Характеристика	Приклади
Локальні системи (on-premises)	встановлюються на серверах підприємства; повний контроль над даними	*1С:Документообіг, BAS Документообіг, M.E.Doc, АРМ "Архівіст"*
Хмарні системи (cloud-based)	забезпечують доступ з будь-якого пристрою; зручні для дистанційної роботи	*Вчасно.Док, Paperless, Google Workspace, Microsoft SharePoint, Zoho WorkDrive, SAP ArchiveLink*
Гібридні системи	поєднують локальне сховище та хмарну реплікацію для резерву	*Alfresco, OpenText, Nextcloud Enterprise*

Основні функціональні можливості сучасних систем:

1. *Електронне підписання* (КЕП, Дія.Підпис) – гарантує автентичність документа.

2. *Розмежування доступу* – кожен користувач бачить лише свої документи.

3. *Індексування та повнотекстовий пошук* – миттєвий доступ за ключовими словами.

4. *Версіонування документів* – зберігає історію змін.

5. *Резервне копіювання (backup)* – дублювання архіву на різних серверах.

6. *Контроль термінів зберігання* – автоматичне нагадування про завершення строку.

7. *Інтеграція з бухгалтерськими системами* – M.E.Doc ↔ ДПС ↔ банк.

Українські технологічні рішення:

M.E.Doc – підтримує електронний документообіг і архівування первинних документів, звітів, накладних.

Вчасно.Док – забезпечує юридично значиме підписання документів, їх зберігання в архіві та пошук за реквізитами.

Paperless – корпоративна система для повного циклу цифрового документообігу.

У державному секторі часто використовують системи *«АСКОД»* та *«Мегаполіс.Док»* – вони сертифіковані для зберігання службових документів.

Довготривале збереження – це гарантія доступності та цілісності документів упродовж усього терміну, передбаченого законодавством (від 3 до 75 років, а іноді – постійно).

Основні принципи довготривалого збереження

1. Незмінність документа

- використання формату PDF/A, TIFF, XML, які не допускають редагування;
- застосування електронного підпису (КЕП), що унеможливлює

підміну.

2. *Дублювання (резервування)*
   - створення кількох копій архіву (на різних серверах, у хмарі, на фізичних носіях);
   - використання RAID-масивів або географічного дублювання (копії у різних дата-центрах).
3. *Регулярне оновлення форматів* архівні системи повинні передбачати міграцію даних у сучасні формати, щоб старі файли не стали «мертвими».
4. *Захист від несанкціонованого доступу* шифрування даних, двофакторна автентифікація, ведення логів користувачів.
5. *Контроль цілісності даних* періодична перевірка контрольних сум (hash) файлів – SHA-256, MD5.
6. *План відновлення після збоїв* (Disaster Recovery Plan) прописані сценарії дій на випадок збою, кібератаки чи втрати сервера.

Таблиця 10.5 – Міжнародні стандарти архівування

Стандарт	Назва	Призначення
ISO 14721:2012 (OAIS)	Open Archival Information System	концептуальна модель архівного зберігання
ISO 19005-1:2005 (PDF/A)	PDF for Archiving	стандарт для довготривалого зберігання документів
ISO 15489-1:2016	Records Management	управління документами протягом життєвого циклу
MoReq2010	Model Requirements for Electronic Records	вимоги до електронних архівів у ЄС

4. Організація електронного архіву: практичні приклади

1. Українська компанія «Нова пошта»

Ситуація:

Щодня обробляються сотні тисяч накладних, актів, звітів та договорів.

Рішення:

Впроваджено систему BAS Документообіг з інтеграцією в ERP.

Усі документи підписуються КЕП через Вчасно.Док.

Архів формується автоматично після завершення бізнес-процесу.

Застосовано хмарне резервування та обмеження доступу за ролями.

Результат:

Зменшення витрат на папір і друк на 70%.

Пошук документа – до 10 секунд замість кількох годин.

Спрощення внутрішнього аудиту та перевірок.

2. Державна установа: Міністерство юстиції України

Ситуація:

Мільйони юридичних документів, наказів і актів, які мають постійний строк зберігання.

Рішення:

Впроваджено СЕД «АСКОД» – офіційна державна система.

Всі документи реєструються, узгоджуються та архівуються в електронній формі.

Підпис – КЕП посадової особи, перевірка дійсності – через ЦСК.

Забезпечено доступ лише авторизованим працівникам.

Результат:

Повна відмова від паперових наказів.

Економія архівних площ.

Прозорість руху документів – можна відстежити кожен етап.

3. Приватне підприємство «Агроінвест» (бухгалтерський кейс)

Ситуація:

Необхідно зберігати первинні документи, акти, рахунки, податкові накладні.

Рішення:

Використання M.E.Doc для формування, підписання і передачі документів.

Налаштовано автоматичний експорт у електронний архів (локальний NAS + резерв у хмарі Google Drive).

Впроваджено PDF/A-формат для зберігання незмінних копій.

Щотижневе резервне копіювання та перевірка контрольних сум файлів.

Результат:

Доступ до документів для аудиту – онлайн.

Скорочення часу на підготовку перевірки ДПС у 4 рази.

Безпаперовий архів бухгалтерії.

4. Банківська установа (міжнародна практика – Німеччина)

Ситуація:

Банк має забезпечити збереження транзакційних документів протягом 10 років.

Рішення:

Використання SAP Records Management.

Дані дублюються у три дата-центри в різних регіонах.

Архівування у форматах XML + PDF/A, перевірка підписів за допомогою PKI.

Щорічна міграція форматів і перевірка цілісності бази даних.

Результат:

Гарантований доступ до будь-якого документа навіть через 10 років.

Повна відповідність вимогам ЄС щодо GDPR і FINREP.

5. Освітній заклад (вітчизняний приклад)

Ситуація:

Потрібно оцифрувати кадрові документи, договори зі студентами, звіти.

Рішення:

Впроваджено Google Workspace + Paperless як єдине середовище

документообігу.

Кожен документ має унікальний QR-код і зберігається у централізованому архіві.

Для збереження – Google Vault (хмарне сховище з юридичною фіксацією).

Для контролю доступу – двохетапна аутентифікація через корпоративну пошту.

Результат:

Безпечний архів студентських справ.

Віддалений доступ для працівників деканату.

Мінімізація ризиків втрати через війну або евакуацію.

5. Безпека цифрового документування

Безпека цифрового документування – це комплекс організаційних, технічних і правових заходів, спрямованих на захист електронних документів від несанкціонованого доступу, втрати, підробки, знищення чи спотворення.

Головна мета: зберегти достовірність, цілісність і доступність документів упродовж усього строку їх зберігання.

Таблиця 10.6 – Основні загрози безпеці електронних документів

Категорія загрози	Приклади
Несанкціонований доступ	крадіжка паролів, хакерські атаки, доступ колишніх працівників
Підробка документів	фальсифікація КЕП, зміна змісту файлів
Втрата даних	збій серверів, віруси, знищення копій архіву
Несумісність форматів	неможливість відкрити старі файли через оновлення ПЗ
Людський фактор	випадкове видалення, неправильне архівування, помилки у правах доступу

Принципи безпеки цифрового документування:

1. *Конфіденційність* — доступ лише для авторизованих користувачів.

2. *Цілісність* — неможливість змінити документ без залишення сліду.

3. *Доступність* — документ має бути доступним, коли це потрібно.

4. *Автентичність* — підтвердження, що документ створений уповноваженою особою.

5. *Невідмовність* — автор не може заперечити створення або підписання документа.

Основні засоби забезпечення безпеки:

1. Кваліфікований електронний підпис (КЕП)

- ✓ Гарантує автентичність і юридичну силу документа.
- ✓ Підтверджує, що дані не були змінені після підписання.
- ✓ Використовується при роботі у M.E.Doc, Вчасно.Док, Paperless, BAS тощо.

2. *Шифрування даних*

- ✓ Застосовується при передачі (TLS/SSL) і зберіганні документів (AES-256).
- ✓ Дозволяє зберігати документи навіть у публічних хмарах без ризику витоку.

3. *Система розмежування прав доступу*

- ✓ Визначає, хто може переглядати, редагувати, видаляти документи.
- ✓ Впроваджується у всіх СЕД (Alfresco, SharePoint).
- ✓ Рекомендується принцип «мінімально необхідних прав».

4. *Резервне копіювання та дублювання*

- ✓ Архіви мають дублюватися у двох різних місцях (локально + хмара).
- ✓ Перевірка працездатності копій – не рідше одного разу на місяць.

5. *Журнали подій (логування)*

- ✓ Фіксують усі дії користувачів: вхід, редагування, підпис, видалення.
- ✓ Дозволяють розслідувати інциденти та запобігати порушенням.

6. *Навчання користувачів*

- ✓ Регулярні інструктажі щодо фішингу, безпечної роботи з

електронними підписами, перевірки посилань.

- ✓ Наявність внутрішньої політики інформаційної безпеки.

Організаційні заходи безпеки:

1) Розробка положення про електронний документообіг.
2) Призначення відповідальної особи за ІТ-безпеку.
3) Ведення реєстру носіїв КЕП.
4) Регулярні аудити інформаційної безпеки.
5) Використання національних засобів криптозахисту (Держспецзв’язок, НБУ).