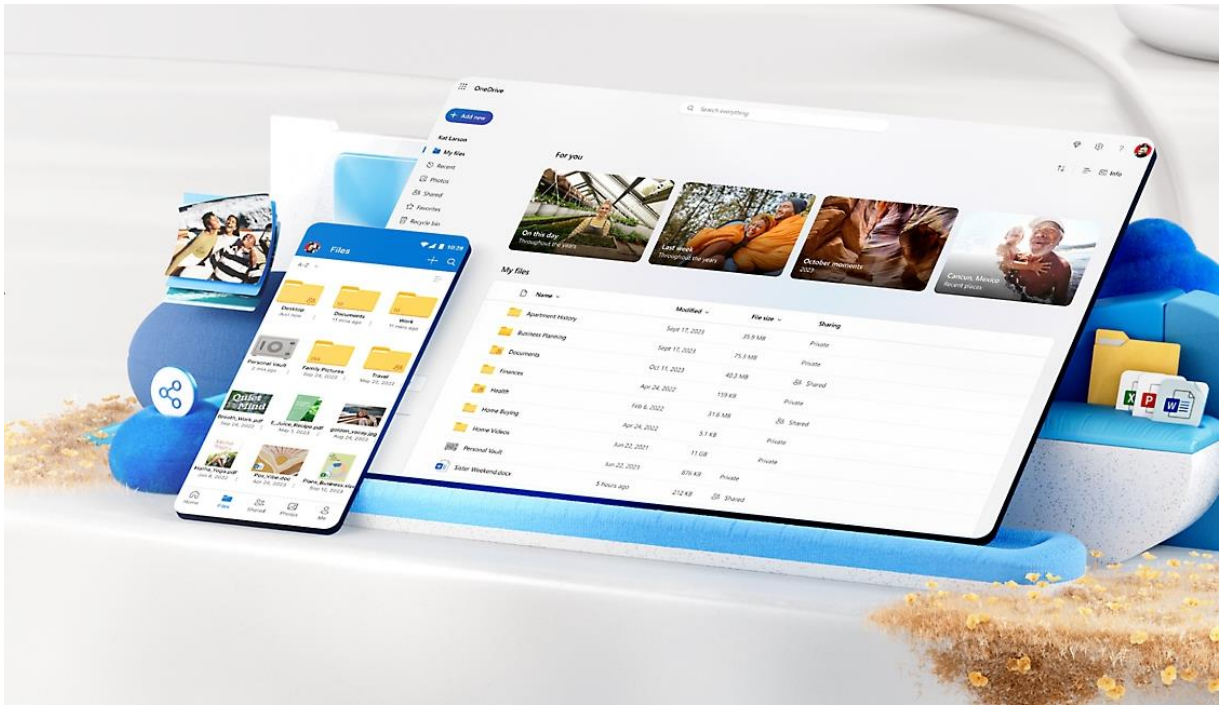
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

В. В. Сьомченко, О. Р. Саєнко

ЕЛЕКТРОННІ СЕРВІСИ ТА ДОКУМЕТООБІГ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальності «Облік і оподаткування»
освітньо-професійної програми «Облік і аудит»



Запоріжжя
2025

Міністерство освіти і науки України
Запорізький національний університет

В. В. Сьомченко, О. Р. Саєнко

ЕЛЕКТРОННІ СЕРВІСИ ТА ДОКУМЕТООБІГ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальності «Облік і оподаткування»
освітньо-професійної програми «Облік і аудит»

Затверджено
вченою радою ЗНУ
Протокол № від 2025 р.

Запоріжжя
2025

УДК 311.3:33(075.8)
С967

Сьомченко В. В., Саєнко О. Р. Електронні сервіси та документообіг : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності «Облік і оподаткування» освітньо-професійної програми «Облік і аудит». Запоріжжя : Запорізький національний університет, 2025. 151 с.

У навчальному посібнику подано програмний матеріал курсу «Електронні сервіси та документообіг»: зміст тем, питання для самоконтролю, тести, практичні завдання для самостійного виконання, перелік рекомендованої для опрацювання літератури.

Увагу акцентовано на визначенні сутності понять «документ» та «документообіг», на основних електронних сервісах і теоретико-методологічних засадах організації сучасної системи документообігу. Розглянуто теоретичні основи, технології, інструменти й методи, що забезпечують створення, обробку, передачу, зберігання та захист електронних документів, а також інтеграцію та використання сучасних електронних сервісів у процесах документообігу.

Для здобувачів ступеня вищої освіти бакалавра спеціальності «Облік і оподаткування», які навчаються за освітньо-професійною програмою «Облік і аудит».

Рецензент

О. В. Гамова, доктор економічних наук, професор, в.о. завідувача кафедри міжнародної економіки, природних ресурсів та економіки міжнародного туризму

Відповідальний за випуск

Н. М. Проскуріна, доктор економічних наук, професор, завідувач кафедри обліку та оподаткування

ЗМІСТ

Вступ…….. 5
РОЗДІЛ 1. ЦИФРОВА ТРАНСФОРМАЦІЯ ДОКУМЕНТООБІГУ ТА ЗВІТНОСТІ В УКРАЇНІ: НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ, ТЕХНОЛОГІЇ ТА СЕРВІСИ 8
ТЕМА 1. ЕВОЛЮЦІЯ ДОКУМЕНТООБІГУ: ВІД ПАПЕРОВИХ СИСТЕМ ДО ЕЛЕКТРОННИХ 8
1. Поняття та значення документа й документообігу для підприємств і організацій……...……... 8
2. Основні етапи переходу від паперових систем до електронних…..……..... 11
3. Переваги та виклики електронного документообігу……...……... 11
ТЕМА 2. ЗАКОНОДАВЧА БАЗА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ 17
1. Нормативно-правове регулювання електронного документообігу……..... 17
2. Правова значущість електронних підписів і документів……..…...… 20
ТЕМА 3. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ТА ІДЕНТИФІКАЦІЯ 27
1. Поняття електронного підпису та його види……...….. 27
2. Кваліфіковані надавачі електронних довірчих послуг……..……... 30
3. Валідація цифрового підпису. Стани повної валідації……..……... 31
4. Методи криптографії. ……...….... 32
5. Види шифрування та обмеження доступу. ……..…… 33
6. Хеш-функція та принципи її роботи……..... 37
7. Різниця цифрового й електронний підписів та варіанти їх використання……. 38
ТЕМА 4. СУЧАСНІ ЕЛЕКТРОННІ СЕРВІСИ ДЛЯ РОБОТИ З ДОКУМЕНТАМИ 43
1. Хмарні сервіси для збереження даних…….…… 43
2. Система управління електронними документами…….…… 45
3. Особливості вибору платформи для організації документообігу…… 58
ТЕМА 5. ДЕРЖАВНІ ОНЛАЙН-СЕРВІСИ У СФЕРІ ПОДАТКОВОЇ, СТАТИСТИЧНОЇ ТА ПЕНСІЙНОЇ ЗВІТНОСТІ 68
1. Електронний кабінет платника податків……...……. 68
2. Електронна звітність до Пенсійного фонду України……...……. 73
3. Взаємодія з Державною службою статистики України……...……. 80
4. Електронна система публічних закупівель Prozorro……...…... 82
5. Сервіс «Дія.Бізнес» і «Дія» як інструменти цифрової трансформації……. 84
6. Інші корисні державні електронні сервіси…….. 86
РОЗДІЛ 2. ІНТЕГРАЦІЯ ЕЛЕКТРОННИХ СЕРВІСІВ І ДОКУМЕНТООБІГУ: БЕЗПЕКА ТА ЗБЕРІГАННЯ ДАНИХ 94
ТЕМА 6. ІНТЕГРАЦІЯ ЕЛЕКТРОННИХ СЕРВІСІВ 94
1. Об’єднання документів із CRM, ERP та іншими корпоративними системами…….…… 94
2. API для інтеграції сервісів……...……..... 96
3. Приклади інтегрованих рішень для бізнесу……..…..... 97
ТЕМА 7. ОРГАНІЗАЦІЯ ЗБЕРІГАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ 104

1. Організація електронного архіву документів……. 104
2. Вимоги щодо зберігання та архівування електронних документів…….. 110
ТЕМА 8. КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ 117
1. Загальні принципи захисту даних (GDPR, Закон України «Про захист персональних даних»)……..……..…..... 117
2. Політики доступу до документів……..... 119
3. Етичні аспекти роботи з електронними сервісами……..….. 120
ТЕМА 9. ІННОВАЦІЇ В ЕЛЕКТРОННИХ СЕРВІСАХ ТА ДОКУМЕНТООБІГУ 128
1. Штучний інтелект та машинне навчання в документообігу……..…….…. 128
2. Використання Blockchain для забезпечення цілісності документів…….... 130
3. Перспективи повної цифровізації документообігу……..……..….. 133
Термінологічний словник……..…….…….. 140
Рекомендована література……..……..…… 144
Використана література……..……..……... 147
Додаток А. Методичні рекомендації до написання есе……. 149

ВСТУП

У сучасну епоху цифровізації всі сфери діяльності суспільства зазнають значних трансформацій, зокрема в організації документообігу. Перехід від традиційних паперових систем до електронних став ключовим етапом розвитку інформаційних технологій, спрямованих на підвищення ефективності роботи, зниження витрат часу та ресурсів, а також забезпечення більшої безпеки й мобільності в управлінні інформацією.

Курс «Електронні сервіси та документообіг» є обов'язковим освітнім компонентом циклу професійної підготовки освітньої програми «Облік і аудит» першого (бакалаврського) рівня.

Метою вивчення дисципліни «Електронні сервіси та документообіг» є засвоєння системи знань і набуття навичок використання сучасних електронних сервісів для організації, управління та захисту документообігу, а також опанування методами інтеграції цифрових технологій у професійну діяльність.

Предметом дисципліни «Електронні сервіси та документообіг» є вивчення теоретичних основ, технологій, інструментів і методів, що забезпечують створення, обробку, передачу, зберігання та захист електронних документів, а також інтеграцію та використання сучасних електронних сервісів у процесах документообігу.

Завдання дисципліни «Електронні сервіси та документообіг»:

− ознайомлення з особливостями системного підходу до дослідження організації як об'єкта впровадження електронного документообігу;

− розуміння основних законодавчих актів і регуляторів, що забезпечують функціонування електронного документообігу;

– засвоєння основних вимог до систем електронного документообігу;

− ознайомлення з особливостями системного підходу до побудови інформаційної моделі організації як основи ефективного впровадження електронного документообігу;

– розгляд новітніх технологій у сфері електронного документообігу, таких як блокчейн, штучний інтелект і хмарні сервіси.

Дисципліна «Електронні сервіси та документообіг» спрямована на формування у здобувачів освіти вмінь і навичок, необхідних для ефективного використання сучасних електронних сервісів і технологій у сфері документообігу.

У результаті вивчення дисципліни «Електронні сервіси та документообіг» здобувач вищої освіти має набути *таких компетентностей:*

– Здатність вчитися і оволодівати сучасними знаннями.

– Здатність до абстрактного мислення, аналізу та синтезу.

– Знання та розуміння предметної області та розуміння професійної діяльності.

– Навички використання сучасних інформаційних систем і комунікаційних технологій.

У результаті вивчення дисципліни «Електронні сервіси та документообіг» здобувач вищої освіти має набути *таких програмних результатів навчання:*

– Знати та розуміти економічні категорії, закони, причинно-наслідкові та функціональні зв'язки, які існують між процесами та явищами на різних рівнях економічних систем.

– Розуміти місце і значення облікової, аналітичної, контрольної, податкової та статистичної систем в інформаційному забезпеченні користувачів обліково-аналітичної інформації у вирішенні проблем у сфері соціальної, економічної та екологічної відповідальності підприємств.

– Володіти методичним інструментарієм обліку, аналізу, контролю, аудиту та оподаткування господарської діяльності підприємств.

– Розуміти особливості практики здійснення обліку, аналізу, контролю, аудиту та оподаткування діяльності підприємств різних форм власності, організаційно-правових форм господарювання та видів економічної діяльності.

– Застосовувати спеціалізовані інформаційні системи і комп'ютерні технології для обліку, аналізу, контролю, аудиту та оподаткування.

– Уміти застосовувати економіко-математичні методи в обраній професії.

– Аналізувати розвиток систем, моделей і методів бухгалтерського обліку на національному та міжнародному рівнях з метою обґрунтування доцільності їх запровадження на підприємстві.

Основою для опанування програмного матеріалу курсу «Електронні сервіси та документообіг» є навчальні дисципліни «Мікроекономіка» «Макроекономіка», «Економічна теорія», «Інформаційні технології в управлінні економічними системами». Своєю чергою знання основних положень електронних сервісів та документообігу необхідні для вивчення таких дисциплін, як «Інформаційні системи і технології в обліку та аудиті», «Фінансовий облік І», «Фінансовий облік ІІ», «Облік і звітність в оподаткуванні», «Управлінський облік».

У змісті навчального посібника розкрито основні принципи роботи сучасних електронних сервісів, їх інтеграції в бізнес-процеси, організації зберігання та захисту електронних документів. Розглянуто інноваційні рішення, які визначають тенденції розвитку цієї сфери, зокрема використання хмарних технологій, блокчейну та штучного інтелекту.

Посібник структурований за логікою послідовного вивчення ключових аспектів електронного документообігу. У ньому містяться як теоретичні відомості, так і практичні рекомендації, що дозволяють здобувачам освіти глибше зрозуміти специфіку сучасних інформаційних систем і підготуватися до їх ефективного використання у професійній діяльності.

Програмний матеріал курсу представлений у дев’яти темах, кожна з яких включає виклад основних теоретичних положень відповідно до питань плану, питання для самоконтролю, тести, завдання для самостійного виконання. Крім того, здобувачам освіти пропонуються питання для поглибленого вивчення кожної з тем.

Використання посібника сприятиме оволодінню базовими поняттями і концептуальними основами електронних сервісів і документообігу, набуттю необхідних умінь і навичок. Посібник стане надійним інструментом для засвоєння знань і набуття навичок, необхідних у сучасному цифровому середовищі, а також допоможе здобувачам вищої освіти адаптуватися до викликів інформаційного суспільства.

РОЗДІЛ 1. ЦИФРОВА ТРАНСФОРМАЦІЯ ДОКУМЕНТООБІГУ ТА ЗВІТНОСТІ В УКРАЇНІ: НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ, ТЕХНОЛОГІЇ ТА СЕРВІСИ

ТЕМА 1. ЕВОЛЮЦІЯ ДОКУМЕНТООБІГУ: ВІД ПАПЕРОВИХ СИСТЕМ ДО ЕЛЕКТРОННИХ

Мета: набуття цілісного уявлення про етапи розвитку систем документообігу, особливості трансформації від паперових до електронних систем; з'ясування переваг і викликів електронного документообігу; засвоєння знань і набуття навичок, необхідних для впровадження та ефективного використання сучасних електронних систем у професійній діяльності.

План

1. Поняття та значення документа й документообігу для підприємств і організацій.
2. Основні етапи переходу від паперових систем до електронних.
3. Переваги та виклики електронного документообігу.

Ключові терміни та поняття: *документ, документообіг, інформація, цифровізація, міжнародний стандарт, життєвий цикл електронного документа*.

1. Поняття та значення документа й документообігу для підприємств і організацій

Документ – це зафіксована інформація на будь-якому матеріальному носії, яка має юридичну, інформаційну або іншу значущість. Документ може бути створений у письмовій, графічній, аудіовізуальній чи цифровій формах. Його основною метою є збереження та передача інформації для забезпечення правових, організаційних, управлінських чи інших функцій.

Визначення поняття «документ» в науковому обігу:

1. Класичне визначення: за Г. А. Бочкарьовим: документ – це матеріальний об'єкт, що містить зафіксовану інформацію, яка може бути використана як доказ діяльності, події або явища. Таке визначення акцентує увагу на фізичному носії інформації.
2. Архівознавчий підхід: за О. С. Зозулею: документ – це матеріальна форма збереження й передачі інформації, яка має юридичну силу та використовується в управлінській або іншій діяльності. Це визначення підкреслює юридичну значущість документа.
3. Інформаційний підхід: за Р. С. Гіляровським: документ – це інформація, зафіксована на матеріальному або електронному носії, яка доступна для передачі та багаторазового використання. Наголос робиться на інформаційному наповненні документа незалежно від його форми.

4. Цифрове визначення: у контексті цифровізації, сучасні дослідники (наприклад, А. А. Єфремова) визначають документ як структуровану інформацію, створену, збережену й опрацьовану в електронному вигляді, яка може мати юридичну силу за умови використання електронного підпису.

5. Міжнародний стандарт (ISO 15489): документ визначається як інформація, створена, отримана чи збережена організацією або фізичною особою як свідчення про діяльність чи транзакцію.

1. Роль документа в бухгалтерському обліку.

Документ є основою бухгалтерського обліку, оскільки саме він фіксує факт господарської операції. Без документального підтвердження жодна операція не може бути відображена в облікових регістрах або фінансовій звітності.

Основні функції документа в бухгалтерії:

– інформаційна: документ відображає повну та достовірну інформацію про операцію;

– юридична: документ підтверджує легітимність здійснених операцій;

– контрольна: документи дозволяють перевірити правильність, своєчасність та законність дій працівників;

– аналітична: дані з документів використовуються для аналізу діяльності підприємства.

2. Види документів у бухгалтерському обліку:

– первинні документи: фіксують факт здійснення операції (накладні, рахунки, акти виконаних робіт);

– зведені документи: агрегують дані з первинних документів для подальшої обробки;

– регістри бухгалтерського обліку: журнали, головна книга;

– фінансова звітність: підсумкова документація, яка надається зовнішнім і внутрішнім користувачам.

3. Вимоги до бухгалтерських документів:

– юридична значущість: кожен документ має бути складений відповідно до законодавчих вимог;

– точність і достовірність: інформація має бути повною, правильною та підкріпленою доказами;

– єдність форми та змісту: документи мають мати стандартизовану структуру, яка легко піддається аналізу та перевірці.

4. Виклики в роботі з документами:

– забезпечення збереження документів упродовж строку їх дії;

– автоматизація обробки великого обсягу документів;

– перехід від паперових документів до електронного документообігу з дотриманням законодавчих вимог.

Документ є невід’ємною складовою бухгалтерського обліку, що забезпечує його прозорість, достовірність і юридичну значущість. З еволюцією інформаційних технологій документи перейшли від паперових форм до цифрових, але їх основна роль – фіксація господарських операцій –

залишається незмінною. Бухгалтерський документ не тільки є джерелом інформації, але й слугує інструментом контролю та управління ресурсами підприємства.

Документообіг – це процес створення, обробки, зберігання, передачі та використання документів в межах організації або між різними організаціями. Документообіг охоплює всі етапи «життєвого циклу» документа: від його створення до архівування або знищення.



Рисунок 1.1 – Життєвий цикл електронного документа

Значення документообігу:

- організація роботи: забезпечує системність та прозорість у роботі з інформацією;
- юридична значущість: документи підтверджують правочини, фінансові операції, виконання зобов’язань;
- прийняття рішень: швидкий доступ до інформації забезпечує ефективне управління;
- збереження історії діяльності: документи слугують архівом, який можна використовувати для аналізу чи звітування.

Види документообігу:

- внутрішній: рух документів між підрозділами однієї організації;
- зовнішній: обмін документами між організаціями, державними

органами, партнерами;

– змішаний: поєднання внутрішніх і зовнішніх процесів.

У традиційній (паперовій) формі документообіг вимагав значних ресурсів (часу, простору, витрат на матеріали). З появою електронних технологій ці процеси стали швидшими, зручнішими та дешевшими.

2. Основні етапи переходу від паперових систем до електронних

Етап 1: Ручне управління паперовими документами:

– використання фізичних носіїв: папір, архіви, сейфи;

– облік та контроль здійснювався вручну;

– основні виклики: трудомісткість, ризик втрати документів, повільна передача інформації.

Етап 2: Використання комп'ютерів для обліку паперових документів:

– початок цифровізації – створення баз даних для реєстрації паперових документів;

– автоматизація певних операцій (наприклад, облік вхідної/вихідної кореспонденції);

– однак основна частина документів залишалася в паперовому вигляді.

Етап 3: Гібридні системи документообігу:

– поява електронних документів, але частина процесів все ще виконувалася на папері;

– використання спеціалізованого програмного забезпечення для обробки документів (наприклад, текстові редактори, електронні таблиці);

– упровадження електронного підпису для окремих документів.

Етап 4: Повний перехід до електронного документообігу:

– інтеграція електронного підпису та електронної печатки;

– використання спеціалізованих платформ для управління документами (ECM – enterprise content management);

– автоматизація процесів документообігу через ERP- та CRM-системи;

– зростання популярності хмарних рішень для зберігання та обміну документами.

3. Переваги та виклики електронного документообігу

Переваги

1. Швидкість обробки документів:

– автоматичне створення, зберігання та передача документів;

– скорочення часу на підготовку та підписання угод, звітів тощо.

2. Економія ресурсів:

– зниження витрат на папір, друк, архівне зберігання;

– можливість зменшення кількості персоналу, зайнятого обробкою паперових документів.

3. Простота доступу:

– можливість роботи з документами у будь-який час і з будь-якого пристрою;

– централізоване зберігання з можливістю пошуку за ключовими

словами.

4. Юридична безпека:

- використання електронного підпису забезпечує юридичну значущість документа;
- легкість перевірки автентичності та цілісності документів.

5. Екологічність:

- скорочення використання паперу сприяє збереженню довкілля.

Виклики

1. Кібербезпека:

- захист документів від несанкціонованого доступу чи викрадення даних;
- загрози вірусів, зломів, витоку інформації.

2. Правові обмеження:

- дотримання норм і стандартів (законодавчі обмеження в різних країнах);
- необхідність адаптації до нових вимог щодо зберігання електронних документів.

3. Технічні складнощі:

- залежність від IT-інфраструктури та технічних засобів;
- потреба в навчанні персоналу новим інструментам.

4. Інтеграція з існуючими системами:

- проблеми сумісності різних платформ і програмного забезпечення;
- складність переходу від старих систем до нових.

5. Первинні витрати:

- високі витрати на впровадження програмного забезпечення, навчання працівників та адаптацію процесів.

Отже, еволюція документообігу – це неминучий процес, який забезпечує підприємствам і організаціям більшу ефективність, прозорість і адаптивність у сучасному світі. Розуміння цієї теми дає змогу оцінити важливість інвестицій у сучасні рішення та їх вплив на стратегічний розвиток компаній.

Тести

1. Що таке документ?

a) тільки паперовий носій інформації
b) зафіксована інформація на матеріальному або електронному носії
c) архівна інформація

2. Яка мета документа?

a) забезпечення конфіденційності
b) збереження та передача інформації
c) захист даних

3. Що є основою бухгалтерського обліку?

a) фінансовий звіт
b) документ
c) регістри

4. Яке визначення документа дає Г. А. Бочкарьов?

a) матеріальний об’єкт із зафіксованою інформацією, що може бути доказом діяльності

b) інформація, доступна для передачі

c) структурована електронна інформація

5. Який підхід акцентує увагу на юридичній значущості документа?

a) інформаційний

b) архівознавчий

c) цифровий

6. Що підкреслює інформаційний підхід до документа?

a) юридичну силу документа

b) фізичний носій інформації

c) інформаційне наповнення документа

7. Що є основною функцією документа в бухгалтерії?

a) фіксація господарської операції

b) захист персоналу

c) формування бюджету

8. До якого етапу переходу належить упровадження електронного підпису?

a) гібридні системи документообігу

b) ручне управління паперовими документами

c) використання комп’ютерів

9. Яка інформація є ключовою у стандарті ISO 15489?

a) документ – це паперовий архів

b**)** інформація як свідчення діяльності чи транзакції

c) захист даних

10. Що забезпечує автоматизація документообігу?

a) швидкість обробки документів

b) збереження паперових архівів

c) ускладнення юридичних процедур

11. Що є прикладом первинного документа?

a) накладна

b) зведений звіт

c) Головна книга

12. Яка функція документа пов’язана з аналізом діяльності?

a) контрольна

b) аналітична

c) інформаційна

13. Який документ фіксує факт операції?

a) зведений звіт

b) первинний документ

c) фінансова звітність

14. Який етап еволюції документообігу включає хмарні рішення?

a) використання комп’ютерів

b) гібридні системи

c) повний перехід до електронного документообігу

15. Що є ключовим викликом електронного документообігу?

a) економія ресурсів

b) кібербезпека

c) простота використання

16. Яка перевага електронного документообігу пов'язана з екологічністю?

a) скорочення використання паперу

b) підвищення юридичної значущості

c) використання фізичних архівів

17. Що є юридичною основою електронного документа?

a) електронний підпис

b) печатка

c) архівування

18. Що охоплює документообіг?

a) увесь життєвий цикл документа

b) лише збереження документа

c) тільки створення документів

19. Який вид документообігу включає обмін з іншими організаціями?

a) внутрішній

b) зовнішній

c) змішаний

20. Що є викликом при інтеграції електронного документообігу?

a) скорочення часу обробки

b) сумісність платформ

c) збільшення обсягів документів

21. Яка вимога до бухгалтерського документа забезпечує відповідність законодавству?

a) точність

b) юридична значущість

c) єдність форми

22. Що включає етап ручного управління документами?

a) використання баз даних

b) електронний підпис

c) архіви та сейфи

23. Який підхід акцентує увагу на створенні структурованої електронної інформації?

a) архівознавчий

b) цифровий

c) класичний

24. Що є основною перевагою хмарних рішень?

a) простота доступу до документів

b) збільшення витрат

c) захист паперових архівів

25. Що є метою зведеного документа?

a) агрегація даних

b) архівування
c) захист інформації

26. Що є прикладом регістра бухгалтерського обліку?

a) Головна книга
b) накладна
c) звіт про фінанси

27. Який етап включає впровадження ERP-систем?

a) ручне управління
b) повний перехід до електронного документообігу
c) використання комп'ютерів

28. Що таке внутрішній документообіг?

a) рух документів між підрозділами однієї організації
b) обмін документами з іншими організаціями
c) зберігання архівів

29. Яка вимога до документа забезпечує зручність аналізу?

a) юридична значущість
b) єдність форми та змісту
c) точність

30. Яка основна мета фінансової звітності?

a) формування внутрішніх наказів
b) надання зовнішнім і внутрішнім користувачам узагальненої інформації про фінансовий стан підприємства
c) архівування документів.

Завдання для мозкового штурму до теми 1 «Еволюція документообігу: від паперових систем до електронних»

Завдання 1. «Порівняння паперових та електронних систем документообігу»

Учасники розподіляються на дві групи. Завдання для першої групи: назвати переваги та недоліки паперової системи документообігу. Завдання для другої групи: назвати переваги та виклики електронної системи документообігу. Після обговорення кожна група презентує результати, а потім разом формулюють висновки.

Завдання 2. «Етапи еволюції документообігу»

Визначити ключові етапи переходу від паперових систем до електронних. Запропонувати можливі причини, які спонукали до змін на кожному етапі. Обговорити, які труднощі могли виникнути на кожному з етапів.

Завдання 3. «Майбутнє документообігу»

Уявити, що документообіг через 10 років зазнав кардинальних змін.

На основі цих змін запропонувати нові можливості та технології, які можуть змінити документообіг у майбутньому. Обговорити, які ризики можуть виникнути з новими технологіями.

Завдання 4. «Роль документів на підприємстві»

Обговорити, які функції виконують документи в сучасній організації (управління, юридична, інформаційна тощо).

Запропонувати ситуації, в яких відсутність належного документообігу може призвести до проблем на підприємстві.

Завдання 5. «Електронний документообіг: за і проти»

Учасники розподіляються на дві групи: «За електронний документообіг» і «Проти електронного документообігу».

Кожна група формулює аргументи на підтримку своєї позиції.

Проводиться дискусія, після якої всі разом визначають основні висновки.

? Питання для самоконтролю

1. Що таке документообіг? Які основні етапи він охоплює?
2. Які функції виконують документи в діяльності підприємства?
3. Чим відрізняється паперовий документообіг від електронного? Назвіть основні переваги кожного.
4. Які етапи еволюції документообігу можна виділити? Які ключові зміни відбулися на кожному з них?
5. Що таке електронний документ? Які вимоги забезпечують його юридичну значущість?
6. Які переваги електронного документообігу порівняно з традиційним паперовим?
7. Які виклики стоять перед підприємствами, що впроваджують електронний документообіг?
8. Як сучасні інформаційні технології впливають на документообіг? Наведіть приклади.
9. Які види документообігу існують залежно від напрямку руху документів?
10. Які ключові ризики необхідно враховувати при переході від паперової системи до електронної?

Питання для поглибленого вивчення теми 1 «Еволюція документообігу: від паперових систем до електронних»

1. Роль документа в управлінському та бухгалтерському обліку: еволюція та сучасні виклики.
2. Порівняння паперових і електронних систем документообігу: переваги та недоліки в контексті підприємницької діяльності.
3. Етапи розвитку документообігу в організаціях: від ручного до автоматизованого управління документами.
4. Значення юридичної сили електронних документів: аналіз сучасних нормативно-правових актів.

5. Автоматизація документообігу: основні технології та їх вплив на ефективність організацій.

6. Виклики електронного документообігу в умовах цифрової трансформації підприємств.

7. Захист інформації в електронному документообігу: проблеми кібербезпеки та шляхи їх вирішення.

8. Вплив хмарних технологій на документообіг: нові можливості та ризики для бізнесу.

9. Перехід від паперових до електронних архівів: досвід та перспективи для організацій.

10. Інтеграція електронного документообігу з іншими бізнес-системами: переваги та проблеми адаптації.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 2. ЗАКОНОДАВЧА БАЗА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Мета: усвідомлення особливостей нормативно-правового регулювання електронного документообігу на національному та міжнародному рівнях; ознайомлення з основними законами, стандартами та вимогами, що регламентують створення, обробку, зберігання та захист електронних документів.

План

1. Нормативно-правове регулювання електронного документообігу.
2. Правова значущість електронних підписів та документів.

Ключові терміни та поняття: *електронний документообіг, законодавчі акти, нормативні документи, міжнародні стандарти, електронний підпис, архівування та зберігання, цілісність документа, ідентифікація учасників, кібербезпека*.

1. Нормативно-правове регулювання електронного документообігу

Нормативно-правове регулювання електронного документообігу є ключовим аспектом для забезпечення юридичної значущості та безпеки електронних документів. Це питання охоплює нормативні акти, які регулюють процес створення, обробки, зберігання та передачі документів в електронному вигляді, а також гарантують їх юридичну силу в різних юрисдикціях.

1) Законодавче визначення електронного документообігу

Електронний документообіг – це сукупність процесів створення, зберігання, обробки, передачі, підписання та архівування документів в електронній формі. Для того щоб ці документи мали юридичну силу, потрібно

дотримуватись низки вимог, які визначають їх правовий статус.

2) Основні законодавчі акти та нормативні документи

1. Законодавство про електронний підпис та цифрові підписи:

Закон України «Про електронний цифровий підпис» (2003 р.): цей закон визначає порядок використання електронного підпису, що є ключовим елементом електронного документообігу. Він надає юридичну силу електронним документам, підписаним таким підписом. Цей законодавчий акт діяв до листопада 2018 р.

Основні положення закону:

– визначення електронного підпису як криптографічного підпису, що підтверджує факт підписання електронного документа;

– встановлення принципу «кваліфікованого електронного підпису» який має таку ж юридичну силу, як і власноручний підпис;

– процедури та правила сертифікації підписів і створення довірчих послуг;

– організації, що надають послуги електронного підпису, повинні бути акредитовані відповідними органами.

Із листопада 2017 року окремими положеннями, а з листопада 2018 року повністю набрав чинності Закон України «Про електронні довірчі послуги» № 2155-VIII. Із 7 грудня 2022 року назва закону доповнена та викладена в такій редакції «Про електронну ідентифікацію та електронні довірчі послуги». Закон регулює питання, пов’язані з використанням електронної ідентифікації та довірчих послуг у сфері електронних комунікацій і взаємодії між громадянами, бізнесом та державними органами.

Закон регламентує:

– встановлює вимоги до систем і засобів, які забезпечують ідентифікацію осіб в електронному середовищі (наприклад, через електронний підпис, електронні паспорти тощо).

– визначає види довірчих послуг, таких як електронний підпис, електронна печатка, електронні часові позначки, сертифікація ключів тощо, а також правила їх надання і використання.

– встановлює вимоги до провайдерів електронних довірчих послуг і органів сертифікації, визначає порядок ліцензування та моніторингу їх діяльності.

– гарантує правову силу та юридичну значущість електронних документів, підписів та інших довірчих послуг, створюючи механізм їх захисту від підробок і забезпечуючи збереження даних.

– передбачає інтеграцію української системи електронної ідентифікації з міжнародними стандартами, що дозволяє здійснювати електронні операції між країнами.

Закон сприяє розвитку електронної економіки, покращує рівень безпеки в електронних комунікаціях та створює правові умови для інтеграції цифрових технологій у повсякденне життя.

Міжнародні стандарти електронного підпису, такі як **eIDAS**

(Європейський регламент щодо електронної ідентифікації та довірчих послуг), визначають міжнародний порядок використання електронних підписів.

Основні положення eIDAS:

– визнання електронного підпису у всіх країнах ЄС, незалежно від країни, де він був створений;

– визначення трьох типів електронного підпису: простий, кваліфікований та вдосконалений, залежно від рівня захисту та юридичної сили;

– порядок використання кваліфікованих електронних підписів для забезпечення юридичної сили документів в електронному вигляді.

2. Закон про документообіг.

Закон України «Про електронні документи та електронний документообіг» (2003 р.): встановлює правові основи для використання електронних документів у різних сферах діяльності, зокрема в організаціях та підприємствах. Це законодавчий акт, який дозволяє застосовувати електронні документи так само, як і паперові.

Основні положення закону:

– визначення юридичної сили електронних документів;

– принципи та умови, за яких електронний документ має таку ж юридичну силу, як паперовий;

– визначення процедур для зберігання електронних документів та їх архівування;

– порядок обміну електронними документами між організаціями, державними установами, юридичними та фізичними особами.

3. Нормативні акти щодо архівування та зберігання електронних документів.

Закон України «Про Національний архівний фонд та архівні установи» № 3814-XII регулює умови зберігання та доступу до архівних документів, включаючи електронні.

Державні стандарти (ДСТУ), що визначають вимоги до формату, зберігання, та доступу до електронних документів, як на рівні держави, так і на рівні підприємств.

4. Міжнародні стандарти та регламенти.

ISO 15489 «Інформаційні та документаційні послуги. Документообіг та архіви» – міжнародний стандарт, що регулює методи та принципи управління електронними документами та їх архівування.

eIDAS (Європейський регламент щодо електронної ідентифікації та довірчих послуг) забезпечує правову основу для використання електронного підпису та електронних документів у Європейському Союзі.

3) Юридична значущість електронних документів

Для того, щоб електронний документ мав юридичну силу, він повинен відповідати певним вимогам:

Електронний підпис: наявність кваліфікованого електронного підпису гарантує, що підписаний документ є автентичним і підтверджує волю підписанта.

Цілісність документа: документ не повинен бути змінений після підписання, що забезпечується технологією криптографічного захисту.

Ідентифікація учасників: законодавство визначає, як організації та фізичні особи можуть підтверджувати свою особистість за допомогою електронних засобів.

4) Виклики та проблеми нормативно-правового регулювання

1) Різноманіття стандартів та технологій: на національному та міжнародному рівнях існує кілька різних стандартів для електронного документообігу. Це може спричиняти проблеми сумісності та інтеграції різних систем.

2) Адаптація до технологічних змін: швидкий розвиток цифрових технологій може призводити до того, що існуючі закони та нормативні акти стають застарілими.

3) Правові аспекти кібербезпеки: забезпечення захисту електронних документів від кібератак є важливим завданням для правового регулювання. Наявність належних законів щодо захисту даних має вирішальне значення для стабільності електронного документообігу.

4) Міжнародне регулювання: хоча існують міжнародні стандарти, країни можуть мати різні підходи до визначення юридичної сили електронних документів, що може призводити до труднощів при міжкрайньому обміні інформацією.

5) Перспективи розвитку нормативно-правового регулювання

1) Єдині міжнародні стандарти: зростаюча глобалізація вимагає гармонізації норм на міжнародному рівні, зокрема у питаннях електронного підпису та документів.

2) Інтеграція новітніх технологій: законодавство повинно адаптуватися до нових технологій, таких як блокчейн та штучний інтелект, для поліпшення безпеки та ефективності електронного документообігу.

Отже, нормативно-правове регулювання електронного документообігу є основою для забезпечення правової сили електронних документів, гарантії їх автентичності та захисту інформації в умовах цифрової трансформації. Однак для успішного розвитку цієї сфери необхідно адаптувати існуючі закони до новітніх технологій та міжнародних стандартів.

2. Правова значущість електронних підписів та документів

Електронні документи мають юридичну силу за умови, що вони відповідають вимогам законодавства щодо їх створення, підписання та зберігання. Важливою умовою є використання кваліфікованого електронного підпису, що забезпечує автентичність документа та його юридичну силу.

Юридична сила електронних документів: законодавство гарантує, що електронні документи, підписані кваліфікованим електронним підписом, мають таку ж юридичну силу, як і паперові документи, якщо їх визнано законними.

Ідентифікація підписанта: для того щоб документ мав юридичну силу, підписант повинен бути правильно ідентифікований. Це забезпечується через кваліфіковані підписи, які використовують криптографічні методи для захисту даних і підтвердження особи.

Переваги електронних підписів та документів:

– захист автентичності та цілісності: електронний підпис гарантує, що документ не був змінений після його підписання, що дозволяє уникнути шахрайства;

– швидкість обробки документів: процеси підписання та обміну електронними документами значно швидші порівняно з паперовим документообігом;

– зниження витрат: використання електронних документів зменшує витрати на папір, друк, поштові послуги та зберігання паперових архівів;

– зручність зберігання та доступу: електронні документи можна зберігати в електронному вигляді, що зменшує потребу в фізичних архівах і забезпечує швидкий доступ до необхідних файлів.

Виклики і проблеми в правовому регулюванні:

– невизначеність стандартів: різноманіття стандартів для електронного підпису може створювати проблеми інтеграції в міжнародних або міжурядових контекстах;

– правові складнощі при переході на електронний документообіг: перехід від паперових до електронних систем документообігу може бути складним, оскільки для цього потрібно змінити законодавство, а також процедури, що включають підписання та зберігання документів;

– кібербезпека: впровадження електронних підписів та документів підвищує необхідність у забезпеченні безпеки даних від хакерських атак і несанкціонованого доступу.

Таблиця 2.1 – Типи загроз кібербезпеки

Загрози кібербезпеки	Характеристика загроз
Програми-вимагачі	Це різновид шкідливого програмного забезпечення. Вони призначені для вимагання грошей за допомогою блокування доступу до файлів комп'ютерної системи до надходження викупу. Перерахування викупу не гарантує відновлення файлів або працездатності системи.
Шкідливе програмне забезпечення	Шкідливе програмне забезпечення призначене для отримання несанкціонованого доступу або пошкодження комп'ютерної системи.
Соціальна інженерія	Це тактика, яку використовують зловмисники, щоб схилити користувача до розкриття конфіденційної інформації. Вони можуть звернутися з проханням про грошові платежі або про отримання доступу до конфіденційних даних. Способи соціальної інженерії можуть застосовуватися разом із погрозами будь-якого з перерахованих вище типів.
Фішинг	Це розсилка підробленої електронної кореспонденції, яка виглядає як повідомлення від надійних джерел. Метою є крадіжка конфіденційних даних, таких як номери кредитних карт та інформація про облікові записи. Це найпоширеніший тип кібератак. Забезпечити захист можна за допомогою вивчення необхідної інформації або установки технологічних рішень, які можуть відфільтрувати шкідливі електронні листи.

Перспективи розвитку законодавства щодо електронних документів:

– інтеграція з новітніми технологіями: законодавство повинно адаптуватися до нових технологій, таких як блокчейн, для забезпечення більш високого рівня безпеки та надійності електронних підписів і документів;

– єдині міжнародні стандарти: зростаюча потреба в міжнародній взаємодії вимагає гармонізації стандартів електронного документообігу для забезпечення безперешкодного обміну електронними документами між різними країнами.

Тести

1. Що таке електронний документообіг?

a) виключно процес підписання документів електронним підписом

b) тільки процес архівування електронних документів

c) сукупність процесів створення, зберігання, обробки, передачі, підписання та архівування документів в електронній формі

2. Який документ регулює порядок використання електронного підпису в Україні?

a) Закон України «Про електронні документи та електронний документообіг»

b) Закон України «Про електронний цифровий підпис»

c) Закон України «Про захист інформації»

3. Що визначає законодавство про електронний документообіг?

a) вимоги до друку та архівування паперових документів

b) правові основи для використання електронних документів у різних сферах

c) правила використання цифрових підписів у звичайних документах

4. Яким чином визначається юридична сила електронного документа?

a) якщо документ зберігається на серверах підприємства

b) якщо він підписаний кваліфікованим електронним підписом

c) якщо він містить електронний штамп організації

5. Яка організація регулює надання послуг електронного підпису в Україні?

a) Державна архівна служба України

b) Міністерство внутрішніх справ України

c) органи, що акредитовані для сертифікації підписів

6. Який міжнародний стандарт визначає порядок використання електронних підписів у ЄС?

a) eIDAS (європейський регламент щодо електронної ідентифікації та довірчих послуг)

b) ISO 15489

c) IETF (internet engineering task force)

7. Який стандарт визначає вимоги до архівування та зберігання електронних документів?

a) ДСТУ 8341

b) ISO 15489

c) ISO 9001

8. Що є основною вимогою для забезпечення цілісності електронного документа?

a) регулярне оновлення програмного забезпечення

b) перевірка документа на наявність помилок

c) використання криптографічного захисту та цифрового підпису

9. Які проблеми можуть виникнути через різноманіття стандартів для електронного документообігу?

a) підвищення рівня безпеки

b) легкість у впровадженні електронного документообігу

c) проблеми сумісності та інтеграції систем

10. Які переваги має використання електронних документів порівняно з паперовими?

a) швидкість обробки та зниження витрат

b) підвищення витрат на зберігання

c) потреба в більшій кількості фізичних архівів

11. Які вимоги до зберігання електронних документів можуть бути визначені законодавством?

a) строки зберігання документів

b) місце зберігання документів на фізичних носіях

c) вимоги до розміру електронних документів

12. Що гарантує кваліфікований електронний підпис?

a) виключно захист від втрати даних

b) автентичність і юридичну силу документа

c) сумісність документа з міжнародними стандартами

13. Що означає принцип «цілісності електронних документів»?

a) документ має містити додаткові цифрові підписи

b) документ повинен бути завжди доступний для редагування

c) документ не повинен бути змінений після його підписання

14. Як забезпечується захист електронних документів від несанкціонованого доступу?

a) використанням лише базових паролів

b) за допомогою шифрування та контролю доступу

c) через доступ до документів лише в робочих годинах

15. Що має бути забезпечено для підтримки юридичної сили електронного документа?

a) фізичний підпис документа

b) кваліфікований електронний підпис та відповідність вимогам зберігання

c) надання документа в паперовому вигляді

16. Що передбачає впровадження новітніх технологій у сферу електронного документообігу?

a) адаптацію законодавства до технологій, таких як блокчейн

b) лише розширення електронних підписів

c) випуск нових форматів документів

17. Що означає резервне копіювання електронних документів?

a) створення додаткових копій документів для їх збереження

b) збереження тільки однієї копії документа

c) випадкове зберігання документів без копій

18. Що включає в себе процес знищення електронних документів?

a) використання методів стирання даних або фізичного знищення носіїв

b) архівування документа на невизначений термін

c) переведення документа в інший формат

19. Що є основною проблемою, пов'язаною з різноманіттям стандартів електронного документообігу?

a) зниження якості документів

b) проблеми інтеграції в міжнародних контекстах

c) збільшення кількості паперових документів

20. Як організації повинні адаптуватися до швидкого розвитку технологій в електронному документообігу?

a) використовувати старі формати зберігання документів

b) відмовитися від упровадження нових технологій

c) переглядати та оновлювати законодавство відповідно до нових технологій.

Завдання для мозкового штурму до теми 2 «Законодавча база електронного документообігу»

Завдання 1. Як можна інтегрувати сучасні технології для автоматизації електронного документообігу в організації?

Які інструменти можуть бути використані для автоматизації процесів створення, підписання та архівування документів?

Як зменшити витрати та час, необхідний для виконання цих процесів?

Завдання 2. Які основні проблеми можуть виникнути під час упровадження електронного документообігу в організації?

Які технологічні чи організаційні труднощі можуть виникнути при переході на електронний документообіг?

Як можна подолати опір персоналу до змін?

Завдання 3. Як підвищити рівень безпеки в електронному документообігу організації?

Які методи захисту інформації (шифрування, цифрові підписи, багаторівнева автентифікація) є найефективнішими для запобігання несанкціонованому доступу до документів?

Як забезпечити захист електронних документів при їх передачі по мережах?

Завдання 4. Як визначити, який тип електронного підпису підходить для різних типів документів в організації?

Які документи потребують кваліфікованого електронного підпису, а які

можуть бути підписані простим електронним підписом?

Як вибір підпису впливає на юридичну силу документа?

Завдання 5. Які переваги та недоліки використання хмарних сервісів для зберігання електронних документів?

Які сервіси є найбільш популярними для зберігання та обміну електронними документами в хмарі?

Як забезпечити безпеку та конфіденційність даних, зберігаючи документи в хмарі?

Завдання 6. Як можна забезпечити довгострокове зберігання електронних документів відповідно до стандартів та вимог законодавства?

Які чинники треба врахувати при виборі засобів для зберігання та архівування електронних документів?

Як часто потрібно перевіряти доступність і цілісність архівованих документів?

Завдання 7. Як можна ефективно управляти доступом до електронних документів для різних категорій співробітників організації?

Які інструменти та системи доступу можна використовувати для управління ролями та правами доступу?

Як правильно налаштувати доступ до конфіденційних документів і забезпечити, щоб тільки авторизовані особи мали до них доступ?

Завдання 8. Які є альтернативи традиційному паперовому документообігу? Як вони можуть змінити роботу організації?

Як впровадження електронних документів змінить структуру комунікації в компанії?

Чи можна зберігати всі внутрішні документи в електронному вигляді без необхідності їх фізичного зберігання?

Завдання 9. Як забезпечити відповідність електронного документообігу міжнародним стандартам і вимогам?

Які міжнародні стандарти повинні бути враховані при впровадженні електронного документообігу?

Як інтегрувати систему електронного документообігу з іншими країнами чи міжнародними організаціями?

Завдання 10. Як оцінити ефективність впровадження електронного документообігу в організації?

Які критерії та показники варто використовувати для оцінки результатів?

Як виміряти економічну ефективність і скорочення часу на обробку документів?

Завдання 11. Як підвищити ефективність електронного документообігу?

Як підвищити інтеграцію між різними інформаційними системами для поліпшення ефективності електронного документообігу?

Які можливості для оптимізації процесів документообігу надає використання технологій штучного інтелекту та машинного навчання?

? Питання для самоконтролю

1. Що таке електронний документообіг? Які основні етапи його впровадження в організаціях?
2. Які нормативно-правові акти регулюють електронний документообіг в Україні?
3. Які вимоги щодо юридичної значущості електронних документів визначає Закон України «Про електронні документи та електронний документообіг»?
4. Що таке кваліфікований електронний підпис? Як він забезпечує юридичну силу електронного документа?
5. Які основні положення регламенту eIDAS і як вони впливають на міжнародний обіг електронних документів?
6. Які проблеми можуть виникати через різноманіття стандартів для електронного підпису на національному та міжнародному рівнях?
7. Які вимоги до зберігання електронних документів визначають законодавство та стандарти?
8. Які технології використовуються для захисту електронних документів від несанкціонованого доступу та забезпечення їх цілісності?
9. Які перспективи розвитку нормативно-правового регулювання електронного документообігу з урахуванням новітніх технологій, таких як блокчейн та штучний інтелект?

Питання для поглибленого вивчення теми 2 «Законодавча база електронного документообігу»

1. Вплив автоматизації процесів електронного документообігу на ефективність роботи організацій.
2. Аналіз сучасних підходів до безпеки електронних документів в умовах кіберзагроз.
3. Інтеграція хмарних технологій у систему електронного документообігу: переваги та недоліки.
4. Ефективність використання електронного підпису для юридично значущих документів у різних країнах.
5. Розробка моделі для прогнозування ефективності впровадження електронного документообігу в організаціях різного масштабу.
6. Юридичні аспекти та стандартизація електронного документообігу в міжнародних організаціях.

7. Механізми і методи забезпечення довготривалого зберігання електронних документів згідно з нормативними вимогами.

8. Роль штучного інтелекту в автоматизації обробки електронних документів і прийнятті рішень.

9. Аналіз соціальних та економічних наслідків впровадження електронного документообігу на підприємствах.

10. Економічні та екологічні переваги переходу від паперового до електронного документообігу в державних установах.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 3. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ТА ІДЕНТИФІКАЦІЯ

Мета: ознайомлення з концепцією електронного цифрового підпису (ЕЦП); усвідомлення його ролі в забезпеченні автентичності, цілісності та юридичної значущості електронних документів; засвоєння методів ідентифікації користувачів в інформаційних системах.



План

1. Поняття електронного підпису та його види.
2. Кваліфіковані надавачі електронних довірчих послуг.
3. Валідація цифрового підпису. Стани повної валідації.
4. Методи криптографії.
5. Види шифрування та обмеження доступу.
6. Хеш-функція та принципи її роботи.
7. Різниця цифрового й електронного підписів та варіанти їх використання.



Ключові терміни та поняття: *електронний цифровий підпис, ідентифікація підписувача, гарантія цілісності, юридична значимість, удосконалений електронний підпис, кваліфікований електронний підпис, надавачі електронних довірчих послуг, валідація підпису, криптографія, шифрування, автентифікація, цифрові сертифікати.*

1. Поняття електронного підпису та його види

Електронний цифровий підпис (ЕЦП) – набір цифрових даних, отриманих на основі електронного документа за допомогою алгоритмів криптографічного перетворення з використанням закритого ключа користувача. ЕЦП являє собою цифровий відбиток певного документа, який, з одного боку, дозволяє переконатися у відсутності спотворень в оригінальному документі, а з іншого – однозначно встановити відповідність цифрового підпису певному

відкритому сертифікату. Завдяки цим своїм властивостям ЕЦП застосовується для заміни рукописного підпису в системах електронної звітності.

Із 3 листопада 2018 року, коли вступив у силу Закон України «Про електронні довірчі послуги», загальноприйнятим став термін «кваліфікований електронний підпис» (КЕП). ЕЦП – це електронний цифровий підпис. Цей термін використовувався до листопада 2018 року. З технічної точки зору між КЕП і ЕЦП різниці немає.

Для застосування ЕЦП особі – власнику підпису генеруються два ключі – особистий (секретний) і відкритий. Ключі становлять пару, тобто один створюється за криптографічним алгоритмом за допомогою іншого.

За допомогою спеціального програмного забезпечення особистим ключем проводиться криптографічне перетворення над цифровою послідовністю, що одержана на основі електронного документа, який підписується. В результаті формується цифрова послідовність, що і являє собою ЕЦП. Підпис зберігається разом з електронним документом, на який був накладений.

Основні функції електронного підпису:

- ідентифікація підписувача – підтвердження особи, яка створила підпис;
- гарантія цілісності – захист від змін після підписання документа;
- юридична значимість – електронний підпис має таку ж силу, як і власноручний підпис, якщо використовується відповідно до законодавства.

Для перевірки ЕЦП документа особа, яка його читає або використовує, має отримати відкритий ключ автора (власника) підпису. Відкритий ключ має бути доступний для всіх зацікавлених у перевірці ЕЦП осіб.

Відкритий ключ поширюється в електронному сертифікаті відкритого ключа. Сертифікат слугує надійним засобом зберігання інформації про власника ключа.

Спеціальне програмне забезпечення за допомогою відкритого ключа проводить зворотне криптографічне перетворення над цифровою послідовністю ЕЦП. У результаті виробляється цифрова послідовність, що відповідає відбитку тексту підписаного документа. ПЗ виробляє відбиток (геш) від тексту документа і порівнює його з отриманим при перетворенні ЕЦП. За умови повного збігу перевірка вважається позитивною – і текст документа, і підпис справжні.

Виокремлюють такі види електронного підпису:

1. ЕЦП – простий електронний цифровий підпис, для якого характерний низький рівень довіри. Проте у листопаді 2018 року даний тип підпису втратив чинність та остаточно замінений на КЕП:

- це дані в електронній формі, які використовуються для ідентифікації підписувача (наприклад, введення пароля, ПІН-коду або електронної пошти);
- має низький рівень безпеки та юридичну силу лише у простих ситуаціях.

2. УЕП – удосконалений електронний підпис, створений з використанням криптографічного перетворення даних. У випадку, якщо в документ, підписаний УЕП, відбулося втручання, це вдасться виявити:

- створюється за допомогою криптографічних методів, забезпечує

унікальність підпису, пов’язаний із підписувачем і даними документа;

– гарантує цілісність документа, але не завжди вимагає сертифікації акредитованим центром.

3. КЕП – кваліфікований електронний підпис, який є аналогічним до УЕП, але додатково відповідає таким критеріям:

– найбільш захищений вид підпису;

– створюється за допомогою засобів криптографічного захисту й засвідчується сертифікатом, виданим акредитованим центром сертифікації ключів;

– має повну юридичну силу, прирівнюється до власноручного підпису.

У таблиці 3.1 наведено порівняльну характеристику електронних підписів.

Таблиця 3.1 – Порівняння видів електронного підпису

Параметр	ЕЦП	УЕП	КЕП
Рівень безпеки	Низький	Середній	Високий
Юридична сила	Локальне використання	Часткова	Повна
Необхідність сертифіката	Ні	Не завжди	Так
Використання	Звичайні операції	Бізнес, документообіг	Державні, юридичні дії

Завдяки використанню КЕП користувачі, що застосовують ЕДО в своїй роботі, отримують низку переваг, а саме:

– можливість укладати угоди швидко та без необхідності особистих зустрічей, що особливо важливо в умовах карантинних обмежень та допомагає диджиталізації внутрішніх процесів компаній;

– високу юридичну силу підписаного електронного документа, що за своєю значущістю прирівнюється до паперового з власноручним підписом;

– конфіденційність інформації завдяки використанню сервісів ЕДО, які не просто забезпечують обмін документами, а й зашифровують їх таким чином, що доступ до них отримує лише особа з ключем;

– можливість легко перевірити достовірність КЕП, яким було підписано електронний документ, та цілісність такого документа на офіційному сайті Центрального засвідчувального органу;

– оптимізацію та вдосконалення бізнес-процесів завдяки зменшенню кількості документації на папері та необхідності вносити дані вручну.

Саме тому КЕП обирають всі підприємці-користувачі ЕДО, які готові рухатися в ногу з часом та використовувати можливості сучасних технологій. Серед них, зокрема, і користувачі найсучаснішого сервісу електронного документообігу Signy, що дозволяє за лічені хвилини підписати документ, надіслати його своєму контрагенту та отримати підписаний ним документ назад.

Таким чином, електронний підпис є універсальним інструментом для підтвердження правочинності електронних документів, а вибір його виду залежить від потреб безпеки та юридичної значимості.

2. Кваліфіковані надавачі електронних довірчих послуг

Центральний засвідчувальний орган впроваджує, підтримує в актуальному стані та публікує на своєму офіційному веб-сайті Довірчий список, в якому міститься інформація про кваліфікованих надавачів електронних довірчих послуг (табл. 3.2) разом з інформацією про кваліфіковані електронні довірчі послуги, які вони надають.

Довірчий список повинен впроваджуватися, підтримуватися в актуальному стані та публікуватися в безпечному режимі з обов'язковим додаванням електронної печатки центрального засвідчувального органу у вигляді, придатному для автоматичної обробки. Інформація, що міститься у Довірчому списку, є відкритою. Обов'язкові вимоги до Довірчого списку встановлюються Кабінетом Міністрів України.

Порядок ведення Довірчого списку затверджується головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг.

Таблиця 3.2 – Кваліфіковані надавачі електронних довірчих послуг

№	Назва юридичної особи	Назва кваліфікованого надавача електронних довірчих послуг
1	Акціонерне товариство комерційний банк «ПРИВАТБАНК»	Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ «ПРИВАТБАНК»
2	Військова частина 2428	Кваліфікований надавач електронних довірчих послуг «Військова частина 2428» Державної прикордонної служби України
3	Генеральний штаб Збройних Сил України	Кваліфікований надавач електронних довірчих послуг «Центр сертифікації ключів Збройних Сил України»
4	Офіс Генерального прокурора	Кваліфікований надавач електронних довірчих послуг органів прокуратури України
5	Державна казначейська служба України	Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України
6	Державне підприємство «Оператор ринку»	Кваліфікований надавач електронних довірчих послуг «АЦСК ринку електричної енергії»
7	Державне підприємство «ДІЯ»	Кваліфікований надавач електронних довірчих послуг «ДІЯ»
8	Державне підприємство «Українські спеціальні системи»	Кваліфікований надавач електронних довірчих послуг Державного підприємства «Українські спеціальні системи»
9	Інформаційно-довідковий департамент ДПС	Кваліфікований надавач електронних довірчих послуг Інформаційно-довідкового департаменту ДПС
10	Міністерство внутрішніх справ України	Кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів МВС України
11	Національний банк України	Кваліфікований надавач електронних довірчих послуг «Акредитований центр сертифікації ключів Національного банку України»
12	Акціонерне товариство	Кваліфікований надавач електронних довірчих

	«Державний ощадний банк України»	послуг – центр сертифікації ключів акціонерного товариства «Державний ощадний банк України»
13	Акціонерне товариство «УкрСиббанк»	Кваліфікований надавач електронних довірчих послуг АТ «УКРСИББАНК»
14	Товариство з обмеженою відповідальністю «Алтерсайн»	Кваліфікований надавач електронних довірчих послуг АЦСК «eSign» ТОВ «Алтерсайн»
15	Товариство з обмеженою відповідальністю «Art master»	Кваліфікований надавач електронних довірчих послуг «MASTERKEY»
16	Товариство з обмеженою відповідальністю «Інтер-Метл»	Кваліфікований надавач електронних довірчих послуг «АЦСК ТОВ Інтер-Метл»
17	Товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна»	Кваліфікований надавач електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
18	Філія «Головний інформаційно-обчислювальний центр» акціонерного товариства «Українська залізниця»	Кваліфікований надавач електронних довірчих послуг ЦСК АТ «УКРЗАЛІЗНИЦЯ»
19	Товариство з обмеженою відповідальністю «ДЕПОЗИТ САЙН»	Кваліфікований надавач електронних довірчих послуг «ДЕПОЗИТ САЙН»
20	Товариство з обмеженою відповідальністю «Ілайф»	Кваліфікований надавач електронних довірчих послуг «eSign» ТОВ «Ілайф»

3. Валідація цифрового підпису. Стани повної валідації

Валідація підпису *(signature validation)* – процес верифікації та підтвердження того, що підпис валідний.

Валідація завжди починається з процесу валідації підпису, що забезпечує довготривалу доступність та цілісність матеріалу валідації.

Одним із перших етапів цього процесу є запуск процесу для підписів із часом та підписів з матеріалами для довгострокової перевірки, які знову запустять процес для базових підписів. Фактично, валідація виконується за життєвим циклом підпису і оцінює стан підпису на основі процесу валідації для першого класу підпису цього життєвого циклу (базовий підпис). Якщо цей процес не призводить до остаточного висновку про валідацію (позитивну чи негативну), то валідацію можна зупинити. Однак, можливо, цей клас підпису не містить інформацію, необхідну для остаточного висновку. В цьому випадку валідація продовжується процесом валідації для наступного посиленого класу підписів (підпис із часом, підпис із матеріалами для довгострокової валідації, підпис, що забезпечує довготривалу доступність і цілісність матеріалу валідації), доки не буде можливим отримати остаточний висновок або відсутні процеси валідації для наступного класу посилених підписів. Результат валідації останнього процесу валідації підпису є остаточним результатом валідації підпису (який може бути невизначеним через відсутність інформації).

Для того щоб завершити валідацію одного з класів підписів, застосовуються кілька складових частин валідації (формат підпису, валідність сертифікату підписування, криптографічна верифікація тощо). Позначення

стану кожної окремої складової частини валідації може бути одним із таких: PASSED, FAILED або INDETERMINATE.

Стан повної валідації одного з класів підпису в контексті визначеної політики валідації підпису має бути таким:

– TOTAL-PASSED – криптографічні перевірки підпису (включаючи перевірки гешей окремих об’єктів даних, які було підписано непрямим чином), а також всі перевірки, передбачені політикою валідації підпису, здійснено успішно.

– TOTAL-FAILED – криптографічні перевірки підпису не вдалися (включно з перевірками гешей окремих об’єктів даних, підписаних непрямим чином), або доведено, що генерація підпису відбувалася після анулювання сертифіката підписання або тому, що підпис не відповідає одному з базових стандартів у тій мірі, в якій складова частина криптографічної верифікації не може обробити його.

– INDETERMINATE – результати проведених перевірок не дозволяють встановити, що підпис TOTAL-PASSED або TOTAL-FAILED.

Індикація основного стану може супроводжуватись додатковою інформацією.

Якщо SVA повертає TOTAL-PASSED для певного підпису, то цей підпис необхідно розглядати як технічно валідний відповідно до обмежень валідації.

Якщо SVA повертає TOTAL-FAILED, підпис не можна вважати технічно валідним.

Якщо SVA повертає INDETERMINATE і якщо докладна інформація вказує, що результат може змінитися при повторному виконанні алгоритму перевірки, то можна повторити валідацію на основі додаткової інформації або пізніше у часі.

4. Методи криптографії

Криптографія – це сукупність методів перетворення даних, спрямованих на приховання їх інформаційного змісту.

Основне призначення криптографії – утаємничити необхідну інформацію. Криптографія надає засоби для захисту інформації і тому є складовою діяльності із забезпечення безпеки інформації. Існують різні засоби втаємничення інформації:

– приховування каналу передачі повідомлення;

– маскування змісту повідомлення з використанням стеганографічних методів;

– ускладнення можливості перехоплення самого повідомлення противником;

– інші.

На відміну від перерахованих методів криптографія не «приховує» повідомлення, а перетворює їх у форму, недоступну для розуміння противником. Таке перетворення забезпечується використанням криптографічних систем.

Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше їх розподіляють залежно від способу використання та за типом ключа:

– безключеві – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);

– перетворення з таємним ключем – використовується ключовий параметр – секретний ключ (симетричне шифрування, цифровий підпис, хеш-функції, ідентифікація);

– перетворення з відкритим ключем – використовують у своїх обчисленнях два ключі – відкритий (публічний) та закритий (приватний) (асиметричне шифрування, цифровий підпис).

5. Види шифрування та обмеження доступу

Методи захисту інформації є основою забезпечення конфіденційності, цілісності та доступності даних. Серед основних методів, які використовуються для захисту інформації, виділяють шифрування та обмеження доступу.

Розглянемо ці два методи детальніше:

1) Шифрування – це процес перетворення зрозумілої інформації в нечитабельну форму за допомогою спеціального алгоритму, що забезпечує її захист від несанкціонованого доступу. Тільки особа, яка має відповідний ключ або механізм для дешифрування, може повернути інформацію до її первісного вигляду.

Загалом виділяють три **методи шифрування –** симетричне, асиметричне та гібридне.

Алгоритми шифрування, що називаються **симетричними**, базуються на принципі того, що і відправники, і одержувачі користуються однаковим ключем. Таємний ключ повинен триматися в секреті й передаватись так, щоб запобігти його перехопленню. В разі якщо таємний ключ захищений, при розшифруванні повідомлення автоматично відбувається автентифікація відправника, тому що саме він є власником ключа, за яким можливо зашифрувати інформацію і саме отримувач має ключ, за допомогою якого можна дешифрувати повідомлення.

Оскільки відправники та одержувачі є єдиними користувачами, які мають цей симетричний ключ, при спробі скористатись несанкціоновано ключем, буде скомпрометовано взаємодію лише цих двох користувачів. Безпека цього типу системи шифрування залежить від збережності захищеності ключа, що використовується в алгоритмі шифрування, а не від зберігання в секреті алгоритму.

Зазвичай симетричний варіант ЕЦП передбачає присутність в системі третьої сторони – «арбітра», який виступає довіреною стороною обох користувачів. Автентифікація документа визначається самим фактом зашифрування його секретним ключем і передачі арбітру. Використовується рідко, тому що ефективних алгоритмів не існує.

Переваги симетричного методу генерування електронного цифрового підпису:

– криптостійкість симетричних схем має високі показники за рахунок стійкості блочних шифрів, що використовуються. Їх надійність також достатньо досліджена;

– якщо стійкість шифру недостатня, його легко замінити іншим.

Недоліки симетричних методів для створення ЕЦП:

– необхідно підписувати кожен із бітів інформації, що значно збільшує підпис (він часто буває на порядок довшим за довжину документа);

– створені для підпису ключі можна використати лише один раз, тому що після підпису розсекречується половина секретного ключа.

Будь-які криптосистеми, в основі роботи яких лежить використання закритого ключа, безпосередньо залежать від ступеня секретності цих даних.

Користувач може зберігати ключ на своєму особистому комп'ютері, наприклад, захистивши його паролем.

Але такий варіант має свої недоліки:

– підписувати документи можна тільки на комп'ютері власника ЕЦП;

– збереження даних ЕЦП безпосередньо залежить від захищеності комп'ютера користувача.

Алгоритми шифрування, які називають **асиметричними** (або шифрування з публічним ключем), на відміну від асиметричних схем, використовують два ключі – секретний ключ (secret key или private key) і відкритий ключ (public key), створені таким чином, що їх послідовне застосування до інформаційного об'єкта не змінює цей об'єкт. Ці ключі різні й не можуть бути отримані один з одного, не дивлячись на те, що вони згенеровані разом. Для зашифрування використовується лише відкритий ключ, для декодування використовується тільки секретний ключ.

Розшифровка коду без знання секретного ключа – це занадто складне завдання.

Зокрема, задача розрахунку секретного ключа за відомим відкритим ключем є практично нерозв'язною. Основною перевагою шифрування з публічним ключем є простий механізм передачі ключів. При з'єднанні з каналом зв'язку передається лише відкритий ключ. Це дозволяє використовувати звичайний канал для цього і виключає потребу спеціального каналу безпеки для пересилання ключа.

В асиметричній моделі побудови ЕЦП є свої недоліки:

– асиметричні схеми ЕЦП базуються, як і асиметричне шифрування, на обрахунково складних задачах (задача дискретного логарифмування або задача факторизації);

– криптостійкість алгоритмів шифрування з відкритим ключем поки що не доведена математично;

– для покращення криптостійкості необхідно робити довжину ключів більшою.

Саме криптосистеми з відкритими ключами широко застосовуються для

генерування ЕЦП. Цифрові підписи, що базуються на асиметричних методах шифрування, дозволяють одержувачу перевірити повідомлення на автентичність джерела інформації (іншими словами, автора інформації), а також перевірити, чи змінилася інформація в процесі передачі адресату. Тому цифрові підписи є засобом автентифікації та контролю цілісності даних.

Гібридне шифрування: Комбінація симетричного та асиметричного шифрування, де асиметричним шифруванням обмінюються ключами, а для фактичного шифрування даних використовується симетричний ключ. Це поєднує ефективність та безпеку.

Призначення шифрування:

– конфіденційність: зашифровані дані не можуть бути прочитані без відповідного ключа;

– ідентифікація: встановлення автентичності джерела інформації, коли в шифруванні використовуються підписані повідомлення;

– цілісність: забезпечення того, щоб дані не були змінені під час передачі.

2) Обмеження доступу – це контроль та управління доступом до інформаційних систем і ресурсів. Це методи, які дозволяють обмежити доступ до важливих або конфіденційних даних тільки авторизованим користувачам.

Основні методи обмеження доступу:

Автентифікація – це процес перевірки особи користувача або системи для надання доступу до певних ресурсів чи інформації. У сучасних системах інформаційної безпеки використовуються різні технології автентифікації, серед яких виділяються двофакторна, біометрична автентифікація та цифрові сертифікати.

Двофакторна автентифікація (2FA) – це метод перевірки особи, який поєднує два незалежних фактори для забезпечення більшої безпеки доступу до системи.

Основні фактори:

– що ви знаєте – наприклад, пароль або ПІН-код;

– що ви маєте – наприклад, мобільний пристрій, токен або смарт-карту;

– ким ви є – біометричні дані, такі як відбиток пальця або розпізнавання обличчя.

Переваги:

– підвищена безпека порівняно з однофакторною автентифікацією;

– знижує ризик несанкціонованого доступу навіть при компрометації пароля.

Приклад роботи: Користувач вводить пароль (перший фактор) і підтверджує вхід через SMS-код або додаток-автентифікатор (другий фактор).

Біометрична автентифікація – використовує фізичні або поведінкові характеристики людини для підтвердження особи. Це унікальний метод, оскільки біометричні дані кожної людини унікальні.

Типи біометричних даних:

– фізичні характеристики: відбитки пальців, розпізнавання обличчя та сканування райдужки ока;

– поведінкові характеристики: динаміка натискання клавіш, характеристика голосу та стиль руху або ходу.

Переваги:

– унікальність та складність підробки;

– зручність для користувачів, оскільки не потрібно запам’ятовувати паролі.

Недоліки:

– можливість збоїв у розпізнаванні через фізичні зміни (травми, старіння);

– ризик витоку біометричних даних (які неможливо змінити, на відміну від паролів).

Цифровий сертифікат – це електронний документ, виданий центром сертифікації (ЦСК), який підтверджує ідентичність користувача або системи та використовується для забезпечення безпечного обміну даними.

Основні елементи сертифіката: ім’я власника сертифіката, відкритий ключ, дані про центр сертифікації та строк дії сертифіката.

Механізм роботи:

– центр сертифікації видає сертифікат користувачу, підтверджуючи його особу;

– сертифікат використовується для автентифікації та встановлення захищеного з’єднання (наприклад, через протокол SSL/TLS);

– підпис власника сертифіката перевіряється за допомогою його відкритого ключа.

Переваги:

– гарантія довіри між сторонами;

– захист від підробки інформації завдяки криптографічним методам.

Недоліки:

– необхідність централізованого управління (ЦСК);

– можливість компрометації або відкликання сертифікатів.

Авторизація: Процес надання прав доступу користувачу після успішної автентифікації. Це визначає, до яких ресурсів користувач може отримати доступ і які операції може виконувати.

Принцип найменших привілеїв: Користувачам надаються лише ті права доступу, які необхідні для виконання їх завдань. Це мінімізує можливість зловживань або несанкціонованого доступу.

Розподіл ролей: Визначення доступу до ресурсів на основі ролей користувачів в організації. Ролі можуть включати адміністраторів, звичайних користувачів, читачів, модераторів тощо.

Мультифакторна автентифікація (MFA): Для підвищення безпеки застосовуються два або більше факторів для підтвердження особи (наприклад, пароль + смарт-карта або пароль + одноразовий код, надісланий на мобільний).

Журнальне ведення та моніторинг доступу: Реєстрація та аналіз всіх спроб доступу до системи для виявлення підозрілих або несанкціонованих дій.

Призначення обмеження доступу:

– захист даних від несанкціонованого доступу: обмеження доступу до важливих даних і систем лише для авторизованих осіб;

– контроль і моніторинг: перевірка дій користувачів і виявлення можливих загроз або зловживань;

– політики безпеки: забезпечення відповідності правилам доступу на основі внутрішніх політик і вимог законодавства (наприклад, GDPR або HIPAA).

Шифрування та обмеження доступу є взаємодоповнюючими методами захисту інформації. Шифрування забезпечує конфіденційність і цілісність даних, а обмеження доступу гарантує, що тільки уповноважені особи можуть отримати доступ до цих даних. Разом вони складають основу для безпеки в інформаційних системах, захищаючи їх від зловмисників і несанкціонованого доступу.

Технології автентифікації (табл. 3.3), такі як двофакторна, біометрична та цифрові сертифікати, спрямовані на забезпечення безпеки в цифровому середовищі.

Таблиця 3.3 – Порівняння технологій автентифікації

Параметр	Двофакторна автентифікація	Біометрична автентифікація	Цифрові сертифікати
Рівень безпеки	Високий	Дуже високий	Дуже високий
Зручність використання	Середня	Висока	Висока
Ризики	Компрометація одного фактора	Витік біометричних даних	Компрометація сертифіката
Сфери застосування	Онлайн-сервіси, банкінг	Смартфони, корпоративні системи	Електронний документообіг

Вибір конкретної технології залежить від рівня захисту, зручності використання та конкретної сфери застосування. У багатьох випадках їх комбінують для досягнення найвищого рівня безпеки.

6. Хеш-функція та принципи її роботи

Документи, що підписуються, мають різну, часто велику, довжину. Саме тому у випадку застосування ЕЦП зручно використовувати документ не в початковому вигляді, а тільки його хеш. *Хеш* – це результат роботи хешфункцій або функцій згортання. Обрахування хеша використовує саме криптографічні хеш-функції для забезпечення виявлення змін документів під час перевірки підпису. Хеш-функції не є частиною алгоритму ЕЦП. Тому може бути використана будь-яка або не використовуватись взагалі.

Хеш-функція призначена для стиснення послідовності вхідних даних довільної довжини в бітовий рядок попередньо визначеного розміру. Це зазвичай кілька десятків або сотень біт. Аналіз, який використовує хеш-функцію, часто використовується для контролю цілісності критичних системних файлів, важливих програм, важливих даних. Моніторинг можна

проводити за необхідності та на регулярній основі.

Спочатку потрібно визначити, цілісність яких файлів необхідно відстежувати. Для кожного файлу його значення обчислюється за допомогою спеціального алгоритму, який зберігає результат. Через деякий час проводиться обрахунок значення його хеша із збереженням результату. Якщо значення відрізняються, інформація, що міститься у файлі, була змінена.

Хеш-функції повинні володіти такими характеристиками:

– повинні мати можливість виконувати перетворення даних довільної довжини у дані фіксованої довжини;

– повинні мати відкритий алгоритм, щоб мати можливість вивчити його криптографічну стійкість;

– вона повинна бути односторонньою, тобто не повинно бути математичного способу визначення вихідних даних із результату;

– ймовірність зіткнень, тобто ймовірність того, що значення хеш-функцій двох різних документів (незалежно від їх довжини) будуть рівні, має бути незначною.

– вона не повинна вимагати великих обчислювальних ресурсів;

– найменша зміна вхідних даних повинна істотно змінити результат.

Використання хеш-функції в алгоритмі створення ЕЦП забезпечує деякі переваги, зокрема:

– складність обрахунків;

– сумісність;

– цілісність.

За рахунок того, що хеш-функція значно зменшує обсяг документа, обрахунки на виході стають швидшими. Тому створювати хеш документа і тільки потім підписувати його – це оптимальне рішення в межах поставленого завдання. Хеш можна використовувати для перетворення будь-якого вхідного тексту в потрібний формат. Якщо не використовувати функції стиснення, то документи великого розміру можна розділяти на менші блоки задля застосування ЕЦП.

Загалом односпрямованість не розуміється як неможливість, а скоріше як велика складність при поверненні повідомлення від свого хешу, оскільки в даний час не існує хеш-функції з доведеною односпрямованістю.

7. Різниця цифрового й електронного підписів та варіанти їх використання

Електронний підпис 2022 має два різновиди:

– удосконалений ЕП. Він створюється у результаті криптографічного перетворення електронних даних із використанням особистого ключа, однозначно пов’язаного з підписантом (пп. «44» ст. 1 Закону України № 2155);

– кваліфікований ЕП (далі – КЕП). Це ускладнений варіант удосконаленого ЕП, який створюється з використанням засобу КЕП і базується на кваліфікованому сертифікаті відкритого ключа (пп. «23» ст. 1 Закону України № 2155).

Різниця між удосконаленим ЕП та КЕП – у ступені захисту та довіри до особистого ключа електронного підпису. Так, у КЕП ключ розміщується на

захищеному засобі (носії) (пп. «17» ч. 1 ст. 1 Закону України № 2155, пп. «12» ч. 2 ст. 23 Закону України № 2155). При застосуванні перевіряються обидва ЕП, але при застосуванні КЕП, окрім перевірки цілісності коду ЕП, перевіряється ще й чи дійсно ключ розташований на такому кваліфікованому засобі, наприклад флешці-токені. Якщо він розташований на іншому засобі, наприклад у результаті копіювання з оригінального кваліфікованого носія ЕП, – система має повідомити, що немає відомостей про те, що особистий ключ зберігається в засобі кваліфікованого ЕП.

Увага: особистий ключ КЕП має бути на захищеному носії.

Виходить, що якщо використовувати для зберігання особистого ключа ЕП звичайну флешку, – це не КЕП, а всього лише вдосконалений ЕП. Згодом для податкових цілей користуватися такими ключами стане не можна.

Пристрій-носій КЕП має відповідати п. 2 Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженому постановою Кабміну від 19.09.2018 № 749 (далі – Порядок №749). Токен – це спеціальна флешка, яка захищена від перезапису/копіювання.

Завдяки такій схемі використання КЕП має вищий рівень довіри, ніж удосконалений ЕП та прирівнюється до звичайного (власноручного) підпису (ч. 4 ст. 18 Закону України №2155).

Тести

1. Що таке електронний цифровий підпис (ЕЦП)?

a) набір цифрових даних для шифрування файлів

b) набір цифрових даних, отриманих на основі електронного документа за допомогою криптографічного перетворення із закритим ключем

c) засіб створення секретних повідомлень

2. Яка основна мета ЕЦП?

a) забезпечення цілісності документа та ідентифікації підписанта

b) захист документів від копіювання

c) оптимізація обміну файлами

3. Що таке відкритий ключ у контексті ЕЦП?

a) особистий ключ для створення ЕЦП

b) захищений файл для шифрування

c) ключ, доступний для перевірки підпису, розміщений у сертифікаті

4. Що перевіряється при валідації підпису?

a) відсутність шкідливого програмного забезпечення

b) цілісність документа і відповідність відкритому ключу

c) час створення файлу

5. Який стан валідації означає, що підпис успішно перевірено?

a) TOTAL-PASSED

b) INDETERMINATE

c) TOTAL-FAILED

6. Який документ регулює електронні довірчі послуги в Україні?

a) Закон «Про інформаційні технології»

b) Закон України «Про електронні довірчі послуги»

c) Постанова Кабінету Міністрів України

7. Що є головним недоліком симетричного шифрування?

a) складність генерації ключів

b) велика тривалість шифрування

c) необхідність секретного обміну ключами

8. У чому головна перевага асиметричного шифрування?

a) простота алгоритмів

b) можливість використання відкритого ключа для передачі

c) відсутність ключів

9. Яка характеристика важлива для криптографічної хеш-функції?

a) можливість зворотного перетворення

b) односторонність обчислень

c) мінімальний розмір результату

10. Як використовується хеш-функція в ЕЦП?

a) для шифрування файлів

b) для створення відбитка документа перед підписанням

c) для генерації ключів

11. Що таке сертифікат відкритого ключа?

a) особистий документ користувача

b) ліцензія на шифрування

c) документ для поширення інформації про відкритий ключ

12. Що означає стан INDETERMINATE при валідації підпису?

a) підпис перевірено успішно

b) підпис недійсний

c) неможливо зробити висновок про дійсність підпису

13. Що є прикладом безключового методу криптографії?

a) симетричне шифрування

b) асиметричне шифрування

c) хеш-функції

14. Що таке довірчий список?

a) перелік користувачів із сертифікатами

b) реєстр кваліфікованих надавачів електронних довірчих послуг

c) база даних хеш-функцій

15. Що є основною перевагою симетричного шифрування?

a) простота передачі ключів

b) висока швидкість шифрування

c) можливість використання відкритого ключа

16. Що таке хеш-функція?

a) алгоритм, який стискає вхідні дані довільної довжини у рядок фіксованого розміру

b) механізм шифрування, що використовує два ключі

c) алгоритм перевірки достовірності сертифікатів

17. Яка властивість хеш-функції дозволяє виявляти зміни в документі?

a) використання асиметричних ключів

b) чутливість до найменших змін у вхідних даних

c) підтримка відкритих стандартів

18. Що є результатом роботи хеш-функції?

a) згортання даних, що має фіксовану довжину

b) підписаний документ

c) зашифрований текст

19. Що є основною відмінністю симетричного та асиметричного шифрування?

a) симетричне шифрування використовує два ключі, асиметричне – один

b) симетричне шифрування використовує один ключ, асиметричне – два

c) обидва методи шифрування використовують однакові ключі

20. У чому полягає перевага асиметричного шифрування?

a) не потребує захищеного каналу для передачі ключа

b) забезпечує швидший обмін ключами

c) використовує менше обчислювальних ресурсів

21. Що може бути недоліком симетричного шифрування?

a) неможливість використання в сучасних системах

b) високий ризик колізій у хеш-функціях

c) потреба в захищеному каналі для обміну ключами

22. Який метод не використовує ключів?

a) хеш-функції

b) асиметричне шифрування

c) симетричне шифрування

23. Що таке криптографічний метод із секретним ключем?

a) алгоритм для перевірки достовірності сертифікатів

b) перетворення, яке не забезпечує автентифікацію

c) метод, що використовує спільний ключ для шифрування та дешифрування

24. Як забезпечується захист у криптографії відкритого ключа?

a) використання однакового ключа для всіх учасників

b) розділення ключів на відкритий і закритий, які математично пов’язані

c) обов’язкове зберігання ключів у захищеному середовищі

25. Яка криптографічна технологія використовується для створення ЕЦП?

a) асиметричне шифрування

b) симетричне шифрування

c) хеш-функція без ключів.

Завдання для мозкового штурму до теми 3 «Електронний цифровий підпис та ідентифікація»

Завдання 1. Визначення терміну електронного цифрового підпису.

Уявіть, що ви повинні пояснити поняття електронного цифрового підпису

(ЕЦП) людині, яка зовсім далека від цього. Створіть просту аналогію або метафору, щоб описати, як працює ЕЦП і чому він надійний.

Наприклад: «ЕЦП – це цифровий замок і ключ». Що ще можна додати для кращого розуміння?

Завдання 2. Кваліфіковані надавачі електронних довірчих послуг.

Розробіть чек-лист для користувача, який хоче обрати надійного надавача електронних довірчих послуг. Які ключові пункти ви включите, щоб переконатися в надійності та законності такого надавача?

Завдання 3. Валідація цифрового підпису.

Запропонуйте стратегії, які можна використовувати в організації для забезпечення регулярної перевірки валідності цифрових підписів на важливих документах. Як можна автоматизувати цей процес? Які кроки необхідно включити?

Завдання 4. Методи криптографії.

Уявіть, що ви працюєте в команді розробників програмного забезпечення. Вам потрібно обрати метод криптографії для шифрування конфіденційної інформації клієнтів. Які чинники ви будете враховувати при виборі методу (безключові, симетричні, асиметричні)? Який метод ви оберете і чому?

Завдання 5. Види шифрування.

Проведіть порівняння симетричного та асиметричного шифрування в форматі «плюси-мінуси» для різних сценаріїв. Наприклад, захист переписки в чаті, підписання фінансових контрактів або передача великих файлів.

Завдання 6. Хеш-функція та принципи її роботи.

Уявіть, що в організації виникла підозра щодо зміни важливих файлів. Як би ви використали хеш-функції для перевірки цілісності цих файлів? Які додаткові заходи можна передбачити, щоб уникнути подібних ситуацій у майбутньому?

? Питання для самоконтролю

1. Що таке електронний цифровий підпис ? Які його основні функції у забезпеченні безпеки даних?
2. Які алгоритми шифрування використовуються для створення ЕЦП? Як вони забезпечують його унікальність?
3. У чому полягають принципи роботи асиметричного шифрування? Як воно використовується в ЕЦП?
4. Як працює хешування? Чому воно важливе для забезпечення цілісності даних в ЕЦП?
5. Які основні нормативно-правові акти регулюють використання ЕЦП у вашій країні чи в міжнародному контексті?
6. У чому полягає різниця між простим електронним підписом,

удосконаленим електронним підписом і кваліфікованим цифровим підписом?

7. Як електронний цифровий підпис змінює процеси документообігу та угод у комерційній сфері?

8. Які потенційні загрози можуть виникати при використанні ЕЦП? Як їм запобігти?

9. Як квантові обчислення можуть вплинути на безпеку та ефективність алгоритмів, які використовуються для створення ЕЦП?

10. Які приклади використання ЕЦП у сфері електронного уряду, онлайн-банкінгу та комунікацій найчастіше зустрічаються?

Питання для поглибленого вивчення теми 3 «Електронний цифровий підпис та ідентифікація»

1. Інноваційні підходи для поліпшення ефективності хеш-функцій.
2. Роль електронного цифрового підпису у сфері онлайн-виборів.
3. Оцінка безпеки симетричного та асиметричного шифрування в умовах квантових обчислень.
4. Використання біометрії для створення електронного цифрового підпису.
5. Захист цифрових підписів у децентралізованих мережах (блокчейн).
6. Правове регулювання використання ЕЦП у міжнародних угодах.
7. Використання штучного інтелекту для детекції підроблених цифрових підписів.
8. Соціальні аспекти впровадження ЕЦП на малих і середніх підприємствах.
9. Аналіз вразливостей алгоритмів шифрування при кібератаках.
10. Перспективи використання кваліфікованих ЕЦП у хмарних сервісах.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 4. СУЧАСНІ ЕЛЕКТРОННІ СЕРВІСИ ДЛЯ РОБОТИ З ДОКУМЕНТАМИ

Мета: засвоєння знань про функціональні можливості електронних сервісів, принципи їх використання, переваги й обмеження; набуття практичних навичок роботи з популярними платформами для управління електронними документами в умовах цифрової трансформації.

План

1. Хмарні сервіси для збереження даних.
2. Система управління електронними документами.
3. Особливості вибору платформи для організації документообігу.

***Ключові терміни та поняття:*** *хмарні сервіси, хмарні платформи, шифрування, автоматизація бекапу, технічна підтримка, система електронного документообігу, інтеграція, етапи впровадження СЕД, BAS Документообіг КОРП, M.E.Doc, FREDO ДокМен, COTA, Dropbox Business, DocuSign, M-Files, Zoho Docs.*

1. Хмарні сервіси для збереження даних

Хмарні сервіси для збереження даних – це віртуальний простір необмежених розмірів, де можна зберігати будь-які дані особистого чи корпоративного характеру.

Отримати доступ до інформації можна шляхом підключення до мережі Інтернет. Таким чином, маючи обліковий запис на сервісі хмари, користувач може входити в нього в будь-якому місці за наявності мережі. Усі моменти щодо обслуговування та безпеки збереження даних беруть на себе постачальники послуги.

Хмарні сервіси *(public cloud services)* – це програми та платформи, які «живуть» та працюють на серверах хмарних операторів. Їхня головна особливість полягає в тому, що створюючи акаунт на такій платформі, можна отримати доступ до власної інформації з будь-якого гаджета в будь-якій точці світу.

Хмарні сервіси трансформують бізнес і надають нові можливості для компаній різного розміру та сфери діяльності. Вони дозволяють ефективніше керувати ресурсами, знижують витрати та відкривають нові горизонти для масштабування та інновацій.

Хмарні платформи дозволяють бізнесу зменшити витрати на придбання та обслуговування фізичних серверів, мережевого обладнання та іншої IT-інфраструктури. Замість інвестицій у власні дата-центри компанії можуть орендувати необхідні обчислювальні ресурси у хмарних провайдерів, сплачуючи лише за те, що дійсно використовується. Це дозволяє зменшити капітальні витрати та перенести їх у категорію операційних, що особливо важливо для стартапів та малого бізнесу.

Одна з основних характеристик хмарних сервісів – їхня гнучкість. Компанії можуть швидко масштабувати ресурси у відповідь на зміни в попиті, наприклад, під час сезонних сплесків активності або раптового масштабування бізнесу. Хмара дає можливість додавати або зменшувати обчислювальні потужності, дисковий простір чи інші ресурси в режимі реального часу, не потребуючи значних затрат часу та коштів на оновлення фізичної інфраструктури.

Ключові переваги використання хмарних сервісів:

Доступність даних з будь-якої точки світу – однією з основних переваг хмарних сервісів є можливість доступу до них з будь-якої точки світу, де є підключення до мережі Інтернет. Це забезпечує гнучкість для бізнесу, дозволяючи співробітникам працювати віддалено, мати доступ до необхідної інформації під час відряджень або з інших локацій. Ця доступність підвищує

продуктивність і покращує взаємодію між командами, незалежно від їхнього місцезнаходження.

Висока надійність та безпека даних – завдяки використанню шифрування, багаторівневого захисту та двофакторної автентифікації компанії можуть бути впевнені у збереженні та захисті своїх даних. Окрім того, хмарні сервіси часто мають вбудовані механізми відновлення даних після збоїв або кібератак, що знижує ризики втрати інформації та мінімізує час простою.

Якщо хмарний оператор, на базі якого працює хмарний сервіс, розміщує своє обладнання в ЦОД, які відповідають рівню надійності TIER III та TIER IV, то ризик аварій зведений до мінімуму, а норми безпеки та процеси відповідають міжнародним стандартам.

Автоматизація бекапу та відновлення даних – один із найважливіших аспектів захисту даних у бізнесі – це регулярне резервне копіювання та швидке відновлення даних у разі необхідності. Хмарний сервіс пропонує автоматизовані рішення для бекапу, що значно спрощує процес збереження даних. Це дозволяє уникнути людського фактора, знизити ризики втрати інформації та забезпечити безперебійний доступ до важливих даних у будь-який час. Автоматизація також дозволяє швидко відновити дані в разі аварійної ситуації, що мінімізує вплив на бізнес-процеси.

Висока швидкість обробки даних – користувачі хмарних сервісів отримують ефективну систему обробки даних, яка не страждає від перевантажень, ненадійності мережі, загроз витоку даних або загальних недоліків, притаманних більшості локальних систем. Хмарні платформи використовують передові алгоритми, які оптимізують роботу серверів і знаходять найефективніші маршрути для спрямування трафіку даних.

Технічна підтримка – адмініструванням хмарних сервісів займається постачальник. Це дає змогу бізнесу зберегти бюджет на наймі та утриманні штату IT-фахівців і зосередитися на розвитку власних сервісів чи послуг.

2. Система управління електронними документами

Система електронного документообігу підприємства – дуже важливе організаційне завдання, без вирішення якого підприємство просто не зможе нормально працювати. Хороший керівник розуміє, що саме грамотно налагоджена система електронного документообігу допоможе уникнути ситуації втрати документів, затягування їхнього погодження, дасть змогу налагодити чітку взаємодію між своїми внутрішніми підрозділами, а також сформувати позитивний імідж у клієнтів і контрагентів.

СЕД також називають EDMS (Electronic Document Management Systems) – система управління електронними документами. Процес документообігу включає в себе ще workflow – робочу послідовність в рамках одного бізнес-процесу. В даному випадку – це отримання документа, його візування, відправка і т.д.

Системи управління документами (DMS – Document Management Systems) – це програмні рішення для зберігання, керування, захисту, передачі та обробки документів в електронному вигляді. Вони дозволяють компаніям

автоматизувати роботу з документами, знижувати витрати, підвищувати ефективність бізнес-процесів та забезпечувати відповідність нормативним вимогам.

Основні переваги електронного документообігу над паперовим. Відмова від друкованих бланків в рази знижує фінансові витрати компанії на управління документами, адже друкований документообіг – це закупівля паперу, різних журналів (вхідної-вихідної кореспонденції), папок і коробок для зберігання, обладнання архівів тощо.

Зростає швидкість пошуку необхідної інформації. Підраховано, що компанія на 1000 співробітників під час переходу на електронний документообіг заощаджує 100-200 людино/років часу, тобто такій кількості співробітників можна знайти краще застосування.

Менеджмент значно спрощується – керівник або співробітник у відрядженні може за необхідності в будь-який час або в будь-якому місці зайти в систему, відредагувати будь-який документ своєї відповідальності завдяки онлайн-доступу до системи.

Кожен керівник, який працював із паперовим документообігом, має «сумний» досвід розміру втраченої вигоди або збитків від помилкового використання старої версії паперового документа або його втрати. Електронна система управління документами дає змогу уникати втрати інформації та плутанини завдяки використанню єдиного інформаційного простору (сервер організації або онлайн-сервіс спеціалізованої компанії).

Безпека зберігання і конфіденційність – для цього створюють централізовані сховища електронних документів. До послуг підприємств є хмарні сервери для зберігання інформації, які забезпечують найвищий рівень захисту від хакерських атак.

Електронні документи корисні для екології, вони знижують навантаження на ліси нашої планети, адже саме з дерев виготовляють папір.

Система електронного документообігу складається з декількох важливих модулів для підтримки введення даних, індексування, обробки документів, управління доступом, маршрутизації документів, системної інтеграції, зберігання.

Кожен із цих модулів відповідає за послідовність і основні принципи документообігу в системі:

– одноразова реєстрація документа з подальшою його ідентифікацією;

– паралельне виконання завдань із можливістю скорочення часу їх руху й оперативністю їх виконання;

– безперервний рух документа з можливістю визначення відповідального за його виконання;

– одна база зберігання документації з виключенням дублювання;

– ефективна система пошуку документів;

– оптимізована система звітності.

Процес впровадження системи електронного документообігу може мати кілька напрямків. Вони залежать від можливостей компанії на етапі, коли система ще не впроваджена, і від очікуваних результатів.

Кожен шлях відрізняється процесом установки, супутніми завданнями і результатами:

Інтеграція – в уже наявну облікову систему, звичну для співробітників, впроваджується зовнішній сервіс. Для користувачів послідовність роботи не змінюється, але всередині процеси оптимізовані краще.

Нове готове рішення з навчанням. Це може бути як заміна з перекладом зі старого, так і повністю нове поняття робочого інструмента в компанії. У будь-якому випадку, така установка системи вимагає навчання і часу для впевненого користування.

Упровадження системи з необхідними доробками для компанії потрібно в тому випадку, коли бізнес-процеси передбачають унікальний ланцюжок передачі даних, тобто стандартні розроблені рішення не до кінця підходять.

Етапи впровадження СЕД. Незалежно від вибору напрямку схема запровадження системи електронного документообігу в основному проходить по одному шляху. Звичайно відмінності існують, хоча б з тієї причини, що сервіси можуть впроваджуватися різні. Щоб встановити систему потрібно:

– досліджувати поточний стан суб'єкта економічної діяльності, підготувати план упровадження;
– адаптувати СЕД під наявні потужності компанії;
– протестувати сервіс;
– навчити персонал;
– внести правки і доопрацювання в процесі експлуатації.

СЕД – автоматизація бізнес-середовища. Робота з документами в системі передбачає їх рух і обробку в рамках одного програмного інструментарію.

Система електронного документообігу працює з такими видами документів:

– бізнес-процеси компанії:
– управління проєктами;
– закупівлі;
– фінанси;
– збут;
– організаційно розпорядчі процеси.

До DMS належить низка сервісів, які допомагають користувачам оптимізувати та автоматизувати створення документів, їх обробку, зберігання, обмін та інші операції з ними. Раніше їхню функцію виконували корпоративні мережі, проте обсяги даних, що постійно зростали, та інші нюанси вимагали більш релевантного рішення.

Основні види СЕД, які найчастіше використовують підприємства.

BAS Документообіг КОРП – це програмний продукт, розроблений для автоматизації документообігу, управління процесами та оптимізації роботи з документами в середніх і великих організаціях. Є частиною лінійки рішень BAS (Business Automation Software) і відповідає сучасним вимогам до електронного документообігу. Програма автоматизації документообігу, яка надає такі можливості:

– робота з будь-якими документами;

– облік вхідної/вихідної кореспонденції з автоматичним формуванням реєстраційних номерів;

– 45 готових інструкцій для роботи з документами;

– повнотекстовий і скорочений пошук;

– сортування документів за типами й формування папок будь-яких структур;

– налаштування різних прав доступу користувача;

– моніторинг за робочим процесом працівників і раціональним використанням робочого часу;

– збереження файлів на зовнішньому носії або в базі даних.

Переваги BAS Документообіг КОРП:

– централізація роботи з документами: всі документи зберігаються в єдиній базі, що спрощує їх пошук і обробку;

– автоматизація процесів: зменшує ручну працю, підвищує швидкість виконання завдань;

– контроль і прозорість: забезпечує чіткий контроль над документами та процесами їх обробки;

– юридична значущість: завдяки електронному підпису всі електронні документи відповідають законодавчим нормам.

BAS Документообіг КОРП підходить для:

– корпоративних організацій зі складною структурою;

– компаній із великим обсягом внутрішніх і зовнішніх документів;

– організацій, які потребують автоматизації процесів погодження, затвердження і обміну документами.

M.E.Doc – це українське програмне забезпечення для автоматизації електронного документообігу, звітності до контролюючих органів, а також для взаємодії між компаніями, контрагентами та державними структурами. M.E.Doc широко використовується бізнесами різного масштабу завдяки своїм функціональним можливостям і простоті у використанні.

Сервісна програма електронного документообігу надає такі опції:

– спільна робота з різними системами обліку;

– звукове сповіщення про отримання файлів;

– автоматична обробка;

– копіювання та архівування файлів;

– створення шаблонів користувачем;

– електронний підпис документів із подальшим надсиланням контрагентам.

Переваги M.E.Doc:

– актуальність даних: система постійно оновлюється відповідно до змін у законодавстві;

– зручний інтерфейс: простота у використанні для бухгалтерів, економістів та інших працівників;

– економія часу: автоматизація звітності та обробки документів знижує затрати часу на рутинні операції;

– юридична значущість: підтримка ЕЦП дозволяє працювати з

електронними документами на законодавчому рівні;

– масштабованість: система підходить як для малих підприємств, так і для великих корпорацій.

Недоліки M.E.Doc:

– залежність від оновлень: постійна необхідність оновлювати програму для актуалізації форм звітності та інших функцій;

– потреба в налаштуванні: для інтеграції з іншими системами можуть знадобитися фахівці;

– залежність від зовнішнього електронного підпису: для роботи із системою потрібні ключі ЕЦП.

FREDO ДокМен – це спеціалізоване рішення для електронного документообігу, яке розроблене для автоматизації обробки документів в організаціях. Ця система використовується в основному для інтеграції з бухгалтерською програмою BAS, а також для роботи з контрагентами в рамках обміну електронними документами. Робота можлива тільки за наявності FREDO Звіт.

Можливості програми:

– забезпечує обмін первинними документами, актами, рахунками-фактурами та іншими документами з контрагентами з допомогою прямого з'єднання або ПТАХ (популярний сервер обміну);

– підтримує роботу з електронними підписами, що дозволяє забезпечити юридичну значущість документів;

– створення шаблонів для документів різних типів;

– отримання файлів від клієнтів, які користуються такою ж програмою або M.E.Doc;

– повністю інтегрується з програмами для обліку, зокрема BAS;

– автоматично синхронізує дані між обліковими програмами та платформою документообігу;

– шифрування і т.д.

Переваги FREDO ДокМен:

– економія часу: завдяки автоматизації обробки документів;

– зменшення витрат: немає потреби у друці та зберіганні паперових копій;

– юридична значущість: документи, підписані через FREDO ДокМен, відповідають законодавчим вимогам.

СОТА – це хмарний сервіс для електронного документообігу та подання звітності, створений компанією, яка розробила M.E.Doc. Він призначений для автоматизації звітності, обміну електронними документами та роботи з контрагентами в онлайн-режимі без необхідності встановлення програмного забезпечення на комп'ютер. Зручний онлайн-сервіс здачі податкової звітності. Працює з податковими накладними та розрахунками коригування; формує декларації, використовуючи книгу доходів; дозволяє відправляти запити в податкову і виконує інші завдання. Всі форми звітів до контролюючих органів можна здавати без установки програмного забезпечення, просто з веб-браузера, доступна з планшета або телефона.

Токени для КЕП. Токенами називаються захищені носії електронних підписів: ключі створюються всередині токена в одному екземплярі та захищені паролем. Токен купується один раз, і користувач більше не платить гроші за створення електронних ключів.

Переваги захищеного носія:

– захист під час генерації, оскільки сам процес відбувається всередині токена;

– захист від несанкціонованого доступу, оскільки ключ не можна скопіювати або подивитися;

– захист під час використання, оскільки токен захищений паролем;

– захист в процесі підписання документів, оскільки всі операції відбуваються всередині пристрою.

Плюси впровадження СЕД.

Для багатьох структур запровадження СЕД означає відмову від звичної паперової роботи. Новий функціонал е-документообігу здається складним і заплутаним, але його актуальність в бізнес-процесах багатьох компаній лише підтверджує значну користь, яку надає автоматизація:

– архівування та управління інформацією, регламентування доступу;

– економія ресурсів за рахунок зменшення витрат на паперове діловодство

– структуризація діяльності кожного співробітника;

– оптимізація бізнес-процесів;

– забезпечення прозорості діяльності організації;

– підтримка системи контролю якості.

Окрім явних плюсів від впровадження ЕДО, деякі системи можуть мати й явні **мінуси**. Таких недоліків може бути кілька. І перший – погана робота техпідтримки. Якщо помилка на стороні замовника була усунена несвоєчасно – це може стати для нього фінансовою втратою.

Обмежена функціональність системи, яка, швидше за все, підкріплена невисокою вартістю. Але обирати такий важливий функціонал варто відповідно до вимог, адже якщо система «не потягне» завдання, то її доведеться або розширювати, або замінювати на іншу.

Складнощі в розумінні системи персоналом. У цьому випадку не варто покладатися на свої власні сили й намагатися розібратися в ній самостійно. Для цього компанія, яка є її постачальником, зобов’язана провести навчання і постійно бути «на зв’язку» для можливої необхідності пояснити той чи інший функціонал.

Виникають помилки при роботі в СЕД. В такому випадку, швидше за все були недопрацювання при її впровадженні. Не варто намагатися все виправити самому – це робота постачальника системи. Важливо повідомити про подібний збій відразу, оскільки в подальшому система може не оновлюватися або взагалі «злетіти».

Запровадження СЕД в компаніях спрощує і скорочує етапи діловодства і дозволяє зосередитися на бізнес-процесах. Зменшення рутинних горизонтальних завдань стимулює структуру ставити вертикальні цілі, що

сприяє розвитку ресурсів і компанії в цілому.

Хмарні DMS-системи звільняють бізнес від необхідності постійно збільшувати простір та потужності для роботи з електронними документами. Крім того, вони приносять величезну користь для стандартизації та координації всього масиву документів компаній-клієнтів. Таке програмне забезпечення дозволяє створити єдину структуру для документообігу, щоб швидко знаходити та обробляти будь-який файл. Воно має чимало й інших, не менш цінних функцій, які наведено нижче.

Нижче розглянуто популярні системи: Dropbox Business, DocuSign, M-Files, Zoho Docs та ін.

1. Dropbox Business

Призначення Dropbox Business – один із найвідоміших сервісів для хмарного зберігання даних, що налічує понад 16 мільйонів користувачів. Окрім стандартного набору інструментів, тут є корпоративна версія Dropbox Business із розширеними можливостями для компаній та робочих груп. Вона вважається популярною програмою для керування документами – її використовують понад 500 000 бізнес-клієнтів.

Основні функції:

– Dropbox Paper дозволяє колективно створювати, редагувати та публікувати документи. У процесі роботи над ними та шерингу дані автоматично синхронізуються в режимі реального часу на всіх підключених пристроях;

– доступ до документів можна надавати навіть стороннім учасникам;

– функція керування теками робочої групи дозволяє гнучко керувати контентом та синхронізувати його;

– завдяки автоматизації користувачі можуть легко та швидко впорядкувати свою роботу шляхом сортування спільних тек, стандартизації імен і тегів;

– функція бекапу допомагає ефективно відновлювати видалені документи та їхні старі версії;

– Dropbox Transfer підтримує передачу файлів об’ємом до 100 ГБ як усередині групи, так і за її межі;

– вбудоване хмарне сховище забезпечує швидкий доступ до документів та інших файлів безпосередньо з робочого столу;

– панель адміністратора надає детальну статистику про дії всіх учасників групи та сторонніх осіб із доступом до даних. Через неї можна переглядати підключені пристрої та не тільки.

Переваги Dropbox Business:

1. Гнучкість – підходить як для малих, так і для великих компаній завдяки масштабованим тарифам.

2. Простота використання – інтерфейс інтуїтивно зрозумілий, що полегшує впровадження серед співробітників.

3. Висока продуктивність – завдяки інтеграції зі сторонніми програмами, компанії можуть оптимізувати робочі процеси.

4. Мобільність – можливість роботи з будь-якого пристрою: ПК, ноутбука, планшета чи смартфона.

Схема роботи Dropbox Business:

1. Завантаження документів – користувачі завантажують документи до хмарного сховища через браузер або додаток.
2. Синхронізація – файли автоматично синхронізуються між усіма підключеними пристроями.
3. Спільна робота – учасники команди можуть переглядати, редагувати та коментувати документи.
4. Моніторинг – адміністратор має доступ до журналу активності, щоб відстежувати зміни й дії користувачів.
5. Безпека – усі файли зберігаються в зашифрованому вигляді, а доступ контролюється через ролі та дозволи.

DMS Dropbox Business пропонує безплатний пробний період на 30 днів. Тариф Standart ($15 на місяць за користувача) дає 5 ТБ місця у хмарі, а план Advanced ($24 на місяць за користувача) – 15 ТБ. Обидва тарифи дозволяють додати до групи від 3 учасників. Для великих компаній система надає план Enterprise з індивідуальними умовами.

2. DocuSign – це платформа для електронного підпису та автоматизації процесів узгодження документів. Вона дозволяє швидко підписувати документи онлайн із юридичною силою.

Основні функції:

- електронний підпис;
- автоматизація процесів узгодження;
- інтеграція з популярними інструментами (microsoft 365, google workspace);
- забезпечення відповідності стандартам (GDPR, eIDAS, ESIGN).

Переваги:

- простота використання;
- підтримка кількох мов;
- безпечне зберігання документів.

Схема роботи DocuSign:

1. Завантаження документа.
2. Визначення областей для підпису.
3. Надсилання документа на підпис.
4. Одержувач підписує документ (через браузер або додаток).
5. Документ автоматично зберігається із журналом дій.

3. M-Files – це потужна платформа керування документами на основі метаданих. M-Files дає змогу кваліфікованим працівникам миттєво знаходити потрібну інформацію в будь-якому контексті, автоматизувати бізнес-процеси та посилити контроль інформації. Вона організовує документи не за папками, а за тегами й атрибутами.

Основні функції:

- обробка постійно зростаючих обсягів документів та надання своїм співробітникам нових інструментів для більш продуктивної співпраці й

ефективного використання робочого часу;

– управління корпоративною інформацію, що дозволяє отримати доступ до всіх документів і процесів з єдиного інтерфейсу;

– об’єднання наявного сховища даних, керування інформацією легко, швидко та безпечно;

– простий доступ до інформації завдяки метаданим;

– автоматизація своїх бізнес-процесів;

– використання інтелектуальних сервісів для роботи з документами;

– забезпечення безпеки й конфіденційності інформації;

– керування версіями файлів;

– інтеграція з ERP, CRM, SharePoint;

– підтримка документів у різних форматах.

Переваги:

– автоматизація бізнес-процесів;

– надійна система контролю версій;

– гнучке налаштування прав доступу до інформації, їх автоматична зміна в ході виконання бізнес-процесів;

– документами можна керувати з настільних комп’ютерів, ноутбуків або мобільних пристроїв у режимі онлайн або офлайн.

Схема роботи M-Files:

1. Завантаження документа.
2. Введення метаданих (назва, автор, дата створення).
3. Зберігання документа у базі даних.
4. Пошук за атрибутами, а не за розташуванням.
5. Розподіл прав доступу між користувачами.

4. Zoho Docs – це хмарна платформа для зберігання, обміну та спільної роботи з документами.

Zoho Docs являє собою пакет із двох десятків веб-бізнес-додатків (офісний пакет, кілька лінійних корпоративних програм – CRM, додаток для ведення проєктів тощо), інтерфейс яких наближений до MS Office зразка версій 2000-XP. Користувачеві виділяється безкоштовно 1 Гб дискового простору для зберігання різноманітних документів (можна завантажувати тільки файли підтримуваних форматів). Користувачі можуть редагувати документи, у тому числі з підтримкою версійності (вони будуть зберігатися під номерами, починаючи з 1.0 (1.1, 1.2 і т.д.), проте для повноцінної участі в цьому процесі потрібно мати обліковий запис на сервісі (інакше внесення правок буде ускладнено).

Основні функції:

– зберігання та синхронізація файлів у хмарі;

– спільна робота над документами в реальному часі;

– інтеграція з іншими інструментами Zoho;

– забезпечення безпеки даних через шифрування.

Переваги:

– простота використання для невеликих команд;

– доступність із будь-якого пристрою;

– інтеграція з іншими хмарними сервісами.

Схема роботи Zoho Docs:

1. Завантаження файлів до хмарного сховища.
2. Надання доступу команді або окремим користувачам.
3. Спільна робота над документами.
4. Збереження змін автоматично у реальному часі.

Таблиця 4.1 – Порівняльна таблиця популярних хмарних систем управління документами

Характеристика	Dropbox Business	DocuSign	M-Files	Zoho Docs
Основне призначення	Хмарне зберігання, синхронізація, спільна робота з файлами	Хмарне зберігання, електронний підпис, управління цифровими транзакціями	Локальне/хмарне зберігання Управління документами та метаданими	Хмарне зберігання, офісні інструменти
Цільова аудиторія	Компанії будь-якого розміру	Юридичні, фінансові, ділові організації	Середній і великий бізнес	Малі та середні компанії
Формати файлів	Усі основні формати файлів	PDF, DOCX, HTML	Усі популярні формати	Усі основні формати файлів
Особливості	– зберігання великих обсягів даних – інтеграція з Microsoft 365 та Google Workspace – автоматична синхронізація	– юридично значущий електронний підпис – підтримка шаблонів – інтеграція з CRM-системами	– управління документами на основі метаданих – інтелектуальний пошук – автоматизація бізнес-процесів	– інтеграція з Zoho Suite – робота з документами в реальному часі – інтеграція з CRM Zoho
Безпека	– AES-256 шифрування – дворівнева автентифікація	– дотримання стандартів eIDAS і ESIGN – високий рівень шифрування	– контроль доступу на рівні метаданих – ISO 27001 сертифікація	– захист паролем – контроль доступу та права на файли
Інтеграція	Slack, Zoom, Salesforce, Adobe Sign	Salesforce, Microsoft 365, Google Drive	Microsoft 365, Salesforce, DocuSign	Zoho Suite, Slack, Dropbox
Мобільний доступ	Додатки для iOS і Android	Додатки для iOS і Android	Додатки для iOS і Android	Додатки для iOS і Android
Пошук	Пошук за іменем файлу або вмістом	Пошук за шаблонами та угодами	Пошук за метаданими	Пошук за іменем файлу
Юридична відповідність	GDPR (General Data Protection Regulation)	ESIGN, GDPR, eIDAS	ISO, GDPR	Відсутня

	HIPAA (Health Insurance Portability and Accountability Act) ISO 27001 SOC 1, SOC 2, SOC 3, eIDAS			
Переваги	– зручність для командної роботи – широка інтеграція з інструментами	– юридична сила електронного підпису – простота використання	– управління даними на основі метаданих – гнучкість в адаптації	– доступна ціна – інтеграція в екосистему Zoho
Недоліки	– обмеження на функції редагування документів; – висока вартість для великих команд	– орієнтованість лише на електронний підпис	– складність для малого бізнесу – висока вартість	– менше функцій порівняно з конкурентами

Окрім того, виокремлюють такі кращі хмарні сервіси для бізнесу (приклади):

1. Microsoft 365 – це хмарний сервіс, який поєднує зручні сучасні інструменти для роботи, що поширюються на основі передплати. У пакет Microsoft 365 входить:

– електронна пошта бізнес-класу на сервері Exchange;

– мобільні та веб-версії Word, Excel, PowerPoint та Outlook;

– портал Sharepoint і публічний сайт-візитівка з простим конструктором сторінок;

– понад 10 додаткових програм (Microsoft Bookings, Planner, Forms тощо);

– чат, виклики і відеоконференції в Microsoft Teams;

– доступ до додатків останньої версії Microsoft Office;

– місце в OneDrive (1 терабайт на користувача).

2. Google One (Диск) – це платний сервіс від Google, який надає користувачам розширене хмарне зберігання даних і додаткові переваги. Він є розширенням базової пропозиції Google Drive та об’єднує всі хмарні сервіси Google під одним тарифним планом за підпискою.

Основні функції та призначення Google One:

– сервіс пропонує більше місця для зберігання даних у хмарі, ніж безкоштовні 15 ГБ, які отримує кожен користувач Google. Це місце використовується для зберігання файлів у Google Drive, фотографій і відео в Google Photos, а також електронної пошти в Gmail;

– доступні плани зберігання варіюються від 100 ГБ до декількох терабайтів;

– Google One дозволяє поділитися підпискою з максимум п’ятьма

членами сім'ї, кожен з яких отримує свій простір для зберігання, але всі вони користуються спільним обсягом;

– користувачі Google One отримують доступ до експертної підтримки від Google, яка може допомогти з питаннями, пов'язаними з Google-продуктами та послугами.

Якщо говорити загалом, які сервіси належать до хмарних сервісів Google, то це Gmail, Google Drive, Google Photos, YouTube, Google Maps, Google Translate тощо.

3. Корпоративна пошта Zimbra – зручне рішення для листування та спільної роботи працівників компанії з будь-якого пристрою. Включає поштовий сервер, календар, органайзер, сховище для файлів та офісні інструменти по роботі з документами.

Поштовий сервер Zimbra розміщується у хмарі GigaCloud і має низку переваг, ось основні з них:

– до хмарної пошти можна підключитися вже через 60 хвилин після замовлення;

– поштовий сервер розміщений у хмарі, яка працює на базі п'яти дата-центрів, що відповідають рівню надійності TIER III та TIER IV. Це дозволяє позбутися єдиної точки відмови в роботі пошти;

– можливість плавного та швидкого нарощування кількості користувачів та функціоналу пошти;

– можливість розміщення поштового сервера Zimbra на майданчику в Україні чи Європі.

4. Вчасно – це український онлайн-сервіс для електронного документообігу (ЕДО), який дозволяє компаніям підписувати, зберігати документи та обмінюватися ними в електронному форматі.

Сервіс спрямований на спрощення і прискорення процесів документообігу, зменшення витрат на паперову роботу та підвищення ефективності бізнес-процесів.

Можливості сервісу:

– доступ до документів із будь-якого пристрою в будь-який час;

– економія понад 90 грн на кожному документі;

– електронна система зберігає документи в хмарному архіві. Будь-який документ можна знайти за 30 секунд;

– надійний захист конфіденційних даних;

– підпис документа одним кліком завдяки наявності мобільного застосунку.

5. Віртуальні робочі столи VDI – це технологія, яка дозволяє створювати та керувати віртуальними робочими столами на віддалених серверах, забезпечуючи користувачам доступ до персоналізованих робочих середовищ з будь-якого пристрою через мережу Інтернет.

VDI базується у приватній хмарі GigaCloud. Спочатку фахівці будують приватну хмару, а потім розгортають під клієнта VDI. Для клієнта нічого не змінюється. На екрані він бачить звичний робочий стіл, ту ж ОС і програми.

Користувач не прив’язаний до конкретного ПК. Щоб відновити роботу з іншого місця, достатньо авторизуватися.

Можливості сервісу:

– зниження витрат: економія на IT-інфраструктурі та підтримці, оскільки локальні пристрої потребують мінімальних ресурсів;

– підвищення мобільності: співробітники можуть працювати з будь-якої точки світу, що особливо важливо в умовах віддаленої роботи;

– підвищення безпеки: централізоване зберігання даних на захищених серверах зменшує ризики витоку інформації;

– простота управління: адміністратори можуть легко налаштовувати, оновлювати та контролювати середовища користувачів.

Огляд найкращих хмарних програм для зберігання наведено в таблиці 4.2.

Таблиця 4.2 – Найкращі хмарні програми для зберігання інформації

Хмарні програми	Найкраще підійде для	Перевага	Межа для безкоштовного користування
Google Drive	Наявні користувачі Android і/або Google Workspace	Продумана потокова передача в порівнянні з офлайн-доступом для економії місця на жорсткому диску	15 ГБ
iCloud	Наявні користувачі пристроїв Apple	Легко вбудовується в пристрої Apple	5 ГБ
Dropbox	Синхронізація та резервне копіювання, що не потребують обслуговування	Легко використовувати для будь-якого пристрою	2 ГБ
Box	Малі підприємства, які шукають альтернативу Google Workspace	Документи та інструменти для спільної роботи для віддалених команд	10 ГБ
OneDrive	Наявні користувачі Microsoft 365 і Office	Інтеграція з Microsoft Office 365, але також доступна для всіх платформ	5 ГБ
Jottacloud	Автоматичне необмежене резервне копіювання та зберігання фотографій	Фактично необмежений обсяг пам’яті	5 ГБ
Koofr	Керування кількома постачальниками хмарних сховищ в одному місці	Платіть лише за потрібне сховище	10 ГБ
iDrive	Простота використання	Автоматичне резервне копіювання всіх ваших пристроїв	10 ГБ
Internxt	Найвищий рівень безпеки	Створення максимального захисту конфіденційності та шифрування простими у використанні	10 ГБ
MEGA	Найдешевше зберігання на високих рівнях	Простий у використанні для всіх із додатковими розширеними функціями для досвідчених користувачів	20 ГБ

Отже, використання хмарних сервісів надає бізнесу значні переваги, що дозволяють підвищити гнучкість, продуктивність і захист даних. Доступність інформації з будь-якого місця, висока надійність та безпека, а також автоматизація бекапу і відновлення даних роблять хмарні технології незамінним інструментом для сучасних компаній, допомагаючи їм ефективніше управляти своїми ресурсами і зосередитися на розвитку основних бізнес-напрямів.

3. Особливості вибору платформи для організації документообігу

Документообіг – невід'ємна складова життя будь-якого підприємства, його кровоносна система. Жодне рішення не може бути впроваджено ефективно, якщо воно не задокументовано. Відбудова процесів обігу документації – це не бюрократія, а обов'язковий крок до нормальної, безперебійної роботи в компанії.

Зараз велика частина ділових документів існує в електронному вигляді. Як і паперові, їх треба заповнювати, реєструвати, систематизувати, зберігати, оновлювати й пересилати потрібним адресатам. Напевно кожному з нас доводилося або самому займатися цією роботою, або чекати, поки це зроблять інші – наприклад, чиновники держустанов. Так що всім відомо, якою стомливою рутиною може стати робота з документами.

Для прискорення і спрощення роботи з документами існують СЕД – системи електронного документообігу. Це пакети з декількох додатків, кожний з яких відповідає за частину операцій з документами. Це шаблони корпоративних документів, реєстрація вхідної кореспонденції, механізми узгодження та затвердження документів, автоматичні звіти і т.д.

Виділяють чотири основних типи СЕД:

– Діловодство – це система кореспонденції і руху документів між агентами та контрагентами;

– Workflow – це налаштування бізнес-процесів, пов'язаних із документообігом;

– Архіви – це зберігання документів із різним рівнем доступу і з можливістю швидкого пошуку.

– ECM – комплексна система управління контентом, включаючи документи, таблиці, файли PDF і т.д. Включає функції всіх перерахованих вище систем.

Упровадження СЕД на підприємстві дозволяє скоротити рутинні процеси, пов'язані з обробкою, заповненням та обміном документами, в кілька разів! Окрім економії часу, СЕД зменшує ризик втрати даних, прискорює робочі процеси і покращує взаємодію усередині компанії, а також з контрагентами.

Як зрозуміти, чи потрібно впроваджувати у компанії СЕД.

При плануванні впровадження СЕД в компанії потрібно відповісти на кілька запитань:

1. Як відбувається обмін документами між відділами, їх обробка та збереження? Чи є можливість за необхідності швидко знайти потрібний документ?

2. Чи є в компанії правила збереження документів – систематизація, термін перегляду, правила зберігання копій і остаточного видалення? Чи виділене місце для архіву? Чи налаштовано регулярний бекап архіву?

3. Який шлях долає документ із моменту створення до відправки в архів? Чи є можливість контролювати цей процес на кожному етапі? Скільки часу займає кожен етап?

4. Чи налаштовані в компанії рівні доступу для різних документів? Чи визначені групи співробітників, кожної з якої присвоюється певний рівень доступу? Чи ідентичні рівні доступу в різних відділах і що відбувається з доступом при обміні документами?

Якщо керівник підприємства або інша відповідальна особа впевнено відповідає на всі ці питання, без впровадження СЕД можна обійтися. Швидше за все через те, що СЕД в даній компанії вже використовується. У всіх інших випадках впровадження СЕД варто запланувати найближчим часом.

Переваги СЕД дає бізнесу

Що отримує бізнес, який впроваджує систему електронного документообігу:

– автоматизація рутинних завдань і економія часу співробітників;

– зменшення впливу людського фактора на помилки в даних і втрату документів;

– прискорення донесення інформації до всіх або деяких співробітників компанії;

– найкращий захист важливої інформації за рахунок налаштування допусків різного рівня;

– прозорість документообігу з можливістю швидко знайти потрібний документ, простежити його шлях в системі і історію редагування;

– відповідність міжнародним стандартам інформаційної безпеки ISO 9000.

П’ять основних критеріїв для вибору оптимальної СЕД:

1. Зручний інтерфейс. Користувальницький інтерфейс – це головний інструмент взаємодії співробітників компанії із системою. Від того, наскільки він зручний, залежить час навчання співробітників роботі з СЕД, а також число помилок в майбутньому і витрати часу на їх виправлення.

2. Налаштування доступів різного рівня. Як правило, документи в компанії мають різні рівні конфіденційності – від загальнодоступних до суперсекретних, в яких міститься фінансова й інша важлива інформація. СЕД повинна надавати можливість налаштування ролей і рівнів доступу для окремих співробітників і для груп, наприклад, відділів.

3. Можливість спільної роботи. Чим більше компанія, тим нижча ймовірність, що над документом буде працювати тільки одна людина. Можливість спільної роботи спрощує і прискорює створення важливих документів, а також їх затвердження у керівництва.

4. Створення автооновлюваного архіву. Середній термін зберігання важливого документа в компанії – три роки. Найважливіші документи можуть

зберігатися безстроково. Для виконання цієї функції СЕД повинна надавати можливість створити архів, налаштувати персоналізований доступ до нього, а також автоматичне створення резервної копії через вказаний проміжок часу.

5. Віддалений доступ. Для адміністраторів системи налаштування зовнішнього доступу – окреме, досить складне завдання. Але без його реалізації неможливо налаштувати віддалену роботу співробітників, що за часів пандемії нівелює вигоди від впровадження СЕД.

Коробкова або кастомна версія СЕД?

Коробкова версія – це готове програмне рішення, а **кастомна** – розробка унікальної системи під вимоги замовника. Вибір типу версії завжди залежить від побажань замовника.

При виборі версії СЕД необхідно звернути увагу на такі моменти:

Пропозиція ринку. Зараз існує безліч готових рішень СЕД для бізнесів будь-якої сфери й розміру. В кожного рішення є свої особливості, але вони доступні до впровадження відразу після покупки. Кастомну версію доведеться розробляти з нуля, і на це знадобиться час.

Вартість упровадження. Для пакетних пропозицій вартість упровадження визначається на початку проєкту і включає описаний пакет послуг. Для кастомної версії вартість впровадження складно прорахувати одразу.

Вартість підтримки. Як правило, налаштування і оптимізація пакетного рішення вважаються окремим проєктом з окремим бюджетом – якщо це не обумовлено зі старту. Підтримка індивідуального рішення входить у вартість, але пов’язана з додатковими труднощами, наприклад, наявністю ресурсів у компанії.

Інтеграції з іншими системами і продуктами. В популярних коробкових рішеннях інтеграція з популярними продуктами або входить в основний пакет, або її легко можна придбати додатково. У компаній-інтеграторів вже є досвід упровадження нового ПЗ та налаштування спільної роботи різних систем.

Попередній аудит перед упровадженням СЕД.

Перед тим, як впроваджувати систему електронного документообігу, необхідно провести аудит. Вивченню підлягають, по-перше, процеси роботи з документами в компанії, по-друге, технічна інфраструктура. Це допоможе правильно підібрати саму систему і необхідний функціонал.

При аудиті поточний стан документообігу описується і фіксується. Ці дані допоможуть згодом оцінити рентабельність встановленої СЕД.

Аудит проводять співробітники компанії-вендора, яка поставляє програмне забезпечення. За підсумками аудиту складається план упровадження СЕД, а також список необхідних інтеграцій. У деяких випадках можуть знадобитися додаткові витрати на оновлення інфраструктури.

Оцінка ефективності впровадження СЕД.

Залежно від обраної системи і встановленого пакета середній термін окупності становить 3-5 років. Але для того, щоб точно розрахувати окупність системи, необхідно провести аудит процесів до її впровадження і зафіксувати показники, про які говорилося вище – наприклад, тривалість шляху документа,

тимчасові витрати на роботу з документами тощо.

Систему можна вважати рентабельною, якщо ефективність роботи персоналу зростає за рахунок економії часу на роботу з документами. В середньому СЕД дозволяє заощадити до шістдесяти відсотків часу. Крім того, потрібно враховувати непрямі вигоди, вартість яких не завжди очевидна. Наприклад, це зменшення втрат інформації та пов'язаних із втратами перебоїв у бізнес-процесах.

Тести

1. Яка основна перевага хмарних сервісів?
a) відсутність доступу з різних пристроїв
b) доступність даних з будь-якої точки світу
c) високі капітальні витрати
2. Що є ключовим аспектом безпеки даних у хмарних сервісах?
a) відсутність шифрування
b) використання багаторівневого захисту та шифрування
c) зберігання даних лише на локальних серверах
3. Що таке DMS (Document Management Systems)?
a) система для онлайн-конференцій
b) програмні рішення для зберігання, керування та обробки документів
c) інструмент для маркетингових кампаній
4. Яка функція Dropbox Paper?
a) обробка фінансових звітів
b) колективне створення, редагування та публікація документів
c) управління правами доступу
5. Який рівень надійності забезпечують ЦОД TIER III та TIER IV?
a) мінімальний
b) середній
c) високий
6. Що таке DocuSign?
a) система для обміну файлами
b) платформа для електронного підпису документів
c) хмарне сховище даних
7. Яка перевага M-Files перед іншими DMS?
a) зберігання документів у папках
b) організація документів за метаданими
c) відсутність інтеграції з іншими системами
8. Яку функцію виконує Dropbox Transfer?
a) створення звітів
b) передача файлів об'ємом до 100 ГБ
c) аналіз даних
9. Який обсяг сховища пропонує тариф Standart у Dropbox Business?
a) 10 ГБ
b) 2 ТБ

c) 5 ТБ

10. Яка ключова перевага хмарних платформ?

a) низька швидкість обробки даних

b) обмежений доступ до даних

c) гнучкість масштабування ресурсів

11. Який хмарний сервіс дозволяє працювати з будь-якого пристрою?

a) Dropbox Business

b) локальні сервери

c) лише ПК

12. Який тариф Dropbox Business підходить для великих компаній?

a) Standard

b) Basic

c) Enterprise

13. Що є ключовим чинником успіху хмарних DMS?

a) відсутність резервного копіювання

b) лише локальна підтримка

c) стандартизація документообігу

14. Яка головна функція Google One?

a) організація конференцій

b) розширене хмарне зберігання даних

c) обробка електронних підписів

15. Що таке Zoho Docs?

a) інструмент для обробки зображень

b) хмарна платформа для зберігання та спільної роботи з документами

c) система бухгалтерського обліку

16. Яка основна перевага Microsoft 365?

a) відсутність мобільних додатків

b) обмежений обсяг сховища

c) інтеграція сучасних інструментів для роботи

17. Який компонент Microsoft 365 дозволяє створювати сайти-візитки?

a) Word

b) SharePoint

c) Excel

18. Що забезпечує двофакторна автентифікація?

a) зменшення кількості користувачів

b) додатковий рівень безпеки

c) автоматичне зберігання даних

19. Який сервіс призначений для зручного електронного листування?

a) Zimbra

b) Google Photos

c) Dropbox Transfer

20. Що є головною особливістю Google Drive?

a) лише локальне зберігання файлів

b) відсутність шифрування

c) зберігання файлів у хмарі з доступом із різних пристроїв

21. Яка ключова перевага хмарних сервісів?

a) висока вартість обслуговування

b) доступність даних з будь-якої точки світу

c) відсутність технічної підтримки

22. Яка платформа використовується для електронного підпису документів?

a) DocuSign

b) Dropbox

c) Google Drive

23. Який із наведених тарифів Dropbox Business передбачає 15 ТБ місця у хмарі?

a) Standart

b) Advanced

c) Premium

24. Що є основною функцією системи M-Files?

a) організація документів за папками

b) зберігання тільки локальних файлів

c) організація документів за тегами й атрибутами

25. Який хмарний сервіс пропонує мобільні та веб-версії Word, Excel, PowerPoint?

a) Zoho Docs

b) Google One

c) Microsoft 365

26. Що забезпечує високу надійність та безпеку даних у хмарних сервісах?

a) шифрування та багаторівневий захист

b) відсутність резервного копіювання

c) локальне збереження даних

27. Що входить до складу Google One?

a) тільки Google Drive

b) тільки Gmail

c) розширене хмарне зберігання для Google Drive, Photos і Gmail

28. Який сервіс надає можливість керування правами доступу за допомогою метаданих?

a) Zoho Docs

b) M-Files

c) Microsoft 365

29. Яка з наведених систем призначена для роботи з календарями та органайзерами?

a) корпоративна пошта Zimbra

b) Google One

c) Dropbox Business

30. Що є основною перевагою хмарних DMS-систем?

a) використання тільки локальної пам’яті

b) автоматизація роботи з документами та зниження витрат
c) відсутність підтримки форматів файлів.

Завдання для мозкового штурму до теми 4 «Сучасні електронні сервіси для роботи з документами»

Завдання 1. Розробка ідеального хмарного сервісу.

Уявіть, що ви створюєте новий хмарний сервіс для зберігання та управління документами.

Які функції ви додасте, щоб сервіс став унікальним?

Як забезпечити максимальну безпеку даних?

Які технології (штучний інтелект, автоматизація) можна використати для покращення роботи?

Завдання 2. Порівняння сервісів.

Група розподіляється на кілька підгруп, кожна з яких досліджує певний хмарний сервіс (наприклад, Google Drive, Dropbox, Microsoft 365, M-Files).

Які переваги та недоліки сервісу ви помітили?

Як він відрізняється від конкурентів?

Що можна вдосконалити?

Завдання 3. Інноваційні сценарії використання.

Уявіть, що хмарні сервіси стануть єдиним способом зберігання даних у майбутньому.

Як це вплине на роботу компаній, урядів і звичайних користувачів?

Які проблеми можуть виникнути? Як їх вирішити?

Як можна використовувати хмарні сервіси для управління нестандартними проєктами (наприклад, в освіті, медицині чи мистецтві)?

Завдання 4. Стратегії управління даними.

Обговоріть, як компанії можуть ефективно керувати великими обсягами даних, використовуючи хмарні DMS-системи.

Як забезпечити швидкий доступ до даних для всіх співробітників?

Які методи можна застосувати для організації та класифікації файлів?

Як використовувати метадані для покращення роботи з документами?

Завдання 5. Безпека в хмарі.

Сформулюйте план забезпечення безпеки даних у хмарних сервісах.

Які технології для шифрування даних є найефективнішими?

Як захиститися від внутрішніх загроз (наприклад, людського фактора)?

Що потрібно для дотримання міжнародних стандартів безпеки?

Завдання 6. Впровадження хмарних технологій у бізнес.

Визначте, як хмарні технології можна інтегрувати в різні бізнес-сфери:

У якій галузі їх використання є найбільш корисним?

Як мотивувати співробітників переходити на нові системи?
Які складнощі можуть виникнути під час впровадження?

Завдання 7. Перспективи розвитку хмарних технологій.
Уявіть, як хмарні сервіси будуть виглядати через 10 років.
Які нові функції можуть з'явитися?
Як зміниться структура ринку хмарних послуг?
Чи можуть хмарні сервіси повністю замінити фізичні носії?

Завдання 8. Кейс-стаді: вирішення конкретної проблеми.
Представте кейс: компанія стикається з проблемою дублювання документів та хаосу в управлінні файлами.
Як хмарні DMS-системи допоможуть вирішити цю проблему?
Які кроки необхідно зробити для впровадження системи?
Як переконатися, що нова система працює ефективно?

Завдання 9. Екологічний аспект хмарних сервісів.
Поясніть, як використання хмарних технологій може сприяти екологічності.
Як хмарні сервіси допомагають зменшити споживання паперу?
Чи існують екологічні ризики через енергоспоживання дата-центрів?
Як компанії можуть оптимізувати використання хмарних сервісів для зменшення вуглецевого сліду?

Завдання 10. Міфи та реальність про хмарні сервіси.
Сформулюйте найпоширеніші міфи про хмарні технології (наприклад, «дані в хмарі небезпечні»).
Як можна спростувати ці міфи?
Які переваги часто недооцінюють?
Як навчити клієнтів і співробітників правильно використовувати хмарні сервіси?

Практичні завдання до теми 4 «Сучасні електронні сервіси для роботи з документами»

Завдання 1: Створення облікового запису.
Навчитися створювати обліковий запис для роботи з хмарними сервісами.
Завдання:
Створіть обліковий запис Google або Microsoft, якщо його ще немає.
Перевірте доступ до Google Drive або OneDrive.
Надайте відповіді на питання:
Як увійти до свого облікового запису?
Які базові функції доступні в безкоштовній версії сервісу?

Завдання 2: Завантаження та організація файлів.
Оволодіти навичками завантаження, створення папок і керування файлами.

Завдання:

Завантажте кілька файлів різних форматів (документ, зображення, відео).

Створіть папки для організації цих файлів.

Перемістіть файли між папками.

Надайте відповіді на питання:

Як відбувається синхронізація файлів між хмарою і пристроєм?

Чи можна надати спільний доступ до папки? Як це зробити?

Завдання 3: Надання доступу до файлів.

Навчитися ділитися файлами та керувати доступом.

Завдання:

Надішліть файл або папку колезі через функцію «Поділитися».

Налаштуйте права доступу (лише перегляд, редагування).

Перевірте, як одержувач може взаємодіяти з файлом.

Надайте відповіді на питання:

Як змінити права доступу після надання?

Що означає «доступ за посиланням»?

Завдання 4: Резервне копіювання даних.

Навчитися використовувати хмарні сервіси для створення резервних копій.

Завдання:

Налаштуйте автоматичне резервне копіювання папки з документами на вашому пристрої.

Перевірте, чи збереглися зміни в документах у хмарі після редагування.

Надайте відповіді на питання:

Як відновити видалений файл з хмарного сховища?

Чи можливо налаштувати вибіркове резервне копіювання?

Завдання 5: Спільна робота над документами.

Оволодіти навичками роботи з документами в режимі реального часу.

Завдання:

Створіть документ у Google Docs або Microsoft Word Online.

Поділіться документом із партнером для спільного редагування.

Разом відредагуйте текст у документі та залиште коментарі.

Надайте відповіді на питання:

Як відстежувати зміни, зроблені іншими користувачами?

Чи можна повернутися до попередньої версії документа?

Завдання 6: Інтеграція з іншими сервісами.

Ознайомитися з можливостями інтеграції хмарних сервісів із сторонніми додатками.

Завдання:

Інтегруйте Google Drive або OneDrive із додатками для роботи з документами (Microsoft Word, Google Docs).

Завантажте файл із хмарного сховища, відредагуйте його та збережіть.

Надайте відповіді на питання:

Які сервіси підтримують прямий доступ до файлів у хмарі?

Чи доступна інтеграція зі сторонніми сервісами для редагування фото чи відео?

Завдання 7: Керування доступом і безпекою.

Освоїти налаштування безпеки облікового запису та хмарних даних.

Завдання:

Активуйте двофакторну автентифікацію для свого облікового запису.

Налаштуйте обмеження доступу для певного файлу або папки.

Перевірте журнали активності у своєму хмарному сховищі.

Надайте відповіді на питання:

Які переваги двофакторної автентифікації?

Як переглянути, хто має доступ до ваших файлів?

Завдання 8: Порівняння хмарних сервісів.

Проаналізувати особливості різних хмарних сервісів.

Завдання:

Дослідіть функції Google Drive, Microsoft OneDrive, Dropbox.

Заповніть таблицю порівняння за критеріями: обсяг сховища, безпека, можливості спільної роботи, ціна.

Надайте відповіді на питання:

Який сервіс підходить для особистого користування, а який – для бізнесу?

Чим відрізняються безкоштовні версії сервісів?

? Питання для самоконтролю

1. Що таке хмарні технології? Як вони використовуються для управління документами?
2. Які основні переваги використання хмарних систем для управління документами порівняно з традиційними методами?
3. Які є ключові типи хмарних послуг (IaaS, PaaS, SaaS)? Яку роль вони відіграють в управлінні документами?
4. Як забезпечується безпека даних у хмарних DMS-системах? Які існують ризики?
5. Які функції пропонують сучасні системи управління документами на основі хмарних технологій?
6. Які основні етапи впровадження хмарних DMS-систем у компанії?
7. Які законодавчі аспекти потрібно враховувати під час використання хмарних сервісів для зберігання документів?
8. Як штучний інтелект та автоматизація впливають на роботу хмарних DMS-систем?
9. Що таке децентралізовані хмарні технології? Які їхні перспективи в управлінні документами?
10. Які критерії важливо враховувати під час вибору хмарної DMS-

системи для компанії?

11. Які тенденції розвитку хмарних технологій в управлінні документами можна очікувати в найближчі роки?

12. Як хмарні технології сприяють організації віддаленої роботи та ефективній взаємодії команд?

Питання для поглибленого вивчення теми 4 «Сучасні електронні сервіси для роботи з документами»

1. Оцінка ефективності хмарних DMS-систем у різних галузях економіки.
2. Шифрування та безпека даних у хмарних сервісах: аналіз сучасних технологій.
3. Вплив хмарних технологій на стратегії управління корпоративними даними.
4. Соціальні та культурні аспекти впровадження хмарних технологій у малих і середніх підприємствах.
5. Автоматизація документів у хмарних сервісах: використання штучного інтелекту та машинного навчання.
6. Екологічна ефективність хмарних сервісів: баланс між енергоспоживанням і економією ресурсів.
7. Перспективи розвитку децентралізованих хмарних технологій.
8. Порівняльний аналіз популярних хмарних DMS-систем.
9. Юридичні аспекти використання хмарних сервісів: конфіденційність і дотримання міжнародних стандартів.
10. Роль хмарних технологій у забезпеченні віддаленої роботи та колаборації.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 5. ДЕРЖАВНІ ОНЛАЙН-СЕРВІСИ У СФЕРІ ПОДАТКОВОЇ, СТАТИСТИЧНОЇ ТА ПЕНСІЙНОЇ ЗВІТНОСТІ

Мета: знайомлення з електронними інструментами взаємодії бізнесу та громадян з державними органами для подання звітності, участі у закупівлях та отримання державних послуг.



План

1. Електронний кабінет платника податків.
2. Електронна звітність до Пенсійного фонду України .
3. Взаємодія з Державною службою статистики України.
4. Електронна система публічних закупівель Prozorro.
5. Сервіс «Дія.Бізнес» і «Дія» як інструменти цифрової трансформації
6. Інші корисні державні електронні сервіси.

***Ключові терміни та поняття:*** *електронна звітність, кваліфікований електронний підпис (КЕП), електронний кабінет платника податків, Додаток 5 (ЄСВ), Кабінет респондента, платформа Prozorro, портал Дія, Портал електронних послуг ПФУ, система ЕСІТС, Єдиний державний реєстр (ЄДР).*

1. Електронний кабінет платника податків

Цифровізація державного управління в Україні спричинила суттєві зміни в механізмах взаємодії між суб'єктами господарювання та органами влади. Особливого значення набуває система електронного подання звітності та використання державних електронних сервісів, які забезпечують оперативність, зручність та прозорість в адмініструванні податків, зборів, пенсійних відрахувань, статистичної звітності, а також у доступі до публічних закупівель та інших державних послуг. Розвиток таких сервісів у межах національної платформи цифрової трансформації має стратегічне значення для формування сучасного електронного уряду.

Одним із ключових елементів у системі податкового адміністрування став Електронний кабінет платника податків, який функціонує на базі веб-порталу Державної податкової служби України. Цей інструмент надає користувачам можливість виконувати практично всі необхідні операції без фізичного відвідування податкових органів. За допомогою електронного кабінету платники податків – як юридичні, так і фізичні особи – можуть здійснювати авторизацію через електронний підпис, переглядати інформацію про себе, подавати податкову звітність (у тому числі з ПДВ, податку на прибуток, єдиного податку, ПДФО, тощо), отримувати податкові повідомлення, довідки та інші документи в електронній формі. Інтерфейс сервісу дозволяє завантажити або сформувати звіт, перевірити коректність заповнення форм, а також здійснити валідацію електронного підпису, що підтверджує справжність документа.

Електронний кабінет платника податків (ЕКПП) – це офіційний електронний сервіс Державної податкової служби України, що забезпечує доступ платників податків до персоналізованої інформації, подання звітності, перегляду розрахунків з бюджетом та комунікації з контролюючими органами. Він став ключовим елементом цифровізації податкових процесів в Україні, спрощуючи взаємодію між платниками податків та податковими органами.

Електронний кабінет платника податків (ЕКПП) є інтегрованою інформаційною системою, що функціонує на базі Державної податкової служби України. Його головним призначенням є забезпечення інтерактивної взаємодії між платниками податків та податковими органами в електронному форматі. Завдяки цьому ресурсу суб'єкти господарювання, фізичні особи-підприємці (ФОП), а також звичайні громадяни мають змогу подавати податкову звітність, отримувати консультації, витяги з реєстрів, повідомлення, перевіряти стан розрахунків із бюджетом, формувати запити тощо.

Сервіс виконує роль цифрового «єдиного вікна», що дозволяє зручно

адмініструвати податки та збори без потреби фізичного відвідування податкових інспекцій. ЕКПП інтегрований із загальнонаціональними реєстрами та інформаційними базами даних, що забезпечує об'єктивність та актуальність інформації, доступної користувачу. Крім того, система дозволяє вести історію подання звітності, зберігати архіви електронних документів, що значно підвищує ефективність ведення обліку.

Основне *призначення ЕКПП* – забезпечення зручного, безпечного та цілодобового доступу платників податків (юридичних та фізичних осіб) до повного спектра податкової інформації та сервісів. ЕКПП функціонує як електронна альтернатива відвідуванню податкової інспекції.

Функціональні можливості кабінету включають:

- перегляд стану розрахунків з бюджетом (переплата, заборгованість);
- подання податкової звітності в електронному вигляді;
- отримання довідок, витягів, повідомлень;
- обмін документами з ДПС;
- ведення листування в електронному форматі;
- отримання квитанцій про обробку документів;
- моніторинг податкових повідомлень-рішень;
- перевірку стану реєстрації ПДВ, ЄП тощо.

ЕКПП складається з двох основних частин: *відкритої (загальнодоступної)* – без авторизації, та *приватної (особистої)* – доступної після входу через КЕП (кваліфікований електронний підпис).

Вхід до ЕКПП можливий лише за наявності *кваліфікованого електронного підпису* (КЕП). Система підтримує сертифікати, видані акредитованими центрами сертифікації ключів (АЦСК), зокрема: *АЦСК ІДД ДПС, ПриватБанк, Україна, Вчасно, Ключ, Траст*, та інші.

Авторизація можлива також через інтеграцію з сервісом *ID.GOV.UA*, що підтримує BankID, MobileID, а також інші форми двофакторної ідентифікації. Для фізичних осіб передбачено спрощений доступ до функцій перегляду персональної інформації, тоді як для юридичних осіб необхідне підтвердження повноважень через електронний підпис відповідального за звітність працівника або керівника.

Електронна ідентифікація – це процес підтвердження особи користувача, що дозволяє убезпечити доступ до податкової інформації. Застосування КЕП унеможливлює несанкціонований доступ до персональних даних та забезпечує юридичну значущість електронних документів.

Із метою безпеки доступу до персоналізованих сервісів, сесії в ЕКПП автоматично завершуються через певний час неактивності. Всі дії в системі фіксуються, а документи, надіслані через кабінет, мають юридичну силу.

Однією з основних функцій електронного кабінету є подання електронної податкової звітності. Платники податків мають можливість створювати, редагувати, підписувати та надсилати звітні документи до ДПС України.

Система підтримує такі види звітності:

- ПДВ – Податкова декларація з податку на додану вартість подається щомісячно та формується відповідно до оновлених форм, що автоматично

завантажуються в ЕКПП;

– ЄП – Декларація платника єдиного податку для фізичних осіб-підприємців та юридичних осіб надається щокварталу або щороку;

– ПДФО – Звіт про доходи, отримані фізичними особами (Форма №1ДФ, нова форма 4ДФ);

– Податок на прибуток підприємств – декларація подається раз на квартал або рік (залежно від облікової політики платника);

– Звітність з ЄСВ – надається окремо, зокрема через форму «Єдиний звіт» з додатками 1-5.

Форма подання звітності включає:

– автоматичну перевірку заповнених полів;

– цифрове підписання КЕП;

– отримання квитанцій №1 і №2 про прийняття або відмову в прийнятті документа.

Після підписання звіту КЕП документ надсилається до ДПС, яка надає *квитанції* про отримання і перевірку звітності. В разі виявлення помилок система одразу інформує платника. Завдяки інтеграції з M.E.Doc, FREDO тощо платник може формувати звітність у сторонніх програмах і завантажувати її до кабінету.

Через електронний кабінет можна отримати низку офіційних документів без відвідування органів ДПС.

Зокрема, користувачі мають змогу сформувати:

– довідку про відсутність заборгованості з податків і зборів;

– витяг з реєстру платників єдиного податку;

– інформацію з реєстру платників ПДВ;

– повідомлення про результати камеральної перевірки;

– рішення про врахування/неврахування податкового кредиту;

– повідомлення про реєстрацію податкових накладних у ЄРПН.

Такі документи формуються автоматично або ж за запитом користувача. Їх можна завантажити у форматі PDF або XML, підписати КЕП та надати третім особам або використовувати у внутрішньому документообігу.

Також є можливість перегляду вхідної/вихідної *електронної кореспонденції*, включаючи листування з податковими органами.

Кожен документ супроводжується QR-кодом та електронним підписом, що дозволяє перевірити справжність документа на сайті ДПС.

ЕКПП повністю сумісний з *кваліфікованим електронним підписом*, який є обов’язковим інструментом у всіх електронних сервісах, що мають юридичну значущість. ЕКПП інтегрується з більшістю популярних програм для підготовки та подання електронної звітності, таких як:

– M.E.Doc – система електронного документообігу, що дозволяє створювати та подавати звіти, акти, накладні, рахунки-фактури, а також вести внутрішній документообіг;

– FREDO – хмарний сервіс для формування звітів, накладних, зв’язків із клієнтами, завантаження податкових накладних з ЄРПН;

– СОТА – онлайн-сервіс, зручний для малих підприємств, який

підтримує інтеграцію з BAS, дає змогу працювати через браузер без встановлення додаткового ПЗ.

Використання цих сервісів дозволяє здійснювати автоматичне підвантаження звітів в ЕКПП, перевірку на відповідність структурам ДПС, автозаповнення на основі первинних документів, масове підписання, синхронізувати облікові дані підприємства, зменшити ймовірність технічних помилок тощо.

Робота з ЕКПП має певні особливості залежно від типу користувача:

1. Для *юридичних осіб* електронний кабінет надає доступ до повного спектра звітних функцій, реєстрації податкових накладних, контролю за податковим кредитом, переплатами, податковими боргами, формування актів звірки, моніторингу розрахунків із бюджетом. Допуск до кабінету здійснюється на підставі КЕП керівника або бухгалтера, який має відповідні повноваження.

2. Для *фізичних осіб-підприємців (ФОП)* система надає доступ до спрощених форм звітності (ЄП, ПДФО), інформування про сплату єдиного соціального внеску, перегляду зведеної податкової інформації. ФОП можуть подавати звітність безпосередньо в кабінеті або через інтегровані сервіси, а також отримувати повідомлення, нагадування, листування з податковими органами.

3. *Громадяни* (непідприємці) можуть через кабінет отримати довідки про доходи, інформацію про суми, сплачені роботодавцем, подати декларацію про майновий стан і доходи, зокрема для цілей податкової знижки (наприклад, у разі оплати за навчання або іпотеку).

Усі користувачі мають можливість архівування звітів, друку квитанцій, створення шаблонів, автоматичного заповнення даних на основі попередніх періодів. Також у кабінеті можна відправляти звернення або заяви в електронній формі.

Для систематизації можливостей електронного кабінету доцільно представити їх у вигляді узагальнюючої таблиці. Вона дозволяє візуально окреслити функціональні блоки сервісу, їхню цільову аудиторію та взаємозв’язок із суміжними інформаційними ресурсами і сервісами. Такий формат не лише полегшує вивчення матеріалу, але й дає змогу побачити, як різні функції кабінету підтримують комплексне податкове адміністрування для юридичних і фізичних осіб.

Таблиця 5.1 – Функціональні можливості Електронного кабінету платника податків

№	Функціональна можливість	Короткий опис	Цільова аудиторія	Пов’язані сервіси/інструменти
1	Доступ до персонального кабінету	Авторизація за допомогою КЕП, MobileID або BankID.	ФОП, фіз. особи, юр. особи	КЕП, BankID, MobileID
2	Подання податкової звітності	Онлайн-заповнення та подача форм (ПДВ, ЄП, ПДФО, декларації тощо)	ФОП, юр. особи	M.E.Doc, FREDO, СОТА, iFin
3	Отримання квитанцій	Квитанції №1 та №2 після обробки звітності	Усі категорії	Внутрішній модуль ДПС

4	Перевірка розрахунків із бюджетом	Дані щодо нарахувань, переплат, заборгованості	ФОП, юр. особи	Система ЄРПН, РЛП
5	Отримання довідок і витягів	Наприклад, витяг з ЄП, довідка про відсутність заборгованості	ФОП, фіз. особи, юр. особи	ЕЦП, внутрішні модулі ДПС
6	Ведення електронного листування	Обмін повідомленнями з ДПС, отримання ППР, запитів	Юр. особи, ФОП	СЕА ПДВ, СЕА РП
7	Інтеграція з обліковими програмами	Завантаження звітів з M.E.Doc, FREDO	Юр. особи	API-сервіси, сторонні ПЗ
8	Управління підписами та сертифікатами	Підписання документів, перевірка валідності, оновлення сертифікатів	Усі категорії	АЦСК ІДД ДПС, КНЕДП
9	Робота з ПН/РК	Реєстрація, моніторинг, облік податкових накладних та розрахунків коригування	Юр. особи	ЄРПН, СЕА ПДВ
10	Моніторинг ризиковості	Інформація про відповідність критеріям ризиковості, індикатори блокування ПН	Юр. особи	ЄРПН, системи моніторингу ДПС
11	Підключення співробітників до кабінету	Делегування доступу до функцій (лише з КЕП)	Юр. особи	Внутрішній модуль ролей користувача
12	Перевірка статусів реєстрації	Статус платника ПДВ, ЄП, перебування на обліку	ФОП, юр. особи	Єдиний реєстр ДПС

Функціонал Електронного кабінету платника податків свідчить про високий рівень цифрової інтеграції між бізнесом, громадянами та податковими органами. Подана таблиця дозволяє системно представити головні можливості сервісу, їхню практичну значущість, технологічну основу та орієнтацію на різні категорії користувачів. Очевидним є прагнення держави мінімізувати людський фактор у податкових процесах, зробити їх автоматизованими, прозорими та максимально доступними. Особливо важливою є інтеграція кабінету з іншими обліковими системами (CRM, ERP, M.E.Doc), що дозволяє безперервно обмінюватися даними та підвищувати продуктивність фінансово-бухгалтерської діяльності на підприємствах.

2. Електронна звітність до Пенсійного фонду України

Портал електронних послуг Пенсійного фонду України (https://portal.pfu.gov.ua) є ключовим інструментом для дистанційної взаємодії громадян та роботодавців з ПФУ. Його структура включає:

- особистий кабінет: доступний для застрахованих осіб, пенсіонерів та страхувальників;
- розділи послуг: подача заяв, перегляд інформації про страховий стаж, пенсійні нарахування тощо;
- інформаційні ресурси: новини, нормативні документи, інструкції.

Доступ до порталу можливий через:

- кваліфікований електронний підпис (КЕП)**:** використовується для авторизації та підписання документів;
- BankID: ідентифікація через банківські системи;
- MobileID: ідентифікація через мобільного оператора.

Ці методи забезпечують безпечний та зручний доступ до електронних послуг ПФУ.

Форма **Додаток 5** до звіту з єдиного соціального внеску (ЄСВ) є важливою складовою системи обліку страхового стажу працівників. Вона подається до Пенсійного фонду України щомісяця і містить детальну інформацію про трудову діяльність осіб, які працюють у роботодавця. Саме цей звіт використовується для формування індивідуальних даних у Реєстрі застрахованих осіб, які безпосередньо впливають на майбутні пенсійні права.

Подання форми Додатку 5 регламентується Законом України «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування» та наказом Міністерства фінансів № 435. Саме ці документи визначають структуру, правила заповнення, терміни подання та відповідальність страхувальників. Порушення цих вимог може спричинити фінансові санкції, а також ускладнення при зарахуванні стажу для працівників.

У **структурі Додатка 5** передбачено подання ідентифікаційних даних страхувальника (найменування, код ЄДРПОУ, адреса), а також відомостей про кожного працівника. Зокрема, зазначається його прізвище, ім'я, по батькові, ідентифікаційний код або серія та номер паспорта. Обов'язковими є дані про дати прийняття на роботу і звільнення, а також тип умов праці. Для кожного працівника зазначається база нарахування ЄСВ, сума заробітної плати та відповідна сума внеску.

Процес підготовки звіту потребує точного збору даних із різних облікових документів: кадрових наказів, табелів робочого часу, розрахункових листків. Після збору інформації бухгалтер формує звіт у форматі XML. Його обов'язково потрібно підписати кваліфікованим електронним підписом (КЕП) і надіслати через електронні канали: або через портал ПФУ, або через сторонні сервіси, як-от M.E.Doc, FREDO, СОТА тощо.

Форма охоплює широкий спектр життєвих ситуацій. Наприклад, у випадку прийняття нового працівника фіксується дата початку роботи, а при звільненні – дата припинення трудових відносин. Якщо у працівника змінилися умови праці (наприклад, перехід на посаду з пільговим стажем), ця інформація також відображається у формі. При відсутності нарахувань у звітному місяці (наприклад, через відпустку без збереження заробітної плати) у відповідних графах вказуються нульові значення.

Подати Додаток 5 необхідно до 20 числа місяця, що настає за звітним. Прострочення або помилки в поданні тягнуть за собою накладення штрафу, відмову в зарахуванні періоду до страхового стажу працівника або інші правові наслідки. Частими помилками є неправильне зазначення ідентифікаційного коду, прізвища працівника, неправильна дата прийняття чи звільнення, помилки в сумах або дублювання записів.

Рекомендовано автоматизувати формування звітності через інтегровані бухгалтерські системи, щоб уникнути людського фактора та забезпечити точність даних. Доцільно також здійснювати внутрішню перевірку файлу перед підписанням та поданням. Усі електронні квитанції, що підтверджують прийняття звіту, необхідно зберігати – вони є доказом виконання зобов'язання перед державою.

Важливість Додатка 5 полягає у його впливі на пенсійне забезпечення працівників. Саме ці дані використовуються для розрахунку страхового стажу, права на пенсію, її виду та розміру. Некоректно поданий або відсутній звіт може призвести до відмови у призначенні пенсії або зменшення її розміру. Тому кожен роботодавець має ставитися до формування цієї звітності з максимальною відповідальністю.

Таблиця 5.2 – Приклад заповнення Додатка 5 (умовні дані)

№	ІПН	Прізвище, ім'я по батькові	Період звітний	Дата прийняття	Дата звільнення	Категорія особи	Заробітна плата, грн	База нарахування ЄСВ, грн	ЄСВ грн
1	1234567890	Іваненко Марія Сергіївна	04.2025	15.03.2025	-	Найманий працівник	12000	12000	2640
2	2345678910	Петренко Олег Ігорович	04.2025	01.01.2024	30.04.2025	Найманий працівник	14500	14500	3190
3	3456789123	Сидорчук Ірина Павлівна	04.2025	10.04.2025	-	Сумісник	8000	8000	1760
4	4567891234	Коваль Богдан Миколайович	04.2025	01.12.2023	-	Найманий працівник	0 (відпустка без збереження ЗП)	0	0

Примітка: ставка ЄСВ = 22% від бази нарахування

Інтеграція електронного кабінету платника з обліковими програмами та спеціалізованими сервісами, зокрема такими, як СОТА, є ключовим чинником у цифровій трансформації процесів подання звітності до Пенсійного фонду України (ПФУ). Така інтеграція забезпечує автоматизацію, підвищення точності та зменшення адміністративного навантаження на бухгалтерські служби.

Сервіс СОТА – це хмарна веб-платформа для створення, подання та обміну електронною звітністю, яка дозволяє підприємствам та фізичним особам-підприємцям (ФОП) оперативно взаємодіяти з державними контролюючими органами, включаючи ДПС, ПФУ, Держстат, Держпраці тощо. СОТА працює у тісній інтеграції з реєстрами ПФУ, що дозволяє швидко формувати звітність, зокрема Додаток 5, без необхідності дублювання даних вручну.

Інтеграція передбачає автоматичне підтягування інформації з облікових систем підприємства (наприклад, BAS, ISpro, M.E.Doc, FREDO, Зарплата+Кадри) у форматі, що відповідає вимогам ПФУ. Це особливо

актуально для великих підприємств із великою кількістю працівників, де ручне введення даних займає багато часу та спричиняє ризики помилок.

Основні переваги інтеграції з обліковими програмами:

– автоматизація процесів – формування звітів (наприклад, Додатка 5) відбувається на основі вже внесених у систему даних щодо нарахувань заробітної плати, табелів обліку робочого часу, наказів про прийняття чи звільнення працівників. Це дозволяє зекономити час бухгалтера і зменшити кількість рутинних операцій.

– підвищення точності звітності: вбудовані алгоритми перевірки коректності даних виявляють помилки ще на етапі створення звіту. Наприклад, СОТА автоматично підсвічує розбіжності між сумою нарахувань та внесками, попереджає про неправильний ІПН чи дублювання записів.

– миттєвий зворотний зв’язок: після подання звіту система надсилає квитанції в реальному часі. Перша квитанція підтверджує доставку звіту до ПФУ, друга – інформує про його прийняття або відхилення з поясненням причин. Це дає змогу оперативно усунути недоліки без порушення термінів подання.

– інтеграція з КЕП. СОТА підтримує підписання звітів за допомогою кваліфікованих електронних підписів будь-яких АЦСК (наприклад, ДП «Дія», АЦСК «Україна», АЦСК ПАТ «Ключ»).

– зберігання історії звітів: у сервісах типу СОТА є можливість архівування звітності, відстеження історії змін і повторного використання шаблонів, що оптимізує документообіг підприємства.

Наприклад, при заповненні Додатка 5 через СОТА достатньо лише синхронізувати дані з кадрової системи, після чого в автоматичному режимі формується XML-файл, який можна одразу підписати та подати. У випадку потреби внесення правок – система дозволяє відкрити звіт у браузері, внести корективи і знову відправити з урахуванням змін.

Інтеграція також сприяє збереженню єдиного інформаційного простору підприємства: всі дані про працівників, облік робочого часу, зарплатні нарахування, податкові зобов'язання та страхові внески акумулюються в єдиній системі, забезпечуючи прозорість і контроль.

Таким чином, впровадження таких інструментів, як СОТА, дозволяє істотно оптимізувати процеси подання звітності, мінімізувати ризики людських помилок і забезпечити повну відповідність вимогам законодавства. Це особливо важливо в умовах динамічного законодавчого середовища та цифровізації адміністративних процедур в Україні.

У сучасних умовах цифровізації соціального страхування важливою складовою забезпечення прозорості та підзвітності у сфері пенсійного забезпечення є можливість працівників самостійно та оперативно *перевіряти свій страховий стаж*. Цей функціонал реалізований через Портал електронних послуг Пенсійного фонду України (ПФУ), який функціонує як інтегрована платформа для надання електронних адміністративних послуг у сфері пенсійного забезпечення.

Страховий стаж – це період (у місяцях, роках), протягом якого особа підлягала загальнообов'язковому державному пенсійному страхуванню та за який щомісяця були сплачені внески у розмірі не менше мінімального страхового внеску. Ці дані є основою для обчислення права особи на пенсію за віком, розмір пенсійних виплат, а також доступ до низки соціальних гарантій.

Портал електронних послуг дозволяє зареєстрованим користувачам (з використанням КЕП або через сервіс ID.GOV.UA) переглядати дані про свій страховий стаж у зручному електронному форматі.

Основні можливості цього інструменту включають:

1. Перегляд персоніфікованої інформації про періоди страхування. Після входу до особистого кабінету користувач може переглянути деталізовану інформацію про періоди офіційного працевлаштування, розмір нарахованої заробітної плати, а також суми сплаченого єдиного соціального внеску (ЄСВ) за кожен місяць. Інформація подається у табличному вигляді з можливістю сортування за роками або роботодавцями.

2. Загальний страховий стаж. Система автоматично обчислює загальну кількість місяців страхового стажу користувача, що особливо корисно напередодні виходу на пенсію або у випадках оформлення соціальних допомог, які залежать від тривалості стажу.

3. Завантаження довідок про стаж. Користувач має можливість сформувати та завантажити офіційну довідку про страховий стаж, яка підписується електронним підписом ПФУ та містить QR-код для перевірки її достовірності. Така довідка є юридично значимим документом і може використовуватись для пред'явлення в органах соціального захисту, банках, роботодавцях тощо.

4. Виявлення неточностей у даних. Доступ до електронної історії стажу дозволяє особі оперативно виявити можливі порушення – наприклад, відсутність звітності від колишнього роботодавця, занижений розмір внесків або неповний період роботи. У разі виявлення таких порушень особа може подати заяву через портал або безпосередньо звернутися до територіального органу ПФУ з відповідними доказами (копії трудової книжки, накази про прийняття, табелі обліку тощо).

5. Моніторинг змін у реальному часі. Сервіс надає можливість постійного контролю за станом свого страхового стажу. Після кожної звітної подачі роботодавця оновлені дані з'являються в електронному кабінеті працівника. Це забезпечує не лише прозорість системи, а й стимулює роботодавців дотримуватись законодавства у частині своєчасної сплати ЄСВ.

Можливість онлайн-контролю за страхуванням має важливе соціально-економічне значення. По-перше, це сприяє формуванню правової культури у працівників: громадяни дедалі більше усвідомлюють залежність між сплатою ЄСВ та майбутніми пенсійними правами. По-друге, це створює додаткову мотивацію для офіційного працевлаштування. По-третє, в умовах високого рівня міграції та трудової мобільності, можливість доступу до своїх даних незалежно від місця перебування – важлива перевага електронного урядування.

Окрім того, сервіс спрощує роботу роботодавців: у разі звернення

працівника щодо неточностей, підприємство може оперативно внести коригування, подати уточнюючі звіти через облікову систему або сервіси на кшталт СОТА, M.E.Doc тощо.

Інструкція «Як перевірити страховий стаж на Порталі електронних послуг ПФУ»:

Крок 1: Перейдіть на сайт ПФУ

Зайдіть на офіційний вебпортал Пенсійного фонду України: https://portal.pfu.gov.ua

Крок 2: Авторизуйтеся в системі

Натисніть кнопку «Вхід» і оберіть спосіб авторизації:

– Кваліфікований електронний підпис (КЕП)
– MobileID
– BankID
– ID.GOV.UA

Крок 3: Зайдіть в особистий кабінет

Після входу відкриється головна панель із переліком доступних електронних послуг.

Крок 4: Оберіть послугу «Мій страховий стаж»

У розділі «Мої дані» або в швидкому доступі натисніть «Страховий стаж».

Ви побачите таблицю з роками, місяцями, роботодавцями, сумами нарахувань і страховим внеском.

Крок 5: Сформуйте довідку

У відповідному розділі натисніть «Сформувати довідку про страховий стаж» → виберіть період → натисніть «Сформувати».

Документ завантажується у форматі PDF із підписом ПФУ та QR-кодом.

Нижче наведена порівняльна таблиця можливостей електронного кабінету.

Таблиця 5.3 – Порівняльна таблиця можливостей електронного кабінету

Функція	Застрахована особа (працівник)	Роботодавець (юридична особа / ФОП)
Перегляд персоніфікованих даних	Так	Ні (тільки по співробітниках у звітах)
Отримання довідки про страховий стаж	Так (з QR-кодом)	Ні
Контроль за поданням ЄСВ звітності	Так (в особистому кабінеті видно щомісячні надходження)	Так (через модулі подання звітності)
Подання звітів до ПФУ	Ні	Так (через Додаток 5, тощо)
Перегляд інформації про нарахування пенсії	Так (у разі наявності права або прогнозу)	Ні
Повідомлення про порушення (відсутність звітності, стажу)	Так	Так (повідомлення про відхилення звіту, помилки)

У межах чинного законодавства України роботодавці зобов'язані повідомляти державні органи про укладення та припинення трудових відносин із працівниками. Одним із ключових інструментів для цього є електронне повідомлення до Пенсійного фонду України (ПФУ), що є складовою звітності з питань єдиного соціального внеску (ЄСВ).

Обов'язок інформування ПФУ про кадрові зміни визначено низкою законодавчих актів:

– Кодекс законів про працю України (ст. 24) – передбачає, що укладення трудового договору можливе лише після повідомлення контролюючого органу;

– Постанова Кабінету Міністрів України № 413 від 17 червня 2015 року – визначає порядок повідомлення про прийняття працівника на роботу;

– Наказ Мінфіну №435 (зі змінами) – регулює форму та структуру звітності з ЄСВ, зокрема Додаток 5, який містить відомості про застрахованих осіб.

Таким чином, ПФУ виступає одержувачем даних, що мають значення для обліку трудового стажу, нарахування страхових внесків, подальших пенсійних прав тощо.

Інформація про прийняття/звільнення працівників включається до Додатка 5 звіту з ЄСВ, який подається щомісяця в електронному вигляді через авторизовані облікові програми (M.E.Doc, СОТА, FREDO, електронний кабінет ПФУ тощо).

Структура повідомлення в Додатку 5 включає:

– дата прийняття/звільнення працівника – відображає момент початку або завершення трудових відносин;

– підстава кадрової дії – номер та дата наказу, розпорядження або іншого розпорядчого документа, що засвідчує факт змін у трудових правовідносинах;

– реквізити працівника – ПІБ, ідентифікаційний номер (або серія і номер паспорта), посада, підстава для страхування;

– тип змін – прийняття, переведення, звільнення (у випадку звільнення також зазначається причина припинення трудового договору);

– дані роботодавця – код ЄДРПОУ, адреса, форма власності тощо.

Умови подання:

– подання здійснюється до початку роботи працівника (у разі прийняття).

– у випадку звільнення – у звіті за той місяць, у якому відбулося припинення трудових відносин.

– звіт завіряється кваліфікованим електронним підписом (КЕП).

Своєчасне подання повідомлення про працівника до ПФУ є обов'язковим не лише з погляду дотримання трудового законодавства, а й у контексті:

– безперервності страхового стажу – внесення даних до Реєстру застрахованих осіб дозволяє нараховувати стаж без розривів;

– коректного відображення пенсійних прав – працівники можуть перевірити інформацію про стаж через портал ПФУ;

– юридичної безпеки роботодавця – уникнення штрафних санкцій за неподання або подання з порушенням строків (розмір штрафу може становити

від 5100 грн за кожне порушення);

– верифікації факту працевлаштування – необхідно при оформленні субсидій, соціальних виплат, підтвердженні доходів тощо.

Для подання повідомлень використовуються:

– Електронний кабінет ПФУ – portal.pfu.gov.ua, розділ «Звітність до ПФУ», меню «ЄСВ. Додаток 5»;

– програмні сервіси обліку – такі як M.E.Doc, FREDO, СОТА, які мають модулі для автоматичного формування звітності з урахуванням кадрових змін;

– система електронної взаємодії органів виконавчої влади (СЕВ ОВВ) – забезпечує автоматичний обмін інформацією між ПФУ та ДПС, органами соцзахисту тощо.

Переваги електронного формату подання:

– оперативність – можливість подати звіт у режимі реального часу.

– зручність – автоматичне підвантаження даних з кадрових і бухгалтерських модулів.

– безпека – передача інформації через захищені канали із застосуванням електронного підпису.

– зворотний зв'язок – роботодавець отримує підтвердження або повідомлення про помилки.

Проблеми та виклики:

– помилки при заповненні – неправильне зазначення дати, ІПН або причин звільнення можуть призвести до відхилення звіту;

– недосконаліть деяких облікових програм – не всі сервіси адаптовані до змін форм звітності;

– несвоєчасне подання – у випадку затримки з поданням даних може бути накладено штраф;

– недостатній рівень цифрової грамотності – особливо серед малих роботодавців.

Повідомлення про прийняття та звільнення працівників є ключовим елементом взаємодії між роботодавцем і Пенсійним фондом України. Електронна форма подання такої інформації значно спрощує процес, підвищує ефективність кадрового обліку та забезпечує прозорість у формуванні трудового стажу працівників. Правильне та своєчасне інформування про зміни у трудових відносинах є не лише вимогою закону, а й важливою умовою для гарантування соціальних прав громадян.

3. Взаємодія з Державною службою статистики України

Статистична звітність – це форма офіційного збору, систематизації та аналізу даних, яка забезпечує Державну службу статистики України (ДССУ) інформацією про соціально-економічні процеси в країні. Кожен суб'єкт господарювання залежно від галузі, форми власності, чисельності працівників та інших критеріїв отримує перелік форм державної статистичної звітності, обов'язкових до подання. Найпоширенішими є:

– Форма 1-ПВ (квартальна, місячна) – подається щодо обліку праці:

чисельність працівників, обсяги фонду оплати праці, відпрацьований час тощо;

– Форма 1-Підприємництво (річна) – включає економічні показники діяльності підприємства;

– Форма 5-ЗЕЗ – подається суб'єктами зовнішньоекономічної діяльності;

– Форма 2-інвестиції, 2-транспорт, 1-буд – залежно від галузі;

– Форма 1-торгівля, 1-послуги – подається відповідно суб'єктами торгівлі та сфери послуг.

Форми змінюються щороку наказами ДССУ, і для кожної з них встановлено терміни подання, заповнення реквізитів, обсяги звітної інформації.

Основним онлайн-ресурсом для роботи зі статистичною звітністю є сайт stat.gov.ua, який надає доступ до:

– законодавства та методології;

– бланків звітності та інструкцій щодо їх заповнення;

– новин і повідомлень щодо термінів подання форм;

– системи «Кабінет респондента», де підприємства отримують персоналізований список форм звітності, які вони зобов'язані подавати згідно з видами діяльності, обсягом операцій та організаційно-правовим статусом. Це дозволяє уникнути надмірного звітного навантаження та не витрачати ресурси на формування непотрібних документів.

Електронний кабінет респондента – це інтерактивна платформа для подання звітності підприємствами. У ньому респондент:

– бачить перелік форм, які він зобов'язаний подавати;

– завантажує файли звітів;

– підписує їх кваліфікованим електронним підписом (КЕП);

– отримує підтвердження про доставку та прийняття звітів ДССУ.

Інтерфейс кабінету простий, із фільтрами за роками, типами форм та статусами подання.

Для подання звітності до ДССУ респондент має пройти реєстрацію в електронному кабінеті:

– переходить на сайт stat.gov.ua → Електронна звітність → Вхід до кабінету;

– ідентифікується за допомогою КЕП;

– після входу в кабінет автоматично відображається перелік форм, що підлягають поданню.

Процес подання звітності складається з таких етапів:

– завантаження бланків статистичних форм (у форматі XML або DBF) із сайту;

– заповнення форм у бухгалтерській або статистичній програмі;

– імпорт заповнених форм до електронного кабінету;

– накладення КЕП (підписання);

– надсилання форми через кабінет.

Після надсилання звіт отримує статус: «Надіслано», «Прийнято», «Відхилено». При прийнятті формується квитанція – офіційне підтвердження

подання звітності. У разі помилок можна отримати повідомлення з поясненням, які саме дані некоректні.

Під час подання статистичних звітів застосовуються стандартизовані формати електронних файлів. Найчастіше використовуються:

– XML – структурований формат, що підтримує логічну перевірку даних;

– DBF – формат баз даних, переважно використовується для старіших форм;

– PDF/RTF – лише для ознайомлення або внутрішнього архівування, офіційно не подаються до ДССУ.

Форми мають бути підписані кваліфікованим електронним підписом (КЕП). Суб'єкт господарювання може використовувати підпис, виданий:

– Акредитованими центрами сертифікації ключів (Надавачами електронних довірчих послуг);

– ДП «Дія», «ПриватБанк», «Україна», «Вчасно» тощо.

Підпис підтверджує справжність і цілісність документа. Без КЕП система не приймає подання. Крім того, часто потрібно підписати документ як бухгалтером, так і керівником підприємства.

Під час електронного подання статистичної звітності респонденти стикаються з низкою типових помилок, зокрема:

– неправильний формат файлу – спроба завантажити файл у PDF або Excel замість XML або DBF;

– помилки в ідентифікаційних кодах – ЕДРПОУ, ІПН або код КОАТУУ введені неправильно;

– неактуальна форма – використання застарілої версії бланка;

– порушення структури файлу – неправильна кількість символів у полях, пропущені обов'язкові реквізити;

– відсутність підпису КЕП або некоректний підпис (наприклад, підпис не належить уповноваженій особі);

– подвійна подача звіту – система може не прийняти повторно надісланий файл або вважати його дублікатом;

– порушення термінів подання – подання після встановленої дати.

Для уникнення цих помилок важливо:

– використовувати актуальні версії програмного забезпечення;

– регулярно перевіряти оновлення форм на сайті stat.gov.ua;

– зберігати копії квитанцій та підтверджень у внутрішньому архіві підприємства.

4. Електронна система публічних закупівель Prozorro

У межах державних електронних сервісів особливе місце посідає система публічних закупівель Prozorro, яка є зразком відкритості та ефективності взаємодії бізнесу з державою. Через платформу Prozorro підприємства можуть подавати тендерні пропозиції, моніторити державні закупівлі, аналізувати тендерну документацію, брати участь у відкритих торгах, укладати електронні договори та оскаржувати результати конкурсів. Процес участі в закупівлях

передбачає створення електронного кабінету учасника, де завантажуються всі необхідні документи, а подальша взаємодія здійснюється виключно в цифровому форматі.

Електронна система публічних закупівель Prozorro – це державна інформаційно-телекомунікаційна система, що забезпечує проведення закупівель товарів, робіт і послуг за бюджетні кошти з максимальною прозорістю. Система працює за принципом «всі бачать все», що означає відкритість інформації на всіх етапах закупівельного процесу, використання електронних підписів, автоматичне інформування про всі етапи тендерів. Окрім того, система дозволяє інтегрувати дані з бухгалтерських систем, ERP-рішень, CRM-платформ, що особливо важливо для великих компаній, які працюють із кількома державними замовниками. Prozorro забезпечує взаємодію між замовниками (органами державної влади, бюджетними установами) та постачальниками (приватними компаніями, фізичними особами-підприємцями).

Система має дворівневу архітектуру:

– центральна база даних (ЦБД) – адмініструється ДП «Прозорро» і містить усю інформацію про закупівлі;

– комерційні майданчики – приватні електронні платформи (наприклад, Zakupki.Prom.ua, E-tender.ua), через які учасники беруть участь у тендерах.

Для участі в публічних закупівлях постачальнику необхідно зареєструватися на одному з авторизованих електронних майданчиків, які підключені до центральної бази Prozorro. Під час реєстрації потрібно надати:

– ідентифікаційні дані юридичної або фізичної особи;

– електронну пошту та номер телефону;

– кваліфікований електронний підпис (КЕП);

– банківські реквізити.

Після реєстрації постачальник має змогу шукати тендери за фільтрами (галузь, регіон, очікувана вартість) і брати участь у закупівлях. Участь передбачає подання цінової пропозиції, документів і, у деяких випадках, гарантії. Всі дії фіксуються в системі та доступні для перегляду іншими учасниками.

Тендерна документація – це основа участі в закупівлі.

Вона включає:

– документи, що підтверджують юридичний статус учасника (витяг з ЄДР, копії установчих документів);

– технічну пропозицію (відповідність технічному завданню замовника);

– цінову пропозицію;

– документи, що підтверджують відсутність підстав для відмови в участі (довідки з податкової, судимостей тощо).

Документи подаються у сканованому вигляді через особистий кабінет на майданчику. Учасник має дотримуватися строків подання та специфікацій, зазначених у тендерній документації. Всі файли підписуються КЕП.

Prozorro підтримує інтеграцію з обліковими та бухгалтерськими системами за допомогою API, що дозволяє:

– автоматично завантажувати документи з бухгалтерських систем до особистого кабінету на майданчику;

– передавати інформацію про укладені договори до систем фінансового обліку;

– формувати аналітичні звіти про участь у закупівлях, ефективність і прибутковість тендерної діяльності.

Це значно зменшує навантаження на бухгалтерів, мінімізує людські помилки та забезпечує оперативність обробки фінансових документів.

У Prozorro реалізований механізм моніторингу публічних закупівель, який здійснюється як автоматично, так і вручну державними органами (Держаудитслужбою, Рахунковою палатою). Для цього використовуються спеціальні ризик-індикатори, зокрема:

– короткий термін подачі пропозицій;

– обмеження конкуренції через вимоги;

– перемога одних і тих самих учасників;

– відсутність зниження ціни в ході аукціону.

Система автоматично фіксує такі ситуації та передає їх для аналізу аудиторам. Окрім того, будь-яка особа може подати звернення щодо ймовірного порушення під час проведення тендеру, і Prozorro забезпечує доступ до всієї історії закупівлі (включно з комунікацією між сторонами та скаргами).

5. Сервіс «Дія.Бізнес» і «Дія» як інструменти цифрової трансформації

У контексті цифрової трансформації особливу роль відіграє також платформа «Дія» та її підпроєкт «Дія.Бізнес». Ці сервіси були розроблені для спрощення адміністративних процедур, автоматизації реєстраційних дій та надання інформаційно-консультаційної підтримки підприємцям. За допомогою застосунку або порталу «Дія» користувачі можуть зареєструвати фізичну особу-підприємця, змінити види діяльності, отримати витяг із реєстру, зареєструвати касовий апарат (ПРРО), подати заяву на отримання державної допомоги, ініціювати процедуру зміни даних у Єдиному державному реєстрі.

«Дія.Бізнес» виступає як освітньо-довідкова платформа, яка містить мапу інституцій підтримки бізнесу, рекомендації щодо ведення підприємницької діяльності, алгоритми для різних видів юридичних процедур. Важливо, що ці сервіси адаптовані під різні цільові аудиторії – від початківців до досвідчених підприємців, що забезпечує комплексність і доступність.

Платформа «Дія.Бізнес» – це державна ініціатива з розвитку підприємництва, створена як частина загальної цифрової трансформації України. Її основна мета – забезпечити підприємців доступом до знань, підтримки, сервісів і консалтингу в онлайн-форматі.

Функціональні можливості платформи включають:

– інформаційне забезпечення: статті, гіди, інструкції щодо ведення бізнесу в Україні (реєстрація ФОП, оподаткування, зміна КВЕДів, вихід на експорт тощо);

– безоплатні консультації: юридичні, фінансові, маркетингові консультації доступні через платформу у форматі онлайн-бронювання;

– мапу підтримки бізнесу: інтерактивна карта з позначенням центрів підтримки бізнесу по всій Україні, включно з хабами Дія.Бізнес, програмами фінансової підтримки, освітніми ініціативами.

Також платформа виконує роль єдиного вікна для доступу до програм від держави, донорів і партнерських організацій, що підтримують мікро-, малий і середній бізнес.

Мобільний застосунок та портал «Дія» – це електронний сервіс, що надає можливості цифрового врядування для громадян і бізнесу. Для підприємців Дія значно спростила юридичні та податкові процедури.

Основні можливості для бізнесу:

– реєстрація ФОП онлайн: за 15 хвилин без візиту до державних органів. Необхідно лише авторизуватися через BankID або КЕП, заповнити форму, обрати КВЕД і систему оподаткування;

– внесення змін до Єдиного державного реєстру (ЄДР): наприклад, зміна адреси, видів діяльності (КВЕД), ПІБ, припинення діяльності;

– сплата податків: перегляд інформації про податкові зобов'язання, подача заяв, оплата ЄП та ЄСВ, перегляд податкової історії;

– перегляд та оновлення даних у державних реєстрах: зокрема, перевірка ліцензій, дозволів, звітності.

Дія також підтримує цифрові документи, що замінюють паперові – ID-картка, закордонний паспорт, РНОКПП, витяги про реєстрацію тощо.

Одна з ключових переваг «Дії» – можливість взаємодії з державою без черг і паперів. Через застосунок або портал можна подати різні види заяв:

– заяви на відкриття або припинення підприємницької діяльності;

– повідомлення про зміну КВЕДів або податкового статусу;

– заяви до ДРАЦС (реєстрація шлюбу, народження) – якщо ці дані важливі для бізнесу (наприклад, при зміні прізвища ФОПа).

Виписки, доступні в електронному форматі:

– виписка з ЄДР: підтвердження статусу юридичної чи фізичної особи-підприємця;

– витяг про доходи: для отримання кредитів, субсидій, грантів;

– підтвердження реєстрації в податкових органах.

Усі документи підписуються КЕП або Дія.Підписом, що дозволяє юридичне значення електронних дій.

Один із принципів ефективної цифрової трансформації – інтегрованість платформ. Дія активно взаємодіє з іншими державними та комерційними системами:

– ЦНАПи: обробляють запити, подані через Дію (наприклад, реєстрація місця проживання чи подача на видачу документа);

– банки-партнери: через Дію можна відкрити банківський рахунок під час реєстрації ФОП. Усе робиться за кілька кліків без особистої присутності;

– державні реєстри: інтеграція з ЄДР, реєстром податкових платників,

реєстром РНОКПП, кадастром, дозволяє отримувати й оновлювати дані в реальному часі;

– сервіси перевірки контрагентів: через платформу доступні витяги з реєстрів юридичних осіб, дозволів, судових рішень, боргів тощо.

Завдяки такій інтеграції Дія фактично перетворюється на багатофункціональний хаб, через який можна не тільки керувати бізнесом, а й перевіряти надійність партнерів.

Станом на 2025 рік платформа «Дія» поступово стає ключовим компонентом національного електронного документообігу, і ця роль лише зростає.

Основні тенденції розвитку:

– розширення функціоналу для бізнесу: планується повністю електронізувати процедури ліцензування, сертифікації, подання податкової звітності;

– цифрові суди та скарги: передбачається інтеграція із системою електронного правосуддя, подача скарг на податкові рішення, листування з органами через Дію;

– електронні трудові книжки: вже реалізована можливість перегляду трудового стажу в додатку, надалі – ведення повноцінного електронного кадрового обліку;

– автоматизовані сервіси: з'являються послуги, які працюють без запиту (наприклад, автоматичне призначення допомог, субсидій), бізнес також отримає подібні послуги (автоматичне нагадування про податки, терміни подачі звітів);

– міжнародна інтеграція: ведеться робота над визнанням українських цифрових документів за кордоном (цифрові паспорти, водійські посвідчення, реєстраційні документи ФОП).

Ці новації не лише зменшують бюрократію, а й сприяють формуванню довіри до держави, економлять ресурси підприємців і підвищують рівень цифрової грамотності населення.

6. Інші корисні державні електронні сервіси

У процесі цифрової трансформації державного управління особливої актуальності набувають електронні сервіси, що забезпечують оперативну взаємодію громадян, бізнесу та органів влади. Крім базових платформ, таких як «Дія», Prozorro чи Електронний кабінет платника податків, в Україні функціонує низка інших електронних сервісів, які значно спрощують доступ до публічної інформації, адміністративних та правових процедур. Ці сервіси охоплюють широке коло напрямів – від електронного правосуддя до державних реєстрів, порталів відкритих фінансів і цифрових інструментів для роботодавців.

Завдяки цим платформам зменшується адміністративне навантаження на бізнес, скорочуються часові та фінансові витрати при поданні звітності, запитів або участі у взаємодії з державою. Вони відіграють ключову роль у

забезпеченні прозорості державних процесів, доступності публічної інформації, контролю за використанням бюджетних коштів і захисту прав громадян.

Електронні інструменти, як-от Єдина судова інформаційна система (ЄСІТС), Єдиний державний реєстр юридичних осіб та фізичних осіб – підприємців, Електронний кабінет роботодавця, а також спеціалізовані портали відкритих даних і фінансів (E-Data, Spending.gov.ua, Opendatabot тощо) виконують свою унікальну функцію в цифровій інфраструктурі України, сприяючи створенню більш ефективного, відкритого та сервісного державного управління.

Електронний суд (офіційно – Єдина судова інформаційно-телекомунікаційна система, ЄСІТС) є платформою, що забезпечує електронний документообіг між судом, учасниками судових процесів, адвокатами, прокурорами, а також іншими зацікавленими сторонами. Завдяки ЄСІТС стало можливим подавати позовні заяви, відзиви, скарги, клопотання, інші процесуальні документи без фізичної присутності в суді.

Ключові переваги:

– швидкість: надсилання документів через електронну систему займає хвилини, а не дні;

– прозорість: можна відслідковувати стан розгляду справи, бачити призначених суддів, календар слухань;

– доказовість: подані документи фіксуються в системі з цифровим підписом, що підтверджує час і джерело подачі.

ЄСІТС дозволяє уникати черг, знижує витрати на доставку паперових документів та підвищує доступ до правосуддя, особливо у воєнний час чи для віддалених регіонів.

Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців і громадських формувань (ЄДР), адміністрований Міністерством юстиції України, є ключовим джерелом достовірної інформації про суб'єктів господарювання.

Основні функції:

– пошук і перегляд відкритої інформації про компанії, ФОПів, ГО;

– замовлення витягів, виписок та довідок – юридично значущих документів, які використовуються для участі в тендерах, відкриття рахунків, укладення договорів;

– подання запитів на реєстраційні дії, зокрема зміни в установчих документах, зміни керівника, адреси, видів діяльності.

Інформація у реєстрі оновлюється щоденно, що гарантує актуальність даних. Використання електронного підпису дозволяє подавати документи дистанційно.

Електронний кабінет роботодавця, створений Державною службою зайнятості, – це онлайн-сервіс для підприємств і організацій, що спрощує комунікацію з центрами зайнятості та дозволяє ефективніше керувати трудовими ресурсами.

Функціональні можливості:

– подання звітів про вакансії, прийом/звільнення працівників;

– отримання рекомендацій щодо підбору персоналу та доступу до резюме зареєстрованих безробітних;

– інформаційна підтримка щодо програм підтримки зайнятості, компенсацій ЄСВ, дотацій на працевлаштування;

– запис на співбесіди, участь у ярмарках вакансій онлайн.

Електронний кабінет також дозволяє укладати договори про стажування, перекваліфікацію, компенсації роботодавцям за працевлаштування ВПО, учасників бойових дій, людей з інвалідністю тощо.

Український уряд активно розвиває інші електронні сервіси для підвищення прозорості та доступності інформації. Найбільш вагомі серед них:

E-Data (https://edata.gov.ua) – портал публічних фінансів України:

– відображає всі транзакції з державного та місцевих бюджетів;

– дозволяє відслідковувати витрати бюджетних установ, дотацій, субвенцій;

– містить модуль Spending.gov.ua – детальний аналіз витрат.

Opendatabot (https://opendatabot.ua) – сервіс моніторингу державних реєстрів:

– автоматичне відстеження змін у ЄДР, судових справах, податковому статусі;

– сповіщення про появу боргів, арештів, податкових накладних;

– інтеграція з месенджерами: Telegram, Viber, Facebook Messenger.

Також існують інші портали:

– data.gov.ua – головний ресурс відкритих державних даних;

– e-licensing.gov.ua – платформа для отримання електронних ліцензій;

– ecomapa.gov.ua – екологічний портал, який відображає проблемні ділянки, забруднення, інтерактивну мапу сміттєзвалищ.

Ці сервіси разом формують єдину цифрову екосистему публічних електронних послуг, яка підтримує прозорість, зручність та ефективність взаємодії громадян і бізнесу з державними структурами. Їх використання не лише спрощує облік, управління і документообіг, а й слугує важливим інструментом у боротьбі з корупцією та в забезпеченні відкритості влади.

Тести

1. Що таке електронний цифровий підпис (ЕЦП)?

a) набір цифрових даних для шифрування файлів

b) набір цифрових даних, отриманих на основі електронного документа за допомогою криптографічного перетворення із закритим ключем

c) засіб створення секретних повідомлень

2. Який орган в Україні відповідає за адміністрування податкової звітності?

a) Пенсійний фонд України

b) Державна податкова служба України

c) Міністерство фінансів України

3. Яка форма звітності подається до ПФУ щодо страхового стажу працівників?

a) 1-ПВ

b) Додаток 5

c) J1312002

4. Яке призначення платформи Prozorro?

a) реєстрація нових підприємств

b) організація публічних закупівель

c) електронний обмін звітністю

5. Який сервіс забезпечує перевірку страхового стажу громадян?

a) Дія.Бізнес

b) eData

c) портал електронних послуг ПФУ

6. Що таке Кабінет респондента на сайті stat.gov.ua?

a) особиста сторінка громадянина

b) електронний інтерфейс для подання статистичної звітності

c) система реєстрації транспортних засобів

7. Для чого використовується система ЕСІТС?

a) обмін процесуальними документами в судовому процесі

b) подання митних декларацій

c) моніторинг страхових внесків

8. Що таке КЕП?

a) комп'ютерна електронна платформа

b) кваліфікований електронний підпис

c) ключ єдиного податку

9. Яка форма використовується для подання інформації про зміну трудових відносин?

a) Форма 20-ОПП

b) Додаток 5

c) 1-Підприємництво

10. Яка інформація міститься у витягу з ЄДР, що подається через «Дію»?

a) лише адреса компанії

b) лише код КВЕД

c) дані про суб'єкта господарювання, КВЕД, форму власності, керівника

11. Який файл зазвичай створюється програмами типу M.E.Doc для подання звітів?

a) .pdf

b) .xml

c) .doc

12. Що таке ризик-індикатори у Prozorro?

a) механізми моніторингу закупівель для виявлення потенційних порушень

b) інструменти обліку ПДВ

c) показники зростання цін

13. Який сервіс надає дані про використання бюджетних коштів?

a) Spending.gov.ua

b) Prozorro

c) OpenDataBot

14. Через який сервіс ФОП може зареєструвати бізнес онлайн?

a) Дія

b) Prozorro

c) Кабінет респондента

15. Яке основне призначення сервісу eData?

a) подання декларацій

b) відкриття інформації про публічні фінанси

c) реєстрація працівників

16. У якому форматі подаються звіти до Держстату?

a) тільки паперовому

b) .doc

c) .xml або .xls через кабінет респондента

17. Як отримати підтвердження про прийняття звіту до ПФУ?

a) через квитанцію № 2 у програмі подання

b) телефонним дзвінком

c) особистим зверненням до ПФУ

18. Який державний сервіс дозволяє подати заяву на допомогу по безробіттю?

a) M.E.Doc

b) Електронний кабінет роботодавця

c) Єдиний державний реєстр

19. Що таке Дія.Бізнес?

a) реєстр платників податків

b) онлайн-платформа для підтримки підприємців: консультації, мапа підтримки, освітні матеріали

c) тендерний майданчик

20. Який ключовий принцип функціонування Prozorro?

a) закритість інформації

b) «Всі бачать усе»

c) державна монополія на участь у тендерах

21. Який файл потрібно завантажити для оновлення кваліфікованого підпису?

a) .doc

b) .pdf

c) .dat або .zs2 (залежно від АЦСК)

22. Яка установа здійснює сертифікацію КЕП в Україні?

a) НБУ

b) Центри сертифікації ключів (АЦСК)

c) Prozorro

23. Який державний ресурс дозволяє перевірити судову справу за номером?

a) Єдиний державний реєстр судових рішень / ЄСІТС

b) Дія.Бізнес

c) Державна податкова служба

24. Яка послуга не надається через платформу «Дія»?

a) зміна місця голосування

b) подання тендерної пропозиції

c) перевірка податкового боргу

25. Що таке OpenDataBot?

a) портал надання держпослуг

b) сервіс для моніторингу державних реєстрів та юридичних ризиків

c) інструмент для судового обліку.

Завдання для мозкового штурму до теми 5 «Подання звітності та державні сервіси»

Завдання 1. Збій у поданні звітності до ПФУ.

Бухгалтер підприємства подав звітність за формою Додаток 5 через програму СОТА. Через годину на електронну пошту прийшло повідомлення про відмову у прийнятті.

Завдання:

Визначте можливі причини відмови та шляхи їх усунення.

Як діяти в умовах наближення граничного терміну подання?

Завдання 2. Помилка в тендерній пропозиції Prozorro.

Фірма подала документи для участі в закупівлі через майданчик Prozorro. Після подання виявилось, що завантажено неактуальну версію довідки про відсутність заборгованості.

Завдання:

Чи можна виправити помилку?

Які дії мають бути вжиті до завершення тендерного терміну?

Завдання 3. Несвоєчасне подання повідомлення про прийняття працівника.

Роботодавець прийняв нового працівника в понеділок, а повідомлення до ПФУ було подано у середу.

Завдання:

Які наслідки такої затримки?

Які нормативно-правові акти регулюють це питання?

Які запобіжні заходи можуть бути впроваджені для уникнення подібного?

Завдання 4. Підприємець-ФОП припустився помилки у звіті з ЄП.

Підприємець самостійно подав податкову декларацію через Електронний кабінет платника, однак забув вказати один з видів діяльності.

Завдання:

Який порядок виправлення звітності в такій ситуації?

Чи передбачені штрафи?

Як перевірити статус звіту?

Завдання 5. Інтеграція M.E.Doc із системою ПФУ не спрацьовує.

Бухгалтер налаштував обмін документами через M.E.Doc, однак при поданні звітності до ПФУ система повертає технічну помилку.

Завдання:

Розробіть алгоритм дій для усунення помилки.

Які служби підтримки можуть бути задіяні?

Як діяти, якщо проблему не вдається вирішити швидко?

Завдання 6. Бізнес планує повний перехід на роботу з Дією.

Молоде підприємство планує використовувати платформу «Дія» для реєстрації ФОП, подачі податкової звітності та отримання витягів з ЄДР.

Завдання:

Оцініть переваги та ризики такого переходу.

Які альтернативи або доповнення до «Дії» варто врахувати?

Завдання 7. Недостовірні дані у реєстрі страхового стажу.

Працівник при перевірці страхового стажу на порталі ПФУ виявив відсутність даних за кілька місяців роботи у 2022 році.

Завдання:

Як з'ясувати причини невідображення даних?

Які дії мають вжити працівник і роботодавець?

Які документи потрібно надати?

? Питання для самоконтролю

1. Які сервіси входять до структури електронного кабінету платника податків?
2. Що таке форма Додаток 5 і які саме дані до неї включаються?
3. Які електронні платформи підтримують автоматизовану взаємодію з ПФУ?
4. Які кроки потрібно пройти для подання статистичної звітності через сайт stat.gov.ua?
5. У чому полягають переваги інтеграції сервісу M.E.Doc або СОТА з державними порталами?
6. Як зареєструвати ФОП через мобільний застосунок «Дія»?
7. Які можливості надає Єдиний державний реєстр у контексті перевірки контрагентів?
8. Які документи можна отримати через портал електронних послуг ПФУ?
9. У чому полягає роль Prozorro в забезпеченні прозорості державних закупівель?
10. Які переваги забезпечує використання КЕП при поданні електронної звітності?

Питання для поглибленого вивчення теми 5 «Подання звітності та державні сервіси»

1. Ефективність електронного кабінету платника податків у процесі адміністрування податкових зобов’язань.
2. Цифровізація подання звітності до ПФУ: проблеми, перспективи, вплив на ринок праці.
3. Інтеграція бухгалтерських програм із державними електронними системами: порівняльний аналіз.
4. Вплив електронних сервісів на спрощення взаємодії бізнесу з державою в умовах воєнного стану.
5. Формування цифрової звітності як інструмент боротьби з корупцією у сфері публічних закупівель.
6. Сервіси «Дія» у сфері обліку та звітності: правове забезпечення та технологічні особливості.
7. Використання ЕСІТС в корпоративному секторі: можливості цифрового правосуддя для бізнесу.
8. Відкриті фінансові дані в E-Data як джерело для моніторингу ефективності використання бюджетних коштів.
9. Упровадження штучного інтелекту в процес обробки звітної інформації у державних сервісах.
10. Механізми кіберзахисту при поданні звітності через державні онлайн-платформи.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

.

РОЗДІЛ 2. ІНТЕГРАЦІЯ ЕЛЕКТРОННИХ СЕРВІСІВ І ДОКУМЕНТООБІГУ: БЕЗПЕКА ТА ЗБЕРІГАННЯ ДАНИХ

ТЕМА 6. ІНТЕГРАЦІЯ ЕЛЕКТРОННИХ СЕРВІСІВ

Мета: засвоєння знань про сучасні технології інтеграції, стандарти обміну даними; визначення переваг використання API та інших інструментів інтеграції; набуття навичок проєктування та аналізу інтегрованих систем для ефективного документообігу.

**План**

1. Об’єднання документів із CRM, ERP та іншими корпоративними системами.
2. API для інтеграції сервісів.
3. Приклади інтегрованих рішень для бізнесу.

***Ключові терміни та поняття:*** *API, CRM, ERP, протоколи, інтерфейси, інструменти, швидкість розробки, масштабованість, безпека, адаптивність, інтеграція платіжних систем, інтеграція з соціальними мережами, інтеграція з хмарними сервісами.*

1. Об’єднання документів із CRM, ERP та іншими корпоративними системами

Об’єднання документів із CRM (Customer Relationship Management), ERP (Enterprise Resource Planning) та іншими корпоративними системами є ключовим аспектом цифрової трансформації бізнесу. Це дозволяє оптимізувати процеси, покращити доступ до інформації та підвищити ефективність роботи організації. Нижче розглянуто основні аспекти цього питання, включаючи виклики, підходи та переваги.

Об’єднання документів передбачає інтеграцію різних корпоративних систем для централізованого доступу, обробки та зберігання інформації. Документи, які можуть бути пов’язані з операційною діяльністю (рахунки, контракти, звіти), автоматично синхронізуються між системами, забезпечуючи їх актуальність і доступність.

Виклики, що виникають при об’єднанні:

1) Технічні проблеми:

- різні формати даних: CRM, ERP та інші системи часто працюють із різними структурами файлів;
- несумісність систем: старі версії програмного забезпечення можуть не підтримувати інтеграцію з новими інструментами;
- складність налаштування API: інтеграція потребує належного налаштування інтерфейсів прикладного програмування.

2) Організаційні складнощі:

- стійкість до змін: співробітники можуть неохоче адаптуватися до нових

робочих процесів;

– висока вартість впровадження: інтеграція вимагає фінансових інвестицій і спеціалістів.

3) Безпека даних:

– передача конфіденційної інформації між системами створює ризики витоків.

Основні підходи до інтеграції документів:

1. Використання API – API дозволяють налаштовувати взаємодію між різними системами. Наприклад: CRM (як-от Salesforce, HubSpot) може бути підключена до ERP (SAP, Oracle) для передачі інформації про клієнтські замовлення. Інструменти документообігу (DocuSign, Adobe Sign) інтегруються через API для автоматизації підписання контрактів.

2. Використання спеціалізованих інтеграційних платформ – Платформи, такі як Zapier, MuleSoft або Microsoft Power Automate, спрощують інтеграцію шляхом налаштування готових модулів.

3. Централізовані системи управління документами (DMS) – DMS, такі як SharePoint, надають можливість об'єднувати документи з різних джерел і забезпечувати контроль доступу.

Переваги об'єднання документів:

1. Підвищення ефективності – автоматизація процесів зменшує час, необхідний на ручну роботу. Миттєвий доступ до документів із різних систем прискорює прийняття рішень.

2. Покращення якості даних – уникнення дублювання інформації. Дані завжди актуальні, оскільки оновлення в одній системі синхронізується з іншими.

3. Покращення досвіду клієнтів – менеджери мають повний доступ до історії клієнта, що сприяє персоналізованому підходу.

4. Відповідність регуляторним вимогам – централізоване зберігання забезпечує контроль версій документів і відповідність стандартам (наприклад, ISO, GDPR).

Галузеві приклади:

1. Логістика – ERP система відстежує запаси, а документи про відвантаження інтегруються в CRM, щоб клієнти отримували актуальну інформацію про доставку.

2. Фінансовий сектор – інтеграція платіжних документів між ERP і системами банківської звітності дозволяє уникнути помилок і прискорює розрахунки.

3. Охорона здоров'я – електронні медичні картки синхронізуються з CRM для ефективного управління контактами пацієнтів і планування лікування.

Майбутні тенденції:

1. Використання штучного інтелекту (AI) – AI може допомогти в автоматичній класифікації документів і пошуку необхідної інформації.

2. Хмарні технології – хмарні платформи забезпечують масштабованість інтеграцій і доступність даних.

Отже, об'єднання документів із CRM, ERP та іншими корпоративними

системами – це інвестиція в майбутнє бізнесу. Незважаючи на технічні й організаційні виклики, інтеграція сприяє ефективності, автоматизації та покращенню конкурентоспроможності. Правильний вибір інструментів і стратегій є ключем до успішного впровадження цього підходу.

2. API для інтеграції сервісів

API – це набір протоколів, інтерфейсів та інструментів, які дозволяють різним програмним системам взаємодіяти одна з одною. API визначає, як програмні компоненти повинні взаємодіяти, забезпечуючи стандартизований спосіб передачі запитів і отримання відповідей.

Існують різні типи API, які можна використовувати для інтеграції:

– REST API – це найбільш популярний тип API для інтеграції сучасних вебсервісів. Він використовує стандарт HTTP для обміну даними у форматах JSON або XML;

– SOAP API – це більш складний формат, який використовує XML для передачі даних, і часто застосовується в ситуаціях, де потрібна висока безпека або транзакційні процеси;

– GraphQL – це API, яке дозволяє запитувати тільки ті дані, які необхідні, що робить його дуже ефективним для клієнтських додатків;

– Webhooks – це тип API, який використовує механізм «push» для передачі даних, коли відбувається певна подія в системі.

Основні переваги API для інтеграції:

– швидкість розробки: використання готових API дозволяє швидше інтегрувати різні сервіси та знижує час розробки;

– масштабованість: API дозволяє легко масштабувати систему, додаючи нові сервіси або підключаючи нові програми;

– безпека: API зазвичай мають вбудовані механізми аутентифікації та авторизації, що забезпечує безпеку передачі даних;

– адаптивність: API дозволяють використовувати різні технології для інтеграції, що дає змогу налаштувати з'єднання між сервісами відповідно до конкретних потреб.

Важливість документованих API:

Якісна документація для API є необхідною умовою для успішної інтеграції. Це дозволяє розробникам швидко зрозуміти, як правильно використовувати API, отримувати від нього потрібні дані і коректно інтегрувати функціональність в інші системи.

Приклади використання API для інтеграції:

– інтеграція платіжних систем: API для платіжних систем, таких як Stripe, PayPal, або банківські API, дозволяють інтегрувати обробку платежів на вебсайті чи в мобільному додатку;

– інтеграція із соціальними мережами: API Facebook, Twitter, Instagram дозволяють взаємодіяти із соціальними мережами, публікувати контент або отримувати дані;

– взаємодія з базами даних: API для баз даних дозволяють інтегрувати

сервіси з різними джерелами даних, забезпечуючи доступ до інформації в режимі реального часу;

– інтеграція з хмарними сервісами: API хмарних сервісів (Google Cloud, AWS, Azure) дозволяють інтегрувати додатки з хмарними інфраструктурами для зберігання даних, обробки обчислень тощо.

Виклики при інтеграції через API:

– необхідність у сумісності: для ефективної роботи API сервіси повинні бути сумісними один з одним. Це може бути складно, якщо один із сервісів використовує старіші технології або специфікації;

– забезпечення безпеки: обробка конфіденційної інформації через API потребує належних заходів безпеки, таких як шифрування даних, автентифікація та авторизація;

– оновлення і зміни API: якщо API постійно змінюється або оновлюється, це може вплинути на стабільність інтеграції та вимагати додаткових налаштувань.

Як обрати API для інтеграції:

– оцініть функціональність та документацію API;

– перевірте стабільність і підтримку API (чи має API підтримку та оновлення);

– оцініть безпеку (шляхом автентифікації, шифрування і контролю доступу);

– перевірте сумісність із вашою системою.

API для інтеграції сервісів відіграють ключову роль у сучасній розробці програмного забезпечення. Вони дозволяють створювати гнучкі, масштабовані та безпечні системи, що взаємодіють між собою. Правильне використання API може значно підвищити ефективність роботи та знизити витрати на розробку, забезпечуючи ефективну взаємодію між різними додатками та сервісами.

3. Приклади інтегрованих рішень для бізнесу

Інтегровані рішення для бізнесу – це комплексні системи або набори інструментів, що дозволяють автоматизувати та покращити роботу підприємств, з'єднуючи різні технології, процеси й сервіси в одну єдину систему. Вони можуть охоплювати різні аспекти бізнес-діяльності, такі як управління ресурсами, фінансами, продажами, маркетингом тощо.

Ось кілька прикладів інтегрованих рішень для бізнесу:

1) ERP-системи (Enterprise Resource Planning).

Приклад: SAP, Oracle ERP, Microsoft Dynamics 365. ERP-системи дозволяють підприємствам автоматизувати основні бізнес-процеси, такі як управління фінансами, постачанням, виробництвом, персоналом, замовленнями та іншими аспектами діяльності. Вони інтегрують ці процеси в єдину платформу, що забезпечує зручність управління та прозорість бізнесу. Наприклад, дані про продажі автоматично передаються в бухгалтерію для обробки фінансових операцій.

2) CRM-системи (Customer Relationship Management).

Приклад: Salesforce, HubSpot, Zoho CRM. CRM-системи дозволяють

компаніям управляти взаємодіями з клієнтами, відстежувати продажі, автоматизувати маркетинг і покращувати обслуговування клієнтів. Вони інтегруються з іншими інструментами (наприклад, електронною поштою, чатами, соціальними мережами), що дозволяє зберігати всю інформацію про клієнтів в одному місці і забезпечувати персоналізоване обслуговування.

3) Інтеграція з платіжними системами.

Приклад: PayPal, Stripe, Square. Інтегровані платіжні рішення дозволяють бізнесам автоматизувати процеси оплати товарів і послуг через різні платіжні шлюзи. Платіжні системи можуть бути інтегровані з вебсайтами, мобільними додатками та ERP-системами для безшовного процесу обробки платежів, що забезпечує зручність як для користувачів, так і для бізнесу.

4) Інтеграція з хмарними сервісами для зберігання даних.

Приклад: Google Drive, Microsoft OneDrive, Amazon S3. Багато бізнесів інтегрують хмарні сховища даних для зберігання документів, звітів, даних про клієнтів та інших важливих файлів. Інтеграція з хмарними сервісами забезпечує доступ до даних в будь-який час із будь-якої точки світу, а також дає можливість автоматично зберігати і синхронізувати файли між різними пристроями.

5) Інтеграція маркетингових інструментів.

Приклад: Mailchimp, Google Ads, Facebook Ads, Hootsuite. Ці інструменти дозволяють бізнесам автоматизувати та інтегрувати маркетингові кампанії через різні платформи: соціальні мережі, електронну пошту, контекстну рекламу. Інтеграція цих сервісів із CRM та аналітичними системами дозволяє ефективно відслідковувати поведінку споживачів і оптимізувати маркетингові зусилля.

6) Інтеграція систем управління проєктами.

Приклад: Asana, Trello, Jira. Інтегровані рішення для управління проєктами дозволяють бізнесам відстежувати прогрес проєктів, координувати роботу команд, планувати ресурси та терміни. Інтеграція з іншими системами (наприклад, з CRM або фінансовими системами) дозволяє автоматизувати процеси і забезпечити прозорість у виконанні завдань.

7) Системи для моніторингу продуктивності та аналітики.

Приклад: Google Analytics, Power BI, Tableau. Ці інтегровані рішення дозволяють бізнесам відстежувати ключові показники ефективності (KPI) і здійснювати глибокий аналіз даних про клієнтів, продажі та операції. Інтеграція з іншими системами, такими як CRM або ERP, дозволяє отримувати більш повну картину про діяльність компанії.

8) Інтеграція із соціальними мережами.

Приклад: Buffer, Sprout Social. Інтегровані рішення для роботи із соціальними мережами дозволяють автоматизувати публікацію контенту, взаємодіяти з підписниками та відстежувати ефективність кампаній у соцмережах. Вони можуть бути інтегровані з CRM та аналітичними інструментами для поліпшення маркетингових стратегій.

9) Інтеграція із системами управління ланцюгом поставок (SCM).

Приклад: Oracle SCM Cloud, SAP SCM. Ці системи дозволяють

автоматизувати процеси закупівель, управління запасами, складування і логістики. Інтеграція з ERP і фінансовими системами дозволяє покращити ефективність ланцюга поставок, зменшити витрати та забезпечити своєчасне постачання товарів.

10) Інтеграція із системами обробки великих даних (Big Data).

Приклад: Hadoop, Apache Spark. Для бізнесів, які працюють із великими обсягами даних, інтеграція з Big Data системами дозволяє обробляти та аналізувати дані в реальному часі, отримуючи важливу інформацію для прийняття управлінських рішень.

Інтегровані рішення для бізнесу дозволяють оптимізувати робочі процеси, покращити взаємодію з клієнтами, знизити витрати і забезпечити більш ефективне управління різними аспектами бізнесу. Вибір конкретного інтегрованого рішення залежить від потреб компанії, її розміру, сфери діяльності та бізнес-цілей.

Тести

1. Яка основна перевага об'єднання документів із CRM та ERP?

a) підвищення витрат на впровадження
b) оптимізація бізнес-процесів
c) складність у налаштуванні

2. Що є основною перешкодою для інтеграції документів між системами?

a) простота налаштування API
b) несумісність систем
c) відсутність автоматизації процесів

3. Що таке REST API?

a) тип API, який використовує HTTP для передачі даних
b) протокол для передачі голосових даних
c) інструмент для створення вебсторінок

4. Який формат даних найчастіше використовує REST API?

a) YAML
b) XML
c) JSON

5. Що таке централізовані системи управління документами (DMS)?

a) платформи для зберігання й управління документами
b) системи для автоматизації продажів
c) інструменти для маркетингових кампаній

6. Що забезпечує використання хмарних сервісів у зберіганні даних?

a) високі витрати
b) доступність даних із будь-якої точки світу
c) уповільнення роботи системи

7. Що є прикладом інтеграційної платформи?

a) Adobe Photoshop
b) Microsoft Power Automate
c) SQL Server

8. Яка перевага використання AI для інтеграції документів?

a) автоматична класифікація документів

b) складність пошуку інформації

c) ручне впровадження змін

9. Що є основною проблемою при використанні API для інтеграції?

a) простота підтримки

b) проблеми сумісності між системами

c) надмірна автоматизація

10. Як називається система, яка автоматизує фінансові операції?

a) CRM

b) DMS

c) ERP

11. Що є основною функцією CRM-систем?

a) зберігання медичних даних

b) управління взаємовідносинами з клієнтами

c) розробка вебсайтів

12. Яка система допомагає відстежувати прогрес проєктів?

a) ERP

b) Asana

c) SharePoint

13. Що є ключовою перевагою інтеграції документів?

a) високі витрати на обслуговування

b) зменшення дублювання даних

c) уповільнення роботи команди

14. Що є прикладом платіжної системи для інтеграції?

a) SharePoint

b) PayPal

c) Jira

15. Що таке SOAP API?

a) API, яке використовує XML для передачі даних

b) інструмент для аналітики

c) платформа для автоматизації

16. Яка система забезпечує інтеграцію маркетингових інструментів?

a) SAP

b) Mailchimp

c) Salesforce

17. Яка функція є ключовою для хмарних сховищ даних?

a) синхронізація файлів

b) управління фінансами

c) відстеження клієнтів

18. Що є прикладом ERP-системи?

a) Microsoft Dynamics 365

b) Google Drive

c) Slack

19. Який інструмент інтегрується для створення платіжних рішень?
a) Tableau
b) Stripe
c) Trello
20. Що забезпечує інтеграція з Big Data?
a) зниження ефективності
b) аналіз даних у реальному часі
c) ускладнення бізнес-процесів
21. Що таке Webhooks?
a) API, яке передає дані при певній події
b) протокол для електронної пошти
c) інструмент для управління завданнями
22. Яка система підтримує управління ланцюгом постачання?
a) Slack
b) SAP SCM
c) Instagram
23. Що є головним завданням інструментів аналітики?
a) взаємодія з клієнтами
b) відстеження ключових показників ефективності
c) управління командою
24. Яка система автоматизує управління документами?
a) SharePoint
b) Twitter
c) Oracle Cloud
25. Що є ключовою функцією інтеграції із соціальними мережами?
a) зменшення охоплення
b) автоматизація публікацій
c) видалення контенту.

Завдання для мозкового штурму до теми 6 «Інтеграція електронних сервісів»

Завдання 1. Виклики інтеграції.

Які ключові технічні, організаційні та безпекові виклики виникають під час інтеграції CRM, ERP та інших систем? Як їх можна вирішити?

Визначте головні проблеми та можливі підходи до їх усунення.

Завдання 2. Ідеальний сценарій інтеграції.

Як виглядає ідеальна інтеграція документів між CRM, ERP та іншими корпоративними системами? Які функції вона повинна виконувати?

Розробіть концепцію ідеального рішення, яке відповідає потребам користувачів.

Завдання 3. Розробка нових функцій API.

Які додаткові функції API можуть зробити інтеграцію більш ефективною

та зручною?

Запропонуйте нові інструменти та підходи для підвищення зручності використання API.

Завдання 4. Платформи інтеграції.

Які переваги або недоліки від використання спеціалізованих платформ (Zapier, MuleSoft, Microsoft Power Automate)? Як можна покращити існуючі рішення?

Проаналізуйте сучасні платформи інтеграції та запропонуйте ідеї для їх удосконалення.

Завдання 5. Вдосконалення DMS.

Як централізовані системи управління документами (наприклад, SharePoint) можуть бути вдосконалені для кращої інтеграції з CRM і ERP?

Знайдіть шляхи оптимізації функціональності DMS для підвищення ефективності.

Завдання 6. Досвід клієнта.

Як інтеграція документів може покращити взаємодію з клієнтами та підвищити їх задоволеність?

Згенеруйте ідеї для підвищення клієнтського досвіду завдяки інтеграції систем.

Завдання 7. Безпека даних.

Які методи та технології можуть бути використані для забезпечення безпеки даних під час інтеграції?

Сформуйте ідеї для підвищення захисту конфіденційної інформації.

Завдання 8. Використання AI.

Як можна застосувати штучний інтелект (AI) для автоматизації інтеграції документів і пошуку необхідної інформації?

Дослідіть можливості AI для оптимізації процесів інтеграції.

Завдання 9. Галузеві приклади.

Які реальні кейси з інтеграції документів у логістиці, фінансах, охороні здоров’я чи інших галузях можна адаптувати до вашого бізнесу?

Дослідіть успішні приклади для створення власних рішень.

Завдання 10. Хмарні інтеграції.

Які переваги надає використання хмарних технологій для інтеграції документів? Як вирішити виклики, пов’язані з переходом на хмарні платформи?

Оцініть можливості хмарних інтеграцій та сформуйте стратегії їх упровадження.

? Питання для самоконтролю

1. Які основні виклики виникають при об’єднанні документів із CRM, ERP та іншими корпоративними системами?
2. Які технічні проблеми можуть виникнути при інтеграції різних систем (наприклад, CRM та ERP)?
3. Які підходи до інтеграції документів найбільш ефективні? Опишіть роль API в цьому процесі.
4. Як спеціалізовані інтеграційні платформи (наприклад, Zapier чи MuleSoft) спрощують процес об’єднання документів?
5. Які переваги об’єднання документів для бізнесу, зокрема для управління ефективністю та покращення якості даних?
6. Яким чином об’єднання документів допомагає в досягненні відповідності регуляторним вимогам (наприклад, GDPR)?
7. У яких галузях найбільше використовуються інтегровані рішення для об’єднання документів (наприклад, логістика, фінанси, охорона здоров’я)?
8. Які майбутні тенденції в об’єднанні документів, зокрема у використанні штучного інтелекту та хмарних технологій?
9. Як API дозволяють здійснювати інтеграцію між різними сервісами, і які їх переваги для бізнесу?
10. Які основні кроки потрібно виконати для вибору правильного API для інтеграції в бізнес-процеси?

Питання для поглибленого вивчення теми 6 «Інтеграція електронних сервісів»

1. Ефективність інтеграції документів у CRM та ERP системах: аналіз продуктивності.
2. Вплив автоматизації документів на точність бізнес-операцій у CRM.
3. Використання штучного інтелекту для аналізу документів в інтегрованих системах.
4. Проблеми інформаційної безпеки при інтеграції документів.
5. Роль API у спрощенні інтеграції документів між корпоративними системами.
6. Аналіз продуктивності інтеграційних платформ для документообігу.
7. Інтеграція документів у системи ERP: вплив на фінансовий менеджмент.
8. Вплив інтеграції документів на управління ланцюгами постачання.
9. Гібридні моделі інтеграції документів: поєднання локальних і хмарних рішень.
10. Майбутнє інтеграції документів: роль блокчейну в управлінні корпоративними даними.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 7. ОРГАНІЗАЦІЯ ЗБЕРІГАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Мета: засвоєння принципів і технологій безпечного та ефективного зберігання електронних документів, забезпечення їх доступності, цілісності та відповідності нормативним вимогам; ознайомлення із сучасними методами архівування, класифікації та резервного копіювання електронних документів, а також із законодавчими нормами й технічними стандартами щодо довготривалого збереження інформації в цифровому форматі.

План

1. Організація електронного архіву документів.
2. Вимоги до зберігання та архівування електронних документів.

Ключові терміни та поняття: *хмарне зберігання, локальне зберігання, електронний архів, довгострокове зберігання, системи архівування, резервне копіювання, інтеграція з архівами, знищення документів, методи знищення, протоколи знищення.*

1. Організація електронного архіву документів

Здатність захистити свою інформацію від сторонніх осіб і запобігти її випадковій втраті відіграють важливу роль. Збереження інформації дуже важливо як для простого користувача, так і для підприємств. Для зберігання даних в електронному вигляді використовуються різноманітні пристрої, деякі з яких відрізняються високою надійністю. Зберігання інформації – найважливіша запорука розвитку людського суспільства, передача знань і руху вперед. Це помітно як на глобальному рівні, так і на рівні конкретної людини або підприємства. Кожному сьогодні доводиться якось по-своєму вирішувати питання, пов’язані зі збереженням цифрових файлів. На щастя, для цього є чимало спеціальних пристроїв і накопичувачів. Але чи всі рішення, девайси і носії можуть бути визнані по-справжньому надійними? На жаль, далеко не всі способи зберігання даних гарантують повну безпеку і, тим більше, зручність.

На електронних носіях у цифровому вигляді, у формі, яка дозволяє здійснити перевірку, необхідно зберігати первинні документи та перелік файлів звітності. Для оподаткування платники податків мають вести облік витрат, доходів та інших фактів, які відносяться до об’єктів оподаткування чи податкових обов’язків, на підставі фінансової звітності, первинних документів, документів, які мають відношення до обчислення і сплати податків і зборів, що передбачені законом. Самі платники податків обов’язково мають забезпечити зберігання вище згаданих документів і документів, які мають відношення до виконання вимог закону.

Способи зберігання електронних документів

Зберігати електронні документи передусім потрібно захищено. З основних способів можна виділити три, які передбачають будь-яку кількість

користувачів архіву та електронних документів:

1. Хмарне зберігання – доступне лише за наявності інтернету, проте є захищеним. Доступ до нього надає провайдер електронного документообігу з можливістю обмеження доступу за ролями та з видачею паролів.

2. Локальне зберігання – вважається найпростішим, адже являє собою папку на робочому столі комп'ютера. Зручний він тим, що всі мають до нього доступ, проте видаляти файли може тільки координатор такого зберігання. Також завантажувати файл у архів необхідно за чіткими правилами, проте гарантій безпеки такий спосіб зберігання не дає.

3. Архів системи електронного документообігу – найчастіше такий спосіб використовується з метою зберігання внутрішнього документообігу, проте його можна використовувати і в зовнішніх цілях. Такий архів надійний, доступ до нього також можна обмежити за ролями до певних документів.

Що повинна забезпечувати система електронних документів.

Першочергово архів електронних документів, здавалось би, мав би просто забезпечувати зберігання даних. Проте, враховуючи використання документів у зовнішніх звітах, перевірках, юридичних запитів, вони мають відповідати низці вимог у процесі їх зберігання:

– доступність до документа через посилання;

– формат документа, який такий же читабельний, як і друкований;

– постійне переформатування документа для зберігання його актуального формату з огляду на зміни в системах електронного обміну;

– маркування документів для їх ідентифікації та швидкого пошуку в архіві.

Електронний архів, система електронного архіву – система структурованого зберігання електронних документів, що забезпечує надійність зберігання, конфіденційність і розмежування прав доступу, відстеження історії використання документа, швидкий і зручний пошук.

Електронний архів відноситься до класу систем управління корпоративним контентом (Enterprise Content Management). Безліч організацій приходить до його впровадження через використання мережевих папок загального користування, але ще не будучи готовими до впровадження систем електронного документообігу, часто громіздких і складних, тому електронні архіви позиціонують як основу документообігу.

Зберігання інформації та документів є одним із найвідповідальніших етапів у циклі інформаційної діяльності. Зберігання документів суворо регламентовано законодавством, особливо, якщо це стосується документів виключної суспільно-економічної цінності.

Діяльність аудіовізуальних та електронних архівів розвивається в межах інформаційного типу суспільних відносин.

До початку 90-х років об'єктом законодавчого регулювання були тільки КФФД як частина ГАФ. Але в міру розвитку інформаційних технологій електронні архіви, які включають у себе програмні ресурси, бази даних та інші групи ресурсів, стали значущим об'єктом законодавчого регулювання і навіть більшою мірою у сфері законотворчого управління.

У межах юридичного забезпечення аудіовізуальних та електронних архівів

основними суб'єктами правовідносин є засоби масової інформації, архіви і меншою мірою фізичні особи. У низці спеціальних законодавчих актів суб'єктом правових відносин виступає держава. Це стосується сфери створення, зберігання і використання тих електронних ресурсів, які можуть містити важливі відомості з точки зору забезпечення державної безпеки. Основним для законодавчої практики є визначення архівів як інформаційних систем. У цій якості архіви включають в себе:

– інформаційні ресурси (носії первинної та вторинної документної інформації);

– інформаційні технології (засоби, що забезпечують збереження документів, забезпечення опису та доступу до документів).

Саме як інформаційні системи аудіовізуальні та електронні архіви стають об'єктом і складовою частина інформаційних відносин. Усі юридичні особи незалежно від форм власності повинні застосовувати спеціальний Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затверджений наказом Мін'юсту від 11.11.2014 р. № 1886. На цей документ потрібно особливо звернути увагу, адже він містить різноманітні вимоги, зокрема щодо:

– найменування файлів електронних документів;
– найменування файлів електронних облікових документів;
– найменування файлів архівних електронних документів.

Серед іншого установи зобов'язані створювати документи постійного та тривалого (понад 10 років) зберігання у двох формах – паперовій та електронній (рис. 7.1).

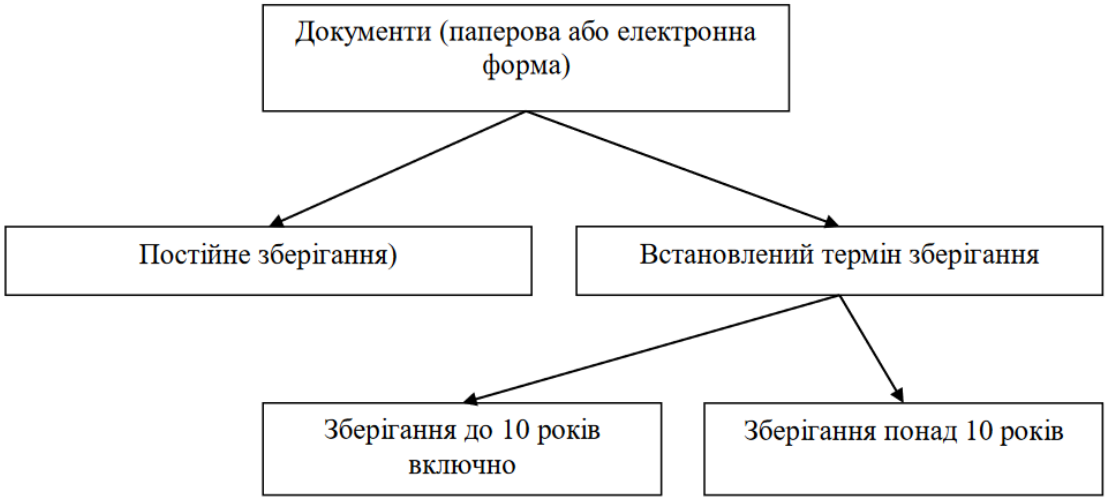


Рисунок 7.1 – Групування документів відносно термінів зберігання

Упровадження такої системи перш за все починається з потреби структурувати електронну інформацію незалежно від того, чи це документи текстові, мультимедіа або графіка: підписані контракти, первинна фінансова, а також технічна та проєктна документація.

Електронний архів включає такі базові функції:

– управління документами та ієрархічною структурою архіву (check-

in/check-out, безпека, управління сервісами, призначення документам атрибутів);

– іміджинг документів (оцифрування, трансформація, подання у різних форматах паперових документів);

– потоковий ввід – прискорення занесення великого масиву типових і різнорідних документів у систему;

– управління Web-контентом;

– системи повідомлень, що дозволяють користувачам обмінюватися повідомленнями, а також призначати завдання й відстежувати статус їх виконання.

Залежно від різновиду системи архіву та її призначення, з'являються специфічні функції, як-от:

– для систем автоматизації архівного діловодства – формування та оформлення архівних справ, автоматичне формування номенклатури справ, облік і контроль використання справ;

– для архівів нормативно-технічної документації – функція актуалізації, що нагадує користувачеві про необхідність перевірити актуальність поданого в системі стандарту;

– для архівів фінансової (платіжної) документації – функція вибірки, що дозволяє в найкоротші терміни вивести весь необхідний перелік документів, що вимагається, наприклад, для податкових перевірок.

Система автоматизації архівного діловодства необхідна для архівного підрозділу підприємства. Допомагає формувати архівні справи, номенклатуру справ, вести облік, контролювати дати обов'язкового зберігання і т. д.

Виділяють такі ***види архіву:***

– електронний архів фінансової (платіжної) документації забезпечує централізований облік і зберігання електронних образів первинних фінансово-економічних документів, договорів та інших документів, що мають відношення до фінансово-економічної діяльності підприємства;

– електронний архів проєктної документації дозволяє проєктним організаціям зберігати весь спектр документів, а саме: креслення, кошториси, пояснювальні записки і багато іншого;

– електронний архів нормативних документів являє собою організований каталог усіх стандартів підприємства, закуплених і (або) розроблених ним. Створення такого архіву тісно пов'язане з проблемою авторського права компаній-розробників стандартів і часто буває однією з умов проходження сертифікації;

– електронний архів технічної документації призначений для організацій, чия діяльність пов'язана з постачанням товарів і забезпечує зберігання супутньої технічної документації (керівництва користувача, технічні характеристики та ін.);

– електронний архів юридичної документації, що містить договори і супутню документацію;

– електронний архів кадрової документації, що використовується для зберігання особових справ, трудових договорів, наказів і розпоряджень,

інструкцій і регламентів усередині компанії;

– електронний архів конструкторської документації дозволяє організувати доступ до копій креслень незалежно від їх давності.

Створення та початок роботи з електронним архівом включає в себе такі кроки:

1. Налаштування необхідних правил доступу та користування системою – хто має можливість переглядати, додавати чи видаляти види документів.
2. Сканування паперових документів для передачі їх до електронного архіву.
3. Маркування документів за певними критеріями для подальшого зручного його пошуку (наприклад, дата, серія, номер, тип).
4. Робота з архівом електронних документів у компанії відповідно до заданих правил.
5. Корегування переліку документів – додавання або вилучення за необхідності.
6. Знищення або зберігання оригіналів на складських площах залежно від необхідності компанії.

2. Вимоги до зберігання та архівування електронних документів

Зберігання та архівування електронних документів – це важливий аспект електронного документообігу, який забезпечує їх безпеку, доступність і юридичну значущість протягом усього періоду їх зберігання. Законодавство, технічні стандарти та кращі практики встановлюють вимоги до зберігання та архівування електронних документів, щоб забезпечити їх автентичність, цілісність та доступність. Порушення цих вимог може призвести до правових і фінансових наслідків для організацій.

Основні вимоги до зберігання електронних документів:

1. Технічні вимоги:

– цілісність та незмінність документа: для збереження цілісності електронних документів застосовуються криптографічні методи, зокрема цифрові підписи та хеш-функції. Це дозволяє гарантувати, що документ не був змінений після його підписання чи створення;

– захист від несанкціонованого доступу: документи мають бути збережені в захищених електронних сховищах, таких як бази даних або спеціалізовані архіви, з доступом, обмеженим для неавторизованих осіб. Для цього використовуються засоби шифрування даних та системи контролю доступу;

– регулярне оновлення програмного забезпечення: оскільки зберігання документів здійснюється на цифрових носіях, необхідно регулярно оновлювати програмне забезпечення для забезпечення сумісності з новими технологіями та протидії застаріванню форматів;

– безперервність зберігання (data redundancy): важливо забезпечити резервне копіювання документів і використання кількох копій для запобігання втратам у разі технічних збоїв або катастрофічних ситуацій.

2. Юридичні вимоги:

– визначення строків зберігання: законодавство та внутрішні нормативні

акти організацій можуть визначати строки, протягом яких документи повинні зберігатися. Наприклад, деякі документи (контракти, податкові звіти, фінансова документація) мають зберігатися впродовж кількох років після завершення їх дії;

– юридична значущість електронних документів: законодавство передбачає, що електронний документ має таку ж юридичну силу, як і паперовий, якщо він підписаний кваліфікованим електронним підписом і відповідає вимогам щодо зберігання;

– дотримання норм щодо конфіденційності: для документів, що містять конфіденційну або персональну інформацію, необхідно забезпечити захист за допомогою механізмів шифрування та контролю доступу відповідно до вимог законів про захист персональних даних та інформаційної безпеки.

3. Формати та сумісність:

– вибір формату документа: для зберігання електронних документів рекомендується використовувати формати, які є широко підтримуваними і мають стандартні технічні вимоги (наприклад, pdf/a для архівування). Вибір формату визначає, як легко буде здійснювати доступ до документів у майбутньому, навіть якщо технології зміняться;

– сумісність з іншими системами: оскільки електронні документи можуть зберігатися в різних програмних системах і платформах, важливо забезпечити сумісність з іншими системами, а також забезпечити можливість міграції даних у разі зміни програмного забезпечення або оновлення технологій.

Вимоги до архівування електронних документів:

1. Архівування та тривале зберігання:

– довгострокове зберігання: архівування електронних документів передбачає їх зберігання на тривалі строки, що можуть варіюватися залежно від типу документа та вимог законодавства. Наприклад, для архівування документів із фінансовими даними та податковими звітами можуть встановлюватися строки до 10 років;

– системи архівування: для ефективного архівування електронних документів організації повинні впроваджувати спеціалізовані архівні системи. Такі системи повинні забезпечувати захист від пошкоджень, зберігання метаданих (дата, час створення, автор, зміни тощо), а також можливість швидкого доступу до документів за необхідності.

Скільки можна зберігати електронні документи. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. Так, документи бухгалтерії необхідно зберігати строком не менше ніж 5 років – рахунки-фактури, накладні, акти. Угоди потрібно зберігати від 5 років до постійного їх утримання – контракти, додаткові погодження, додатки. Інші документи в середньому мають знаходитися в архіві близько 5 років – довідки, листи, специфікації.

Так, залежно від змістового наповнення виокремлюють такі терміни зберігання: 1 рік; 3 роки; 5 років; 10 років; 75 років; постійно.

При цьому потрібно пам’ятати, що стосовно бухгалтерських документів,

реєстрів та звітної документації строк зберігання встановлюється (з урахуванням терміну забезпечення ревізії) з 1 січня року, наступного за роком закінчення справи щодо процесу діловодства.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері, який більш детально наведено в таблиці 7.1.

Таблиця 7.1 – Строки зберігання первинних документів

№	Вид документа
3 роки	
1	Розрахункові відомості сплати внесків до різних фондів
2	Договори кредитні, застави, гарантії, переведення боргу (після закінчення строку дії договору)
3	Відомості на виплату грошей (за відсутності розрахунково-платіжних відомостей – 75 років)
4	Довіреності (у т. ч. анульовані) на одержання грошових сум і товарно-матеріальних цінностей; на одержання зарплати та інших виплат
5	Документи (копії звітів, витяги з протоколів, висновки, заяви, довідки, списки працівників) про виплату допомоги, пенсій, оплату листків непрацездатності з фонду соціального страхування
6	Документи (заяви, рішення, довідки, листи) про оплату відпусток у зв'язку з навчанням, одержання пільг із податків тощо
7	Документи (акти, відомості, листи) про взаєморозрахунки між організаціями
8	Протоколи взаємозаліків
9	Документи (акти, процентовки, довідки, рахунки) про приймання виконаних робіт
10	Первинні документи та додатки до них, що фіксують факт виконання господарських операцій і стали підставою для записів у регістрах бухобліку та податкових документах (касові, банківські документи, ордери, повідомлення банків і переказні вимоги, виписки банків, корінці квитанцій, банківських чекових книжок, наряди на роботу, акти про приймання, здавання і списання майна й матеріалів, квитанції і накладні з обліку ТМЦ, рахунки-фактури, авансові звіти тощо)
11	Податкові накладні
12	Документи (плани, звіти, протоколи, акти, довідки, доповідні записки) документальних ревізій, перевірок та аудиту фінансово-господарської діяльності, контрольно-ревізійної роботи, у т.ч. перевірок каси, правильності стягнення податків тощо
13.	Документи (довідки, акти, зобов'язання, листи) щодо розтрат, недостач, розкрадань
14.	Документи (протоколи засідань інвентаризаційних комісій, акти інвентаризації, інвентаризаційні описи, порівняльні відомості) про інвентаризацію основних засобів, нематеріальних активів, грошових коштів, матеріальних цінностей тощо
10 років	
15.	Аналітичні документи (таблиці, доповіді, доповідні записки тощо) до річних звітів і балансів
75 років	
16.	Розрахунково-платіжні відомості (особові рахунки) працівників, аспірантів, студентів
До ліквідації підприємства	
17.	Звіти (відомості) про нарахування та перерахування страхових внесків на державне та недержавне соціальне страхування (пенсійне, на випадок безробіття, у зв'язку з тимчасовою непрацездатністю тощо: зведені річні й з більшою періодичністю; річні й з більшою періодичністю
18.	Документи (протоколи, акти, звіти, відомості переоцінки й визначення зношеності основних засобів) про переоцінку основних фондів, нематеріальних активів, незавершеного будівництва

2. Копії та резервне копіювання:

– резервне копіювання: всі важливі електронні документи повинні регулярно резервуватися, щоб уникнути їх втрати в разі аварій або збоїв у системах зберігання. Зазвичай створюються декілька копій, що зберігаються в

різних фізичних або хмарних місцях;

– інтеграція з архівами: архівування електронних документів також повинно бути інтегровано в загальну стратегію інформаційного управління підприємства. Архіви повинні відповідати вимогам зберігання та доступності інформації на всіх етапах її життєвого циклу.

3. Доступність та інтеграція:

– безперервний доступ до архівованих документів: незважаючи на те, що документи можуть бути архівовані на довгий термін, організації повинні забезпечити безперешкодний доступ до них для перевірки, відновлення або використання в разі необхідності;

– відновлення з архіву: архівовані документи повинні бути збережені таким чином, щоб їх можна було швидко відновити за необхідності. Важливо використовувати систему, яка дозволяє відновити документи в їхній первісній формі без втрат даних.

Архівування також доцільно виконувати перед кожним сеансом сервісного обслуговування (розрахунку підсумків, перепроведення документів, тестування даних та ін.) (рис. 7.2).

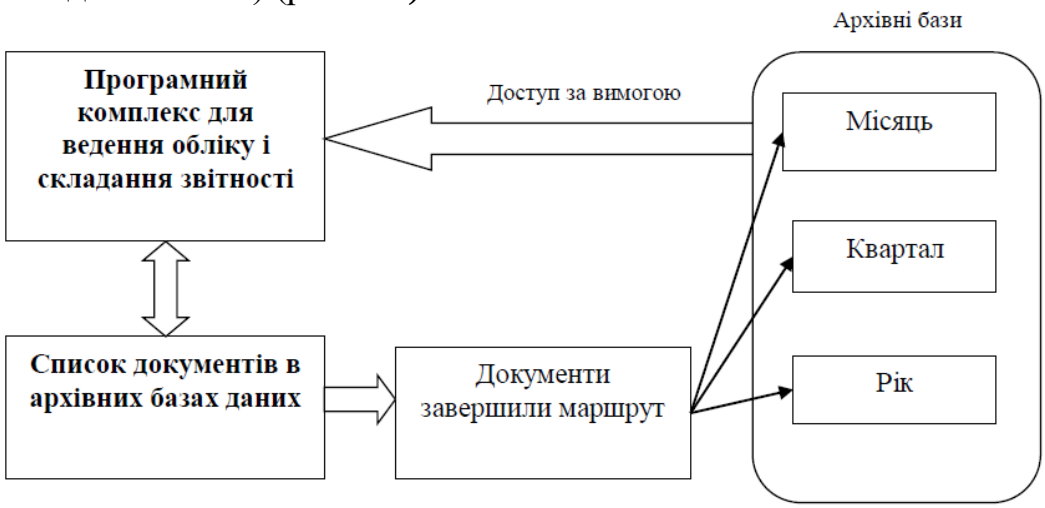


Рисунок 7.2 – Загальна архітектура архівації документів програмних продуктів

Вимоги до знищення електронних документів:

– знищення документів: після закінчення строку зберігання документи повинні бути знищені, щоб запобігти витоку конфіденційної інформації або порушенню норм законодавства щодо захисту персональних даних;

– методи знищення: для безпечного знищення електронних документів використовуються спеціалізовані методи стирання даних, що гарантують, що інформація не може бути відновлена після її видалення. Наприклад, використання методів багаторазового стирання або фізичного знищення носіїв інформації;

– протоколи знищення: організації повинні дотримуватися протоколів і стандартів для знищення електронних документів, що забезпечує контроль за цим процесом і підтверджує його відповідність нормативним вимогам.

Перспективи вдосконалення зберігання та архівування електронних документів. Із розвитком технологій, таких як **блокчейн**, нові можливості відкриваються для забезпечення безпеки та зберігання електронних документів. Технології блокчейн можуть стати важливим інструментом для забезпечення незмінності та автентичності документів, а також для їх архівування в дистрибутивних реєстрах, що забезпечить новий рівень захисту від несанкціонованого доступу та змін.

Зберігання та архівування електронних документів є складним і важливим процесом, що потребує дотримання численних технічних і юридичних вимог. Від правильного підходу до збереження та архівування документів залежить їхня юридична сила, доступність у майбутньому, а також захист від несанкціонованого доступу і втрат.

Тести

1. Який із способів зберігання електронних документів є найбільш надійним?

a) локальне зберігання
b) хмарне зберігання
c) архів системи електронного документообігу

2. Яка основна вимога до електронного документа?

a) цілісність та незмінність документа
b) легкість доступу
c) підтримка всіх форматів

3. Які документи мають бути збережені в електронному вигляді на термін не менше 5 років?

a) протоколи засідань
b) бухгалтерські документи
c) листи кореспонденції

4. Як називається система, що забезпечує зберігання та управління електронними документами?

a) архівна система
b) система електронного архіву
c) документообігова система

5. Який формат документа є найкращим для архівування?

a) PDF
b) PDF/A
c) DOCX

6. Який із способів зберігання документів має мінімальну безпеку?

a) архів системи електронного документообігу
b) локальне зберігання
c) хмарне зберігання

7. Що з перерахованого є важливою функцією електронного архіву?

a) маркування документів для швидкого пошуку
b) використання лише одного формату для документів

c) виключення доступу до документів для співробітників

8. Яка основна причина для впровадження електронного архіву в організаціях?

a) підвищення вартості зберігання

b) забезпечення збереження та зручного доступу до документів

c) зменшення обсягу фізичного простору

9. Яка вимога до зберігання електронних документів є юридичною?

a) захист від технічних збоїв

b) юридична значущість документів

c) наявність цифрового підпису

10. Як часто необхідно оновлювати програмне забезпечення для збереження електронних документів?

a) кожного року

b) регулярно для сумісності з новими технологіями

c) тільки за необхідності

11. Яка кількість копій необхідна для забезпечення безперервності зберігання документів?

a) 1 копія

b) кілька копій для резервного копіювання

c) 5 копій

12. Який термін зберігання документів для бухгалтерії?

a) 3 роки

b) 5 років

c) 10 років

13. Яка із систем архіву використовується для зберігання фінансової документації?

a) архів проєктної документації

b) електронний архів фінансової документації

c) електронний архів конструкторської документації

14. Що необхідно зробити для початку роботи з електронним архівом?

a) налаштувати правила доступу до документів

b) прочитати документи архіву

c) підготувати фізичні копії документів

15. Яка з перерахованих функцій є специфічною для архівів фінансової документації?

a) оцифрування документів

b) функція вибірки документів для податкових перевірок

c) формування архівних справ

16. Яка основна мета електронного архіву у проєктній документації?

a) зберігання листів

b) збереження креслень і технічних характеристик

c) архівування фінансових документів

17. Яка інформація не повинна бути доступна в електронному архіві?

a) листи від постачальників

b) конфіденційна інформація без належного захисту

c) документи, які були підписані

18. Як часто необхідно здійснювати резервне копіювання електронних документів?

a) щоразу, коли додаються нові документи

b) регулярно, щоб уникнути втрати даних

c) тільки в разі великих оновлень

19. Що є частиною юридичних вимог для зберігання електронних документів?

a) вибір безпечного носія

b) визначення строків зберігання документів

c) знищення документів після закінчення терміну зберігання

20. Яка функція є основною для архіву нормативно-технічної документації?

a) формування архівних справ

b) актуалізація стандартів та перевірка їх відповідності

c) створення шаблонів для документів

21. Які документи повинні зберігатися в електронному вигляді на тривалий строк?

a) короткострокові контракти

b) фінансові звіти та податкові документи

c) листи та кореспонденція

22. Яка з цих функцій є загальною для всіх типів електронних архівів?

a) управління доступом до документів

b) оцифрування документів

c) формування фінансової документації

23. Як забезпечується захист від несанкціонованого доступу до документів?

a) оновлення програмного забезпечення

b) засоби шифрування та контроль доступу

c) регулярне оновлення бази даних

24. Який із цих типів архіву призначений для зберігання особистих справ співробітників?

a) архів проєктної документації

b) електронний архів кадрової документації

c) архів фінансової документації

25. Яка з вимог до електронного архіву є технічною?

a) збереження юридичної значущості

b) цілісність та незмінність документа

c) виконання юридичних норм.

Завдання для мозкового штурму до теми 7 «Організація зберігання електронних документів»

Завдання 1. Пошук нових способів захисту електронних документів.

Як можна підвищити рівень безпеки зберігання електронних документів?

Які технології чи інструменти можна додати до сучасних систем для збереження конфіденційності та цілісності даних?

Розгляньте можливості використання блокчейн-технологій, багатофакторної автентифікації та інших інновацій.

Завдання 2. Розробка інтерфейсу для системи електронного архіву.

Яким має бути інтерфейс системи зберігання електронних документів, щоб забезпечити простоту і зручність користувачів?

Як можна полегшити процес пошуку і сортування документів за допомогою метаданих?

Завдання 3. Моделювання сценаріїв для зберігання документів із різним терміном зберігання.

Як організувати зберігання документів з різними термінами (1 рік, 3 роки, 5 років, 10 років)?

Як забезпечити доступ до них на різних етапах життя документа?

Як автоматизувати процес архівування і знищення за встановленими термінами?

Завдання 4. Аналіз впливу цифрових підписів на юридичну значущість електронних документів.

Як впливає використання цифрових підписів на юридичну силу електронних документів?

Які переваги й недоліки використання цифрових підписів у системах електронного документообігу?

Завдання 5. Розробка стратегії для впровадження електронних архівів в організаціях.

Які основні кроки має виконати компанія для впровадження електронного архіву?

Як можна здійснити перехід від паперових архівів до електронних? Які проблеми можуть виникнути на етапі цього переходу?

Завдання 6. Оцінка юридичних ризиків при порушенні вимог до зберігання електронних документів.

Які юридичні наслідки можуть виникнути в разі порушення вимог до зберігання електронних документів?

Як можна знизити ці ризики, застосовуючи технології або внутрішні політики?

Завдання 7. Розробка політики доступу до електронних документів за ролями.

Як організувати доступ до архіву в компанії?

Які критерії для розмежування прав доступу до документів з різною важливістю і конфіденційністю?

Завдання 8. Використання хмарних технологій для зберігання електронних архівів.

Як хмарні технології змінюють підхід до зберігання електронних документів?

Які плюси та мінуси хмарного зберігання в контексті електронних архівів?

Завдання 9. Аналіз майбутнього розвитку електронних архівів.

Як будуть розвиватися системи електронного архіву в найближчі 10-20 років?

Які нові технології можуть вплинути на еволюцію зберігання електронних документів?

Завдання 10. Моделювання та автоматизація процесу архівування документів.

Як автоматизувати процес архівування в організації?

Які програмні рішення можуть полегшити цей процес і зробити його більш ефективним та безпечним?

? Питання для самоконтролю

1. Що таке електронний архів і для чого він потрібен? Опишіть основні функції електронного архіву та поясніть його значення в сучасному світі.
2. Перелічіть основні способи зберігання електронних документів. Порівняйте хмарне зберігання, локальне зберігання та архіви систем електронного документообігу.
3. Які вимоги повинна виконувати система електронного архіву? Охарактеризуйте критерії доступності, формату та зручності пошуку документів.
4. Які технічні вимоги до зберігання електронних документів? Поясніть, як забезпечується цілісність, незмінність і захист від несанкціонованого доступу.
5. Що таке юридична значущість електронного документа? Обґрунтуйте, за яких умов електронний документ прирівнюється до паперового.
6. Чому важливо обирати правильний формат для зберігання документів? Розкажіть про популярні формати, що забезпечують тривале зберігання (наприклад, PDF/A).
7. Як організувати доступ до електронного архіву? Поясніть, як налаштування прав доступу та ролей впливає на безпеку документів.
8. Які етапи створення електронного архіву?
9. Перерахуйте ключові кроки, включаючи сканування, маркування та структурування документів.
10. Які строки зберігання електронних документів встановлені законодавством?
11. Наведіть приклади строків для бухгалтерських, податкових та інших документів.
12. Які системи автоматизації архівного діловодства існують? Охарактеризуйте різновиди архівів, наприклад, архіви фінансової, технічної чи кадрової документації.

Питання для поглибленого вивчення теми 7 «Організація зберігання електронних документів»

1. Еволюція стандартів для зберігання електронних документів у різних юрисдикціях.
2. Вплив хмарних технологій на ефективність та безпеку електронних архівів.
3. Правові аспекти цифрових підписів в електронних архівах.
4. Моделі управління доступом до електронних архівів в організаціях.
5. Технології для автоматичного архівування документів: переваги та недоліки.
6. Ризики та способи забезпечення юридичної значущості електронних архівів у разі їх знищення або пошкодження.
7. Вплив інтелектуальних технологій на організацію електронних архівів.
8. Економічна ефективність упровадження електронних архівів у державних установах.
9. Тенденції та майбутнє електронних архівів у контексті захисту персональних даних.
10. Динаміка змін в управлінні електронними архівами в умовах цифрової трансформації бізнесу.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 8. КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Мета: засвоєння основних принципів забезпечення конфіденційності та захисту персональних даних в умовах електронного документообігу; ознайомлення з нормативно-правовими актами, що регулюють захист даних, а також сучасними методами та технологіями захисту інформації; визначення ефективних заходів для мінімізації загроз, що стосуються інформаційної безпеки та приватності.

План

1. Загальні принципи захисту даних (GDPR, Закон України «Про захист персональних даних»).
2. Політика доступу до документів.
3. Етичні аспекти роботи з електронними сервісами.

Ключові терміни та поняття: *політика доступу до документів, оптимізація доступу, контроль і моніторинг, прозорість, захист конфіденційної інформації, шифрування, журнали подій, антивірусний захист.*

1. Загальні принципи захисту даних (GDPR, ЗУ «Про захист персональних даних»)

Захист персональних даних є важливим аспектом у сучасному цифровому світі. Регламенти, такі як Загальний регламент захисту даних ЄС (GDPR) та Закон України «Про захист персональних даних» (ЗУ «Про захист персональних даних»), встановлюють стандарти обробки, зберігання та захисту персональних даних. Розглянемо основні принципи цих нормативно-правових актів (табл. 8.1).

Таблиця 8.1 – Порівняльна характеристика основних принципів Закону України «Про захист персональних даних» та GDPR

Принцип	GDPR	Закон України «Про захист персональних даних»
Законність, справедливість і прозорість	Обробка даних повинна бути законною, прозорою та справедливою щодо суб'єкта даних. Це передбачає чітке інформування осіб про цілі, обсяг і методи обробки їхніх даних.	Вимагає отримання згоди суб'єкта даних та забезпечення інформованості.
Цільове обмеження	Дані обробляються виключно для визначених і законних цілей. Їх не можна використовувати для інших цілей без додаткової згоди.	Обробка повинна відповідати встановленим цілям або згоді суб'єкта.
Мінімізація даних	Збираються лише ті дані, які необхідні для конкретних цілей.	Регламентує збір лише необхідного обсягу даних.
Точність даних	Дані повинні бути точними та актуальними, з можливістю їх виправлення чи видалення.	Передбачає забезпечення коректності та своєчасного оновлення даних.
Обмеження терміну зберігання	Дані зберігаються тільки до досягнення мети їх обробки.	Забороняє тривале зберігання даних після досягнення мети.
Цілісність і конфіденційність	Дані повинні бути захищені від втрати, пошкодження чи несанкціонованого доступу.	Вимагає забезпечення конфіденційності та захисту даних.
Підзвітність	Контролер повинен демонструвати відповідність вимогам регламенту.	Вимагає від суб'єктів господарювання дотримання правил захисту персональних даних та надання звітності щодо їхньої обробки.
Права суб'єктів даних	Забезпечує права: доступ, виправлення, видалення, обмеження обробки, перенесення даних, заперечення проти обробки, підпадати під рішення, засновані виключно на автоматизованій обробці тощо.	Включає права: знати мету обробки, вимагати виправлення чи видалення даних, знати про джерела збору даних, відкликати згоду на обробку даних.
Міжнародна співпраця	Передача даних дозволяється лише за умови забезпечення адекватного рівня захисту.	Вимагає гарантій захисту при транскордонній передачі даних.
Відповідальність за порушення	Значні штрафи: до 20 млн євро або 4% річного обороту компанії.	Встановлює адміністративну та кримінальну відповідальність за порушення законодавства.
Попередній аналіз ризиків	Перед обробкою даних із високими ризиками (наприклад, використання чутливих даних) вимагається оцінка впливу на захист даних (Data Protection Impact Assessment, DPIA).	Закон також враховує необхідність оцінки ризиків, особливо для чутливих даних.
Обов'язкове повідомлення про витік даних	Контролери повинні повідомляти органи нагляду про порушення захисту даних протягом 72 годин.	Закон передбачає обов'язковість інформування у разі порушення безпеки даних.

Захист персональних даних є ключовим елементом сучасного управління інформацією. Дотримання принципів GDPR та Закону України «Про захист персональних даних» дозволяє забезпечити безпеку даних і довіру користувачів до систем, які їх обробляють.

2. Політика доступу до документів

Політика доступу до документів є ключовим аспектом управління інформацією в будь-якій організації. Вона визначає, хто, коли і за яких умов може отримати доступ до документів, що зберігаються в організації. Ця політика охоплює як фізичні, так і електронні документи, забезпечуючи конфіденційність, цілісність і доступність інформації.

1) Цілі політики доступу до документів

- забезпечення безпеки інформації: захист конфіденційних даних від несанкціонованого доступу;
- дотримання законодавства: відповідність вимогам регуляторів і нормативних актів (наприклад, GDPR, ISO 27001);
- оптимізація доступу: забезпечення швидкого доступу до інформації для уповноважених осіб;
- контроль і моніторинг: відстеження доступу до документів для запобігання витокам або зловживанням.

2) Основні принципи політики доступу:

- рівень доступу: доступ до документів базується на ролі або посаді співробітника в організації (рольовий доступ);
- прозорість: користувачі повинні бути інформовані про правила доступу до документів та їх права;
- мінімізація доступу: доступ обмежується лише тими документами, які необхідні для виконання службових обов’язків;
- контроль і аудит: ведеться облік усіх операцій доступу до документів, щоб забезпечити прозорість і можливість перевірки;
- захист конфіденційної інформації: документи з високим рівнем конфіденційності мають посилені механізми захисту.

3) Компоненти політики доступу до документів

- класифікація документів: усі документи розподіляються за категоріями на основі рівня конфіденційності (відкриті, внутрішні, конфіденційні, строго конфіденційні);
- механізми автентифікації: використання паролів, двофакторної автентифікації або біометричних даних для ідентифікації користувачів;
- резервне копіювання: регулярне створення резервних копій для забезпечення доступності документів у разі аварії;
- процедури видалення: чітко визначені правила знищення або архівування документів, які більше не потрібні;
- реєстр доступу: фіксація всіх операцій доступу (хто, коли і до яких документів отримував доступ).

4) Ролі та відповідальність

- користувачі: дотримання політики доступу та захист документів;

– адміністратори: створення та підтримка системи доступу, моніторинг її роботи;

– керівники: визначення рівня доступу для співробітників;

– відповідальні за безпеку: розробка та реалізація заходів захисту документів.

5) Технологічні аспекти політики доступу

– системи управління доступом (Access Control Systems): забезпечують автоматизацію процесу розподілу доступу;

– шифрування: захист документів від несанкціонованого прочитання навіть у разі їх викрадення;

– журнали подій: записи всіх операцій доступу для аналізу та розслідувань;

– антивірусний захист: забезпечує безпеку документів у цифровому середовищі.

6) Законодавчі вимоги

Політики доступу до документів мають враховувати вимоги національного законодавства та міжнародних стандартів, зокрема:

– GDPR (ЄС): правила захисту персональних даних і обмеження доступу;

– ISO 27001: вимоги до інформаційної безпеки та управління доступом;

– Закон України «Про захист персональних даних»: визначає права суб'єктів даних і відповідальність за порушення.

7) Ризики порушення політики

– несанкціонований доступ до конфіденційної інформації;

– втрата або витік даних через недотримання процедур;

– юридична відповідальність через порушення законодавства.

8) Рекомендації для ефективної політики

– проводити регулярні аудити доступу до документів;

– навчати персонал правил політики доступу;

– оновлювати політику відповідно до змін у законодавстві чи бізнес-процесах;

– упроваджувати сучасні технології захисту інформації.

Політики доступу до документів є невід'ємною частиною управління інформацією в сучасних організаціях. Їх правильне впровадження дозволяє мінімізувати ризики, пов'язані з витоками даних, і забезпечити ефективну роботу всіх підрозділів.

3. Етичні аспекти роботи з електронними сервісами

У сучасному світі електронні сервіси стали невід'ємною складовою життя людей, організацій та держави. Їх широке впровадження приносить багато переваг – зручність, швидкість обміну інформацією, автоматизація процесів. Однак паралельно з технічними досягненнями постають і серйозні етичні виклики, які потребують уваги як з боку розробників сервісів, так і з боку користувачів.

Одним із *ключових етичних аспектів є захист конфіденційності та приватності*. Електронні сервіси збирають та обробляють значні обсяги

персональних даних: від контактної інформації до фінансових або медичних відомостей. Це створює ризики зловживань, витоків даних або їх комерційного використання без згоди користувача. Етичною є така практика, коли користувачі поінформовані про те, які саме дані збираються, як довго вони зберігаються, та з якою метою будуть використані. У свою чергу, компанії повинні дотримуватися принципів прозорості, мінімізації даних, захисту інформації за допомогою технічних і правових засобів.

Ще одним важливим питанням є *етика використання алгоритмів та штучного інтелекту*. Багато сервісів автоматизують прийняття рішень, наприклад, щодо надання кредитів, розміщення реклами чи модерації контенту. Небезпека полягає в тому, що такі алгоритми можуть бути упередженими, непрозорими або дискримінаційними. Відповідальні компанії зобов'язані забезпечити відкритість принципів роботи таких систем, можливість пояснення автоматичних рішень, а також надати механізм оскарження або корекції результатів.

Також важливу роль відіграє цифрова доброчесність – це *моральне ставлення до інформаційної діяльності в інтернеті*. Вона передбачає недопустимість:

- плагіату;
- підробки контенту;
- навмисного поширення неправдивої інформації;
- маніпуляцій або використання ботів.

Кожен користувач повинен діяти відповідально, поширюючи інформацію лише з перевірених джерел і дотримуючись загальних норм етики онлайн-комунікації.

Окрім того, етика цифрових сервісів включає питання соціальної інклюзії – *доступність технологій для всіх груп населення*, зокрема людей з інвалідністю, осіб похилого віку або тих, хто має обмежений доступ до інтернету. Розробники сервісів повинні враховувати потреби цих груп, створювати доступний інтерфейс, адаптувати вміст до різних форматів сприйняття, забезпечувати можливість зворотного зв'язку.

Не менш важливим є й право на забуття – *можливість користувача видалити свої персональні дані з електронного сервісу*. Це право є проявом поваги до приватного життя людини та її бажання контролювати власну цифрову присутність. Компанії, які надають електронні послуги, повинні створити прості та зрозумілі механізми реалізації цього права.

У сучасному інформаційному суспільстві електронні сервіси охоплюють майже всі сфери діяльності: банківську справу, освіту, охорону здоров'я, державне управління, комерцію, соціальні мережі тощо.

Масове використання цих сервісів породжує нові етичні виклики, які не завжди можуть бути вирішені виключно правовими методами.

Етика у сфері цифрових технологій стосується насамперед чесності, відповідальності, справедливості, рівності доступу та захисту гідності людини.

Основні етичні проблеми роботи з електронними сервісами, їхній зміст та приклади прояву наведено в таблиці 8.2.

Таблиця 8.2 – Основні етичні проблеми роботи з електронними сервісами

№	Етична проблема	Сутність проблеми	Приклади прояву
1	Конфіденційність і захист даних	Незаконне збирання, зберігання або передача персональних даних	Витік медичних записів, передача персональних даних рекламним агентствам
2	Непрозорість алгоритмів	Користувачі не знають, як працюють алгоритми та чому ухвалюються певні рішення	Алгоритм автоматично відмовляє у кредиті без пояснення причин
3	Цифрова нерівність	Обмеження доступу до сервісів для певних соціальних або вікових груп	Вебпортал недоступний для людей з вадами зору або без стабільного інтернету
4	Порушення авторських прав	Незаконне копіювання, поширення або використання інтелектуальної власності	Завантаження чужих фотографій, текстів або відео без зазначення авторства
5	Кібербулінг та електронна агресія	Агресивна, принизлива або образлива поведінка в онлайн-середовищі	Анонімні образи, переслідування в соціальних мережах, погрози через месенджери
6	Відсутність відповідальності	Уникнення відповідальності за дії сервісу або наслідки цифрових рішень	Ігнорування розробниками скарг на помилки або шкоду, завдану через програму
7	Маніпуляції та фейки	Поширення неправдивої або маніпулятивної інформації для впливу на свідомість людей	Використання ботів для штучного збільшення популярності, фабрикація новин
8	Відмова у праві на забуття	Неможливість видалити свої персональні дані або обліковий запис	Сервіс не надає опції видалення акаунта чи історії активності

Наведені в таблиці 8.2 етичні проблеми свідчать про те, що розвиток електронних сервісів неминуче супроводжується новими моральними викликами. Ці виклики охоплюють як технічні, так і гуманітарні аспекти – від безпеки персональних даних до недопущення дискримінації, інформаційної маніпуляції чи цифрової ізоляції окремих груп.

Ігнорування етичних норм у цифровому середовищі може призвести до втрати довіри користувачів, порушення прав людини та навіть до юридичних санкцій. Натомість упровадження етичних стандартів – таких як прозорість, відповідальність, інклюзивність і повага до приватності – сприяє створенню справедливого та безпечного цифрового простору.

Таким чином, етична рефлексія має стати невід’ємною складовою розробки, впровадження та використання електронних сервісів як у державному, так і в приватному секторі.

Електронні сервіси дедалі активніше впроваджуються в ключові сфери суспільного життя – освіту, державне управління та бізнес. Вони полегшують комунікацію, автоматизують процеси, підвищують ефективність і прозорість. Однак одночасно з технічними можливостями виникають і етичні виклики, пов’язані з конфіденційністю, відповідальністю, справедливістю та рівним доступом. Саме тому роль етики в цих сферах набуває першочергового

значення, адже нехтування моральними принципами може призвести до зловживань, соціальної нерівності та недовіри до цифрових інструментів.

В освітньому процесі використання електронних платформ має базуватися на чесності здобувачів освіти і викладачів. Важливо запобігати академічному шахрайству, плагіату, маніпуляціям з електронною звітністю.

У державному управлінні важливо дотримуватися принципу доброчесності: електронні послуги не повинні бути інструментом контролю за громадянами чи обмеження їхніх прав. Електронне голосування, цифрові паспорти, електронні заяви мають бути прозорими, захищеними і доступними для перевірки.

У бізнесі використання даних клієнтів для аналітики чи маркетингу має відбуватися з дотриманням добровільної згоди. Етичний бізнес підвищує лояльність клієнтів і репутацію компанії.

Отже, етика є критично важливою складовою впровадження електронних сервісів у сфері освіти, державного управління та бізнесу. В освітньому процесі вона сприяє формуванню академічної доброчесності та захищає права учасників освітнього середовища. В публічному секторі етичні норми є гарантією прозорості, справедливості й довіри громадян до цифрових послуг. У бізнесі дотримання етичних стандартів забезпечує лояльність клієнтів, репутацію компаній і довготривалу конкурентну перевагу. Лише за умови усвідомлення та дотримання етичних принципів цифрові технології можуть справді служити суспільству, зберігаючи його гуманістичні цінності.

Загалом, етичні аспекти використання електронних сервісів охоплюють питання поваги до особистості, захисту прав, прозорості, відповідальності та справедливості. Вони є важливими не лише з морального погляду, а й як умова сталого розвитку цифрового середовища, де кожен користувач може відчувати себе захищеним, поінформованим і рівноправним учасником цифрової взаємодії.

Тести

1. Що є основним принципом обробки персональних даних згідно з GDPR?

a) дані можуть оброблятися без згоди суб’єкта

b) обробка даних повинна бути законною, прозорою та справедливою

c) обробка даних дозволена для будь-якої мети

2. Яке правило стосується мінімізації даних?

a) збираються лише ті дані, які необхідні для конкретних цілей

b) дані можуть збиратися без обмежень

c) дані повинні зберігатися без визначених термінів

3. Що передбачає принцип цільового обмеження?

a) дані можна використовувати для будь-яких цілей

b) дані обробляються лише для визначених і законних цілей

c) дані обробляються без згоди суб’єкта

4. Як забезпечується точність даних?

a) забороняється виправлення даних

b) дані повинні бути точними та актуальними
c) дані можуть бути застарілими

5. Що включає підзвітність контролера згідно з GDPR?
a) відсутність обов'язку звітувати
b) демонстрація відповідності вимогам регламенту
c) вільний доступ до персональних даних

6. Що означає принцип обмеження терміну зберігання?
a) дані зберігаються лише до досягнення мети їх обробки
b) дані зберігаються без обмежень
c) дані видаляються тільки після запиту суб'єкта

7. Яке право має суб'єкт даних згідно з GDPR?
a) можливість видалення даних контролером
b) доступ до своїх даних та їх виправлення
c) повна заборона на обробку своїх даних

8. Який штраф передбачено за порушення GDPR?
a) до 1 млн євро
b) до 2% річного обороту компанії
c) до 20 млн євро або 4% річного обороту компанії

9. Що вимагає Закон України «Про захист персональних даних»?
a) отримання згоди суб'єкта даних
b) вільну передачу даних третім сторонам
c) збереження даних без термінів

10. Яке правило стосується конфіденційності даних?
a) дані повинні бути доступними всім
b) дані захищені від втрати, пошкодження чи несанкціонованого доступу
c) дані можна поширювати без обмежень

11. Що є метою політики доступу до документів?
a) забезпечення безпеки інформації
b) надання доступу до всіх документів усім співробітникам
c) відмова від моніторингу доступу

12. Що включає контроль і аудит доступу до документів?
a) облік усіх операцій доступу до документів
b) відсутність моніторингу
c) надання доступу без реєстрації

13. Який принцип забезпечує мінімізацію доступу?
a) надання доступу всім працівникам
b) обмеження доступу до необхідних документів
c) зняття обмежень на доступ

14. Як забезпечується прозорість політики доступу?
a) приховування правил доступу
b) інформування користувачів про правила доступу
c) доступ лише для адміністрації

15. Що є ключовою технологією захисту документів?
a) використання незахищених систем
b) шифрування даних

c) відмова від автентифікації

16. Який стандарт міжнародного рівня регулює політику доступу?

a) ISO 27001
b) ISO 14001
c) ISO 9001

17. Що є складовою автентифікації в політиці доступу?

a) використання паролів, двофакторної автентифікації чи біометрії
b) відсутність засобів захисту
c) використання лише паролів

18. Який ризик можливий через порушення політики доступу?

a) втрата або витік даних
b) повний контроль над доступом
c) відсутність загроз

19. Що включає класифікація документів?

a) вільний доступ до всіх документів
b) розподіл документів за рівнем конфіденційності
c) архівування без розподілу

20. Що є ключовим правом суб'єкта даних?

a) знати мету обробки своїх даних
b) відмова від доступу до даних
c) передача даних без його згоди.

Завдання для мозкового штурму до теми 8 «Конфіденційність та захист персональних даних»

Завдання 1. Загальні принципи захисту даних (GDPR, ЗУ «Про захист персональних даних»).

Учасники розподіляються на дві групи.

Завдання для першої групи: дати відповіді на питання:

1. Як забезпечити прозорість політики конфіденційності для різних аудиторій (співробітників, клієнтів, партнерів)?
2. Які інструменти можна використати для автоматизації обмеження термінів зберігання даних?

Завдання для другої групи: дати відповіді на питання:

3. Як навчати співробітників правильного поводження з персональними даними?
4. Яким чином компанія може мінімізувати ризики витоку даних у разі кібератаки?
5. Як зробити обробку даних відповідною до законодавства, зберігаючи при цьому ефективність бізнес-процесів?

Після обговорення групи презентують результати, а потім разом формулюють висновки.

Завдання 2. Політики доступу до документів.

Учасники розподіляються на дві групи.

Завдання для першої групи: дати відповіді на питання:

1. Як визначати й актуалізувати рівні доступу для співробітників у великих компаніях?

2. Які механізми перевірки можна впровадити для моніторингу доступу до конфіденційних документів?

3. Яким чином забезпечити швидкий і безпечний доступ до документів під час роботи з віддаленими командами?

Завдання для другої групи: дати відповіді на питання:

4. Як ефективно обмежувати доступ до застарілих документів без шкоди для операційної діяльності?

5. Які технології можна застосувати для автоматизації процесу зміни прав доступу?

Після обговорення групи презентують результати, а потім разом формулюють висновки.

Завдання 3. Етичні аспекти роботи з електронними сервісами.

Учасники розподіляються на дві групи.

Завдання для першої групи: дати відповіді на питання:

1. Як впроваджувати етичні принципи у процес збору та обробки даних користувачів?

2. Які кроки потрібно зробити для перевірки алгоритмів на наявність упередженості?

Завдання для другої групи: дати відповіді на питання:

3. Як забезпечити обізнаність користувачів про те, як використовуються їхні дані?

4. Як уникнути дискримінації при автоматизованій обробці даних (наприклад, у системах кредитного скорингу)?

5. Як етично працювати з чутливими даними (біометрія, медична інформація тощо) в міжнародному контексті?

Після обговорення групи презентують результати, а потім разом формулюють висновки.

Завдання 4. Інновації та вдосконалення.

Учасники розподіляються на дві групи.

Завдання для першої групи: дати відповіді на питання:

1. Які нові технології можна застосувати для посилення безпеки персональних даних?

2. Як використовувати штучний інтелект для прогнозування потенційних загроз і атак на дані?

3. Які переваги можуть дати інтеграція блокчейн у процеси управління доступом до документів?

Завдання для другої групи: дати відповіді на питання:

4. Як створити екосистему, де захист даних буде частиною культури компанії?

5. Які інноваційні підходи можна використати для підвищення довіри

клієнтів до захисту їхніх даних?

Після обговорення групи презентують результати, а потім разом формулюють висновки.

? Питання для самоконтролю

1. Які основні принципи захисту персональних даних визначає GDPR (Загальний регламент захисту даних)?
2. Як концепція «мінімізації даних» допомагає знижувати ризики при обробці персональних даних?
3. Які основні моделі доступу до документів існують в організаціях? Які їхні переваги та недоліки?
4. Як політика доступу до документів може бути адаптована до специфіки юридичних організацій або медичних установ?
5. Які методи автентифікації є найбільш ефективними для захисту доступу до чутливої інформації і чому?
6. Як багатофакторна автентифікація допомагає забезпечити високий рівень безпеки для користувачів і організацій?
7. Які етичні проблеми можуть виникнути при використанні штучного інтелекту для обробки персональних даних?
8. Як забезпечити прозорість у роботі з алгоритмами, що впливають на права користувачів у цифрових платформах?
9. Які технології використовуються для виявлення аномальних доступів до даних? Як вони допомагають підвищити безпеку інформації?
10. Які потенційні юридичні наслідки можуть виникнути через порушення політики доступу до документів на підприємстві?

Питання для поглибленого вивчення теми 8 «Конфіденційність та захист персональних даних»

1. Аналіз ефективності застосування принципу мінімізації даних в умовах цифровізації бізнес-процесів.
2. Вплив глобальних стандартів захисту даних (GDPR) на політики конфіденційності в малих і середніх підприємствах.
3. Правові та етичні виклики у впровадженні GDPR в країнах, що не є членами ЄС.
4. Оцінка впливу високих штрафів згідно з GDPR на поведінку корпорацій щодо захисту персональних даних.
5. Аналіз моделей доступу до документів в організаціях: від централізованого до децентралізованого управління доступом.
6. Інтеграція технологій блокчейн для забезпечення прозорості доступу до документів у юридичних організаціях.
7. Оцінка ефективності різних систем автентифікації (біометрія, двофакторна автентифікація, тощо) для покращення захисту документів.
8. Розробка політик доступу до документів для організацій, що

працюють із чутливою інформацією (медичні установи, фінансові структури).

9. Етика використання штучного інтелекту для обробки персональних даних: можливості та загрози.

10. Прозорість алгоритмів: вплив алгоритмічних рішень на права людини та етичні стандарти в цифрових платформах.

11. Етичні аспекти збору та зберігання біометричних даних: порівняльний аналіз міжнародних стандартів і національних практик.

12. Вплив цифрових технологій на конфіденційність персональних даних у різних культурних і правових контекстах.

13. Використання машинного навчання для виявлення аномальних доступів до даних і потенційних порушень безпеки.

14. Розробка моделі оцінки ризиків для захисту даних в умовах роботи з великими даними (Big Data).

15. Інтеграція IoT та захист персональних даних: дослідження етичних і правових проблем.

16. Дослідження впливу культури організацій на ефективність політик доступу до конфіденційних документів.

17. Міжнародна співпраця в захисті персональних даних: правові та етичні виклики для глобальних корпорацій.

18. Етичні питання автоматизованого прийняття рішень на основі персональних даних: виклики та потенціал.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕМА 9. ІННОВАЦІЇ В ЕЛЕКТРОННИХ СЕРВІСАХ ТА ДОКУМЕНТООБІГУ

Мета: розгляд сучасних інноваційних рішень у сфері електронного документообігу та сервісів; аналіз їх вплив на оптимізацію бізнес-процесів і підвищення ефективності роботи організацій; ознайомлення з новітніми технологіями, такими як блокчейн, штучний інтелект, автоматизація процесів та хмарні обчислення; розвиток навичок критичного оцінювання їх потенціалу для впровадження в практику.

План

1. Штучний інтелект та машинне навчання в документообігу.
2. Використання Blockchain для забезпечення цілісності документів.
3. Перспективи повної цифровізації документообігу.

Ключові терміни та поняття: *штучний інтелект, машинне навчання, автоматизація обробки документів, інтелектуальне сортування*

документів, розпізнавання текстів, аналіз ризиків, Blockchain, цілісність документів, автентифікація, авторизація, дистрибутивність, масштабованість, цифровізація документообігу, глобальна інтеграція.

1. Штучний інтелект та машинне навчання в документообігу

Електронний документообіг став невід'ємною складовою сучасного бізнесу та адміністративної сфери. Проте його розвиток ще не завершений, і перед ним стоїть багато цікавих викликів. Розглянемо, які саме перспективи чекають на нас у майбутньому.

Попереду нас чекають значні технологічні та функціональні розширення:

1. Штучний інтелект і машинне навчання. Одним із ключових трендів є розвиток штучного інтелекту (ШІ) та машинного навчання. ШІ може значно полегшити та автоматизувати обробку документів, виявлення помилок і зв'язків між ними. Штучний інтелект здатен забезпечити більш точну та ефективну роботу з цифровими документами, роблячи їх обробку швидшою та економнішою. Машинне навчання дозволяє системам адаптуватися до специфіки конкретної компанії, прогнозуючи потреби користувачів.

Штучний інтелект – це комплекс методів і технологій, що дозволяють створювати системи, які можуть імітувати людське мислення, вирішувати складні завдання та приймати рішення на основі отриманих даних.

Машинне навчання є складовою ШІ, яка полягає у створенні алгоритмів, які дозволяють комп'ютерним системам навчатися без безпосереднього програмування. На основі даних комп'ютер самостійно розвиває моделі, що дозволяють отримувати точні прогнози та автоматизувати рутинні процеси.

Використання штучного інтелекту й машинного навчання у документообігу:

– автоматизація обробки документів: ШІ та МН дозволяють швидко обробляти великі обсяги документів (наприклад, рахунки-фактури, контракти, заяви тощо). Алгоритми машинного навчання можуть ідентифікувати шаблони, виявляти типи документів та автоматично заповнювати відповідні поля;

– інтелектуальне сортування документів: ШІ дозволяє сортувати документи відповідно до їх категорій та важливості. Наприклад, документи з конфіденційною інформацією автоматично виділяються та підлягають посиленому захисту;

– оптимізація процесу погодження документів: машинне навчання допомагає спрощувати процес погодження документів шляхом прогнозування ймовірності схвалення або необхідності доповнень. Це скорочує час ухвалення рішень;

– розпізнавання текстів (OCR): завдяки алгоритмам ШІ можливе автоматичне розпізнавання тексту з відсканованих документів, що дозволяє ефективно перетворювати паперові документи в цифрові;

– автоматизоване управління контрактами: МН допомагає контролювати виконання контрактів, автоматично нагадуючи про закінчення терміну дії або

підвищення цінових параметрів;

– захист конфіденційної інформації: ШІ дозволяє виявляти потенційні порушення конфіденційності, аналізуючи доступ до документів і виявляючи підозрілі дії;

– аналіз ризиків: штучний інтелект використовує машинне навчання для оцінки ризиків, наприклад, аналізуючи юридичні документи з метою виявлення ризиків або невідповідностей.

Основні переваги:

– швидкість обробки: ШІ значно прискорює процес обробки документів;

– зменшення людського втручання: зменшує необхідність ручного введення даних і скорочує ймовірність помилок;

– підвищення точності: завдяки машинному навчанню системи здатні приймати точніші рішення;

– оптимізація витрат: автоматизація процесів дозволяє знизити витрати на обробку документів;

– покращення безпеки: інтелектуальні системи можуть виявляти ризики й забезпечувати контроль доступу.

Упровадження ШІ та МН змінює традиційні **трудові функції** у документообігу. Менеджери з інформаційних технологій повинні адаптуватися до нових технологій і навчатися працювати з алгоритмами машинного навчання. Професії, які пов’язані з рутинними завданнями, можуть бути оптимізовані, дозволяючи працівникам зосередитися на творчих і стратегічних аспектах.

Штучний інтелект і машинне навчання мають значний потенціал для перетворення документообігу в організаціях. Вони дозволяють автоматизувати рутинні процеси, поліпшити якість обробки інформації та підвищити продуктивність.

Однак упровадження цих технологій потребує ретельного планування, дотримання етичних стандартів і забезпечення безпеки даних. Вибір правильних алгоритмів та їх інтеграція з існуючими системами мають ключове значення для успішного застосування ШІ в документообігу.

2. Використання Blockchain для забезпечення цілісності документів

Blockchain (блокчейн) – це дистрибутивна технологія бази даних, що забезпечує безпечне та прозоре зберігання інформації без необхідності в центральному органі контролю. Ключова особливість блокчейн-технології полягає в її здатності зберігати дані у вигляді послідовності блоків, що зв’язані між собою за допомогою криптографії. Кожен блок містить інформацію про попередній блок, що унеможливлює його зміни без порушення всього ланцюга, що надає йому високий рівень безпеки. Вже сьогодні Blockchain активно використовується в різних сферах, і одним з основних напрямків є забезпечення цілісності документів.

Цілісність документів – це здатність документа зберігати свою точність, повноту та незмінність протягом всього циклу його існування. Це означає, що

документ не може бути змінений або підроблений без виявлення змін. Це особливо важливо для юридичних, фінансових, медичних та інших документів, де кожен етап їх обробки має критичне значення для їх довіри і значення.

Як Blockchain забезпечує цілісність документів?

– не змінюваність інформації: кожен документ, що додається в блокчейн, отримує унікальний цифровий підпис, що включає відбиток (хеш) цього документа. Якщо зміни вносяться в документ після його реєстрації в системі, то відбиток змінюється, що робить підробку або модифікацію документа помітною. Цей процес неможливо змінити без зміни всієї історії, що робить зловживання неможливим без виявлення;

– прозорість: Blockchain є відкритою системою, тому всі учасники мають доступ до записів і можуть перевірити кожну зміну, що відбулася з документом. Це забезпечує прозорість і дозволяє верифікувати автентичність документів;

– автентифікація та авторизація: за допомогою криптографії, Blockchain дозволяє підтверджувати, хто створив або змінив документ, а також коли це було зроблено. Це важливо для встановлення законності і достовірності документа;

– дистрибутивність: блокчейн має дистрибутивну природу, тобто копії всіх записів зберігаються на численних комп'ютерах (вузлах) у мережі. Це означає, що навіть якщо один із вузлів зазнає атаки або збою, інформація залишається доступною і незмінною на інших вузлах. Таким чином, втрата даних або їх маніпуляція через збої або атаки неможлива.

Ключові переваги використання Blockchain для цілісності документів:

– захист від підробок: завдяки криптографії та незмінності записів, Blockchain забезпечує максимальний захист документів від підробок. Кожен запис і зміни до нього записуються в блокчейн як незмінний ланцюг інформації, що робить несанкціоновані зміни відразу помітними;

– полегшення процесу автентифікації та верифікації: Blockchain дозволяє легко підтвердити автентичність документа, оскільки кожен блок містить інформацію про попередні етапи верифікації. Це дозволяє швидко і безпечно здійснювати перевірку документа без необхідності звертатися до централізованих реєстрів;

– інтеграція з існуючими системами: Blockchain можна інтегрувати у вже існуючі інформаційні системи для забезпечення збереження даних із високим рівнем захисту. Це особливо корисно для організацій, які мають великі обсяги документів, що потребують перевірки та автентифікації;

– зниження витрат на зберігання і обробку документів: замість витрат на фізичне зберігання документів або використання дорогих централізованих серверів для зберігання даних, Blockchain дозволяє організаціям економити ресурси завдяки дистрибутивній природі технології;

– поліпшення процесів аудиту і моніторингу: усі операції з документами автоматично реєструються в блокчейні, що створює повний і незмінний аудит-

трек (журнал). Це дозволяє згодом переглядати всю історію змін документа, що особливо корисно для юридичних і фінансових організацій.

Приклади використання Blockchain для цілісності документів:

– юридичні документи: Blockchain використовують для забезпечення автентичності юридичних документів, таких як контракти, заповіти, угоди. Наприклад, у країнах, де є високий рівень підробки контрактів, використання Blockchain допомагає запобігти таким злочинам;

– вибори та голосування: у системах електронного голосування блокчейн може забезпечити цілісність результатів голосування, гарантувати, що жоден голос не буде змінено або втрачено, і що кожен голос можна перевірити та відслідкувати;

– цифрові ідентифікаційні документи: уряди деяких країн розробляють системи для видачі цифрових ідентифікаційних документів на базі блокчейн, що дозволяє уникнути шахрайства та підробок при використанні паспортів та інших документів;

– фінансові документи: Blockchain може бути використаний для забезпечення цілісності фінансових звітів і контрактів. Це важливо для боротьби з маніпуляціями на фондових ринках, а також для аудиту фінансових операцій.

Хоча Blockchain має величезний потенціал у забезпеченні цілісності документів, існують деякі ***виклики, які можуть ускладнити його впровадження:***

– складність інтеграції з існуючими системами: багато організацій використовують традиційні централізовані системи для зберігання і обробки документів, що може створити труднощі при інтеграції їх із дистрибутивною природою Blockchain. Потрібні спеціалізовані розробки та стандарти, щоб забезпечити ефективне поєднання нової та старої інфраструктури.

– масштабованість: Blockchain-технологія може мати проблеми з масштабованістю при обробці великих обсягів даних. Як правило, для кожного запису в блокчейні необхідно зберігати значну кількість інформації, що може призвести до збільшення часу обробки та зростання витрат.

– захист персональних даних: в умовах дедалі суворіших вимог до захисту персональних даних (наприклад, згідно з GDPR у Європейському Союзі) може виникнути необхідність удосконалення алгоритмів анонімізації та шифрування даних на блокчейні, щоб забезпечити відповідність вимогам законодавства.

Технологія Blockchain надає значний потенціал для забезпечення цілісності документів у різних сферах, включаючи право, фінанси, медицину та урядування. Вона не лише захищає документи від підробок, але й забезпечує прозорість і довіру до інформації, що зберігається. Однак для повного впровадження цієї технології необхідно врахувати певні виклики, такі як стандартизація, інтеграція з існуючими системами та питання масштабованості. Незважаючи на це, Blockchain потенційно спроможний стати основним інструментом для захисту документів в майбутньому.

3. Перспективи повної цифровізації документообігу

Цифровізація документообігу є однією з ключових складових розвитку сучасного суспільства та економіки. Вона охоплює процеси переведення документів і операцій з паперових форм у електронний вигляд та автоматизацію роботи з ними.

В умовах глобалізації, технологічних змін і потреби в підвищенні ефективності роботи бізнесу, державних структур і організацій, перспективи повної цифровізації документообігу набувають особливо важливого значення:

1) Цифровізація документообігу передбачає використання цифрових технологій для створення, обробки, зберігання, передачі та архівації документів в електронному вигляді, що дозволяє замінити традиційні паперові документи на їх цифрові аналоги. Це включає в себе застосування таких інструментів, як електронні підписи, системи управління документообігом (DMS), технології автоматизації та обробки даних.

2) Технології, що сприяють цифровізації документообігу забезпечують не тільки переведення документів у цифровий формат, а і їх збереження, обробку, пошук та передавання:

- електронний документообіг: автоматизовані системи для управління створенням, зберіганням, обробкою та передачею документів. Це забезпечує ефективну організацію роботи з документами в межах організації та з її зовнішніми партнерами;
- електронний підпис: технологія, яка дозволяє юридично підтверджувати справжність та автентичність електронних документів. Залежно від країни електронні підписи можуть мати різний рівень правової сили, що важливо для міжнародного документообігу;
- хмарні технології: дозволяють зберігати та обробляти документи в інтернеті, забезпечуючи доступ до них з будь-якої точки світу за допомогою різних пристроїв;
- штучний інтелект (ШІ) та машинне навчання: використовуються для автоматизації процесів документообігу, таких як сортування, категоризація, пошук, перевірка документів на наявність помилок і несуттєвих змін;
- Blockchain: дає змогу забезпечити цілісність і незмінність цифрових документів, що важливо для критичних бізнес-процесів, юридичних угод, державних реєстрів тощо.

3) Цифровізація документообігу дає організаціям, державним установам та підприємствам низку важливих **переваг**:

- зниження витрат: завдяки відмові від використання паперу, друку, транспортування документів та зберігання їх у фізичних архівах можна значно знизити витрати на офісну інфраструктуру, а також скоротити час, витрачений на пошук та обробку документів;
- підвищення ефективності та автоматизація процесів: цифрові системи дозволяють автоматизувати рутинні завдання, такі як сортування документів, перевірка, підписання та обмін інформацією. Це скорочує час, необхідний для виконання операцій, зменшує людський фактор і підвищує точність процесів;
- покращення доступності та мобільності: цифрові документи доступні з

будь-якої точки світу через інтернет, що дозволяє працювати з ними віддалено, зменшує затримки і забезпечує зручний доступ до необхідної інформації;

– забезпечення безпеки і конфіденційності: цифрові технології дозволяють застосовувати високий рівень захисту даних за допомогою шифрування, електронних підписів і захищених з'єднань. Зниження можливості втрати чи пошкодження документів завдяки їх зберіганню в цифровому вигляді на сервері або в хмарі;

– легкість у пошуку та аналізі інформації: зберігання документів в електронному вигляді дозволяє здійснювати швидкий пошук необхідних файлів за допомогою спеціалізованих інструментів, таких як системи управління документообігом (DMS), що оптимізує процеси.

4) Незважаючи на численні переваги, існують і **певні труднощі при впровадженні** повної цифровізації документообігу:

– правові та нормативні бар'єри: однією з головних перешкод є необхідність адаптації законодавства до нових реалій, пов'язаних із цифровими підписами, електронними документами та їх юридичною силою. У різних країнах різні підходи до визнання електронних документів;

– захист персональних даних: цифрові документи можуть містити чутливу інформацію, що потребує посилених заходів щодо захисту персональних даних. Порушення цих вимог може призвести до серйозних наслідків для організацій і установ;

– технічні обмеження: враховуючи необхідність у потужних технологіях, таких як хмарні системи, а також вартість модернізації інфраструктури, деякі організації можуть стикатися з фінансовими і технічними труднощами;

– опір змінам з боку співробітників: багато співробітників можуть відчувати незручності або страх перед впровадженням нових технологій, що створює додаткові бар'єри при переході на цифровий документообіг.

5) Перспективи майбутнього цифровізації документообігу. Майбутнє цифровізації документообігу здається вельми обнадійливим завдяки кільком важливим тенденціям:

– розвиток штучного інтелекту і автоматизація процесів: очікується, що в майбутньому ШІ відіграватиме важливу роль у цифровізації документообігу, зокрема через автоматизацію процесів обробки документів, їх аналізу та створення на основі попереднього контексту. Це дозволить значно знизити витрати часу та зусиль;

– інтеграція з іншими технологіями: всі технології будуть взаємодіяти між собою для забезпечення більш ефективного функціонування документообігу. Наприклад, Blockchain і ШІ можуть допомогти зберігати документи надійно і з високою швидкістю, з автоматичними перевірками їх автентичності;

– безпека даних і конфіденційність: для забезпечення безпеки та конфіденційності цифрових документів розвиватимуться нові методи захисту інформації, включаючи біометричну і багатофакторну автентифікацію, що дозволить усунути ризики витоку даних.

– глобальна інтеграція: цифровізація документообігу забезпечить безперешкодний обмін інформацією між різними країнами і організаціями,

допомагаючи створювати єдині платформи для міжнародної співпраці у сфері бізнесу, фінансів, медицини та державного управління.

Приклади впровадження цифровізації документообігу

– **Естонія**: Європейський лідер у сфері цифровізації. Вся державна документація, від реєстрації бізнесу до медичних записів, зберігається та обробляється в електронному вигляді.

– **Сингапур**: У Сингапурі активно використовується електронний документообіг для обміну бізнес-документами та надання адміністративних послуг, що дозволяє знижувати витрати та пришвидшувати процеси.

– **Україна**: В Україні також активно працюють над цифровізацією документообігу, зокрема через запуск платформ, таких як «Дія», для надання електронних послуг громадянам і бізнесу.

Перспективи повної цифровізації документообігу є дуже обнадійливими. Вона обіцяє значне підвищення ефективності, зниження витрат, поліпшення доступності та зручності роботи з документами. Однак для досягнення цих цілей необхідно вирішити правові, технічні та організаційні питання. Інтеграція передових технологій, таких як штучний інтелект, Blockchain, хмарні сервіси і електронні підписи, стане основою для створення глобальної, безпечної та ефективної системи документообігу.

У підсумку, майбутнє електронного документообігу обіцяє нам низку інновацій та покращень. Штучний інтелект, блокчейн, мобільні технології та кібербезпека відіграють ключову роль у цьому розвитку. Застосування цих технологій сприятиме більшій ефективності, безпеці та зручності обробки даних, а також подальшому прогресу у сфері цифрового документообігу.

Тести

1. Який ключовий тренд змінює документообіг?
a) штучний інтелект і машинне навчання
b) використання друкованих документів
c) підвищення кількості ручної праці
2. Що забезпечує автоматизацію обробки документів?
a) використання ручного введення даних
b) алгоритми машинного навчання
c) паперові шаблони
3. Як штучний інтелект може допомогти в розпізнаванні тексту?
a) зменшуючи обсяг документів
b) завдяки алгоритмам ocr (розпізнавання тексту)
c) використовуючи хмарні системи
4. Яка перевага цифрового документообігу найбільш суттєва?
a) підвищення кількості паперових архівів
b) зниження витрат на друк і зберігання
c) збільшення ручної роботи
5. Що є основною функцією Blockchain у документообігу?
a) забезпечення цілісності та незмінності документів

b) полегшення паперового зберігання

c) прискорення ручного пошуку

6. Який інструмент дозволяє юридично підтвердити автентичність електронного документа?

a) OCR-система

b) електронний підпис

c) хмарні технології

7. Що є головним обмеженням Blockchain у документообігу?

a) проблеми з масштабованістю

b) відсутність доступу до інтернету

c) низький рівень захисту

8. Як можна зменшити людський фактор у документообігу?

a) упровадивши ручне введення даних

b) автоматизувавши рутинні процеси

c) збільшивши кількість паперових документів

9. Що дозволяє швидко знайти потрібний документ?

a) системи управління документообігом (dms)

b) пошук у паперових архівах

c) ручне сортування файлів

10. Яка технологія використовується для зберігання документів у мережі?

a) OCR

b) хмарні технології

c) ручні сервіси

11. Що є ключовою перевагою штучного інтелекту в роботі з документами?

a) прогнозування потреб користувачів

b) збільшення часу на обробку

c) ручна перевірка

12. Який метод шифрування забезпечує безпеку документів у Blockchain?

a) використання паролів

b) криптографія

c) хмарне шифрування

13. Яке основне завдання електронного підпису?

a) зменшення кількості документів

b) підтвердження автентичності документів

c) ручне редагування

14. Що дозволяє поліпшити доступність до цифрових документів?

a) використання паперових архівів

b) хмарні технології

c) ручна обробка

15. Як Blockchain запобігає підробці документів?

a) забезпечує незмінність інформації

b) встановлює фізичний контроль

c) зменшує обсяг документів

16. Що є основним завданням OCR-систем у документообігу?

a) сортування документів

b) автоматичне розпізнавання тексту

c) архівування файлів

17. Що є основною перевагою інтеграції Blockchain з існуючими системами?

a) забезпечення прозорості даних

b) збільшення обсягів паперових документів

c) підвищення людського втручання

18. Що сприяє зниженню витрат у цифровому документообігу?

a) використання паперових архівів

b) автоматизація процесів

c) збільшення ручної роботи

19. Що є ключовим викликом для впровадження цифрового документообігу?

a) підвищення кількості паперових документів

b) правові та нормативні бар'єри

c) низька якість цифрових документів

20. Як забезпечується захист конфіденційної інформації у цифровому документообігу?

a) використання ручних методів

b) шифрування даних

c) сортування документів вручну.

Завдання для мозкового штурму до теми 9 «Інновації в електронних сервісах та документообігу»

Завдання 1. Штучний інтелект у документообігу.

1. Як можна інтегрувати штучний інтелект у процеси обробки документів на підприємстві?

2. Які проблеми або виклики можуть виникнути при впровадженні ШІ для автоматизації рутинних завдань?

3. Запропонуйте нові функції для систем управління документообігом на основі ШІ, які могли б зробити роботу ефективнішою.

Завдання 2. Blockchain для забезпечення цілісності документів.

1. Визначте, які саме процеси документообігу у вашій сфері можна захистити за допомогою блокчейну.

2. Запропонуйте сценарії використання блокчейну для перевірки автентичності документів та забезпечення їх незмінності.

3. Які ризики або обмеження можуть виникнути при використанні блокчейну в документообігу? Як їх подолати?

Завдання 3. Цифровізація документообігу.

1. Які кроки потрібно зробити, щоб перевести документообіг вашої

організації повністю в цифровий формат?

2. Обговоріть переваги та недоліки використання хмарних технологій для зберігання електронних документів.

3. Запропонуйте, як цифровізація може сприяти підвищенню ефективності роботи вашої команди або організації.

Завдання 4. Інноваційні рішення для автоматизації.

1. Які нові технології або тренди, окрім ШІ та блокчейну, можуть бути корисними для автоматизації документообігу?

2. Які процеси, що наразі виконуються вручну, можна автоматизувати? Як це вплине на продуктивність?

3. Розробіть концепцію інтелектуальної системи, яка могла б адаптуватися до потреб конкретної організації.

Завдання 5. Етичні аспекти і безпека.

1. Які етичні виклики можуть виникати при використанні ШІ у роботі з конфіденційними документами?

2. Як забезпечити захист персональних даних в умовах цифровізації документообігу?

3. Обговоріть, які заходи можна вжити для забезпечення довіри до автоматизованих систем документообігу.

Завдання 6. Створення стратегії впровадження.

1. Розробіть покроковий план впровадження автоматизації документообігу з використанням ШІ та блокчейну.

2. Як забезпечити навчання персоналу для роботи з новими технологіями?

3. Сформулюйте своє бачення ідеального цифрового документообігу через 5 років.

? Питання для самоконтролю

1. Що таке автоматизація документообігу? Які основні переваги вона забезпечує?

2. Які функції виконує штучний інтелект у системах автоматизації документообігу?

3. Як технологія блокчейн забезпечує безпеку й прозорість документообігу?

4. Що таке смарт-контракти? Яку роль вони відіграють в автоматизованих процесах?

5. Як цифровізація впливає на ефективність роботи організацій?

6. Назвіть основні виклики, які можуть виникнути при впровадженні блокчейну в документообіг.

7. Які види документів найчастіше автоматизуються за допомогою ШІ?

8. Чому важливо враховувати етичні аспекти при обробці конфіденційної інформації?

9. Які ключові платформи або програми використовуються для автоматизації документообігу?

10. Як оцінити економічну вигоду від упровадження автоматизованої системи документообігу?

Питання для поглибленого вивчення теми 9 «Інновації в електронних сервісах та документообігу»

1. Оптимізація обробки текстових даних у документообігу за допомогою глибокого навчання.
2. Розробка інтелектуальних систем управління документообігом на основі машинного навчання.
3. Використання генеративного штучного інтелекту для створення та перевірки шаблонів документів.
4. Дослідження впливу блокчейну на забезпечення автентичності та незмінності електронних документів.
5. Енергоефективні алгоритми консенсусу для документо-орієнтованих блокчейн-систем.
6. Інтеграція блокчейну з існуючими системами електронного документообігу.
7. Аналіз бар'єрів цифровізації документообігу в державному секторі.
8. Порівняльне дослідження ефективності цифрових платформ документообігу в різних галузях.
9. Вплив цифровізації на екологічний аспект документообігу.
10. Упровадження IoT у процеси документообігу.
11. Дослідження впливу штучного інтелекту та блокчейну на безпеку електронних підписів.
12. Застосування хмарних обчислень у масштабованих системах документообігу.
13. Економічна ефективність впровадження автоматизованих систем документообігу.
14. Соціальний вплив автоматизації документообігу: вплив на зайнятість і компетенції працівників.
15. Роль цифрової грамотності у впровадженні автоматизації документообігу.
16. Етичні виклики використання штучного інтелекту в роботі з конфіденційними документами.
17. Юридичні аспекти використання блокчейну для зберігання офіційних документів.
18. Розробка політик безпеки для автоматизованих систем документообігу.

Примітка: Результати поглибленого вивчення питання (одного на власний вибір) рекомендовано оформити у вигляді есе (див. додаток А).

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

API – це набір протоколів, інтерфейсів та інструментів, які дозволяють різним програмним системам взаємодіяти одна з одною.

BAS Документообіг КОРП – це програмний продукт, розроблений для автоматизації документообігу, управління процесами та оптимізації роботи з документами в середніх і великих організаціях.

Blockchain (блокчейн) – це дистрибутивна технологія бази даних, що забезпечує безпечне та прозоре зберігання інформації без необхідності у центральному органі контролю.

DocuSign – це платформа для електронного підпису та автоматизації процесів узгодження документів.

FREDO ДокМен – це спеціалізоване рішення для електронного документообігу, яке розроблене для автоматизації обробки документів в організаціях.

Google One (Диск) – це платний сервіс від Google, який надає користувачам розширене хмарне зберігання даних і додаткові переваги.

M.E.Doc – це українське програмне забезпечення для автоматизації електронного документообігу, звітності до контролюючих органів, а також для взаємодії між компаніями, контрагентами й державними структурами.

M-Files – це потужна платформа керування документами на основі метаданих, дає змогу кваліфікованим працівникам миттєво знаходити потрібну інформацію в будь-якому контексті, автоматизувати бізнес-процеси та посилити контроль інформації.

Microsoft 365 – це хмарний сервіс, який поєднує зручні сучасні інструменти для роботи, що поширюються на основі передплати.

Zoho Docs – це хмарна платформа для зберігання, обміну та спільної роботи з документами.

Автентифікація – це процес перевірки особи користувача або системи для надання доступу до певних ресурсів чи інформації.

Авторизація – це процес надання прав доступу користувачу після успішної автентифікації.

Валідація підпису (signature validation) – це процес верифікації та підтвердження того, що підпис валідний.

Відкритий ключ – це параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб’єктам відносин у сфері використання електронного цифрового підпису.

Віртуальні робочі столи VDI – це технологія, яка дозволяє створювати та керувати віртуальними робочими столами на віддалених серверах, забезпечуючи користувачам доступ до персоналізованих робочих середовищ із будь-якого пристрою через мережу Інтернет.

Вчасно – це український онлайн-сервіс для електронного документообігу (ЕДО), який дозволяє компаніям підписувати, зберігати документи та обмінюватися ними в електронному форматі.

Гарантія цілісності – це захист від змін після підписання документа.

Двофакторна автентифікація (2FA) – це метод перевірки особи, який поєднує два незалежних фактори для забезпечення більшої безпеки доступу до системи.

Документ – це зафіксована інформація на будь-якому матеріальному носії, яка має юридичну, інформаційну або іншу значущість.

Документ – це інформація, зафіксована на матеріальному або електронному носії, яка доступна для передачі та багаторазового використання.

Документ – це матеріальна форма збереження й передачі інформації, яка має юридичну силу та використовується в управлінській або іншій діяльності.

Документ – це матеріальний об’єкт, що містить зафіксовану інформацію, яка може бути використана як доказ діяльності, події або явища.

Документообіг – рух документів в організації з моменту їх створення або одержання і до завершення виконання або відправлення.

Документообіг – це процес створення, обробки, зберігання, передачі та використання документів у межах організації або між різними організаціями.

Електронна ідентифікація – це вимоги до систем і засобів, які забезпечують ідентифікацію осіб в електронному середовищі (наприклад, через електронний підпис, електронні паспорти тощо).

Електронний документообіг – це сукупність процесів створення, зберігання, обробки, передачі, підписання та архівування документів в електронній формі.

Електронний документообіг (обіг електронних документів) – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних.

Електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис (ЕЦП) – це набір цифрових даних, отриманих на основі електронного документа за допомогою алгоритмів криптографічного перетворення з використанням закритого ключа користувача.

Журнальне ведення та моніторинг доступу – це реєстрація та аналіз всіх спроб доступу до системи для виявлення підозрілих або несанкціонованих дій.

Захист даних від несанкціонованого доступу – це обмеження доступу до важливих даних і систем лише для авторизованих осіб.

Ідентифікація підписувача – це підтвердження особи, яка створила підпис.

Кастомна версія СЕД – це розробка унікальної системи під вимоги замовника.

Контроль і моніторинг – це перевірка дій користувачів і виявлення можливих загроз або зловживань.

Коробкова версія СЕД – це готове програмне рішення.

Криптографія – це сукупність методів перетворення даних, спрямованих на приховання їх інформаційного змісту.

Машинне навчання – це складова ШІ, яка полягає у створенні алгоритмів, які дозволяють комп'ютерним системам навчатися без безпосереднього програмування.

Обмеження доступу – це контроль та управління доступом до інформаційних систем і ресурсів.

Особистий ключ – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Політика безпеки – це забезпечення відповідності правилам доступу на основі внутрішніх політик і вимог законодавства.

Реінжиніринг адміністративних процесів – це фундаментальне перепроєктування діяльності органів публічного управління за допомогою підйому технічних, організаційних, технологічних і методологічних рішень на новий рівень, створення нових, ефективних процесів в управлінні для досягнення високої ефективності за такими показниками, як вартість, якість, строки надання послуг.

Розподіл ролей – це визначення доступу до ресурсів на основі ролей користувачів в організації.

Система електронного архіву – це система структурованого зберігання електронних документів, що забезпечує надійність зберігання, конфіденційність і розмежування прав доступу, відстеження історії використання документа, швидкий і зручний пошук.

СОТА – це хмарний сервіс для електронного документообігу та подання звітності, створений компанією, яка розробила M.E.Doc.

Токен – це спеціальна флешка, яка захищена від перезапису/копіювання.

УЕП – це вдосконалений електронний підпис, створений з використанням криптографічного перетворення даних.

Хеш – це результат роботи хешфункцій або функцій згортання.

Хмарні сервіси (public cloud services) – це програми та платформи, які «живуть» та працюють на серверах хмарних операторів.

Хмарні сервіси для збереження даних – це віртуальний простір необмежених розмірів, де можна зберігати будь-які дані особистого чи корпоративного характеру.

Цифрові сертифікати – це електронний документ, виданий центром сертифікації (ЦСК), який підтверджує ідентичність користувача або системи та використовується для забезпечення безпечного обміну даними.

Цифровізація документообігу – це використання цифрових технологій для створення, обробки, зберігання, передачі та архівації документів в електронному вигляді, що дозволяє замінити традиційні паперові документи на

їх цифрові аналоги.

Цілісність документів – це здатність документа зберігати свою точність, повноту та незмінність протягом усього циклу його існування.

Шифрування – це процес перетворення зрозумілої інформації в нечитабельну форму за допомогою спеціального алгоритму, що забезпечує її захист від несанкціонованого доступу.

Штучний інтелект – це комплекс методів і технологій, що дозволяють створювати системи, які можуть імітувати людське мислення, вирішувати складні завдання та приймати рішення на основі одержаних даних.

Юридична значимість – електронний підпис має таку ж силу, як і власноручний підпис, якщо використовується відповідно до законодавства.



РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Архівна справа та електронний документообіг : метод. посіб. Київ : Держархівслужба, 2021. 175 с.
2. Барабаш Л. А. Інтеграція сучасних інформаційних систем у сфері документообігу. Львів : ЛНУ, 2021. 180 с.
3. Бочкарьов Г. А. Документ як носій інформації: традиційні та нові підходи. *Документознавство та інформаційна діяльність*. 2012. № 1. С. 12–16.
4. Власов К. С. Сучасні електронні сервіси для документообігу : посібник. Харків : Вид-во ХНУ, 2021. 210 с.
5. Гаврилюк О. М. Електронний документообіг у сучасній організації : монографія. Київ : НАДУ, 2020. 245 с.
6. Гіляровський Р. С. Інформаційні технології в документознавстві : навч. посіб. Харків : Право, 2015. 192 с.
7. Державна архівна служба України. Методика організації електронного архіву. Київ, 2020. 84 с.
8. Державна служба спеціального зв’язку та захисту інформації України : реком. з інформаційної безпеки електронного документообігу. Київ, 2022. 100 с.
9. ДСТУ 2392:2021 «Система стандартів у галузі інформації, бібліотечної та видавничої справи. Терміни та визначення понять». Київ : ДП «УкрНДНЦ», 2021. 64 с.
10. ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів». Київ : ДП «УкрНДНЦ», 2020. 56 с.
11. ДСТУ 4543:2021 «Інформаційно-документаційне обслуговування. Загальні положення». Київ : ДП «УкрНДНЦ», 2021. 72 с.
12. ДСТУ 8302:2015 «Бібліографічне посилання. Загальні положення та правила складання». Київ : ДП «УкрНДНЦ», 2015. 48 с.
13. ДСТУ EN 319 102-1:2018 «Електронна ідентифікація та довірчі послуги. Сертифікати для електронного підпису та печатки». Київ : ДП «УкрНДНЦ», 2018. 58 с.
14. ДСТУ EN ISO 9001:2018 «Системи управління якістю. Вимоги». Київ : ДП «УкрНДНЦ», 2018. 140 с.
15. ДСТУ ISO 15489-1:2018 «Інформація та документація. Управління документами. Ч. 1: Поняття та принципи». Київ : ДП «УкрНДНЦ», 2018. 48 с.
16. Єфремова А. А. Електронний документ: сучасні підходи до визначення. *Інформаційне суспільство*. 2020. № 3(25). С. 34–39.
17. Загальні положення про електронний документообіг в Україні : метод. реком. Київ : Мін’юст, 2021. 102 с.
18. Зозуля О. С. Архівознавство : навч. посіб. Київ : Ліра-К, 2017. 248 с.
19. Інформаційна безпека в електронних системах : навч. посіб. / за ред. І. Г. Ткаченка. Київ : КНТЕУ, 2020. 204 с.
20. Карпенко М. Ю. Електронний документообіг у професійній

діяльності : конспект лекцій / М. Ю. Карпенко; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2020. 67 с.

21. Корчинська В. Електронний підпис: правові та технічні аспекти. Київ : Юрінком Інтер, 2020. 212 с.

22. Кукарін О. Б. Електронний документообіг та захист інформації : навч. посіб. / за заг. ред. Н. В. Грицяк. Київ : НАДУ, 2015. 84 с.

23. Кулинич М. Б. Електронний документообіг в обліку і оподаткуванні : метод. вказівки до практичних занять. Луцьк : Волинський національний університет імені Лесі Українки, 2022. 47 с.

24. Лавриненко В. Інноваційні технології у сфері електронного документообігу. Одеса : ОНУ, 2020. 250 с.

25. Ніколаєв І.В. Електронний документообіг : метод. вказівки до вивчення дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти всіх форм навчання за спеціальністю 029 «Інформаційна, бібліотечна та архівна справа». Кропивницький : ЦНТУ, 2020. 32 с.

26. Паламарчук О. О. Організація зберігання електронних документів. Вінниця : ВНТУ, 2021. 124 с.

27. Плаксієнко В. Я., Назаренко І. М., Гаркуша С. А. Безпаперова бухгалтерія на підприємстві : навч. посіб. / за ред. В. Я. Плаксієнка. Київ : «Центр учбової літератури», 2018. 252 с.

28. Про електронний цифровий підпис : Закон України № 852-IV від 22.05.2003. URL:https://zakon.rada.gov.ua/laws/show/852-15

29. Про електронні довірчі послуги : Закон України № 2155-VIII від 05.10.2017. URL:https://zakon.rada.gov.ua/laws/show/2155-19

30. Про електронні документи та електронний документообіг : Закон України № 851-IV від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15

31. Про електронну ідентифікацію та електронні довірчі послуги : Закон України № 5280-VI від 16.12.2022. URL:https://zakon.rada.gov.ua/laws/show/5280-20

32. Про Національний архівний фонд та архівні установи : Закон України № 3814-XII від 24.12.1993. URL: https://zakon.rada.gov.ua/laws/show/3814-12

33. Регламент ЄС eIDAS (Electronic Identification, Authentication and Trust Services) № 910/2014 від 23.07.2014. URL:https://eur-lex.europa.eu

34. Романенко Т. А. Електронні сервіси в управлінні бізнес-процесами : монографія. Харків : УкрІНТЕІ, 2021. 198 с.

35. Хмарні технології в електронному документообігу : збірник статей / за ред. П. І. Савчука. Київ : Академія, 2022. 280 с.

36. Шебаніна О. В. Електронний документообіг : конспект лекцій для здобувачів освітнього ступеня «бакалавр» спеціальності 073 «Менеджмент» денної форми навчання. Миколаїв : Миколаївський національний аграрний університет, 2021. 69 с.

37. Besser T. R. Digital Preservation and Archiving: A Practical Guide for Libraries, Archives, and Museums. London : Facet Publishing, 2017. 248 p.

38. Blythe C. E-Discovery and Digital Evidence: A Comprehensive Guide for

Legal Professionals. Oxford : Oxford University Press, 2020. 304 p.

39. eIDAS and Trust Services: Implementation guide / European Commission. Brussels, 2019. 150 c.

40. Gartner, Inc. Digital Transformation in Document Management and Collaboration. Stamford : Gartner Inc., 2021. 115 p.

41. ISO 14721:2020 «Open Archival Information System (OAIS) – Reference Model». Geneva: International Organization for Standardization, 2020. 58 c.

42. ISO 15489-2:2001 «Information and documentation – Records management – Part 2: Guidelines». Geneva : International Organization for Standardization, 2001. 66 c.

43. ISO 30301:2019 «Information and documentation – Management systems for records – Requirements». Geneva : International Organization for Standardization, 2019. 48 c.

44. ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements». Geneva : International Organization for Standardization, 2022. 60 c.

45. Rogers P. Information Management in the Cloud: How Cloud Computing Is Changing the Way We Think About Information. New York : McGraw-Hill Education, 2020. 192 p.

46. SO 27018:2019 «Code of practice for protection of personal data in the cloud». Geneva : International Organization for Standardization, 2019. 78 p.



ВИКОРИСТАНА ЛІТЕРАТУРА

1. Архівна справа та електронний документообіг : метод. посіб. Київ : Держархівслужба, 2021. 175 с.
2. Барабаш Л. А. Інтеграція сучасних інформаційних систем у сфері документообігу. Львів : ЛНУ, 2021. 180 с.
3. Бочкарьов Г. А. Документ як носій інформації: традиційні та нові підходи. *Документознавство та інформаційна діяльність.* 2012. № 1. С. 12–16.
4. Власов К. С. Сучасні електронні сервіси для документообігу : посіб. Харків : Вид-во ХНУ, 2021. 210 с.
5. Гаврилюк О. М. Електронний документообіг у сучасній організації : монографія. Київ : НАДУ, 2020. 245 с.
6. Гіляровський Р. С. Інформаційні технології в документознавстві : навч. посіб. Харків : Право, 2015. 192 с.
7. ДСТУ 8302:2015 «Бібліографічне посилання. Загальні положення та правила складання». Київ : ДП «УкрНДНЦ», 2015. 48 с.
8. ДСТУ EN 319 102-1:2018 «Електронна ідентифікація та довірчі послуги. Сертифікати для електронного підпису та печатки». Київ : ДП «УкрНДНЦ», 2018. 58 с.
9. Єфремова А. А. Електронний документ: сучасні підходи до визначення. *Інформаційне суспільство.* 2020. № 3(25). С. 34–39.
10. Зозуля О. С. Архівознавство : навч. посіб. Київ : Ліра-К, 2017. 248 с.
11. Карпенко М. Ю. Електронний документообіг у професійній діяльності : конспект лекцій / М. Ю. Карпенко; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2020. 67 с.
12. Кукарін О. Б. Електронний документообіг та захист інформації : навч. посіб. / за заг. ред. Н. В. Грицяк. Київ : НАДУ, 2015. 84 с.
13. Кулинич М. Б. Електронний документообіг в обліку і оподаткуванні : метод. вказівки до практичних занять. Луцьк : Волинський національний університет імені Лесі Українки, 2022. 47 с.
14. Матвієнко О., Цивін М. Основи організації електронного документообігу : навч. посіб. Київ : Центр учбової літератури, 2008. 112 с.
15. Ніколаєв І. В. Електронний документообіг : метод. вказівки до вивчення дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти всіх форм навчання за спеціальністю 029 «Інформаційна, бібліотечна та архівна справа». Кропивницький : ЦНТУ, 2020. 32 с.
16. Паламарчук О. О. Організація зберігання електронних документів. Вінниця : ВНТУ, 2021. 124 с.
17. Плаксієнко В. Я., Назаренко І. М., Гаркуша С. А. Безпаперова бухгалтерія на підприємстві : навч. посіб. / за ред. В. Я. Плаксієнка. Київ : Центр учбової літератури, 2018. 252 с.
18. Про електронний цифровий підпис : Закон України № 852-IV від 22.05.2003. URL:https://zakon.rada.gov.ua/laws/show/852-15

19. Про електронні довірчі послуги : Закон України № 2155-VIII від 05.10.2017. URL:https://zakon.rada.gov.ua/laws/show/2155-19

20. Про електронні документи та електронний документообіг : Закон України № 851-IV від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15

21. Про електронну ідентифікацію та електронні довірчі послуги : Закон України № 5280-VI від 16.12.2022. URL:https://zakon.rada.gov.ua/laws/show/5280-20

22. Про Національний архівний фонд та архівні установи : Закон України № 3814-XII від 24.12.1993. URL: https://zakon.rada.gov.ua/laws/show/3814-12

23. Регламент ЄС eIDAS (Electronic Identification, Authentication and Trust Services) № 910/2014 від 23.07.2014. URL:https://eur-lex.europa.eu

24. Шебаніна О. В. Електронний документообіг : конспект лекцій для здобувачів освітнього ступеня «бакалавр» спеціальності 073 «Менеджмент» денної форми навчання. Миколаїв : Миколаївський національний аграрний університет, 2021. 69 с.

25. eIDAS and Trust Services: Implementation guide / European Commission. Brussels, 2019. 150 с.

Додаток А

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО НАПИСАННЯ ЕСЕ

До кожної теми навчальної дисципліни «Електронні сервіси та документообіг» здобувачам освіти пропонуються питання для поглибленого вивчення, одне з яких (на власний вибір) рекомендовано представити у формі есе.

Есе являє собою індивідуальну письмову роботу невеликого обсягу (3-5 сторінок) й відносно вільної композиції, що презентує авторське бачення сутності певного питання (теми, проблеми). У перекладі з англійської есе означає «нарис», «спробу самостійного аналізу». Цей вид письмової роботи носить творчий характер. У ньому здобувач освіти має змогу не лише презентувати індивідуальний погляд на певне питання, а й аргументувати власну точку зору.

Ефективність есе як індивідуального практичного завдання пояснюється тим, що його написання максимально мобілізує інтелектуальні можливості, демонструє знання автора, його ерудицію, здатність до самостійного мислення, вміння висловити й аргументувати свої думки.

Загальні вимоги до структури есе:

Вступ – викладення загальної тези (твердження); визначення актуальності теми (проблеми) та окреслення мети, яку ставить перед собою автор. Важливо правильно сформулювати питання, на які передбачається знайти відповідь.

Основна частина – розвиток однієї думки або ж трансформація однієї думки в іншу; наведення не менше двох-трьох аргументів на користь висловленої тези, кожен з яких має бути підтверджений прикладами, фактами (оптимальний алгоритм: теза – її аргументація).

Висновок – узагальнення, що підтверджує наведену тезу, вираження авторського бачення.

Кількість тез і аргументів залежить від теми (проблеми) та логіки розвитку думки.

Поради автору есе:

– Аналізувати факти й робити аргументовані висновки.

– Відмовитися від банальних стилістичних фраз.

– Виявляти авторське «я», уникаючи при цьому використання займенника *я.*

– Демонструвати глибоке розуміння теми (проблеми) та вміння її розкрити; висловлюватися точно, лаконічно, логічно; чітко і грамотно формулювати думки.

– Прагнути до вичерпності теми (проблеми).

– Приділяти увагу не лише змістовому, а й мовно-стилістичному вдосконаленню роботи.

– Прагнути максимально зацікавити читача (слухача).

Критерії якості есе:

самостійність;

критичний аналіз;

аргументованість власної позиції;

оригінальність вирішення проблеми;

індивідуальний авторський стиль.

Найбільш часті помилки при написанні есе:

1. Порушення логіки викладу матеріалу.
2. Відсутність або брак доказів, узагальнень, висновків.
3. Надмірне й поверхове оперування даними, що зводиться лише до констатації фактів замість їх узагальнення та аргументації.
4. Переказування чужих думок за відсутності власного бачення, творчого підходу до розкриття запропонованої теми чи вирішення поставленої проблеми.

Навчальне видання
(*українською мовою*)

Сьомченко Вікторія Вікторівна
Саєнко Олена Романівна

ЕЛЕКТРОННІ СЕРВІСИ ТА ДОКУМЕНТООБІГ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальності «Облік і оподаткування»
освітньо-професійної програми «Облік і аудит»

Рецензент *О.В. Гамова*
Відповідальний за випуск *Н. М. Проскуріна*
Коректор *О. Р. Саєнко*