

Міністерство освіти і науки України
Національний університет водного
господарства та природокористування

Л.О. Маланчук
Я.В. Гонгадзе

ОСНОВИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ТА ЕЛЕКТРОННОГО УРЯДУВАННЯ

Навчальний посібник

Рівне-2025



Міністерство освіти і науки України
Національний університет водного господарства та
природокористування

Л. О. Маланчук
Я. В. Гонгадзе

**ОСНОВИ ЕЛЕКТРОННОГО
ДОКУМЕНТООБІГУ ТА
ЕЛЕКТРОННОГО УРЯДУВАННЯ**

Навчальний посібник

Рівне-2025

УДК 35.077.1:004.4(075.8)

М18

Рецензенти:

Сафоник А. П., доктор технічних наук, професор, директор навчально-наукового інституту енергетики, автоматики та водного господарства;

Микитин Т. М., доктор економічних наук, завідувач кафедри документальних комунікацій та менеджменту Рівненського державного гуманітарного університету, м. Рівне;

Іванишин Є. С., заступник міського голови з питань діяльності виконавчих органів влади, м. Рівне.

Рекомендовано Вченою радою Національного університету водного господарства та природокористування.

Протокол № 4_від 25 квітня 2025 р.

Маланчук Л. О., Гонгадзе Я. В.

М18 Основи електронного документообігу та електронного урядування: навч. посіб. [Електронне видання]. – Рівне : НУВГП, 2025. – 245 с.

ISBN 978-966-327-634-2

У навчальному посібнику розглянуто основи електронного документообігу, включаючи принципи створення та обробки електронних документів, їх правовий статус, а також збереження та архівацію. Окремо висвітлено роль електронного підпису в документах. Також розкрито основи електронного документообігу, функції систем документообігу та забезпечення безпеки даних, а також інновації в цій сфері.

Посібник також охоплює сутність електронного урядування, етапи його розвитку в Україні та переваги цієї системи, а також питання безпеки в електронному урядуванні. Розглянуто електронні звернення та петиції в Україні. Окремо висвітлено основи цифрової компетенції, важливість цифрової грамотності населення та аналіз цифрової грамотності в Україні, зокрема через Портал Дія.

УДК 35.077.1:004.4(075.8)

ISBN 978-966-327-634-2

© Л. О. Маланчук,
Я. В. Гонгадзе, 2025
© НУВГП, 2025

ЗМІСТ

ПЕРЕДМОВА	4
РОЗДІЛ 1 ВИЗНАЧЕННЯ ОСНОВНИХ ТЕРМІНІВ	5
1.1. Електронний документ.....	5
1.2. Електронний документообіг.....	10
1.3. Електронне урядування.....	13
1.4. Цифрова компетенція (грамотність).....	19
РОЗДІЛ 2 ЕЛЕКТРОННИЙ ДОКУМЕНТ.....	25
2.1. Принципи створення та обробки електронних документів.....	25
2.2. Правовий статус електронного документа.....	32
2.3. Збереження та архівація електронних документів	38
2.4. Електронний підпис та його роль в електронному документі	47
РОЗДІЛ 3 ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ	58
3.1. Основні функції систем електронного документообігу.....	58
3.2. Забезпечення безпеки і конфіденційності даних.....	65
3.3. Системи електронного документообігу	82
3.4. Інновації та новітні технології в електронному документообігу..	97
РОЗДІЛ 4 ЕЛЕКТРОННЕ ВРЯДУВАННЯ	110
4.1. Основні етапи розвитку електронного врядування в Україні	110
4.2. Переваги електронного врядування.....	115
4.3. Безпека електронного врядування	125
4.4. Електронні звернення та електронні петиції в Україні.....	144
РОЗДІЛ 5 ЦИФРОВА ГРАМОТНІСТЬ.....	154
5.1. Важливість цифрової грамотності населення	154
5.2. Аналіз цифрової грамотності населення України	159
5.3. Портал Дія для підвищення цифрової грамотності населення в Україні	177
ЗАВДАННЯ ДЛЯ ПРАКТИЧНИХ ЗАНЯТЬ	189
ПАКЕТ СИТУАЦІЙНИХ ВПРАВ	191
МОДУЛЬНІ ТЕСТОВІ ЗАВДАННЯ.....	197
СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ.....	232
СПИСОК ЛІТЕРАТУРИ	240

ПЕРЕДМОВА

У сучасному світі цифрові технології та інноваційні методи управління інформацією займають центральне місце у розвитку майже всіх сфер людської діяльності. Від цифровізації бізнес-процесів до створення нових форм урядових послуг – цифрові інструменти стають основою для підвищення ефективності та якості роботи. Перехід до електронного формату дозволяє значно спростити та прискорити обробку інформації, зменшити витрати часу та ресурсів, а також підвищити доступність і зручність для користувачів. Такі технології змінюють традиційні підходи до ведення документації, відкриваючи нові перспективи для збереження, обробки та передачі даних.

Одним із ключових елементів цифрової трансформації є поширення електронного документообігу та впровадження систем електронного урядування. Ці процеси створюють нові можливості для значної оптимізації взаємодії між різними суб'єктами: державними органами, підприємствами та громадянами. Заміна паперових документів на електронні не тільки знижує витрати на матеріали та час, але й дозволяє значно скоротити бюрократичні бар'єри. Впровадження електронного урядування сприяє прискореному обміну інформацією, покращенню доступу до державних послуг і більшій прозорості роботи урядових установ, що, в свою чергу, підвищує рівень довіри та ефективності управлінських процесів у країні.

Даний електронний навчальний посібник має на меті допомогти студентам і фахівцям розібратися в основах електронного документообігу та електронного урядування, розкрити ключові аспекти використання електронних документів у сучасному управлінському процесі. Посібник охоплює теоретичні основи, технологічні принципи та практичні інструменти, що використовуються для ефективного управління інформацією в електронному вигляді.

Цей навчальний посібник стане корисним як для студентів, так і для фахівців, які бажають вдосконалити свої навички в галузі електронного документообігу та електронного урядування.

РОЗДІЛ 1. ВИЗНАЧЕННЯ ОСНОВНИХ ТЕРМІНІВ

1.1. Електронний документ

Електронний документ представляє собою важливий об'єкт сучасного інформаційного віку, що відрізняється своєрідністю та унікальністю у контексті традиційних, паперових документів. Замість концептуальної прив'язаності до фізичного формату, електронні документи існують в електронному просторі, сприяючи зручності, швидкості та надійності в аспектах зберігання, передачі та обробки інформації. Це безумовно, виходить за межі аналогії з паперовими аналогами, репрезентуючи складний інформаційний об'єкт, здатний акумулювати різноманітні дані, взаємодіяти з іншими електронними системами та відзначати значущий прогрес у технологічному плані.

Електронні документи відзначаються не лише можливістю утримання текстового змісту. Вони включають мультимедійні компоненти, мають інтерактивний характер та можуть бути об'єктом автоматизованих процесів. Застосування електронних підписів, засобів ідентифікації та систем контролю доступу розширює перспективи забезпечення безпеки та конфіденційності документальної інформації.

Перехід до електронних документів не лише модифікує методику обробки інформації, але і революціонізує сприйняття сутності «документа». У цьому аспекті розуміння особливостей та ролі електронних документів виявляється стратегічно важливим для просування суспільства в інформаційній епосі.

Згідно Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851–IV: «Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною» [33].

Отже, електронний документ – це інформаційний об'єкт, що існує у цифровій формі та призначений для зберігання, передачі,

обробки та використання електронними засобами. На рис. 1.1 представлено ключові ознаки та особливості електронних документів.

Цифровий формат	•електронні документи зберігаються у цифровій формі, часто у вигляді файлів, які можна зберігати на комп'ютерах, серверах чи хмарних сервісах.
Структуровані дані	•електронні документи можуть містити структуровані дані, такі як текст, таблиці, графіка, звуки, відео тощо.
Електронний підпис	•деякі електронні документи можуть мати електронний підпис для підтвердження автентичності та цілісності інформації.
Легка редагованість	•електронні документи можуть бути легко редаговані за допомогою відповідного програмного забезпечення, що дозволяє вносити зміни у текст
Передача через мережу	•електронні документи можуть бути легко передані через мережі, що спрощує їх обмін між користувачами та організаціями.
Ідентифікація та контроль доступу	•електронні документи можуть мати вбудовані засоби ідентифікації та контролю доступу для забезпечення безпеки та обмеження прав доступу.
Зберігання у хмарі	•електронні документи можуть бути збережені у хмарних сервісах, що дозволяє зручний доступ до них з різних пристроїв та місць.
Можливість автоматизації обробки	•електронні документи можуть бути оброблені автоматично за допомогою програмних рішень, що спрощує рутинні операції та прискорює робочі процеси.

Рис. 1.1. Ключові ознаки та особливості електронних документів

Нижче представлено ширше описання ключових ознак електронних документів.

Цифровий формат, як визначальний аспект електронних документів, є основою для їхнього існування та функціонування в електронному середовищі. Ця характеристика не лише визначає фізичну форму зберігання, але й відкриває перед нами новий вимір можливостей та викликів.

Цифровий формат дозволяє електронним документам існувати як файлові структури, які зберігаються у спеціальних форматах, таких як PDF, DOCX, або інших, що визначають спосіб представлення та обробки інформації. У порівнянні з традиційними паперовими аналогами, цей формат не лише забезпечує ефективне зберігання, але й визначає механізми доступу, обміну та обробки даних.

Електронні документи, які використовують цифровий формат, можна зберігати на різних пристроях, таких як комп'ютери, сервери або в хмарних сервісах, що розширює їхню доступність і обмін між різними користувачами. При цьому, використання стандартизованих форматів дозволяє забезпечити сумісність та універсальний доступ до інформації. Цифровий формат також сприяє безпеці та цілісності інформації, забезпечуючи можливість використання електронних підписів та інших методів електронної аутентифікації. Він дозволяє контролювати доступ до документів, а також забезпечує можливість ведення журналів змін, що підвищує рівень безпеки та можливостей контролю за документом.

У світлі цих факторів, цифровий формат не лише є технічним аспектом зберігання електронних документів, але і стає ключовим фундаментальним елементом для їхньої функціональності, безпеки та взаємодії в сучасному інформаційному суспільстві.

Електронні документи, які є ключовим елементом інформаційного середовища, проявляють свою важливість через здатність вміщувати в себе різноманітні та структуровані дані. Вони функціонують як носії інформації, вміщуючи у собі не лише текстові матеріали, але й таблиці, графічні елементи, аудіо та відео, що забезпечує не тільки множинність форматів, але й створює згаджену і структуровану систему для зручності взаємодії та обробки інформації.

Одним із важливих аспектів сучасних електронних документів є їхній потенціал для використання електронних підписів. Ці цифрові підписи виступають як механізм верифікації, підтверджуючи як автентичність документа, так і непорушність його вмісту. Впровадження електронних підписів залежить від застосування комплексу криптографічних принципів, що не лише підвищують рівень

безпеки інформації, але і забезпечують надійність та впевненість в її автентичності. Такий підхід до зберігання та обробки інформації у форматі електронних документів визначає сучасні стандарти інформаційної безпеки та відкриває перспективи для подальшого розвитку цього важливого компонента цифрової епохи.

Легкість редагування електронних документів обумовлюється їх здатністю до ефективної модифікації за допомогою спеціалізованого програмного забезпечення. Ця характеристика передбачає можливість виразного впливу на текстовий контент, а також можливість додавання чи вилучення інформації. Такий підхід дозволяє не лише адаптувати вміст документу до конкретних вимог та уточнень, але й забезпечує гнучкість у процесі його редагування, що, в свою чергу, підвищує ефективність та точність передачі інформації.

Ефективність передачі електронних документів через мережі стає визначальною рисою їхньої функціональності, що значно полегшує процес обміну інформацією між різними користувачами та організаціями. Ця можливість забезпечує швидке та ефективне взаємодію, сприяє зручності спільної роботи та взаємодії, а також відкриває можливості для розширених обмінів інформацією в динамічному електронному середовищі.

Ідентифікація та контроль доступу в електронних документах відображають сучасні стратегії забезпечення інформаційної безпеки та управління конфіденційністю. Ці вбудовані засоби створюють просторові рамки для захисту інформаційних ресурсів та обмеження прав доступу до них. Механізми ідентифікації надають можливість однозначного визначення особи, яка звертається до документа, використовуючи різноманітні технології, такі як біометричні дані, ідентифікатори або електронні підписи.

Контроль доступу реалізується за допомогою механізмів, що визначають, які особи чи групи користувачів мають право на отримання конкретного рівня доступу до документа. Це включає в себе встановлення правил, обмежень та механізмів перевірки автентичності для забезпечення високого ступеня захисту інформації в електронних документах. Такий комплексний підхід до ідентифікації та контролю доступу визначає стандарти безпеки в інформаційних системах, забезпечуючи надійний механізм управління доступом та конфіденційністю в електронному середовищі.

Зберігання електронних документів у хмарних сервісах виступає як ключовий елемент в організації і управлінні цифровим контентом.

Ця сучасна парадигма забезпечує віддалений та безпечний доступ до інформації з різних місць та пристроїв. Хмарні сервіси, використовуючи високопродуктивні інфраструктурні рішення, надають миттєву можливість зберігання, синхронізації та обміну документами, а також забезпечують автоматизовані засоби резервного копіювання.

Цей підхід до зберігання у хмарі дозволяє впроваджувати стратегії масштабованості та гнучкості в управлінні інформаційним потоком. Зокрема, він надає можливість ефективно використовувати ресурси обчислювальних центрів, прискорюючи процеси обробки та забезпечуючи високий рівень надійності та доступності даних. Отже, використання хмарних сервісів для зберігання електронних документів стає стратегічною деталлю у сучасному цифровому управлінні інформацією, забезпечуючи зручність та безпеку доступу до ресурсів з будь-якого місця та пристрою.

Можливість автоматизації обробки електронних документів є важливим аспектом в сучасних інформаційних системах, який зумовлює високий рівень ефективності та оптимізації корпоративних робочих процесів. Застосування програмних рішень для автоматичної обробки електронних документів дозволяє здійснювати рутинні операції без значного втручання людського фактору, що сприяє не лише збільшенню продуктивності, але і уникненню помилок, пов'язаних з ручним втручанням.

Даний підхід значно розширює межі можливостей обробки інформації в електронних документах, шляхом впровадження автоматизованих алгоритмів та передових технологій обробки природної мови. Програмні рішення для автоматизації обробки даних здатні ефективно виявляти ключові елементи тексту, розпізнавати структуру даних, а також виконувати інші складні завдання, які раніше потребували значних людських ресурсів і часу. Таке вдосконалення значно полегшує робочі процеси, підвищуючи швидкість та точність обробки інформації.

Такий підхід визначається як важливий крок вперед у сфері оптимізації бізнес-процесів, забезпечуючи не лише швидкість та точність обробки інформації, але і ресурсозбереження. Здатність до автоматизованої обробки електронних документів виявляється ключовою у забезпеченні підприємств із сучасними інструментами для швидкої та ефективної реакції на потреби ринку та підвищенні

конкурентоспроможності в умовах стрімкого розвитку інформаційних технологій.

Отже, підсумовуючи, можна зазначити, що в сучасному світі електронні документи виявляються не лише необхідним елементом, але і невід'ємною складовою в різноманітних сферах діяльності, включаючи бізнес, освіту, науку, організаційне управління та інші. Це визначається суттєвими перевагами, які вони пропонують у порівнянні з традиційними паперовими документами.

У сфері бізнесу електронні документи забезпечують швидкий та зручний обмін інформацією, полегшуючи ведення ділової переписки, укладання угод та здійснення транзакцій. Освітні установи використовують електронні документи для зручного надання та обміну матеріалів, організації зберігання інформації та ведення електронних журналів. У науковій сфері вони стають важливим інструментом для зберігання та обробки дослідницьких даних, а також для публікації наукових статей.

Організаційне управління отримує вигоди від використання електронних документів через їхню здатність до автоматизації процесів, що спрощує прийняття рішень та забезпечує ефективну взаємодію між структурними підрозділами.

Таким чином, електронні документи, завдяки своїм перевагам у вигляді швидкості, ефективності та зручності, стали невід'ємною частиною сучасного інформаційного суспільства, широко застосовуючись в різних сферах людської діяльності.

1.2. Електронний документообіг

Визначення електронного документообігу відіграє ключову роль у розумінні цього концепту та визначенні його місця в сучасному управлінні документами. Електронний документообіг являє собою систему обробки та управління документами у цифровій формі, яка замінює традиційні паперові процеси.

Електронний документообіг – це система обробки, передачі, зберігання та управління електронними документами у віртуальному середовищі.

В табл. 1.1 представлено основні ознаки та особливості електронного документообігу.

Таблиця 1.1

Основні ознаки та особливості електронного документообігу

Ознака	Характеристика
Електронний формат	документи зберігаються та передаються у цифровому форматі, такому як PDF, DOCX, або інші електронні формати, що дозволяє ефективно керувати ними без потреби у фізичному паперовому вигляді.
Цифровий підпис	використання електронних підписів для підтвердження автентичності та цілісності документів, забезпечуючи їхню юридичну обов'язковість.
Автоматизація процесів	електронний документообіг надає можливість автоматизації різних етапів документообігу, що сприяє швидкому та ефективному обігу документів.
Електронна передача інформації	заміна паперових документів електронними дозволяє швидше та зручніше обмінюватися інформацією між сторонами.
Контроль доступу	забезпечення заходів безпеки та контролю доступу до електронних документів, щоб гарантувати їхню конфіденційність.
Інтеграція з іншими системами	можливість інтеграції електронного документообігу з іншими корпоративними системами для спрощення обміну даними та підвищення ефективності бізнес-процесів.
Електронна архівація	можливість довготривалого зберігання електронних документів відповідно до законодавства та стандартів.
Відстеження статусу	можливість відстежувати стан обробки документів, визначення відповідальних осіб та часових рамок.
Зменшення паперового обігу	Однією з головних переваг є зменшення використання паперу, що сприяє екологічній діяльності та зменшенню витрат.

Забезпечення відповідності законодавству є ключовим аспектом ефективного функціонування електронного документообігу (ЕДО). У сучасному інформаційному суспільстві, де перехід до цифрового обігу документів стає невід'ємною частиною корпоративної та державної діяльності, необхідно враховувати та дотримуватися комплексу нормативних вимог.

Законодавство визначає не лише технічні аспекти електронного документообігу, а й встановлює правові норми, що забезпечують законність, конфіденційність та цілісність оброблюваної інформації. Зокрема, обов'язковою є використання електронних підписів для підтвердження автентичності та цілісності електронних документів.

Крім того, система електронного документообігу повинна враховувати вимоги щодо зберігання та доступу до електронних документів протягом визначеного терміну відповідно до чинного законодавства. Ефективна електронна архівація та відстеження статусу документів сприяють не лише виконанню вимог законодавства, а й відповідають принципам ефективного управління інформацією.

Забезпечення відповідності є також гарантом довіри в електронному середовищі, що дозволяє учасникам обміну інформацією впевнено використовувати електронний документообіг для ведення своєї діяльності. Вирішення питань щодо конфіденційності, безпеки та взаємодії з іншими системами допомагає створити ефективну та легкодоступну інфраструктуру електронного документообігу, що відповідає вимогам сучасного правового середовища. Зрештою, впровадження та підтримка електронного документообігу, який відповідає законодавчим стандартам, сприяє вдосконаленню корпоративного управління та підвищує загальну ефективність бізнес-процесів та загальнодержавного управління.

Електронний документообіг має визначальне значення як для державних установ, так і для сектору бізнесу, забезпечуючи ключові переваги та сприяючи впровадженню ефективних та сучасних підходів до обігу інформації.

Для держави, впровадження електронного документообігу є кроком у напрямку створення прозорої та ефективної системи управління документами. Це сприяє зменшенню бюрократії, прискоренню прийняття рішень та підвищенню якості публічних послуг. Забезпечення електронної доступності до документів полегшує співпрацю між державними органами та забезпечує більший рівень відкритості та відповідальності в управлінні.

У сфері бізнесу, електронний документообіг виконує критичну роль у підвищенні ефективності операцій та витрат. Відмінність в обробці та передачі електронних документів дозволяє підприємствам швидше реагувати на зміни на ринку, вдосконалювати комунікацію з партнерами та клієнтами, а також забезпечує безпеку та конфіденційність бізнес-інформації. Відмова від паперового документообігу також сприяє сталому розвитку, зменшенню екологічного впливу та оптимізації робочих процесів.

Загалом, електронний документообіг відіграє важливу роль у підвищенні ефективності управління, покращенні якості послуг та

сприяє сталому розвитку, що робить його ключовим елементом в сучасному інформаційному суспільстві.

Додатково, електронний документообіг відкриває нові можливості для аналізу та обробки великого обсягу даних, що є важливим для прийняття стратегічних рішень. Цифрові технології, вбудовані в електронний документообіг, дозволяють автоматизувати аналітичні процеси, що сприяє вдосконаленню прогнозування та плануванню.

Для держави, електронний документообіг є інструментом управління даними, який допомагає в ефективному моніторингу соціально-економічних показників, підтримці взаємодії з громадськістю та формуванні інноваційної політики. Застосування цифрових технологій також сприяє підвищенню кількісної та якісної доступності публічної інформації для громадськості. Для держави, впровадження електронного документообігу стає стратегічним кроком у напрямку розвитку цифрової економіки. Це сприяє залученню інвестицій, створенню сприятливого бізнес-середовища та забезпеченню конкурентоспроможності на міжнародному рівні.

У сфері бізнесу, електронний документообіг сприяє формуванню більш гнучких та адаптивних моделей бізнес-процесів, що є важливим в умовах швидких змін у бізнес-середовищі. Застосування цифрових підходів також дозволяє створювати аналітичні звіти та панелі управління для забезпечення більш глибокого розуміння діяльності підприємства.

Отже, електронний документообіг виявляється не лише ефективним інструментом для забезпечення додержання нормативів та прискорення бізнес-процесів, але й ключовим фактором для вдосконалення аналітичних та стратегічних можливостей як для держави, так і для бізнесу.

1.3. Електронне урядування

Електронне урядування – це використання інформаційно-комунікаційних технологій (ІКТ) для поліпшення та оптимізації процесів управління державою, надання послуг громадянам та підприємствам через електронні канали. Це включає в себе впровадження електронних систем, які дозволяють взаємодіяти з державними органами, подавати документи, отримувати інформацію та отримувати різноманітні громадські послуги онлайн.

На рис. 1.2 представлено основні аспекти електронного урядування.



Рис. 1.2. Основні аспекти електронного урядування

Електронне урядування зумовлює впровадження різноманітних стратегій та інструментів для покращення взаємодії між державними органами та громадянами. У цьому контексті, перше визначення полягає у створенні електронних сервісів для громадян, таких як електронна реєстрація податків та онлайн-запис на прийом до лікаря, що сприяє зручності та швидкості взаємодії з урядовими органами.

Другий аспект – електронна адміністрація – передбачає використання інформаційно-комунікаційних технологій для автоматизації та оптимізації внутрішніх процесів державних структур, зокрема, ведення електронної документації та звітності.

Третій аспект – електронна взаємодія між урядовими органами – полягає в впровадженні систем обміну даними та інформацією, сприяючи ефективному обслуговуванню громадян та бізнесу.

Електронна взаємодія між урядовими органами представляє собою важливий крок в напрямку модернізації державного управління. Цей аспект визначається впровадженням інноваційних систем обміну даними та інформацією, спрямованих на створення ефективних механізмів обслуговування громадян та бізнесу. Метою електронної взаємодії між урядовими органами є забезпечення оперативності та координації в обробці інформації між різними секторами влади. Це

передбачає створення централізованих електронних платформ та баз даних, які дозволяють автоматизовано обмінюватися необхідною інформацією між різними гілками уряду. Такий підхід сприяє не тільки швидшому обробленню документації, але й раціоналізації взаємодії між державними структурами, знижуючи бюрократичні бар'єри та забезпечуючи більшу точність та достовірність інформації. Ефективна електронна взаємодія також відкриває нові можливості для громадян та бізнесу. Громадяни можуть швидше та зручніше отримувати різноманітні громадські послуги, отримувати інформацію та виражати свої погляди через електронні канали. Для бізнесу це означає спрощений доступ до даних та послуг, що сприяє ефективнішому веденню бізнес-процесів та підвищує загальну конкурентоспроможність.

Таким чином, розвинута електронна взаємодія між урядовими органами визначається як стратегічний елемент, спрямований на створення високопродуктивного та гнучкого державного апарату, який насамперед спрощує життя громадян та стимулює розвиток бізнес-середовища.

Інформаційна безпека, як четвертий аспект електронного урядування, націлена на розробку та впровадження ефективних стратегій та технологічних заходів для захисту конфіденційної інформації та забезпечення безпеки електронних транзакцій між урядовими органами та громадянами.

Однією з ключових вимог є розробка та впровадження систем шифрування, які забезпечують захист від несанкціонованого доступу до конфіденційної інформації. Крім того, важливо розглядати аспекти аутентифікації, авторизації та аудиту, щоб гарантувати, що тільки повноважені особи мають доступ до важливих державних даних.

Заходи із забезпечення інформаційної безпеки також включають в себе регулярні аудити та оцінки ризиків, щоб визначити потенційні слабкі місця в системах та вчасно їх усунути. Важливим елементом є інформування громадськості та підприємств про загрози та заходи безпеки, що дозволяє встановлювати свідоме та відповідальне ставлення до використання електронних послуг та обміну інформацією.

Постійний моніторинг та оновлення систем інформаційної безпеки стають необхідністю в умовах постійно зростаючого рівня кіберзагроз. Інвестиції в сучасні технології та вдосконалення методів кіберзахисту є стратегічно важливими для забезпечення стійкості та

надійності інформаційних систем урядових органів під час виконання їхніх обов'язків перед громадянами та підприємствами.

Створення електронного середовища для бізнесу, як п'ятий аспект електронного урядування, представляє собою стратегічний напрям, спрямований на поліпшення взаємодії між державними структурами та підприємствами з метою стимулювання ефективного ведення бізнесу в умовах цифрової трансформації.

Важливим елементом цього аспекту є створення онлайн-систем, які надають підприємствам можливість подавати звітність, взаємодіяти з державними органами та отримувати ліцензії без необхідності фізичного присутності. Це сприяє значній економії часу та ресурсів для бізнес-середовища, сприяючи швидшому та ефективнішому вирішенню різних питань та формальностей.

Підприємства можуть використовувати онлайн-платформи для подачі податкової звітності, моніторингу фінансових показників та співпраці з державними структурами без перешкод. Отримання ліцензій та інших дозвільних документів через електронні канали сприяє швидкішому запуску та розвитку підприємств, зменшуючи бюрократичні бар'єри.

В цілому, створення електронного середовища для бізнесу визначається як ключовий чинник підтримки підприємницької активності та сприяння розвитку економіки. Цей аспект не лише полегшує взаємодію між бізнесом та урядовими органами, але й стимулює інновації та підвищення конкурентоспроможності підприємств в умовах сучасного цифрового середовища.

Електронне урядування відіграє важливу роль у трансформації сучасного управління, сприяючи покращенню ефективності, доступності та прозорості діяльності урядових органів. Ця ініціатива розширює можливості громадян, бізнесу та урядових структур шляхом впровадження електронних сервісів, онлайн-взаємодії та автоматизації процесів. Електронне урядування спрощує процедури подання документів, оплати податків, отримання громадських послуг та забезпечує ефективний обмін інформацією між урядовими органами. В результаті цього воно сприяє зростанню економічної конкурентоспроможності, підвищує рівень задоволеності громадян, спрощує бізнес-процеси та сприяє створенню відкритого та прогресивного суспільства.

Запровадження електронного урядування охоплює різні рівні та взаємовідносини між різними учасниками. В аналізі сутності е-

урядування виділяють кілька основних рівнів та просторових характеристик, які представлено на рис. 1.3.



Рис. 1.3. Види взаємовідносин у системі електронного урядування

Запровадження електронного урядування охоплює різні рівні та взаємовідносини між різними учасниками. В аналізі сутності е-урядування виділяють кілька основних рівнів та просторових характеристик:

1. G2C (Government to Citizen) – «Уряд – Громадяни»: цей рівень включає в себе електронні сервіси та інтеракції між державними органами і громадянами. Приклади включають онлайн-подання документів, електронні системи оплати податків, електронні голосування та інші послуги, які спрощують взаємодію громадян із урядом.

2. G2B (Government to Business) – «Уряд – Бізнес»: на цьому рівні здійснюється електронна взаємодія між державними органами і підприємствами. Приклади включають електронне подання звітності, отримання ліцензій, е-закупівлі та інші послуги, спрямовані на полегшення ділового середовища.

3. G2G (Government to Government) – «Уряд – Уряд»: на цьому рівні державні органи взаємодіють між собою електронним шляхом. Приклади включають обмін даними між різними урядовими

відомствами, електронні системи звітності та інші інструменти співпраці.

Додатково до зазначених рівнів, іноземні науковці, як Ч. Фанг, виділяють інші моделі е-урядування:

- C2G (Citizen-to-Government) – «Громадяни – Уряд»: цей рівень означає електронні ініціативи та звернення громадян до уряду, такі як петиції, електронна зворотна зв'язок та інші форми взаємодії;

- B2G (Business-to-Government) – «Бізнес – Уряд»: ця модель включає в себе електронні послуги та взаємодії підприємств з державними органами, які спрощують бізнес-процеси;

- G2N (Government-to-Nonprofit) – «Уряд – Неурядові організації»: взаємодія між урядом та неурядовими організаціями через електронні засоби;

- N2G (Nonprofit-to-Government) – «Неурядові організації – Уряд»: здійснення електронних звернень та взаємодія неурядових організацій з урядом;

- G2E (Government-to-Employee) – «Уряд – Державні службовці»: взаємодія між урядом та державними службовцями через електронні системи [24].

Ці рівні та моделі дозволяють оцінити різноманітні аспекти впровадження електронного урядування та спростити взаємодію між різними учасниками процесу.

Важливість електронного урядування в сучасному світі стає невід'ємною складовою сучасного державного управління. Цей стратегічний підхід до організації взаємодії між урядовими органами, громадянами та підприємствами визначається рядом ключових аспектів.

По-перше, електронне урядування сприяє покращенню доступу громадян до громадських послуг, спрощує адміністративні процедури та робить їх більш ефективними. Підприємства також виграють від електронного середовища, отримуючи зручний доступ до послуг та можливість швидкого вирішення різних питань.

По-друге, електронна взаємодія між урядовими органами сприяє покращенню координації та обміну інформацією, що в свою чергу підвищує швидкість та ефективність надання послуг.

По-третє, важливість інформаційної безпеки визначається необхідністю захисту конфіденційної інформації та забезпечення безпеки електронних транзакцій урядових органів та громадян.

По-четверте, створення електронного середовища для бізнесу допомагає у розвитку підприємництва, спрощує процеси ведення бізнесу та стимулює інновації.

Узагальнюючи, електронне урядування виступає як ключовий механізм для підвищення доступності, ефективності та прозорості у державному управлінні, що сприяє розвитку сучасного суспільства та покращенню якості життя громадян.

1.4. Цифрова компетенція (грамотність)

Цифрова грамотність або цифрова компетенція – це набір навичок і знань, необхідних для успішної взаємодії з інформаційними технологіями та цифровим середовищем. Вона включає в себе розуміння та вміння взаємодіяти з інформацією, використовуючи електронні пристрої та мережі.

Цифрова компетенція включає в себе ряд навичок та знань, які дозволяють ефективно користуватися інформаційно–комунікаційними технологіями (ІКТ). Складові цифрової компетенції можуть варіювати в залежності від конкретного контексту, але загально визнані елементи включають такі (рис. 1.4).

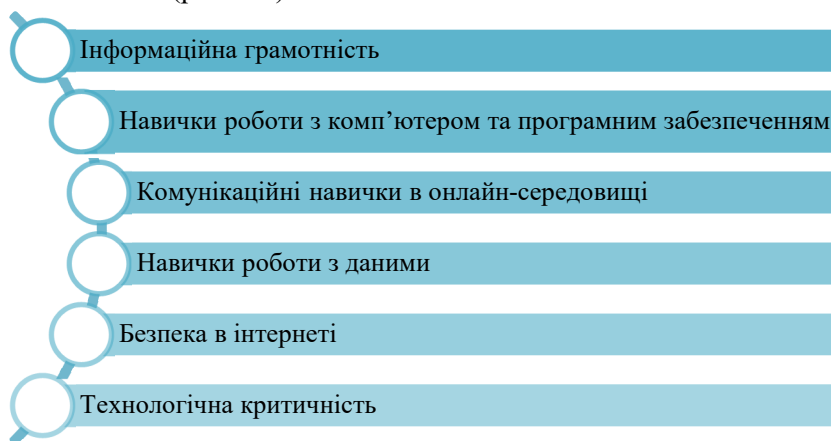


Рис. 1.4. Елементи цифрової компетенції

Зазначені навички важливі в сучасному світі, оскільки відображають реалії цифрової епохи. Цифрова компетенція дозволяє людям ефективно функціонувати в сучасному інформаційному суспільстві, знаходити роботу, розвивати бізнес, а також активно

взаємодіяти в соціальних та культурних процесах. Освоєння цих навичок робить людину більш конкурентоспроможною на ринку праці та сприяє її особистому та професійному розвитку.

Для більшого розуміння представлених елементів цифрової компетенції нижче наведена їх ширша характеристика.

Інформаційна грамотність – це ключовий елемент успішного функціонування в сучасному світі, насиченому різноманітною та постійно зростаючою інформацією. Ця навичка передбачає не просто уміння отримувати дані, але і здатність аналізувати їх критично, оцінювати надійність джерел, обирати найбільш відповідні та корисні інформаційні ресурси та використовувати їх ефективно для рішення конкретних завдань.

Перш за все, інформаційна грамотність передбачає вміння ефективно знаходити інформацію. Це включає в себе вміння користуватися різними джерелами, такими як книги, статті, інтернет–ресурси, бази даних, і знаходити в них необхідні дані. Далі, важливо вміти оцінювати інформацію. Інформаційний грамотний людина вміє розпізнавати факти від думок, оцінювати авторитетність джерел, аналізувати точки зору та розуміти можливі обмеження або приховані інтереси. Обирання правильних джерел та інформаційних ресурсів – ще один важливий аспект інформаційної грамотності. Це передбачає здатність розрізняти надійні джерела від ненадійних, а також обирати інформацію, яка найбільше відповідає потребам та меті користувача. Не менш важливим елементом інформаційної грамотності є вміння використовувати різні технічні інструменти для отримання, обробки та передачі інформації. Це може включати в себе вміння працювати з пошуковими системами, використовувати соціальні мережі, аналізувати дані за допомогою спеціальних програм тощо.

Інформаційна грамотність стає дедалі важливішою у сучасному суспільстві, де обсяг інформації зростає експоненційно, а зміст стає все різноманітнішим і доступнішим.

Навички роботи з комп'ютером та програмним забезпеченням є необхідним елементом сучасної професійної та особистої активності. Ці навички охоплюють широкий спектр інструментів та технологій, які включають в себе вміння користуватися операційними системами, офісними пакетами, редакторами графіки та іншими програмами.

Операційні системи є основним інтерфейсом між користувачем та комп'ютером. Навички роботи з операційними системами, такими як Windows, macOS, Linux, включають в себе уміння ефективно

взаємодіяти з графічним інтерфейсом, встановлювати та видаляти програми, керувати файлами та налаштовувати системні параметри.

Офісні пакети, такі як Microsoft Office, Google Workspace або LibreOffice, стали необхідним інструментарієм для багатьох професійних та особистих завдань. Вміння працювати з текстовими процесорами, електронними таблицями, презентаційними програмами та іншими компонентами офісного пакету дозволяє ефективно створювати, редагувати та обмінюватися документами. Редактори графіки, такі як Adobe Photoshop, GIMP чи Canva, вимагають специфічних навичок для створення та редагування зображень, логотипів та ілюстрацій. Робота з цими програмами передбачає розуміння основ дизайну, обробки зображень та використання різних інструментів. Навички роботи з комп'ютером також можуть включати в себе здатність встановлювати та оновлювати програмне забезпечення, роботу з веббраузерами, знання основ програмування для автоматизації завдань чи створення скриптів.

Ці навички не тільки полегшують виконання різноманітних завдань, але і роблять користувача більш конкурентоспроможним на ринку праці, дозволяючи ефективно взаємодіяти з сучасною технологічною інфраструктурою.

Комунікаційні навички в онлайн-середовищі стають все більш важливим аспектом особистого, професійного та академічного життя, оскільки спілкування в Інтернеті стає невід'ємною частиною нашої щоденної діяльності. Ці навички охоплюють різноманітні аспекти, такі як ефективне використання електронної пошти, соціальних мереж та месенджерів. Електронна пошта є одним з основних інструментів для офіційного та професійного спілкування в онлайн-середовищі. Комунікаційні навички в цьому контексті включають в себе написання чітких та конкретних повідомлень, вміння створювати формальні листи, роботу з вкладеннями та відповідь на повідомлення вчасно.

Соціальні мережі відіграють ключову роль у взаємодії та обміні інформацією в онлайн-середовищі. Важливо володіти навичками створення та редагування профілю, публікації відповідального та збалансованого контенту, а також взаємодії з іншими користувачами через коментарі, повідомлення та обговорення.

Месенджери, такі як WhatsApp, Telegram, стають все більш популярними для швидкого та неформального обміну повідомленнями в робочих чи особистих групах. Комунікаційні навички в цьому випадку включають вміння ефективно використовувати функції

месенджерів, включаючи групові чати, стікери та голосові повідомлення.

До інших ключових аспектів комунікаційних навичок в онлайн–середовищі відносяться вміння адаптувати стиль комунікації відповідно до аудиторії, розуміння нюансів мовлення в інтернеті, етикету в онлайн–спілкуванні та вміння вирішувати конфлікти в цифровому середовищі.

Навички ефективної комунікації в онлайн–середовищі є важливим елементом успішної взаємодії та співпраці в сучасному світі.

Навички роботи з даними нині визнаються однією з найбільш важливих у навчанні, професійній діяльності та особистому розвитку. Вони включають в себе не лише технічний аспект, такий як ефективне використання інструментів для збору та обробки даних, але і аналітичне мислення, необхідне для вибіркового використання інформації та отримання цінних висновків.

Починаючи зі збору даних, важливо визначати джерела, які найкраще відповідають поставленим завданням, а також враховувати їхню достовірність. При обробці даних виникає необхідність в ефективному їхньому фільтруванні, агрегації та перетворенні, щоб отримати чітку та корисну інформацію.

Застосування статистичних та аналітичних методів для аналізу даних дозволяє виявляти тенденції, залежності та кореляції, що може служити підґрунтям для прийняття обґрунтованих рішень. Вміння визначати ключові показники та робити аналітичні висновки стає невід’ємною частиною цих навичок.

Важливо також вміти візуалізувати дані, оскільки чітка графіка та діаграми сприяють кращому розумінню інформації та полегшують комунікацію результатів. Здатність представляти дані в зрозумілій формі є ключовою, особливо у відкритому для всіх груповому середовищі.

Навички роботи з даними не обмежуються тільки технічними аспектами, але також вимагають розвитку критичного мислення, логічного аналізу та етичного використання інформації. Вони стають ключем до успіху в умовах постійного зростання обсягів даних та їхнього впливу на сучасне суспільство.

Безпека в інтернеті є невід’ємною частиною сучасного цифрового життя і включає в себе розуміння основних понять, пов’язаних із збереженням конфіденційності, захистом від вірусів та

шкідливих програм, безпекою паролів та іншими аспектами цифрової безпеки.

Безпека в інтернеті включає:

1. Збереження конфіденційності: важливо розуміти, як зберігати та захищати особисті дані в інтернеті. Це включає в себе правильне використання конфіденційних інформаційних ресурсів, управління налаштуваннями приватності в соціальних мережах, а також усвідомлення ризиків, пов'язаних із наданням особистої інформації.

2. Захист від вірусів та шкідливих програм: використання надійного антивірусного програмного забезпечення та системного оновлення допомагають у запобіганні інфікуванню комп'ютера вірусами та шкідливими програмами. Регулярне оновлення програм та операційних систем є ключовим для підтримання безпеки комп'ютерної системи.

3. Безпека паролів: сильні та унікальні паролі є важливою ланкою в цифровій безпеці. Рекомендується використовувати довгі паролі, які містять букви різного регістру, цифри та спецсимволи. Важливо уникати використання одного пароля для всіх сервісів та регулярно їх оновлювати.

4. Фішинг та соціальна інженерія: розуміння та визнання фішингових атак та інших видів соціальної інженерії є важливим для уникнення шахрайства та захисту особистої інформації. Необхідно бути обережним із наданням конфіденційних даних в ненадійних джерелах.

5. Резервне копіювання даних: забезпечення регулярного резервного копіювання важливої інформації допомагає у відновленні даних у випадку втрати або атаки вірусами.

Ці аспекти безпеки в інтернеті взаємодіють для створення цілісної стратегії цифрової безпеки, що допомагає уникати ризиків та забезпечити безпеку особистої та професійної інформації в онлайн-середовищі.

Технологічна критичність – це здатність глибоко розуміти технології, їх можливості та обмеження, і водночас відчувати відповідальність за їх використання. Це охоплює більше, ніж просто вміння користуватися новими гаджетами чи програмами. Технологічно критична особа спроможна об'єктивно оцінювати, які проблеми можуть вирішити конкретні технології та наскільки ефективно вони це роблять. Важливо також усвідомлювати етичні аспекти використання

технологій, включаючи питання приватності, безпеки та справедливості. Технологічна критичність означає розуміння можливих негативних впливів технологій на суспільство та готовність адаптуватися до швидких змін у технологічному середовищі. Це не тільки володіння конкретними навичками, але й уміння поглядати на технології як на інструмент для досягнення конкретних цілей, а не як кінцеву мету саму по собі. Технологічна критичність – це своєрідний фільтр, через який проходить кожне нове технічне рішення або інновація, щоб визначити їхню справжню цінність та можливі ризики.

Отже, цифрова компетентність є невід’ємною частиною сучасного життя. Володіння цифровими навичками стає ключем до конкурентоспроможності на ринку праці, сприяє інноваціям та розвитку суспільства. Такий розвиток є стратегічно важливим для досягнення особистого успіху, конкурентоспроможності економіки та сталих інновацій у всіх сферах життя.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Що таке електронний документ, і чим він відрізняється від традиційних паперових документів?
2. Які ключові ознаки електронних документів визначені в Законі України «Про електронні документи та електронний документообіг»?
3. Які переваги надає використання електронних підписів у електронних документах?
4. Які характеристики цифрового формату електронних документів визначають їхню функціональність та безпеку?
5. Як електронний документообіг сприяє автоматизації та ефективності обробки документів у цифровому середовищі?
6. Як електронне урядування змінює взаємодію між державними органами та громадянами, підприємствами?
7. Чому цифрова компетентність є важливою для ефективного використання електронних технологій у сучасному інформаційному суспільстві?

РОЗДІЛ 2. ЕЛЕКТРОННИЙ ДОКУМЕНТ

2.1. Принципи створення та обробки електронних документів

Створення та обробка електронних документів є важливими етапами в процесі організації документообігу, що значно підвищує ефективність роботи з інформацією в сучасних умовах. Завдяки електронним технологіям стало можливим не лише швидко створювати документи, а й ефективно їх обробляти, зберігати, передавати та архівувати, що є критично важливим для досягнення високої продуктивності та зниження витрат. Водночас, забезпечення безпеки та цілісності електронних документів, їх автентичності, а також відповідність чинному законодавству стають основними вимогами до процесу їх створення та обробки. У цьому розділі будуть розглянуті ключові принципи, які визначають основи правильної організації створення та обробки електронних документів, а також механізми забезпечення їх надійності, доступності та конфіденційності.

В табл. 2.1 представлено етапи створення електронного документа.

Таблиця 2.1

Етапи створення електронного документа

Етап	Опис
1	2
1. Визначення мети документа	На цьому етапі необхідно чітко визначити цілі, для яких створюється документ, його призначення та основні завдання.
2. Вибір формату документа	Визначення формату, який буде використовуватися для створення документа (наприклад, DOCX, PDF, XML), в залежності від вимог та призначення.
3. Створення структури документа	Розробка логічної та зрозумілої структури документа: заголовки, вступ, основна частина, висновки, додатки.
4. Написання основного змісту	Написання тексту документа з урахуванням вимог до мови, стилістики та формулювання. Важливо дотримуватись чіткої та зрозумілої викладеності.
5. Оформлення документа	Форматування документа відповідно до встановлених вимог щодо шрифтів, абзаців, заголовків, списків та інших елементів.
6. Перевірка документу	На цьому етапі документ перевіряється на наявність помилок, неточностей та відповідність вимогам. Це також включає перевірку граматики та орфографії.

1	2
7. Додавання підписів та метаданих	Якщо це необхідно, додається електронний підпис, а також метадані (наприклад, автор, дата створення, тип документа) для зручності подальшої обробки та зберігання.
8. Збереження документа	Збереження документа в обраному форматі на відповідному носії чи в системі для подальшого використання або передачі.
9. Передача документа	Передача документа отримувачу (наприклад, через електронну пошту, в систему документообігу або за допомогою інших каналів зв'язку).

Першим етапом у створенні електронного документа є визначення його мети. Цей етап є критично важливим, оскільки від нього залежить, як буде побудовано весь подальший процес. На цьому етапі потрібно чітко розуміти, для чого створюється документ і які завдання він має виконати. Це може бути звіт для внутрішнього використання, договір між компаніями, інструкція для працівників або заявка на отримання фінансування.

Наприклад, якщо документ створюється для надання керівництву звіту про виконання фінансового плану за квартал, то він має містити аналіз виконаних показників, порівняння з плановими значеннями, а також рекомендації щодо коригування стратегії. Тому, на етапі визначення мети, необхідно чітко встановити, яку інформацію має містити документ і як вона повинна бути представлена.

Другим етапом є вибір формату документа. Формат визначає, як буде структуровано та відображено вміст документа, а також забезпечує сумісність з різними програмами та системами. Наприклад, для текстових документів зазвичай використовуються формати DOCX (Microsoft Word) або PDF, для таблиць – XLSX (Microsoft Excel), а для документів, що містять структуровані дані, – XML або JSON.

Якщо документ має бути переданий для перегляду або друку, формат PDF є найбільш підходящим, оскільки він гарантує, що зовнішній вигляд документа залишиться незмінним на будь-якому пристрої. Якщо документ створюється для редагування, зручнішими будуть формати DOCX або RTF, оскільки вони дозволяють вносити зміни без втрати форматування.

На цьому етапі визначається структура документа, тобто як будуть розподілені його основні частини. Структура може включати

заголовок, вступ, основний текст, висновки, додатки та інші елементи. Важливо, щоб структура була логічною та зручною для користувачів, що дозволить швидко знайти потрібну інформацію.

Наприклад, для звіту про фінансові результати структура може виглядати так:

1. Заголовок: «Звіт про фінансові результати за 4 квартал 2024 року».
2. Вступ: опис мети звіту та основних показників.
3. Основний текст: детальний аналіз фінансових результатів, порівняння з плановими показниками.
4. Висновки: рекомендації для покращення фінансових показників.
5. Додатки: таблиці, графіки, діаграми, що підтверджують дані.

Чітко визначена структура дозволяє користувачам швидко орієнтуватися в документі та ефективно використовувати інформацію.

На цьому етапі безпосередньо пишеться основний текст документа. Тут важливо дотримуватись чіткої і логічної послідовності викладу думок. Текст повинен бути зрозумілим, лаконічним і відповідати цілям документа. Для офіційних документів особливо важливо дотримуватись правильного стилю і формулювань, щоб уникнути двозначностей і непорозумінь.

Наприклад, у звіті з фінансової діяльності основний зміст може включати порівняння фактичних витрат з плановими, аналіз причин відхилень і пропозиції щодо коригування бюджетних показників. Під час написання важливо використовувати чіткі факти і цифри, а не зайві загальні фрази.

Оформлення документа включає його форматування і наведення у відповідність до стандартів. Це може включати налаштування шрифтів, розмірів, відступів, абзаців, нумерації сторінок, додавання заголовків та підзаголовків. Оформлення має бути єдиним для всіх документів, що створюються в організації, щоб забезпечити консистентність і зручність у користуванні.

Наприклад, у звіті або презентації може бути використаний один стиль шрифтів для заголовків (наприклад, Arial 14 pt), а для основного тексту – інший стиль (Times New Roman 12 pt). Важливо дотримуватися єдиної палітри кольорів та розміру шрифтів, щоб документ виглядав професійно.

Після того як основний зміст написано та документ оформлений, наступним кроком є його перевірка. Цей етап включає перевірку наявності помилок у тексті, граматичних і орфографічних помилок, а також перевірку на відповідність документу поставленим цілям і вимогам. Крім того, на цьому етапі перевіряється правильність посилань на нормативні документи, дані з таблиць і графіків.

Наприклад, перед тим як відправити звіт, необхідно переконатись, що всі цифри у фінансових таблицях відповідають реальним показникам, і що всі посилання на нормативно-правові акти правильні і актуальні. Якщо документ має бути підписаний, перевіряється правильність підписів та реквізитів.

Після того, як документ написаний, відредагований і перевірений, необхідно додати підпис, якщо це передбачено. Для електронних документів це може бути електронний підпис або інші засоби аутентифікації, які підтверджують автентичність і правомочність документа. Крім того, на цьому етапі додаються метадані: дата створення, автор, тип документа та інша інформація, яка полегшує збереження і подальшу обробку документа.

Наприклад, у звіті може бути вказано, що документ підписано електронним підписом керівника компанії, а також вказано дату створення документа і його тип (звіт, фінансовий, 2024 рік).

Після того, як документ готовий, його потрібно зберегти. Це може бути збереження на комп'ютері або у хмарному сховищі, якщо документ потрібно передати кільком користувачам. Важливо вибрати правильний формат для збереження, а також забезпечити належний рівень захисту документа. Для конфіденційних або юридично важливих документів може бути використана система захисту паролем або шифрування.

Наприклад, документ можна зберігати в хмарі з доступом за паролем, щоб лише авторизовані особи могли його переглядати чи редагувати. Це також дозволяє зберігати резервні копії документа на випадок втрати даних.

Останній етап створення електронного документа – це його передача. Документ може бути переданий різними способами: через електронну пошту, через систему електронного документообігу, або шляхом завантаження на веб-платформу для доступу інших користувачів. Важливо враховувати тип документа та особливості передачі, зокрема безпеку передачі і можливість відстеження процесу.

Наприклад, звіт про виконану роботу може бути надісланий через систему електронного документообігу, де він автоматично потрапить до відповідальних осіб для подальшої обробки і затвердження.

На рис. 2.1 представлено основні правила при обробці електронних документів.



Рис. 2.1. Основні правила при обробці електронних документів

Цілісність електронного документа полягає в забезпеченні того, щоб він не був змінений після створення чи підписання без відома автора або уповноваженої особи. Цей принцип забезпечує достовірність інформації та дозволяє гарантувати, що документ зберігається в тому вигляді, в якому він був створений або підписаний.

Для забезпечення цілісності застосовуються різноманітні технології: криптографія, електронні підписи, хешування тощо. Наприклад, використання електронного підпису гарантує, що документ не було змінено після його підписання. Криптографічні методи забезпечують перевірку цілісності даних під час передачі або зберігання.

Безпека електронних документів є ключовим принципом, що забезпечує захист даних від несанкціонованого доступу, змін або втрати. Для цього застосовуються різні методи шифрування, а також доступ до документів обмежується відповідно до прав доступу користувачів.

Захист конфіденційної інформації, що міститься в електронних документах, є особливо важливим у разі обробки персональних даних або фінансової інформації. Документи можуть шифруватися на етапі передачі або зберігання, що робить їх недоступними для сторонніх осіб.

Один із прикладів – використання SSL (Secure Socket Layer) для захищеного обміну даними через Інтернет. Це дозволяє забезпечити конфіденційність під час обміну документами, коли вони передаються через незахищену мережу.

Принцип доступності забезпечує можливість швидкого доступу до електронного документа для осіб, які мають відповідні права доступу. Важливо, щоб документи були збережені в системах, які гарантують їх надійне та тривале зберігання, забезпечуючи можливість їх відновлення у разі необхідності.

Для цього використовуються хмарні платформи та системи архівування, які дозволяють зберігати великий обсяг даних і здійснювати доступ до них за допомогою пошукових інтерфейсів. Одним із прикладів є використання систем електронного документообігу (СЕД), де всі документи зберігаються в централізованій базі даних і мають чітке позначення за метаданими, що дозволяє швидко знаходити необхідну інформацію.

Автоматизація процесу обробки документів допомагає значно підвищити ефективність роботи. Це включає автоматичне читування даних із документів, їх сортування, відправку на відповідальні особи або підрозділи, а також застосування шаблонів для спрощення процесів.

Наприклад, у великих компаніях можна автоматизувати процес перевірки коректності документів, відправки їх на підпис чи затвердження через системи електронного документообігу. Такі системи можуть автоматично визначати тип документа, перевіряти

його відповідність стандартам та спрямовувати його до відповідних відділів для подальшої обробки.

Ідентифікація та автентифікація – це принципи, які сприяють тому, щоб кожен електронний документ був віднесений до конкретної особи або організації, а також підтвердження, що документ справжній і не підроблений.

Для цього використовуються різні методи: електронний підпис, паролі, одноразові коди для доступу. Наприклад, щоб підтвердити автентичність документа, можна використовувати електронний підпис, який дозволяє перевірити, хто є автором документа та що він не був змінений після підписання.

Принцип масштабованості передбачає можливість розширення системи обробки електронних документів для роботи з великими обсягами інформації або численними користувачами без втрати продуктивності.

Інтеграція з іншими системами підприємства, такими як бухгалтерія, CRM-системи, управління персоналом, дозволяє автоматично створювати, обробляти та зберігати документи в єдиній екосистемі. Наприклад, якщо підприємство використовує систему управління взаємодією з клієнтами (CRM), то автоматична генерація договорів або рахунків-фактур може бути інтегрована прямо в цю систему.

Принцип трансформації та конвертації визначає здатність системи обробки документів змінювати формат документа для подальшого використання. Це важливо в умовах, коли документи повинні бути передані або збережені в іншому форматі для зручності або сумісності з іншими програмами.

Наприклад, часто виникає необхідність перетворення документів з формату Word в PDF для архівування, або з формату Excel у формат XML для інтеграції з іншими інформаційними системами. Програмне забезпечення може автоматично виконувати ці трансформації на етапі обробки документів.

Контроль версій є важливим принципом обробки електронних документів, який дозволяє відслідковувати зміни, внесені до документа протягом його існування. Кожна зміна в документі зберігається в системі, і користувачі можуть переглядати історію змін, що дозволяє відновити попередні версії документів у разі необхідності.

Наприклад, в процесі створення звіту чи договору кілька різних осіб можуть вносити зміни до одного і того ж документа. Система

обробки документів фіксує ці зміни, і кожен новий варіант документа отримує унікальний ідентифікатор, що дозволяє легко відстежувати, хто і коли вніс зміни.

Інтернаціоналізація та сумісність з міжнародними стандартами є важливими принципами обробки електронних документів, особливо для компаній, що працюють на глобальному рівні. Це включає в себе використання міжнародних стандартів для форматів документів (наприклад, PDF/A для архівування), а також забезпечення можливості перекладу документів на різні мови та інтеграції з різними системами, які використовуються в інших країнах.

Прикладом є використання стандарту EDI (Electronic Data Interchange) для обміну електронними документами між компаніями на міжнародному рівні, що дозволяє автоматизувати процеси передачі документів і уникнути помилок через людський фактор.

2.2. Правовий статус електронного документа

Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851–IV встановлює нормативні основи для функціонування електронних документів у правовому просторі країни [33]. Його основна мета – регулювання юридичної природи електронного документу та визначення принципів його взаємодії в електронному документообігу. Згідно з цим законом, важливо підкреслити, що сама електронна форма не може ставити під сумнів юридичну силу електронного документа.

Цей закон став відповіддю на стрімкий розвиток інформаційних технологій та перехід суспільства до цифрової епохи. Він визнає, що електронні документи, як еквівалент традиційних паперових, мають таку ж юридичну значимість і є дійсними та обов’язковими для сторін у правовідносинах.

Окрім того, закон визначає механізми забезпечення достовірності електронних документів, зокрема через використання цифрових підписів та інших засобів електронної аутентифікації, які відповідають стандартам безпеки. Встановлення цих норм та стандартів сприяє не лише правильному функціонуванню електронного документообігу, а й забезпеченню конфіденційності та недоторканості інформації.

Отже, Закон визнає переваги та важливість використання електронних документів у сучасному інформаційному суспільстві,

забезпечуючи їм відповідний правовий статус та гарантуючи їхню юридичну обов'язковість.

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про електронні комунікації», «Про електронну ідентифікацію та електронні довірчі послуги», «Про обов'язковий примірник документів», «Про Національний архівний фонд та архівні установи», та Законом України «Про електронні документи та електронний документообіг» № 851–IV від 22 травня 2003 року, а також іншими нормативно–правовими актами.

В табл. 2.2 представлено законодавча база регулювання використання електронних документів та їх коротка характеристика.

Таблиця 2.2

Законодавча база використання електронних документів в Україні

№ з/п	Закон України	Дата та номер	Характеристика
1	2	3	4
1.	«Про електронні документи та електронний документообіг»	від 22.05.2003 № 851–IV	Цей Закон визначає ключові організаційно–правові принципи використання електронних документів та проведення електронного документообігу [33].
2.	«Про інформацію»	від 02.10.1992 № 2657–XII	Цей Закон регулює процеси, пов'язані з створенням, збором, отриманням, зберіганням, використанням, поширенням, охороною та захистом інформації [34].
3.	«Про захист інформації в інформаційно–комунікаційних системах»	від 05.07.1994 № 80/94–ВР	Цей Закон визначає порядок взаємодії в галузі захисту інформації у сфері інформаційних, електронних комунікаційних та інформаційно–комунікаційних систем [35].
4.	«Про державну таємницю»	від 21.01.1994 № 3855–XII.	Цей Закон встановлює правила для регулювання відносин у суспільстві, пов'язаних з класифікацією інформації як державної таємниці, її засекречуванням, розсекречуванням матеріальних носіїв та захистом державної таємниці, спрямованим на забезпечення національної безпеки України [36].

1	2	3	4
5.	«Про електронні комунікації»	від 16.12.2020р. № 1089–IX	Цей Закон встановлює юридичні та організаційні засади державної політики в галузі електронних комунікацій та управління радіочастотним спектром. Крім того, він визначає права, обов'язки та відповідальність фізичних і юридичних осіб, що беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами [37].
6.	«Про електронну ідентифікацію та електронні довірчі послуги»	від 05.10.2017 № 2155–VIII	Цей Закон встановлює правові та організаційні принципи електронної ідентифікації та надання електронних довірчих послуг. Визначаються права та обов'язки суб'єктів у відносинах, пов'язаних з електронною ідентифікацією та довірчими електронними послугами. Також встановлюється порядок здійснення державного контролю за дотриманням вимог законодавства у цих сферах [38].
7.	«Про обов'язковий примірник документів»	від 09.04.1999 № 595–XIV	Цей Закон встановлює юридичні принципи функціонування системи обов'язкового примірника документів та регулює інформаційні відносини, що стосуються доповнення національного інформаційного фонду України [39].
8.	«Про Національний архівний фонд та архівні установи»	від 24.12.1993 № 3814–XII	Цей Закон встановлює норми, що стосуються створення, обліку, зберігання та використання Національного архівного фонду, а також інші ключові аспекти архівної справи [40].
9.	«Про електронну комерцію»	від 03.09.2015 № 675–VIII	Цей Закон визначає основні організаційно-правові принципи у сфері електронної комерції в Україні. Він встановлює правила здійснення електронних правочинів за допомогою інформаційно-комунікаційних систем та регламентує права і обов'язки учасників відносин у цій сфері [41].

Якщо Верховна Рада України виражає свою згоду на обов'язковість міжнародного договору, який має пріоритет перед законами країни, і встановлює правила, відмінні від тих, що передбачені внутрішнім законодавством, то відповідно до цього

положення застосовуються норми та правила міжнародного договору. Це визначено для забезпечення виконання зобов'язань, які Україна приймає на міжнародному рівні.

Такий підхід відображає засаду пріоритету міжнародного права, яку держава приймає, згоджуючись на обов'язковість конкретного міжнародного договору. Відповідно до цієї засади, у разі конфлікту між положеннями внутрішнього законодавства та положеннями міжнародного договору, застосовуються норми міжнародного договору, які є визначальними та обов'язковими для країни.

Це забезпечує відповідність законодавства України міжнародним нормам та стандартам і вказує на зобов'язання країни виконувати свої міжнародні зобов'язання навіть у випадках, коли вони відрізняються від внутрішнього законодавства.

Нижче, додано перелік нормативних актів які регулюють використання електронних документів:

1. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну, затвердженої постановою Кабінету Міністрів України від 17 січня 2018 року № 55 [48];

2. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання (Наказ Мін'юсту 11.11.2014 р. № 1886/5):

2.1. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання;

2.2. Перелік форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання;

2.3. Вимоги до структури та змісту XML-схеми архівних електронних документів;

2.4. Вимоги щодо найменування файлів електронних документів;

2.5. Вимоги щодо найменування файлів електронних облікових документів;

2.6. Вимоги щодо найменування файлів архівних електронних документів;

2.7. Вимоги до структури та змісту XML-схеми електронного примірника описів справ постійного зберігання;

2.8. Вимоги щодо найменування файлів електронних примірників описів справ постійного зберігання;

2.9. Вимоги до структури та змісту XML–схеми обкладинок архівних електронних справ;

2.10. Вимоги щодо найменування файлів обкладинок архівних електронних справ [47].

3. Деякі питання документування управлінської діяльності
Вимоги до форматів даних електронного документообігу в органах державної влади. Постанова від 17 січня 2018 р. № 55 [48].

4. Уніфікована система організаційно–розпорядчої документації. Вимоги до оформлення документів ДСТУ 4163:2020 [27].

5. Правила публікування інформації архівних документів. ДСТУ 9031:2020 [28].

6. Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів. Постанова КМУ від 12 грудня 2023 р. № 1298 [49].

7. Листи ДФС стосовно використання електронних документів:

7.1. Лист ДФС від 04.05.2016 № 9985/6/99–95–42–01–16–01–15 – щодо можливості використання ЕЦП при оформленні первинних облікових документів [43].

7.2. Лист ДПС України від 26.12.2011 р. № 10406/7/18–4017 «Про визнання органами ДПС електронних первинних документів» [44].

7.3. Лист ДФС від 03.03.2017 № 4451/6/99–99–14–03–03–15 – щодо використання документів, створених в електронному вигляді, в якому ДФС не заперечує використання електронних документів, але зазначає ряд застережень:

– «у разі складання та зберігання первинних документів і реєстрів бухгалтерського обліку з використанням електронних засобів оброблення інформації підприємство зобов’язане за свій рахунок виготовити їх копії на паперових носіях на вимогу інших учасників господарських операцій, а також правоохоронних органів та відповідних органів у межах їх повноважень, передбачених законами (пункт 6 статті 9 Закону № 996);

– посадова (службова) особа контролюючого органу, яка проводить перевірку, у випадках, передбачених Кодексом, має право отримувати від платника податків або його законних представників копії документів, що належать до предмета перевірки. Такі копії

повинні бути засвідчені підписом платника податків або його посадової особи та скріплені печаткою (за наявності) (пункт 85.8 статті 85 Кодексу)» [45].

На рис. 2.2 представлено підстави, які мають виконуватись одночасно для прийняття (використання) електронного документу.

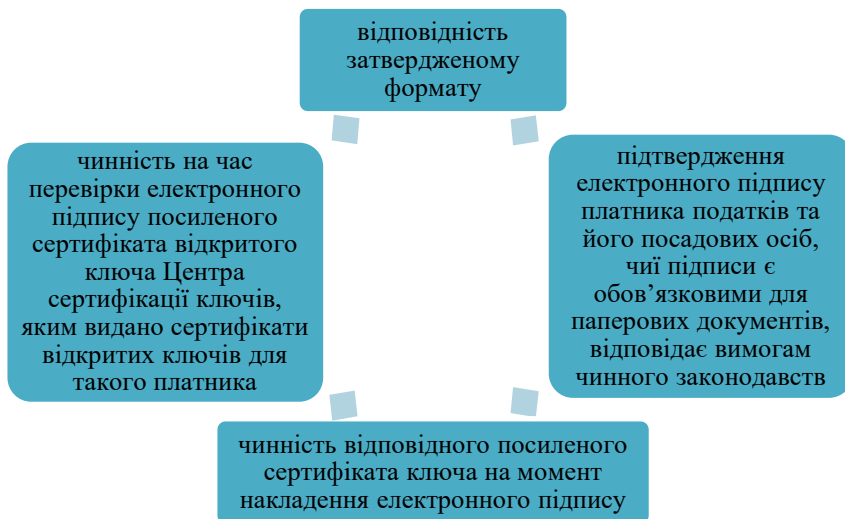


Рис. 2.2. Підстави, які мають виконуватись одночасно для прийняття (використання) електронного документу

Оригіналом електронного документа визнається його електронний варіант, що має всі необхідні реквізити, згідно з положеннями статті 7 Закону № 851. Для надання вірогідності та юридичної сили, електронний документ обов'язково підтверджується електронним підписом автора або підписом, що має такий самий юридичний статус, як власноручний підпис. У випадках, коли один електронний документ направляється різним адресатам чи зберігається на кількох електронних носіях, кожен з таких електронних варіантів розглядається як самостійний оригінал. Це забезпечує гнучкість в обігу та зберіганні електронних документів, дозволяючи кожному екземпляру мати відповідність статусу оригіналу. Такий підхід враховує сучасні реалії електронного документообігу та забезпечує їхню правову визнаність та надійність.

Відповідно до Закону України «Про електронні документи та електронний документообіг» Розділ 2. Стаття 8 зазначено: «електронний документ не може бути застосовано як оригінал:

- 1) свідоцтва про право на спадщину;
- 2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;
- 3) в інших випадках, передбачених законом» [33].

Отже, оригінальність електронного документа визначається наявністю обов'язкових реквізитів та підтверджується електронним підписом, що забезпечує його юридичну силу. Кожен електронний екземпляр, навіть якщо він надсилається різним адресатам або зберігається на кількох носіях, вважається самостійним оригіналом. Однак законодавство передбачає обмеження щодо застосування електронних документів як оригіналів у певних випадках, що сприяє правовій упорядкованості електронного документообігу.

2.3. Збереження та архівація електронних документів

Відповідно до Закону України «Про електронні документи та електронний документообіг» Розділ 3 Стаття 13: суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації таким чином, щоб можливо було перевірити цілісність цих документів безпосередньо на зазначених носіях. Важливо враховувати, що строк зберігання електронних документів на електронних носіях повинен відповідати законодавчому строку, передбаченому для аналогічних паперових документів [33].

У випадку, коли неможливо дотримуватися строків зберігання, встановлених для паперових документів, суб'єкти електронного документообігу повинні застосовувати стратегію дублювання, створюючи кілька копій електронних документів на різних електронних носіях. Ці копії повинні піддаватися періодичному копіюванню відповідно до визначених в законодавстві процедур обліку та копіювання документів.

У випадку, коли неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у формі паперових копій, здатних замінити оригінал електронного документа. При копіюванні електронних документів з електронних носіїв обов'язково проводиться

перевірка цілісності даних на цих носіях, щоб забезпечити дотримання стандартів та вимог законодавства [33].

На рис. 2.3 представлено обов'язкові вимоги визначені законодавством України при зберіганні електронних документів.

1. Доступність для подальшого використання інформації в електронних документах

- інформація, що міститься в електронних документах, повинна бути доступною з метою подальшого використання. Це передбачає, що дані повинні бути легко розпізнавані, розуміються та використовуються без перешкод для забезпечення продовження їхнього циклу життя.

2. Можливість відновлення у форматі створення електронного документа

- забезпечення можливості відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний. Це передбачає, що система повинна зберігати оригінальний формат документа для забезпечення його інтегритету та можливості точного відтворення.

3. Збереження інформації для визначення походження та призначення електронного документа

- у випадку наявності, інформація, яка дає можливість встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання, повинна зберігатися. Це включає в себе всі необхідні метадані для ідентифікації та аутентифікації документа впродовж його життєвого циклу.

Рис. 2.3. Обов'язкові вимоги визначені законодавством України при зберіганні електронних документів

Доступність для подальшого використання інформації в електронних документах є важливим аспектом ефективного управління даними та забезпеченням сталого розвитку в сучасному інформаційному середовищі. Це визначення надає ключові принципи, які важливо враховувати для забезпечення ефективного функціонування та використання електронних документів:

– легкість розпізнавання: забезпечення того, що інформація в електронних документах представлена таким чином, щоб її можна було легко впізнати та ідентифікувати. Це може включати чітку структуру

документа, використання стандартів форматування та зрозумілі назви файлів;

- легкість розуміння: забезпечення того, що інформація в електронних документах виражена зрозуміло і послідовно. Це може включати використання зрозумілої лексики, структурованих таблиць та графіків для полегшення інтерпретації даних;

- легкість використання: створення умов для ефективного використання інформації в електронних документах без труднощів або перешкод. Це включає в себе можливість швидкого доступу до необхідної інформації, можливість редагування та взаємодії з документом без значних зусиль;

- забезпечення циклу життя інформації: інформація в електронних документах залишалася актуальною та корисною протягом усього її життєвого циклу. Це включає в себе регулярне оновлення, архівацію та, при необхідності, видалення застарілої інформації.

Доступність для подальшого використання є ключовим елементом для забезпечення ефективного використання інформаційних ресурсів та їхнього внеску у розвиток різних сфер діяльності.

Можливість відновлення електронного документа у форматі його створення, відправлення чи отримання є фундаментальним аспектом ефективного управління електронною інформацією. Це визначення висвітлює необхідність збереження оригінального формату документа для забезпечення його цілісності та точного відтворення у майбутньому.

Зберігання оригінального формату є гарантією того, що електронні документи залишаються доступними та функціональними протягом їхнього життєвого циклу. Це особливо важливо у випадках, коли документи можуть бути подані періодичним аудитом, або коли потрібно використовувати їх у майбутніх процесах аналізу чи взаємодії.

Забезпечення можливості точного відтворення оригінального формату також дозволяє враховувати технологічні аспекти розвитку інформаційних систем. З часом можуть з'являтися нові версії програм та технології, і збереження оригінального формату документа гарантує його сумісність та доступність, навіть у змінених технічних умовах.

Це визначення висвітлює стратегічний підхід до управління електронними документами, що враховує потребу у збереженні оригінальності формату як ключового елементу для забезпечення

сталої, ефективної та безпечної обробки інформації в сучасному цифровому середовищі.

Збереження інформації для визначення походження та призначення електронного документа є фундаментальним елементом сучасного електронного документообігу, оскільки це дозволяє забезпечити не лише правову, але й технічну вірогідність цього документа протягом усього його життєвого циклу.

Передбачається, що відомості про походження, такі як дані про автора, дату та час створення, а також контекстуальна інформація про вихідні джерела та методи формування, повинні бути збережені у вигляді метаданих. Це не лише сприяє визначенню автентичності документа, але й надає можливість встановлення, як він інтегрується в загальний контекст бізнес-процесів.

Зокрема, інформація щодо призначення документа, така як відомості про отримувачів, терміни відправлення та отримання, створює основу для контролю за тим, як документи передаються та використовуються в рамках організаційних процесів. Зберігання цих даних впродовж усього життєвого циклу електронного документа забезпечує не тільки відповідність законодавчим вимогам, але й дозволяє ефективно вирішувати завдання аудиту та моніторингу, підвищуючи рівень впевненості в їхній легітимності та інтегрованості.

Суб'єкти електронного документообігу можуть забезпечувати виконання вимог щодо збереження електронних документів, на які накладені електронні підписи або печатки, за допомогою використання електронної довірчої послуги для зберігання електронних підписів, печаток, електронних позначок часу та відповідних сертифікатів. Це відбувається відповідно до положень Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Зазначені суб'єкти можуть користуватися електронними довірчими послугами для забезпечення інтегрованого та надійного збереження електронних документів, зокрема тих, на які накладені електронні підписи чи печатки. Використання електронних позначок часу та сертифікатів, пов'язаних із зазначеними послугами, сприяє встановленню та підтвердженню часових рамок, а також достовірності електронних документів.

Цей підхід не лише відповідає вимогам законодавства, але і надає стійкий та ефективний механізм збереження електронних документів, забезпечуючи їхню вірогідність та невід'ємність протягом усього періоду зберігання.

Створення архівів електронних документів, їх подання до архівних установ України та зберігання відбувається відповідно до визначених законодавством процедур та нормативів. Цей процес є важливою складовою ефективної архівної політики та забезпечує дотримання стандартів управління документами в цифровому відомстві.

Згідно з чинним законодавством України, архівування електронних документів передбачає точне дотримання визначених вимог і процедур. Це включає в себе створення архівів, які чітко визначають структуру та зміст електронних документів, а також відповідають вимогам щодо їхнього подання до архівних установ.

Подання електронних документів до архівних установ України передбачає ретельну ідентифікацію та каталогізацію цих документів, забезпечуючи їхню доступність та відтворюваність у майбутньому. Окрім того, зберігання в архівних установах повинно відповідати стандартам забезпечення безпеки, конфіденційності та довгостроковій цілісності електронних документів.

Електронний архів – це систематизована та структурована збірка електронних документів або інших цифрових об'єктів, яку зберігають для подальшого використання чи референції. Створення електронного архіву передбачає впорядкування, каталогізацію та забезпечення доступу до електронних документів чи файлів для забезпечення їхньої легкої ідентифікації, використання та збереження протягом тривалого часу.

Основні кроки для створення електронного архіву представлено на рис. 2.4.

Строки зберігання електронних документів регулюються законодавством, в залежності від їх виду.

Документи бухгалтерії, такі як рахунки–фактури, накладні, акти, зазвичай підпадають під строк зберігання не менше ніж 5 років. Це важливо для забезпечення можливості перевірки фінансових операцій та відповідності їхнього обліку законодавчим нормам.

Угоди, такі як контракти, додаткові погодження та додатки, можуть підпадати під різні строки зберігання, що зазвичай визначаються їхнім характером та юридичною важливістю. Це може варіюватися від 5 років до постійного утримання, залежно від умов угоди та вимог законодавства.

Інші документи, такі як довідки, листи, специфікації, зазвичай зберігаються в архіві приблизно 5 років. Це дозволяє забезпечити

достатній термін для подальшого використання та можливості відновлення інформації, якщо це необхідно.



Рис. 2.4. Основні кроки для створення електронного архіву

Планування створення електронного архіву включає в себе необхідні кроки для чіткого визначення його цілей, обсягу та вимог до

забезпечення безпеки та конфіденційності. Визначення мети архіву допомагає уточнити, яку інформацію та ресурси слід включити в архів, забезпечуючи спрямованість процесу його створення. Обсяг зберігання визначає, які типи електронних документів, дані чи об'єкти будуть включені в архів, враховуючи їхню важливість та значущість для організації чи проекту. Це дозволяє ефективно керувати обсягом інформації та забезпечувати фокус на збереженні ключових ресурсів. Розробка стратегії зберігання та доступу є важливою складовою планування, оскільки визначає методи та засоби організації та зберігання електронних документів. Враховуючи технічні та організаційні аспекти, стратегія забезпечує не лише ефективне управління архівом, але і забезпечує легкий доступ до інформації, коли це необхідно. Узгоджене та докладне планування створення електронного архіву допомагає визначити його оптимальні характеристики, забезпечуючи високий рівень ефективності, безпеки та відповідності вимогам зберігання електронних документів.

Ідентифікація документів у контексті створення електронного архіву включає в себе процес визначення конкретних електронних документів чи об'єктів, які будуть включені в архів для подальшого зберігання та використання. Цей етап планування ідентифікує різноманітні типи інформації, які можуть включати текстові документи, мультимедійні файли, електронні таблиці та інші формати. У процесі ідентифікації визначаються основні характеристики кожного документа, такі як його тип, формат, важливість, терміни зберігання, а також зв'язки з іншими документами. Це дозволяє точно визначити обсяг інформації, яка буде включена в архів, і забезпечити відповідність стратегії зберігання. Зокрема, текстова інформація може включати документи у форматі текстових файлів, електронні таблиці можуть містити фінансові дані, а мультимедійні файли можуть включати фотографії, відео чи аудіозаписи. Цей різноманітний характер ідентифікованих об'єктів визначає мультимодальність електронного архіву, що враховує різні формати та види інформації для забезпечення повноти та репрезентативності.

Створення структури та каталогізація в рамках створення електронного архіву передбачає визначення логічного та організованого порядку зберігання електронних документів. Цей етап планування включає в себе розробку системи категоризації та організації, що має за мету забезпечити легкий доступ та ефективне управління архівом. Під визначенням структури розуміється

установлення логічних відносин та ієрархії між різними категоріями та типами документів. Це може включати створення папок або розділів, що відображають організаційну структуру чи характеристики документів. Кожна структурна одиниця має чітко визначені параметри та функції. Каталогізація, у свою чергу, означає присвоєння унікальних ідентифікаторів, ключових слів або кодів кожному електронному документу для його однозначної ідентифікації та класифікації. Каталог може включати метадані, такі як дата створення, автор, ключові терміни та інші характеристики, що полегшують пошук та організацію. Кожен електронний документ повинен бути чітко ідентифікований в межах створеної структури та каталогу, що забезпечує легке виявлення та управління інформацією. Цей підхід дозволяє оптимізувати процеси пошуку та забезпечує систематизований та ефективний доступ до електронних документів в архіві.

Вибір засобів для зберігання електронних документів – важливий етап створення електронного архіву. Це включає в себе вибір технологій та програм, таких як системи управління документами (DMS), обліково-архівні програми, електронні сховища та системи автоматизованого документообігу (ECM). Однією з ключових задач є створення структури та каталогу, щоб чітко ідентифікувати та організувати кожен електронний документ. Такий підхід дозволяє забезпечити ефективне управління архівом та легкий доступ до інформації в майбутньому.

Забезпечення безпеки та конфіденційності електронного архіву передбачає визначення та впровадження механізмів, спрямованих на захист цифрової інформації. Серед основних заходів можна виокремити регулярне резервне копіювання для можливості відновлення даних, використання механізмів автентифікації та авторизації для обмеження доступу, застосування шифрування для конфіденційної інформації. Також важливим є впровадження системи моніторингу та аудиту для відслідковування активності користувачів та визначення відповідності забезпечення безпеки стандартам. Забезпечення фізичної безпеки приміщень, де розташований архів, також є обов'язковим. Крім того, визначення політик безпеки та навчання персоналу щодо їх виконання і правильного використання системи є важливою складовою безпечного та надійного функціонування електронного архіву.

Реалізація процесу створення електронного архіву включає в себе проведення кроків, передбачених планом, з метою ефективного

здійснення цього процесу. Це охоплює імпорт електронних документів у систему, їхню ідентифікацію та каталогізацію. На початковому етапі, проводиться імпорт електронних документів у визначені архівні системи з використанням відповідних інструментів. Після цього, здійснюється ідентифікація, яка включає в себе розпізнавання основних характеристик кожного документа, таких як тип, формат, важливість, та установлення зв'язків між документами. Далі, здійснюється каталогізація, що передбачає присвоєння унікальних ідентифікаторів чи ключових слів кожному документу та його впорядкування відповідно до створеної структури та каталогу. Цей процес допомагає забезпечити легкий доступ, ефективне управління та організацію електронних документів у межах архіву. Реалізація включає в себе строге дотримання розробленого плану, а також може передбачати введення додаткових заходів контролю якості, щоб забезпечити точність та повноту ідентифікації та каталогізації електронних документів у створеному архіві.

Тестування та підтримка є важливими етапами у процесі управління електронним архівом. Під час тестування проводяться перевірки для оцінки ефективності та правильності створеного архіву. Це включає в себе перевірку функціональності системи, правильності ідентифікації та каталогізації документів, а також перевірку систем безпеки та конфіденційності. Тестування спрямоване на виявлення можливих проблем та забезпечення оптимальної продуктивності архіву. Підтримка архіву забезпечується регулярним оновленням системи та внесенням необхідних змін у випадку зміни вимог чи стандартів. Також важливо враховувати розвиток технологій та забезпечити адаптацію архіву до нових вимог і викликів. Підтримка може також включати надання консультацій користувачам, вирішення проблем та забезпечення безперебійної роботи системи протягом часу. Тестування та підтримка створеного архіву є невід'ємною частиною процесу управління електронною інформацією, що гарантує його ефективність та відповідність вимогам упродовж тривалого періоду експлуатації.

Створення електронного архіву вимагає інтегрованого підходу, який включає в себе дотримання стандартів та уважне врахування особливостей зберігання електронних документів. Основною метою є забезпечення доступності та цілісності цих документів у майбутньому. Необхідно дотримуватися визначених стандартів якісної організації електронного архіву, включаючи ефективні механізми ідентифікації,

каталогізації та зберігання документів. Комплексний підхід передбачає впровадження сучасних технологій та методів управління даними, щоб забезпечити оптимальну функціональність та легкість доступу. Специфіка зберігання електронних документів, така як застосування ефективних систем резервного копіювання, захист від несанкціонованого доступу та збереження метаданих для визначення походження та призначення документів, викликає необхідність уважного врахування цих аспектів при проектуванні та реалізації архівного середовища. Комплексний підхід і врахування специфіки забезпечують створення електронного архіву, який відповідає вимогам сучасності та гарантує довгострокову доступність та цілісність електронних документів.

2.4. Електронний підпис та його роль в електронному документі

Електронний підпис визначає себе як критичний елемент в цифровому оточенні, функціонуючи як ефективний механізм для забезпечення надійності та безпеки електронних взаємодій. Він слугує рядом важливих цілей:

- електронний підпис дозволяє впізнавати особу чи організацію, яка здійснює підпис чи взаємодію в цифровому середовищі. Це стає ключовим елементом в уникненні підробок та забезпеченні правильності учасників електронних процесів;

- електронний підпис гарантує, що дані, які були підписані, залишаються незмінними. Це важливо для уникнення будь-яких недозволених змін чи порушень цілісності інформації під час її передачі;

- використання електронного підпису сприяє створенню довіри між учасниками електронних операцій. Довіра є ключовою умовою для успішної електронної комунікації та транзакцій;

- електронний підпис є ефективним інструментом для забезпечення конфіденційності та захисту електронних даних від несанкціонованого доступу чи зміни;

- багато країн закріплюють юридичну силу для електронних підписів, надаючи їм той самий статус, що і традиційним паперовим підписам, що робить їх юридично обов'язковими.

Електронний підпис значно полегшує та покращує ефективність електронних операцій, забезпечуючи високий рівень довіри та безпеки в цифровому світі.

Законодавство України передбачає регулювання різних форм підписів, які виходять за межі звичайного підпису на папері. На рис. 2.5 представлено види підписів та їх визначення.



Електронний підпис-це електронні дані, що приєднуються підписувачем до інших електронних даних або логічно пов'язані з ними, призначені для використання як підпис.



Удосконалений електронний підпис – це форма електронного підпису, що виникає в результаті криптографічного перетворення електронних даних, пов'язаних із підписом.



Кваліфікований електронний підпис – це вдосконалений електронний підпис, який генерується за допомогою кваліфікованого електронного підпису та ґрунтується на кваліфікованому сертифікаті відкритого ключа



Електронний підпис одноразовим ідентифікатором - це дані у електронній формі у вигляді послідовності букв і цифр, що приєднуються особою, яка прийняла пропозицію (оферту) укласти електронний договір, до інших електронних даних і відправляються іншій стороні цього договору.

Рис. 2.5. Форми електронних підписів

Електронний підпис (ЕП) представляє собою важливий інструмент в електронному середовищі, який гарантує безпеку, автентичність та цілісність електронних документів та транзакцій. Законодавство, зокрема Закон України «Про електронну ідентифікацію та електронні довірчі послуги», визначає ЕП як електронні дані, що приєднуються підписувачем до інших електронних даних або логічно пов'язані з ними і використовуються як підпис.

ЕП може приймати різні форми, включаючи простий скан зображення підпису на паперовому носії. Однак важливо відзначити, що ЕП не обмежується лише цією простою формою. Він також охоплює удосконалені та кваліфіковані підписи, які використовують криптографічні методи для створення електронного підпису.

Удосконалений ЕП створюється шляхом криптографічного перетворення електронних даних, пов'язаних із підписом. Цей вид підпису використовує засіб удосконаленого електронного підпису та особистий ключ, що є чітко пов'язаним з підписувачем. Його основні функції включають забезпечення електронної ідентифікації підписувача та виявлення будь-яких порушень цілісності електронних даних, пов'язаних з цим підписом.

Удосконалений електронний підпис (УЕП) представляє собою високорівневу форму електронного підпису, який виникає в результаті криптографічного перетворення електронних даних, що з ним пов'язані. Цей вид підпису створюється за допомогою засобу удосконаленого електронного підпису та особистого ключа, який однозначно пов'язаний з підписувачем.

Основна функція УЕП полягає в забезпеченні безпеки та відстеження електронних даних, які пов'язані з цим підписом. Використовуючи криптографічні методи, УЕП гарантує, що дані, які підписані, залишаються незмінними, а також надає можливість здійснювати електронну ідентифікацію підписувача.

Положення статті 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» чітко визначає основні аспекти удосконаленого електронного підпису та його роль в електронному середовищі. Варто зауважити, що банки часто використовують удосконалені електронні підписи для забезпечення високого рівня безпеки та впевненості в транзакціях, особливо коли вони не мають власного постачальника кваліфікованих електронних послуг. УЕП є важливим елементом цифрової безпеки, що сприяє надійній електронній ідентифікації та захисту електронних даних у високоризикових операціях.

Кваліфікований електронний підпис (КЕП) є вищим рівнем безпеки в рамках електронного підпису, відповідно до визначень Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (пункт 27 статті 1). Цей вид підпису є формою удосконаленого електронного підпису, який формується з

використанням засобу кваліфікованого електронного підпису та базується на кваліфікованому сертифікаті відкритого ключа.

Кваліфікований електронний підпис отримує свою юридичну значимість через наявність кваліфікованого сертифікату відкритого ключа, який підтверджує валідність підпису та ідентифікацію особи, яка його створила. Цей сертифікат видається кваліфікованим постачальником електронних довірчих послуг, що забезпечує додатковий рівень надійності та довіри до електронного підпису.

Основна мета кваліфікованого електронного підпису полягає в створенні вірогідного та безпечного інструменту для підтвердження ідентифікації та автентифікації особи, а також забезпечення можливості підробки чи модифікації підписаних електронних документів чи транзакцій. КЕП є необхідним для ряду важливих галузей, включаючи фінанси, юридичні та бізнесові транзакції, де важливо зберігати високий ступінь юридичної сили та довіри.

Електронний підпис одноразовим ідентифікатором – це дані у електронній формі, представлені у вигляді послідовності букв та цифр, які приєднуються до інших електронних даних особою, яка прийняла пропозицію (оферту) щодо укладення електронного договору. Ці дані надсилаються іншій стороні цього договору згідно з положеннями пункту 6 статті 3 Закону України «Про електронну комерцію».

Електронний підпис одноразовим ідентифікатором є ефективним засобом забезпечення визначення та підтвердження волевиявлення сторін при укладенні електронних угод. Використання такого підпису спрощує та забезпечує безпеку електронних комерційних транзакцій, дозволяючи сторонам взаємодіяти в цифровому середовищі, зберігаючи при цьому важливість конфіденційності та невідмінності угод.

Згідно з положеннями Закону України «Про електронну ідентифікацію та електронні довірчі послуги», визначено використання удосконаленого електронного підпису (УЕП), який має відмінності у рівні захисту інформації порівняно з кваліфікованим електронним підписом (КЕП).

В контексті носіїв ключів для КЕП і УЕП, важливо відзначити різноманітність методів зберігання, яка відображає динаміку сучасних технологій та потреб користувачів. Ключі електронного підпису (КЕП і УЕП) є критичним елементом цифрової безпеки, і їхні носії визначають різницю у рівнях захисту та зручності використання.

Ключі КЕП, що генеруються на захищеному носії, такому як вбудована пам'ять пристрою, або можуть розміщуватися на захищеному сервері, демонструють високий ступінь безпеки. Це може бути вбудована пам'ять у фізичних пристроях або ж віддалені сервери, забезпечуючи непростий доступ до ключа. Особливо ефективним варіантом є «хмарне» зберігання, де ключ знаходиться в безпечному хмарному середовищі, що гарантує надзвичайний рівень захисту та гнучкість управління. У випадку УЕП, ключ формується у файлі і зберігається на стандартних носіях, таких як флеш-накопичувачі чи CD-диски. Цей підхід надає користувачам простоту та зручність зберігання та обміну ключами, але водночас потребує уважності щодо фізичного захисту цих носіїв. Особливо важливою є безпека від несанкціонованого доступу та можливість вчасної зміни ключів.

Однією з основних відмінностей полягає в тому, що ключ УЕП може бути скопійований та розповсюджений різними електронними засобами, включаючи електронну пошту. Навпаки, ключ КЕП використовується лише на тому пристрої, на якому він був сформований.

Зазначено, що візуально користувач не зможе розрізнити КЕП від УЕП, і для перевірки електронного підпису слід звертатися до веб-ресурсу центрального засвідчувального органу (ЦЗО). Процедура включає завантаження будь-якого підписаного файлу, після чого на веб-сайті буде надано інформацію щодо застосованого виду електронного підпису –КЕП чи УЕП – в документі.

Кваліфіковані надавачі електронних підписів видають ключі у різних формах, кожна з яких має свої особливості щодо зберігання та використання. Основні форми ключів електронного підпису представлено в табл. 2.3.

Кожен з цих видів ключів використовується для різних типів електронних підписів та має свої переваги та обмеження з точки зору безпеки та зручності використання.

На веб-ресурсі Центрального засвідчувального органу (ЦЗО) доступний абсолютно вичерпний перелік усіх кваліфікованих надавачів електронних підписів (КЕП), і на даний момент їх кількість перевищує двадцять. Кожен з цих надавачів має власний веб-сайт, на якому детально описаний процес видачі ключів.

Законодавство у сфері електронних довірчих послуг встановлює єдиний для всіх надавачів перелік документів, необхідних для отримання ключів електронного підпису. Це забезпечує єдність

стандартів і уніфікований підхід до процесу аутентифікації та видачі ключів. Користувачі можуть бути впевнені в справедливості та консистентності вимог незалежно від обраного ними надавача послуг.

Таблиця 2.3

Основні форми ключів електронного підпису

Назва	Опис	Характеристика
Файловий ключ	Зберігається у вигляді файлу на комп'ютері, USB-флешці чи іншому носії інформації	Легко копіюється і може бути збережений у будь-якому місці. Використовується для створення удосконаленого електронного підпису (UEP).
Апаратний ключ (токен)	Знаходиться на захищеному USB-носії (токені).	Неможливо скопіювати, оскільки ключ фізично зберігається на апаратному пристрої. Забезпечує високий рівень надійності.
Хмарний ключ	Зберігається в хмарному сховищі, доступ до якого можливий з будь-якого пристрою з виходом в Інтернет.	Власник має доступ з двофакторною авторизацією. Забезпечує зручний та безпечний доступ до ключа.
Mobile ID	Зберігається у файлі на SIM-карті смартфона.	Для використання потрібно ввести номер телефону і PIN-код. Забезпечує високий рівень надійності, оскільки ключ фізично знаходиться на SIM-карті.

Загальна державна нормативна база забезпечує прозорий та однозначний порядок взаємодії між надавачами електронних підписів та їхніми клієнтами. Це сприяє високому рівню довіри до електронних підписів та їхній широкій інтеграції в різноманітні сфери суспільства і бізнесу.

На рис. 2.6 представлено перелік документів, які потрібні для отримання кваліфікаційного електронного підпису.

Сертифікат для кваліфікаційного електронного підпису (КЕП) видається на період до двох років, що забезпечує ефективний механізм безпеки та запобігання можливості компрометації ключової інформації. Після закінчення цього терміну необхідно провести процедуру оновлення сертифіката, що дозволяє підтримувати високий

рівень захисту. Оновлення сертифіката КЕП виконується зазвичай у режимі онлайн, що спрощує та прискорює весь процес для власників електронних підписів. Цей підхід дозволяє уникнути зайвих зусиль і забезпечити безперервне функціонування електронних підписів без значних перерв у роботі користувача.

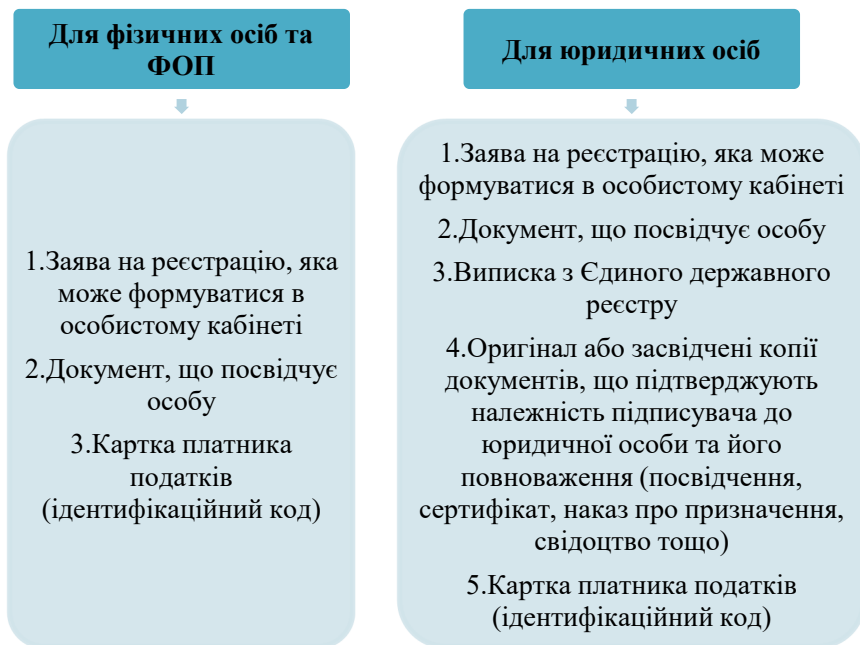


Рис. 2.6. Перелік документів, які потрібні для отримання кваліфікаційного електронного підпису

Важливою перевагою обмеження терміну дії сертифіката є можливість оперативно реагувати на зміни в безпеці та швидко впроваджувати нові технології та шифрування. Такий підхід є стандартною практикою в області електронних довірчих послуг і дозволяє підтримувати високий рівень безпеки та довіри у цифровому середовищі. Електронний підпис грає важливу роль у забезпеченні безпеки та вірогідності електронних документів.

На рис. 2.7 представлено основні функції та роль електронного підпису в електронних документах.

Аутентифікація особи	•засіб ідентифікації особи в документі, гарантує, що лише власник має доступ до ключа.
Цілісність документа	•будь-яка зміна в тексті веде до зміни підпису.
Неможливість відмови	•власник не може заперечити свій підпис, оскільки приватний ключ-унікальний і доступний лише йому.
Юридична цінність	•у багатьох країнах суди та правові органи визнають документи, підписані електронно.
Забезпечення конфіденційності	•електронний підпис, у поєднанні із шифруванням приватним ключем, забезпечує конфіденційність електронного документа..

Рис. 2.7. Основні функції та роль електронного підпису в електронних документах

Аутентифікація особи через електронний підпис є важливим елементом цифрової безпеки та інформаційної безпеки. Здійснення ідентифікації особи у цифровому середовищі стає необхідністю у зв'язку з розширенням використання електронних документів та транзакцій в інтернеті.

Електронний підпис, що використовується для аутентифікації особи, визначає, хто саме стоїть за конкретним електронним документом чи транзакцією. Він вирішує проблему визначення авторства та вірогідності джерела інформації в цифровому форматі.

Головною перевагою електронного підпису в аутентифікації є те, що він гарантує, що тільки власник приватного ключа, який використовується для створення електронного підпису, має повний контроль над своєю ідентичністю в цифровому просторі. Це створює надійний механізм захисту від несанкційованого доступу та підробки.

Такий підхід стає особливо важливим у фінансових та юридичних операціях, де достовірність та вірогідність інформації мають велике значення. З визнанням юридичної сили електронних

підписів у багатьох країнах, вони стають основою для підтвердження автентичності та валідності електронних документів у судовому порядку. Такий механізм аутентифікації не лише спрощує процеси електронного обігу документів, але й забезпечує високий рівень безпеки в цифровому просторі.

Цілісність документа, забезпечена електронним підписом, є ключовою складовою безпеки в цифровому середовищі. Електронний підпис гарантує, що електронний документ залишається недоторканим та незмінним після його підписання. Кожна найменша зміна в тексті чи вмісті документа призведе до автоматичної зміни електронного підпису.

Ця механіка стає надійним засобом виявлення будь-яких спроб незаконної або несанкційованої модифікації документа. Такий підхід особливо важливий в областях, де важлива вірогідність та непорушеність інформації, таких як фінанси, юриспруденція, та медицина.

Забезпечуючи цілісність електронних документів, електронний підпис не лише допомагає уникнути випадків недозволених змін чи підробок, але і забезпечує впевненість у тому, що інформація, що міститься в документі, залишається точною та достовірною протягом усього цифрового життєвого циклу документа.

Принцип «неможливості відмови» у сфері електронного підпису виступає як надійний механізм підтвердження автентичності та непорушності підписаного документа. Електронний підпис не лише фіксує факт того, що конкретна особа підписала документ, але й надає об'єктивний доказ цього факту.

Важливою особливістю цього принципу є те, що особа, яка створила електронний підпис, не може відмовитися від свого підпису. Це впливає з того, що приватний ключ, що використовується для створення підпису, є унікальним і єдино доступним власнику. Такий унікальний характер приватного ключа гарантує, що жодна інша особа не може втверджувати, ніби вона стояла за підписом.

Цей аспект електронного підпису визначає його важливість в правовому та комерційному середовищі. Визнання неможливості відмови є ключовим у вирішенні судових питань, а також в області укладення та виконання контрактів, оскільки факт підпису вважається безспірним та невідворотним. Такий підхід робить електронні підписи не лише зручними та ефективними, але й вкрай надійними засобами управління цифровими транзакціями та документами в сучасному світі.

Юридична цінність електронного підпису є важливою складовою його призначення в сучасному правовому середовищі. У багатьох країнах електронний підпис наділено такою ж юридичною силою, як і традиційний, ручний підпис, що визначає його правомірність та придатність для використання в судових процесах і правових транзакціях.

Визнання електронного підпису судами та правовими органами визначає його правомірність як засобу підтвердження ідентичності та непорушності електронних документів. Це важливо в контексті сучасних електронних та онлайн-транзакцій, де документообіг та угоди можуть відбуватися в цифровій формі.

Цей підхід до юридичної вартості електронного підпису полегшує та прискорює юридичні процеси, зменшуючи необхідність використання паперових документів та фізичних підписів. Відзначаючи його правомірність, суди визнають ефективність електронного підпису в сучасному цифровому світі, сприяючи тим самим розвитку безпечних та зручних електронних технологій в правовій сфері.

Забезпечення конфіденційності є ключовою аспектом використання електронного підпису в цифровому середовищі. Якщо електронний документ шифрується за допомогою приватного ключа, електронний підпис виступає не лише як підтвердження автентичності, а й як ефективний механізм забезпечення конфіденційності інформації.

Процес шифрування за допомогою приватного ключа перетворює електронний документ у зашифрований формат, доступ до якого має лише той, хто володіє відповідним приватним ключем. Отже, електронний підпис, якщо використовується разом із шифруванням, не лише підтверджує авторство та цілісність документа, але і гарантує, що лише власник приватного ключа може розшифрувати та отримати доступ до змісту документа.

Цей додатковий шар безпеки стає надійним заходом для захисту конфіденційної інформації в електронних документах. Застосування електронного підпису для шифрування дозволяє впевнено передавати та обробляти конфіденційну інформацію в цифровому форматі, зберігаючи високий ступінь безпеки та обмежуючи доступ лише до тих, хто має необхідні ключі. Такий підхід допомагає вирішувати важливі завдання забезпечення приватності та конфіденційності в електронному середовищі.

Електронні підписи стають все більш популярними в електронному документообігу і транзакціях завдяки їхній ефективності в забезпеченні важливих аспектів безпеки та вірогідності у світі цифрових технологій. Ці підписи визнані в багатьох країнах як інструменти, що мають таку ж юридичну силу, як і традиційні паперові підписи, забезпечуючи надійність в цифрових відносинах.

Використання електронних підписів дозволяє ефективно вирішувати завдання ідентифікації особи, гарантування цілісності електронних документів, неможливості відмови від підпису та забезпечення конфіденційності через використання шифрування. Визнання їхньої правомірності у судових та комерційних справах підкреслює їхню значущість в сучасному цифровому середовищі.

Застосування електронних підписів активно розширюється в фінансових установах, угодах, медичних системах та інших галузях, надаючи важливий інструмент для безпечного та вірогідного проведення електронних транзакцій та обміну інформацією. У світі, де цифрова трансформація набуває все більшого значення, електронні підписи виступають як важливий елемент, сприяючи розвитку ефективних та безпечних цифрових практик.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які етапи передбачаються при створенні електронного документа? Поясніть основні етапи.

2. Які принципи забезпечують цілісність та безпеку електронних документів? Наведіть приклади технологій, що використовуються для цього.

3. Як електронний підпис забезпечує юридичну силу електронного документа? Які його основні функції?

4. Що таке удосконалений електронний підпис (УЕП) і чим він відрізняється від кваліфікованого електронного підпису (КЕП)?

5. Які вимоги визначені законодавством України щодо збереження електронних документів? Як забезпечується їхня доступність і цілісність?

6. В чому полягає роль електронного підпису у процесах аутентифікації та забезпечення конфіденційності в електронних документах?

7. Як відбувається передача електронного документа в систему документообігу? Які важливі аспекти слід враховувати при передачі документа через різні канали зв'язку?

РОЗДІЛ 3. ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ

3.1. Основні функції систем електронного документообігу

Системи електронного документообігу (СЕД) є ключовим інструментом сучасного управління інформаційними потоками в організаціях, що дозволяє значно підвищити ефективність роботи та забезпечити прозорість ділових процесів. Основними функціями таких систем є автоматизація процесів створення, обробки, передачі, зберігання та пошуку документів, що сприяє зменшенню витрат часу і ресурсів, пов'язаних із традиційними методами документообігу. СЕД інтегруються в інформаційну інфраструктуру підприємства, забезпечуючи централізований доступ до даних, контроль за виконанням завдань і підвищення рівня безпеки інформації.

На рис. 3.1 представлено основні функції систем електронного документообігу.

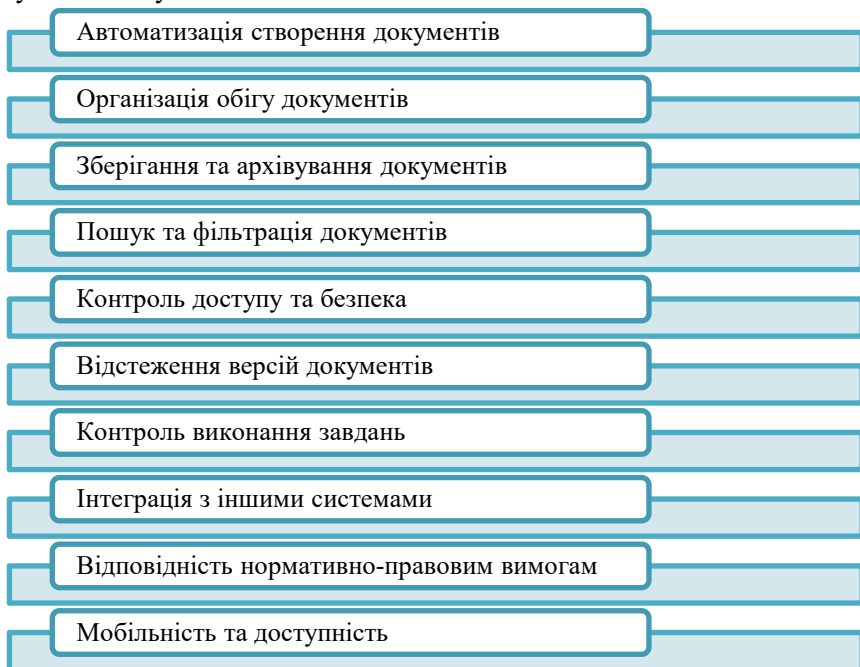


Рис. 3.1. Основні функції систем електронного документообігу

Автоматизація створення документів є однією з ключових функцій систем електронного документообігу, яка дозволяє суттєво

підвищити ефективність та точність ділових процесів. Вона передбачає використання шаблонів документів, що забезпечує стандартизацію їх змісту та структури, зменшуючи ймовірність помилок під час створення. Завдяки автоматичному заповненню даних система може використовувати інформацію з наявних баз даних або інших джерел, зменшуючи необхідність ручного введення і, таким чином, скорочуючи час, необхідний для підготовки документів. Інтеграція з іншими інформаційними системами, такими як CRM чи ERP, дозволяє автоматично вивантажувати дані про клієнтів, контракти або транзакції, що забезпечує швидке формування документів, адаптованих до конкретних потреб користувачів. У результаті автоматизація створення документів сприяє підвищенню продуктивності співробітників, зниженню витрат на рутинні операції та покращенню загальної якості документаційних процесів.

Організація обігу документів є важливою функцією систем електронного документообігу, що сприяє структурованому та ефективному управлінню інформаційними потоками в організації. Ця функція забезпечує чітке визначення маршруту передачі документів між користувачами, відділами чи структурними підрозділами, що дозволяє уникнути плутанини, затримок та дублювання завдань. Завдяки встановленим регламентам і правилам документообігу кожен учасник процесу має чітко окреслені обов'язки та часові рамки виконання завдань. Це забезпечує своєчасну передачу документів на відповідні етапи їх обробки, підписання чи затвердження. Додатково система може використовувати автоматичні сповіщення, які інформують користувачів про нові завдання або необхідність виконання певних дій. Такий підхід підвищує прозорість документообігу, мінімізує людський фактор та знижує ризик втрати або некоректної обробки інформації. Організація обігу документів дозволяє оптимізувати внутрішні процеси, підвищити їх продуктивність і забезпечити якісну взаємодію між різними рівнями управління.

Зберігання та архівування документів є важливим елементом систем електронного документообігу, що забезпечує централізоване управління інформаційними ресурсами організації. Централізоване збереження документів у електронному вигляді дозволяє уникнути дублювання інформації, оптимізувати використання серверних ресурсів та забезпечити високий рівень безпеки даних. Довготривале зберігання документів відповідає нормативним і законодавчим

вимогам, дозволяючи зберігати важливу інформацію протягом визначених строків без ризику її втрати чи пошкодження. Електронні архіви забезпечують швидкий та зручний доступ до документів, що знижує час на пошук необхідної інформації та підвищує ефективність роботи співробітників. Завдяки функціоналу системи, користувачі можуть знаходити потрібні документи за різними критеріями, такими як метадані, реквізити чи ключові слова. Крім того, можливість резервного копіювання та відновлення даних у разі технічних збоїв забезпечує додатковий рівень надійності. Таким чином, зберігання та архівування документів у сучасних системах електронного документообігу сприяє раціональному використанню інформації, зменшенню ризиків її втрати та підвищенню загальної продуктивності організації.

Пошук та фільтрація документів є однією з найбільш корисних функцій систем електронного документообігу, яка дозволяє користувачам швидко знаходити необхідну інформацію серед великого обсягу даних. Ця функція забезпечує можливість пошуку документів за різними критеріями, такими як ключові слова, реквізити, дати створення, авторство чи метадані, що значно спрощує процес навігації у великій базі даних. Інтеграція інтелектуальних алгоритмів пошуку дозволяє враховувати не лише точні відповідності запиту, але й контекстний зміст, що підвищує точність результатів. Завдяки функціям фільтрації користувачі можуть сортувати результати за різними параметрами, такими як дата створення чи актуальність документа. Це дозволяє мінімізувати витрати часу на ручний перегляд файлів та забезпечує ефективність роботи навіть у великих організаціях. Крім того, функція пошуку та фільтрації сприяє оперативному прийняттю управлінських рішень, оскільки доступ до необхідної інформації відбувається в режимі реального часу. Таким чином, ця функція є невід’ємним інструментом підвищення продуктивності працівників та забезпечення швидкості виконання бізнес-процесів.

Контроль доступу та безпека є критично важливими функціями систем електронного документообігу, які спрямовані на забезпечення конфіденційності, цілісності та доступності даних. Управління правами доступу ґрунтується на ролях користувачів, що дозволяє чітко визначити, які дії з документами можуть виконувати різні категорії співробітників залежно від їх посадових обов’язків. Такий підхід забезпечує мінімізацію ризику несанкціонованих змін або втрат

важливої інформації. Захист даних від несанкціонованого доступу реалізується за допомогою багаторівневих систем автентифікації, використання паролів, одноразових кодів або біометричних методів ідентифікації.

Крім того, застосування криптографічних методів, таких як електронний підпис та шифрування, гарантує автентичність документів і забезпечує їх юридичну силу. Це особливо важливо для документів, що мають значення для правових чи фінансових взаємодій. Резервне копіювання та системи відновлення також є частиною комплексного підходу до безпеки, що дозволяє уникнути втрати даних через технічні збої чи кібератаки. Таким чином, контроль доступу та забезпечення безпеки даних у системах електронного документообігу є основою для ефективної роботи організації та збереження її інформаційних активів.

Відстеження версій документів є важливою функцією систем електронного документообігу, яка спрямована на забезпечення прозорості та контрольованості процесів роботи з документами. Ця функція дозволяє зберігати історію змін кожного документа, що включає детальний запис усіх редагувань, зазначення часу їх внесення, а також ідентифікацію користувачів, які виконували відповідні дії. Завдяки цьому можливо відновити попередні версії документів у разі виникнення помилок або потреби в аналізі змін.

Збереження версій сприяє ефективному управлінню документацією в умовах командної роботи, де кілька осіб можуть одночасно працювати над одним файлом. Коментарі до змін, які додаються під час редагування, забезпечують додатковий контекст і пояснення для учасників процесу. Такий підхід мінімізує ймовірність виникнення непорозумінь та підвищує якість співпраці між членами команди.

Крім того, функція відстеження версій є невід’ємною складовою забезпечення відповідності нормативним вимогам, оскільки дозволяє документувати всі зміни та підтверджувати відповідність процедур внутрішнього контролю. У підсумку, відстеження версій документів сприяє ефективній організації робочих процесів, підвищенню довіри до системи електронного документообігу та забезпеченню збереження інформаційної цілісності.

Контроль виконання завдань у системах електронного документообігу є важливою функцією, що дозволяє організувати і моніторити виконання задач, пов’язаних із обробкою, затвердженням чи іншими діями над документами. Ця функція забезпечує автоматичне

відстеження прогресу виконання завдань, зокрема, фіксацію статусу кожного етапу, таких як «на розгляді», «виконано», «очікує затвердження», що дозволяє керівникам і співробітникам бачити загальну картину стану робочих процесів.

Система автоматично надає звіти про статуси завдань, що допомагає виявляти затримки, неузгодженості чи недоліки в роботі, а також оперативно приймати коригувальні рішення. Нагадування про терміни виконання задач, реалізовані через електронні сповіщення, допомагають уникнути прострочень і сприяють дотриманню встановлених дедлайнів.

Ця функція особливо корисна у великих організаціях, де одночасно виконується багато завдань, і необхідно координувати дії між різними підрозділами. Контроль виконання завдань сприяє підвищенню відповідальності співробітників, зменшенню ризику втрати важливих документів і забезпеченню більшої прозорості процесів. У результаті це дозволяє оптимізувати робочі процеси, покращити їх якість і забезпечити досягнення бізнес-цілей у встановлені терміни.

Інтеграція систем електронного документообігу з іншими інформаційними платформами, такими як ERP, CRM чи бухгалтерські системи, є важливою функцією для створення єдиної інформаційної інфраструктури організації. Ця інтеграція забезпечує безперебійну передачу даних між різними системами, що дозволяє уникнути дублювання інформації та зменшити ризик помилок, пов'язаних із ручним введенням даних. Наприклад, об'єднання з ERP-системами забезпечує автоматичний обмін інформацією про замовлення, постачання чи складські операції, що значно спрощує управління логістичними процесами.

Інтеграція з CRM-системами дозволяє автоматизувати процеси створення і відстеження документів, пов'язаних із взаємодією з клієнтами, такими як контракти, рахунки чи комерційні пропозиції. У випадку бухгалтерських систем електронний документообіг сприяє швидшому формуванню фінансових звітів, облікових документів та узгодженню транзакцій.

Єдина інформаційна інфраструктура сприяє підвищенню прозорості та узгодженості процесів, дозволяючи різним відділам організації працювати в єдиному цифровому середовищі. Це, у свою чергу, покращує управлінські рішення, оптимізує внутрішні процеси та підвищує загальну ефективність роботи компанії. Інтеграція з іншими

системами є основою цифрової трансформації, що дозволяє організаціям залишатися конкурентоспроможними в умовах сучасного ринку.

Відповідність нормативно-правовим вимогам є однією з основних функцій систем електронного документообігу, що забезпечує легітимність і правову силу документаційних процесів. Ця функція передбачає інтеграцію інструментів, які підтримують чинні законодавчі стандарти, такі як використання цифрового підпису, електронної печатки та захищеного зберігання документів. Цифровий підпис гарантує автентичність і цілісність документа, а також підтверджує його походження, що є важливим для юридичного оформлення взаємодії між сторонами. Електронна печатка додає додатковий рівень захисту, забезпечуючи неможливість несанкціонованого внесення змін до документів.

Система також враховує вимоги щодо строків зберігання документів та їх архівування відповідно до нормативів, що дозволяє уникнути правових порушень у разі перевірок або судових розглядів. Використання стандартизованих форматів і шифрування даних забезпечує захист документів від несанкціонованого доступу, що відповідає вимогам з кібербезпеки.

Дотримання нормативно-правових вимог у системах електронного документообігу не лише забезпечує законність процесів, але й підвищує довіру партнерів, клієнтів і контролюючих органів до організації. Це дозволяє зменшити ризики, пов'язані з юридичними та регуляторними аспектами, і сприяє стабільній роботі компанії в умовах сучасного правового поля.

Мобільність та доступність є важливими характеристиками сучасних систем електронного документообігу, які забезпечують безперебійний доступ до документів з будь-яких пристроїв, таких як комп'ютери, планшети чи смартфони. Ця функція дозволяє співробітникам працювати з документами незалежно від їхнього фізичного розташування, що є особливо актуальним в умовах віддаленої роботи чи частих відряджень. Завдяки використанню хмарних технологій, документи зберігаються у захищених централізованих сховищах, що дозволяє миттєво отримувати доступ до них через інтернет.

Системи електронного документообігу часто оснащуються адаптивними інтерфейсами, які забезпечують зручність використання на різних пристроях, а також підтримкою офлайн-доступу до ключових

документів, що дозволяє працювати навіть за відсутності підключення до мережі. Налаштовані права доступу гарантують безпеку інформації під час роботи з мобільних пристроїв, запобігаючи несанкціонованому використанню даних.

Мобільність та доступність системи сприяють підвищенню гнучкості роботи співробітників, дозволяючи їм ефективно виконувати завдання в реальному часі та оперативно реагувати на зміни. Це підвищує продуктивність і сприяє кращій адаптації організації до сучасних умов бізнесу, де мобільність є одним із ключових факторів успіху.

Отже, системи електронного документообігу виступають невід'ємним елементом сучасного управління організаційними процесами, забезпечуючи ефективність, прозорість і безпеку роботи з документами. Основні функції таких систем – автоматизація створення документів, організація їх обігу, централізоване зберігання, зручний пошук, контроль доступу, відстеження змін, моніторинг виконання завдань, інтеграція з іншими інформаційними платформами, відповідність нормативно–правовим вимогам, а також забезпечення мобільності та доступності – є ключовими інструментами оптимізації бізнес–процесів. Завдяки цим функціям організації можуть стандартизувати документообіг, знизити операційні витрати, мінімізувати ризики помилок і забезпечити високу швидкість реагування на виклики динамічного ринкового середовища.

Системи електронного документообігу створюють єдину інформаційну інфраструктуру, яка сприяє інтеграції внутрішніх процесів із зовнішніми бізнес–активностями, підвищуючи конкурентоспроможність підприємств. Забезпечення відповідності законодавчим нормам і впровадження сучасних технологій, таких як цифровий підпис і хмарні рішення, гарантують легітимність та надійність документообігу. Мобільність і доступність сприяють адаптації до нових форматів роботи, зокрема віддаленої, що є важливим у сучасних умовах глобалізації.

Таким чином, впровадження систем електронного документообігу не лише сприяє цифровій трансформації організації, але й створює умови для підвищення ефективності її діяльності, забезпечуючи довготривалі стратегічні переваги в умовах зростаючої конкуренції та вимогливості ринку.

3.2. Забезпечення безпеки і конфіденційності даних

Забезпечення безпеки і конфіденційності даних є ключовим аспектом сучасного інформаційного суспільства, що відіграє вирішальну роль у забезпеченні стабільного функціонування організацій, державних інституцій та захисту прав громадян. Інформація, як один із найбільш стратегічних ресурсів, перебуває під постійною загрозою з боку внутрішніх і зовнішніх чинників, таких як кібератаки, витоки даних, несанкціонований доступ, а також технічні збої. У цих умовах розробка та впровадження надійних механізмів захисту інформації є пріоритетним завданням для кожної організації, яка прагне забезпечити цілісність, доступність і конфіденційність своїх даних.

Безпека даних охоплює широкий спектр заходів, спрямованих на захист інформаційних систем, мереж та баз даних від потенційних загроз, це включає технічні засоби, такі як шифрування, багаторівнева автентифікація, системи виявлення та запобігання вторгненням, а також організаційні заходи, зокрема політики управління доступом, регулярний аудит інформаційної інфраструктури та навчання співробітників. Конфіденційність даних, як складова загальної безпеки, орієнтована на обмеження доступу до інформації виключно для уповноважених осіб, що дозволяє зберігати комерційну таємницю, персональні дані клієнтів та інші критично важливі відомості в недоторканності.

У глобалізованому світі, де обсяги оброблюваних даних стрімко зростають, а цифрові технології стають все більш інтегрованими в усі сфери життя, питання безпеки та конфіденційності інформації набувають ще більшої актуальності. Їх ефективне забезпечення є основою для підтримки довіри між бізнесом, клієнтами та партнерами, а також для дотримання вимог міжнародного та національного законодавства. У результаті, ці аспекти стають визначальними для конкурентоспроможності організацій і їхньої здатності адаптуватися до викликів сучасного цифрового середовища.

В табл. 3.2 представлено аспекти забезпечення безпеки даних у сучасних інформаційних системах.

Таблиця 3.1

Аспекти забезпечення безпеки даних у сучасних інформаційних
системах

№ з/п	Аспект безпеки	Опис	Приклади реалізації
1	2	3	4
1.	Конфіденційність	Захист даних від несанкціонованого доступу, забезпечення доступу лише для уповноважених осіб.	Шифрування даних, політики управління доступом, VPN.
2.	Цілісність	Забезпечення точності та повноти даних, а також захист від їх модифікації без дозволу.	Використання хешування, цифрових підписів, контроль даних.
3.	Доступність	Гарантування безперебійного доступу до даних для уповноважених користувачів.	Резервне копіювання, системи аварійного відновлення, клауд-сервіси.
4.	Ідентифікація	Встановлення особи користувача перед наданням доступу до системи або даних.	Використання логінів і паролів, біометричної аутентифікації.
5.	Аутентифікація	Підтвердження особи користувача для перевірки його прав доступу.	Двофакторна автентифікація, смарт-картки, токени.
6.	Авторизація	Контроль рівня доступу користувачів до інформаційних ресурсів.	Ролі користувачів у системі, політики доступу на основі обов'язків.
7.	Моніторинг і аудит	Відстеження дій користувачів та аналіз активності для виявлення загроз.	Логування подій, системи виявлення вторгнень (IDS).
8.	Захист від загроз	Запобігання ризикам, пов'язаним із кібератаками, вірусами або іншими загрозами.	Антивірусне програмне забезпечення, файрволи, системи DDoS-захисту.

продовження табл. 3.1

1	2	3	4
9.	Резервне копіювання	Створення копій даних для відновлення у разі втрат або пошкоджень.	Автоматичні бекапи, хмарні системи зберігання резервних даних.
10.	Навчання персоналу	Інформування працівників про сучасні загрози та методи забезпечення безпеки.	Семінари, тренінги, регулярні перевірки знань співробітників.

Конфіденційність даних визначається як здатність забезпечити доступ до інформації виключно уповноваженим особам чи системам. Вона є важливим компонентом забезпечення безпеки, оскільки несанкціонований доступ може призвести до витоку інформації, що завдає шкоди репутації, фінансових втрат чи юридичних наслідків.

Основні заходи забезпечення конфіденційності в сучасних інформаційних системах представлено на рис. 3.2.

Забезпечення конфіденційності даних є одним із основних чинників, що визначають рівень довіри до організації з боку її клієнтів, ділових партнерів та регуляторних органів. Сучасний бізнес вимагає від компаній максимальної прозорості у питаннях захисту особистої та комерційної інформації, тому впровадження надійних механізмів безпеки є важливим показником відповідальності та професіоналізму організації. Надійний захист даних демонструє компетентність організації, що здатна ефективно реагувати на потенційні загрози і забезпечити безпеку своїх інформаційних ресурсів у будь-яких умовах. Застосування сучасних технологій, таких як шифрування даних, механізми аутентифікації та авторизації, а також політики управління доступом, дозволяє значно знизити ймовірність витоку інформації, що є критично важливим для збереження конкурентних переваг організації. Ці технології не лише мінімізують ризики фінансових і юридичних збитків, але й суттєво підвищують рівень організаційної безпеки, знижуючи уразливість до зовнішніх і внутрішніх загроз. Дотримання принципів конфіденційності даних дозволяє не лише забезпечити стабільність бізнес-процесів, а й знизити ризики репутаційних втрат, які можуть виникнути в разі компрометації даних, що, в свою чергу, може мати значний негативний вплив на довіру клієнтів і партнерів. У довгостроковій перспективі ефективне управління конфіденційністю сприяє зміцненню позицій організації на

ринку, формуванню позитивного іміджу та підвищенню лояльності всіх зацікавлених сторін, що є важливим фактором для сталого розвитку та успіху на конкурентному ринку.

Шифрування даних



- шифрування перетворює інформацію у зашифрований формат, який може бути прочитаний лише за наявності ключа розшифрування. Цей метод захисту особливо важливий для передачі даних через публічні мережі, зберігання конфіденційної інформації в хмарних сервісах або резервних копіях. Сучасні алгоритми, такі як AES (Advanced Encryption Standard), забезпечують високий рівень захисту, мінімізуючи ризик доступу злоумисників до інформації.

Політика управління доступом



- встановлення чітких правил та процедур, які визначають, хто має право доступу до даних, є необхідним для забезпечення конфіденційності. Реалізація системи розмежування доступу базується на ролях користувачів у системі (Role-Based Access Control, RBAC), що забезпечує відповідність прав доступу посадовим обов'язкам. Наприклад, фінансові дані доступні лише співробітникам бухгалтерії, тоді як технічні документи обмежені для інженерного персоналу.

Віртуальні приватні мережі (VPN)



- використання VPN дозволяє створити безпечний канал передачі даних через загальнодоступні мережі. Це знижує ризик перехоплення інформації злоумисниками та гарантує конфіденційність навіть під час віддаленої роботи. VPN особливо ефективні для організацій, де співробітники працюють з конфіденційними даними за межами офісу.

Рис. 3.2. Основні заходи забезпечення конфіденційності в сучасних інформаційних системах

Наступним аспектом забезпечення безпеки даних у сучасних інформаційних системах розглянемо цілісність даних.

Цілісність даних визначається як здатність забезпечити їх точність, повноту та захист від несанкціонованих модифікацій. Цей

аспект є особливо важливим у критичних сферах, таких як фінансові операції, медична інформація або державне управління, де спотворення даних може мати серйозні наслідки. Забезпечення цілісності дозволяє гарантувати, що дані залишаються незмінними протягом їх життєвого циклу, якщо зміни не були авторизовані відповідальними особами.

На рис. 3.3 представлено основні заходи забезпечення цілісності даних.

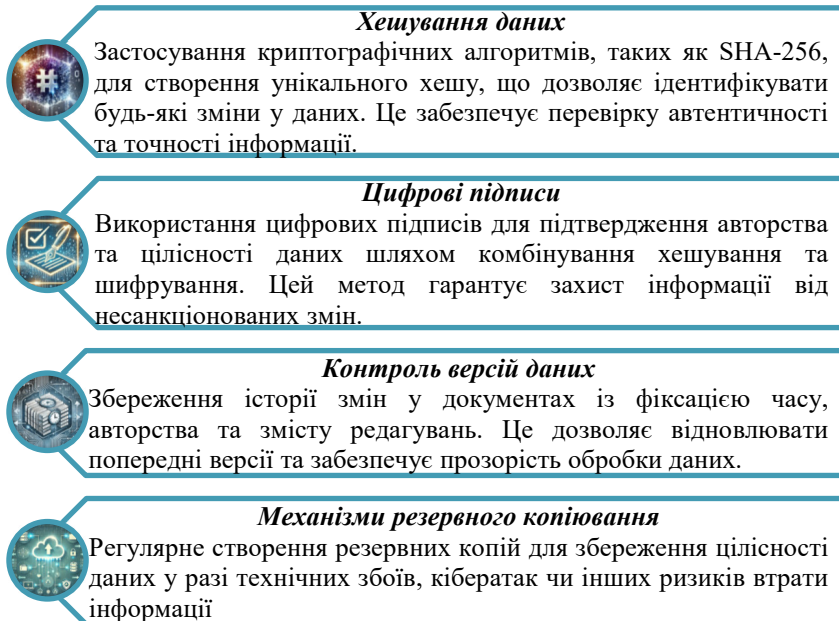


Рис. 3.3. Основні заходи забезпечення цілісності даних

Забезпечення цілісності даних базується на використанні сучасних технологій і методів, які гарантують точність, повноту та захист інформації від несанкціонованих змін. Одним із ключових механізмів є хешування, що застосовує криптографічні алгоритми, такі як SHA-256, для створення унікального хешу, який дозволяє виявити будь-які зміни у даних. Цифрові підписи комбінують хешування та шифрування, забезпечуючи підтвердження авторства і захист від модифікацій. Контроль версій даних дозволяє зберігати історію змін із чіткою фіксацією авторства, часу і змісту редагувань, що сприяє прозорості та можливості відновлення попередніх станів. Додатково, механізми резервного копіювання створюють копії даних для запобігання їх втраті через технічні збої чи кібератаки. Усі ці методи

формують комплексний підхід до забезпечення цілісності даних, що є основою для надійності інформаційних систем і прийняття коректних управлінських рішень.

Доступність є ключовим аспектом забезпечення безпеки інформаційних систем, що спрямований на гарантування безперебійного доступу до даних для уповноважених користувачів у будь-який час та за будь-яких обставин. Цей аспект є критично важливим у сучасних умовах, коли організації активно використовують цифрові інструменти для обробки, зберігання та передачі даних. Перебої у доступі до інформації можуть призводити до значних фінансових втрат, зниження продуктивності праці, компрометації процесів управління та ризику втрати довіри клієнтів.

1. Резервне копіювання. Резервне копіювання є одним із базових методів забезпечення доступності даних. Воно передбачає регулярне створення резервних копій інформації, які зберігаються у фізично або логічно відокремлених місцях. У разі технічних збоїв, помилок користувачів або кібератак ці копії дозволяють швидко відновити дані до їх початкового стану. Для підвищення ефективності резервного копіювання використовуються автоматизовані системи, що забезпечують регулярність цього процесу і знижують ризик людських помилок.

2. Системи аварійного відновлення. Системи аварійного відновлення (Disaster Recovery) є спеціалізованими рішеннями, які дозволяють швидко відновити функціонування інформаційних систем після критичних інцидентів, таких як вихід з ладу серверів, природні катастрофи або масштабні кібератаки. Вони включають резервні сервери, детально розроблені плани відновлення роботи та інструменти моніторингу, які забезпечують безперервність доступу до критично важливих даних. Упровадження таких систем є стратегічно важливим для організацій, діяльність яких залежить від постійного функціонування інформаційної інфраструктури.

3. Клауд-сервіси. Хмарні сервіси виступають одним із найефективніших інструментів забезпечення доступності даних. Використання хмарних платформ дозволяє зберігати дані у розподілених сховищах, що забезпечує їхню доступність навіть у разі локальних технічних збоїв. Крім того, провайдери хмарних послуг надають додаткові механізми захисту, такі як географічно розподілені резервні копії та висока масштабованість ресурсів, що дозволяє адаптуватися до змін у навантаженні системи.

Гарантування доступності даних є основою для забезпечення безперервності бізнес-процесів, підвищення ефективності роботи та збереження довіри клієнтів. Резервне копіювання, системи аварійного відновлення та хмарні сервіси формують багаторівневий підхід до вирішення цієї задачі. Використання цих інструментів дозволяє організаціям мінімізувати ризики, пов'язані з втратою доступу до інформації, і забезпечити стабільність функціонування навіть у критичних ситуаціях. У підсумку, доступність даних є ключовим чинником, що сприяє підвищенню стійкості та конкурентоспроможності організації у сучасному цифровому середовищі.

Ідентифікація є фундаментальним елементом системи інформаційної безпеки, що спрямований на визначення особи користувача перед наданням доступу до інформаційних ресурсів або систем. Цей процес забезпечує початковий рівень захисту, оскільки дозволяє відокремити уповноважених користувачів від несанкціонованих осіб. Ідентифікація є першим етапом комплексного процесу контролю доступу, що включає аутентифікацію та авторизацію, і є базовою передумовою для забезпечення конфіденційності, цілісності та доступності даних.

Ідентифікація є ключовим елементом забезпечення контролю доступу до інформаційних ресурсів, оскільки вона гарантує, що лише уповноважені особи мають можливість взаємодіяти з даними або системами. Встановлення особи кожного користувача є не лише засобом запобігання несанкціонованому доступу, але й важливою передумовою для реалізації інших аспектів безпеки, таких як моніторинг дій користувачів та управління доступом. Ідентифікація дозволяє створити точний облік усіх взаємодій із системою, що підвищує рівень прозорості операцій та забезпечує можливість простежити, хто і коли здійснював ті чи інші дії. Це, у свою чергу, знижує ризик зловживань або порушень і сприяє підвищенню відповідальності користувачів за свої дії в системі. Завдяки цьому ідентифікація не лише захищає ресурси організації, але й створює умови для формування культури безпеки та підвищення загальної довіри до інформаційних систем.

На рис. 3.4 представлено методи ідентифікації.

Методи ідентифікації включають використання логінів і паролів, які є найпоширенішим способом ідентифікації користувачів через їх унікальність і простоту. Логін ідентифікує особу, а пароль підтверджує

її повноваження, хоча цей метод вразливий до атак при слабких паролях. Альтернативою є біометрична ідентифікація, яка забезпечує високу надійність завдяки використанню унікальних фізичних характеристик, таких як відбитки пальців чи розпізнавання обличчя, що робить її зручною та безпечною.



Логіни і паролі. Використання унікальних логінів і паролів є найбільш поширеним методом ідентифікації. Логін ідентифікує користувача, а пароль виступає як підтвердження його особи. Попри поширеність цього методу, він має певні обмеження, зокрема залежність від складності та секретності пароля, що робить його вразливим до атак методом перебору або соціальної інженерії. Для підвищення безпеки рекомендується застосовувати політики створення складних паролів і періодичної їх зміни.

Біометрична ідентифікація. Сучасні системи все частіше використовують біометричні дані, такі як відбитки пальців, розпізнавання обличчя або райдужної оболонки ока, для ідентифікації користувачів. Цей метод забезпечує високий рівень надійності, оскільки біометричні параметри є унікальними для кожної особи та важко підробляються. Біометрична ідентифікація забезпечує зручність для користувачів, оскільки виключає необхідність запам'ятовувати складні паролі.



Рис. 3.4. Методи ідентифікації

Ефективна ідентифікація є важливим інструментом для запобігання несанкціонованому доступу, захисту даних та забезпечення відповідності організації вимогам інформаційної безпеки. Використання сучасних методів ідентифікації, таких як багатофакторний підхід, який поєднує логіни, паролі та біометричні дані, дозволяє підвищити рівень захисту інформаційних систем. У підсумку, ідентифікація сприяє побудові надійного цифрового середовища, яке підтримує довіру користувачів і забезпечує стабільність бізнес-процесів.

Аутентифікація є одним із ключових процесів забезпечення інформаційної безпеки, який виконує функцію підтвердження особи

користувача та перевірки його прав доступу до інформаційних систем, даних або ресурсів. Цей процес спрямований на запобігання несанкціонованому доступу, забезпечуючи, що лише уповноважені особи отримують доступ до критично важливої інформації. Аутентифікація відіграє важливу роль у захисті конфіденційності, цілісності та доступності даних, особливо в умовах зростаючого числа кіберзагроз.

Процес аутентифікації розпочинається з ідентифікації користувача, під час якої система отримує унікальний ідентифікатор (наприклад, логін). Далі проводиться перевірка, яка підтверджує, що користувач є тим, за кого себе видає. Аутентифікація гарантує, що система надає доступ лише тим, хто має відповідні права, мінімізуючи ризик витоку чи компрометації даних. У сучасних інформаційних системах аутентифікація також є основою для аудиту дій користувачів, дозволяючи відслідковувати активність і забезпечувати прозорість операцій.

На рис. 3.5 представлено методи аутентифікації.

<i>Двофакторна аутентифікація (2FA)</i>	• використовує комбінацію пароля та одноразового коду для підвищення безпеки.
<i>Смарт-картки</i>	• фізичні носії з вбудованим чипом для ідентифікації користувача.
<i>Токени</i>	• пристрої або програми, які генерують одноразові паролі для доступу.
<i>Біометрична аутентифікація</i>	• використовує унікальні фізичні характеристики, такі як відбитки пальців чи розпізнавання обличчя
<i>Одноразові паролі (OTP)</i>	• паролі, які діють лише для однієї сесії чи операції.

Рис. 3.5. Методи аутентифікації

Двофакторна аутентифікація (2FA) є одним із найпоширеніших і ефективних методів захисту доступу до інформаційних систем. Вона ґрунтується на використанні двох незалежних факторів, що включають щось, що знає користувач (наприклад, пароль), і щось, що він має (наприклад, код підтвердження, отриманий через SMS або мобільний

додаток). Такий підхід значно підвищує рівень безпеки, оскільки зломисникам необхідно одночасно володіти обома факторами для отримання доступу. Цей метод широко використовується в онлайн-банкінгу, корпоративних системах і сервісах електронної пошти, де безпека даних є критично важливою.

Смарт-картки є фізичними пристроями, які містять вбудований чип для зберігання даних автентифікації. Вони використовуються для підтвердження особи користувача та надання доступу до систем або даних. Для доступу користувач вводить PIN-код, що додає додатковий рівень захисту. Смарт-картки популярні у корпоративному середовищі, державних установах і банківському секторі завдяки їх високій надійності та зручності. Вони також забезпечують захист від несанкціонованого доступу навіть у разі втрати або крадіжки пристрою, оскільки чип блокується після кількох невдалих спроб введення PIN-коду.

Токени є пристроями або програмними додатками, які генерують одноразові паролі (ОТР) для доступу до інформаційних систем. Апаратні токени зазвичай мають невеликі розміри і забезпечують додатковий рівень захисту, оскільки вони функціонують незалежно від комп'ютерних систем. Програмні токени, у свою чергу, інтегровані в мобільні пристрої, що робить їх зручними у використанні. Токени широко застосовуються у системах, де потрібен високий рівень безпеки, таких як банківські транзакції або віддалений доступ до корпоративних мереж.

Біометрична аутентифікація використовує унікальні фізичні характеристики користувача для підтвердження його особи. До таких характеристик належать відбитки пальців, розпізнавання обличчя, райдужної оболонки ока або навіть голосу. Цей метод забезпечує високий рівень безпеки, оскільки фізичні ознаки користувача складно підробити чи передати іншій особі. Біометрія стає дедалі популярнішою завдяки її зручності та інтеграції у сучасні пристрої, такі як смартфони або ноутбуки. Використання біометрії значно спрощує процес автентифікації, усуваючи необхідність запам'ятовувати складні паролі.

Одноразові паролі (ОТР) є ключовим компонентом багатьох систем автентифікації. Ці паролі діють лише для однієї сесії чи операції, що унеможливує їх повторне використання навіть у разі перехоплення. ОТР генеруються за допомогою спеціальних алгоритмів, які враховують поточний час або події, пов'язані з конкретним

користувачем. Цей метод широко застосовується у банківській сфері, для підтвердження онлайн–платежів чи доступу до критично важливих систем. Завдяки своїй динамічності ОТР є ефективним способом запобігання атакам методом підбору паролів.

Усі ці методи автентифікації формують багаторівневий підхід до забезпечення безпеки інформаційних систем. Вони доповнюють одне одного, підвищуючи надійність і знижуючи ризики несанкціонованого доступу. Вибір конкретного методу залежить від специфіки системи, рівня загроз і потреб організації, але комбінування кількох методів є найбільш ефективним способом забезпечення захищеності даних.

Ефективна аутентифікація є важливим чинником захисту інформаційних ресурсів від несанкціонованого доступу. Впровадження сучасних методів, таких як двофакторна автентифікація, смарт–картки та токени, дозволяє мінімізувати ризики втрати даних, підвищити довіру до інформаційних систем і забезпечити відповідність організації сучасним стандартам кібербезпеки. У результаті аутентифікація стає основою для побудови надійної інформаційної інфраструктури, яка підтримує стабільність бізнес–процесів і захищає інтереси організації в умовах зростаючих кіберзагроз.

Авторизація є одним із ключових етапів забезпечення інформаційної безпеки, який визначає рівень доступу користувача до інформаційних ресурсів на основі його повноважень. Цей процес відбувається після успішної ідентифікації та аутентифікації користувача і полягає у перевірці його прав на виконання певних дій, таких як читання, редагування чи видалення даних. Авторизація є важливим механізмом для запобігання несанкціонованим діям, які можуть призвести до втрати, пошкодження або витоку інформації.

Основою системи авторизації є ролі користувачів, які визначають набір доступних їм ресурсів і функцій у системі. Ролі призначаються відповідно до посадових обов'язків користувачів, що забезпечує чітке розмежування прав доступу. Наприклад, у корпоративній системі менеджери можуть мати доступ до звітності, тоді як технічний персонал має доступ до інфраструктурних даних. Такий підхід дозволяє мінімізувати ризик помилок чи зловживань шляхом обмеження користувачів лише тими ресурсами, які їм дійсно необхідні для виконання робочих завдань.

Політики доступу, засновані на обов'язках, є важливим елементом авторизації, що забезпечує автоматизацію управління доступом. Вони визначають, які дії можуть виконувати користувачі на

конкретних ресурсах залежно від їхніх ролей чи ситуації. Наприклад, політики можуть дозволяти доступ до певних даних лише у робочі години або обмежувати доступ під час виконання критичних операцій. Такий підхід забезпечує більшу гнучкість і точність у керуванні доступом, знижуючи ризик небажаних змін у системі.

Ефективна авторизація також включає механізми моніторингу та реєстрації дій користувачів. Це дозволяє відстежувати, хто і коли виконував певні дії в системі, що підвищує прозорість процесів і полегшує виявлення потенційних загроз. Крім того, регулярний аудит політик доступу дозволяє своєчасно виявляти та виправляти порушення або невідповідності в налаштуваннях доступу.

Авторизація є критично важливою для забезпечення захищеності інформаційних систем, оскільки вона гарантує, що кожен користувач має доступ лише до тих ресурсів, які необхідні для виконання його завдань. Завдяки використанню ролей користувачів, політик доступу та механізмів моніторингу, організації можуть значно підвищити рівень контролю над інформаційними ресурсами та мінімізувати ризики, пов'язані з людським фактором чи зовнішніми загрозами. У результаті авторизація стає одним із найважливіших інструментів захисту конфіденційної інформації та забезпечення безперервності бізнес-процесів.

Моніторинг і аудит є важливими складовими системи інформаційної безпеки, які забезпечують контроль над діями користувачів та операціями у інформаційній системі. Моніторинг дозволяє в реальному часі відстежувати активність у системі, включаючи спроби доступу, зміну даних або виконання критично важливих операцій. Аудит, у свою чергу, виконує ретроспективний аналіз дій, зберігаючи записи про події, які відбувалися в системі. Разом ці інструменти спрямовані на виявлення потенційних загроз і забезпечення відповідності процесів встановленим політикам безпеки.

Одним із основних інструментів моніторингу є логування подій, яке автоматично фіксує всі значущі дії у системі. Лог-файли містять інформацію про те, хто, коли і які дії виконував, а також деталі про успішність чи невдачу цих операцій. Це дозволяє створити детальну картину активності в системі, що є основою для виявлення аномалій, таких як незвичні спроби доступу чи неавторизовані зміни даних. Для ефективного управління логами використовуються спеціалізовані системи збору та аналізу, які автоматизують процес обробки великих обсягів даних.

Системи виявлення вторгнень (IDS) є важливим компонентом моніторингу, який дозволяє виявляти загрози у реальному часі. Вони аналізують трафік у мережі та активність користувачів, використовуючи алгоритми для ідентифікації підозрілих дій. Наприклад, IDS може попередити про спроби несанкціонованого доступу, використання відомих вразливостей чи аномальну поведінку в системі. Інтеграція IDS з іншими інструментами моніторингу дозволяє швидко реагувати на інциденти, запобігаючи їх ескалації.

Аудит системи безпеки є невід’ємним елементом забезпечення її надійності. Регулярне проведення аудитів дозволяє виявляти порушення політик доступу, невідповідності в налаштуваннях безпеки та інші проблеми, які можуть поставити під загрозу конфіденційність чи цілісність даних. Аудит також є важливим засобом відповідності вимогам нормативно-правових актів і стандартів, таких як GDPR або ISO 27001.

Моніторинг і аудит у комплексі забезпечують прозорість і контроль за інформаційними ресурсами організації. Вони дозволяють виявляти та реагувати на загрози у реальному часі, а також формувати стратегії для вдосконалення системи безпеки. У результаті ці інструменти сприяють підвищенню надійності інформаційної системи, мінімізації ризиків втрати даних і збереженню довіри з боку користувачів, клієнтів та партнерів.

Захист від загроз є однією з функцій системи інформаційної безпеки, яка спрямована на запобігання ризикам, пов’язаним із кібератаками, шкідливим програмним забезпеченням, несанкціонованим доступом та іншими потенційними загрозами. Сучасні інформаційні системи є вразливими до широкого спектру загроз, які можуть призвести до втрати, компрометації або пошкодження даних. Для ефективного захисту організації впроваджують комплекс заходів і технологій, які забезпечують виявлення, запобігання та нейтралізацію загроз. Зокрема, застосування систем моніторингу та аналізу мережевого трафіку дозволяє своєчасно виявляти аномалії, що можуть свідчити про спроби атак, а також автоматичні оновлення програмного забезпечення, що забезпечують виправлення вразливостей у реальному часі.

На рис. 3.6 представлено основні елементи захисту від загроз.



Рис. 3.6. Основні елементи захисту від загроз

Антивірусне програмне забезпечення є основним елементом захисту кінцевих точок, що виявляє та нейтралізує шкідливі програми, такі як віруси, трояни, шпигунські програми і руткіти, що можуть потрапити на пристрої користувачів. Ці програми постійно сканують файли та програми, виявляючи підозрілі модифікації чи поведінку, що може свідчити про наявність шкідливого коду. Оскільки зловмисники постійно розробляють нові методи проникнення, антивірусні програми оновлюються, щоб вчасно виявляти і блокувати нові типи загроз. Таким чином, антивірусне ПЗ є важливим елементом першої лінії оборони в системах, що працюють з конфіденційними або важливими даними.

Файрволи є важливою складовою захисту мережі, виконуючи функцію моніторингу та контролю трафіку, що проходить між

внутрішньою мережею організації та зовнішнім світом. Вони блокують або дозволяють з'єднання на основі визначених політик безпеки, що забезпечує захист від несанкціонованих доступів і потенційно небезпечного трафіку. Файрволи можуть фільтрувати пакети даних на основі різних параметрів, таких як IP-адреса, порти, протоколи і типи з'єднань. Вони також можуть виявляти і блокувати спроби злому, відслідковуючи аномальну активність або спроби відправки шкідливих запитів до внутрішніх ресурсів.

Системи захисту від розподілених атак типу «відмова в обслуговуванні» (DDoS) є спеціалізованими інструментами для боротьби з атаками, спрямованими на перевантаження ресурсів мережі або серверів організації за допомогою великої кількості запитів. Ці системи автоматично виявляють підвищену активність, характерну для DDoS-атак, і розподіляють навантаження, фільтруючи шкідливий трафік, що дозволяє зберігати доступність критично важливих сервісів. Вони можуть використовувати різні методи, такі як аналіз поведінки трафіку, ідентифікація аномальних запитів або впровадження «чистих» проходів для легітимних користувачів, що дозволяє зберегти працездатність інфраструктури навіть під час атаки.

Системи виявлення вторгнень (IDS) є критичним елементом для моніторингу і захисту інформаційних систем від несанкціонованих спроб доступу. Вони аналізують мережевий трафік та поведінку користувачів у реальному часі, виявляючи підозрілі дії, які можуть свідчити про спробу вторгнення або злому. IDS використовують різноманітні методи для виявлення загроз, включаючи підписи атак, аналіз аномалій і поведінкові патерни, що дозволяє вчасно ідентифікувати загрози до того, як вони завдадуть шкоди системі. Вони можуть бути інтегровані з іншими системами безпеки, такими як файрволи та системи реагування на інциденти (IPS), для автоматизованого блокування підозрілих дій.

Шифрування є ключовим методом захисту конфіденційності даних, що забезпечує їх недоступність для злоумисників навіть у разі перехоплення. За допомогою шифрування, дані перетворюються в нерозбірливий формат, який можна повернути до вихідного вигляду лише за допомогою спеціального ключа. Це гарантує, що навіть якщо злоумисники отримають доступ до зашифрованих файлів, вони не зможуть їх використовувати без відповідного ключа для дешифрування. Шифрування застосовується як для збереження даних

на дисках, так і для захисту інформації при передачі по мережах, що робить його важливим елементом в захисті конфіденційної інформації.

Автоматизовані системи оновлення є важливим інструментом для підтримки безпеки інформаційних систем. Вони забезпечують своєчасне впровадження останніх патчів і оновлень програмного забезпечення, що дозволяє усувати відомі вразливості та знижувати ризик експлуатації цих слабких місць зловмисниками. Автоматизація цього процесу критична для великих організацій, оскільки вона дозволяє зменшити ризики, пов'язані з людським фактором і забезпечити швидке реагування на нові загрози, не витрачаючи час на вручну управління оновленнями.

Навчання персоналу є важливою складовою частиною стратегії кібербезпеки, оскільки люди часто є найслабшою ланкою в системі захисту. Навчання включає інформування співробітників про актуальні кіберзагрози, методи соціальної інженерії, як уникнути фішинг-атак, та правильні процедури щодо обробки конфіденційних даних. Систематичне навчання допомагає підвищити обізнаність співробітників, зменшуючи ймовірність помилок, що можуть призвести до компрометації інформації або збоїв у роботі системи. Таким чином, підвищення кіберграмотності працівників є необхідним елементом комплексного підходу до захисту від загроз.

Резервне копіювання є однією з складових стратегії забезпечення безпеки даних у сучасних інформаційних системах, оскільки воно гарантує можливість відновлення даних у разі їх втрати, пошкодження або пошкодження через несанкціонований доступ. Зі збільшенням обсягів даних і важливості інформаційних ресурсів для функціонування організацій, питання ефективного резервного копіювання стає особливо актуальним для забезпечення цілісності, доступності та довготривалості збереження даних. Створення резервних копій дозволяє організаціям відновлювати свої інформаційні системи і бази даних після технічних збоїв, природних катастроф, кібератак або людських помилок, що може запобігти великим фінансовим втратам і порушенню нормальної діяльності.

Основними методами резервного копіювання є автоматичні бекапи та хмарні системи зберігання даних.

1. ***Автоматичні бекапи.*** Автоматичне резервне копіювання є процесом, за якого створення копій даних здійснюється без втручання користувачів, згідно з заздалегідь налаштованим графіком. Автоматизація цього процесу знижує ймовірність людських

помилки і забезпечує своєчасне створення резервних копій. Такі системи дозволяють обирати тип бекапів (повні, інкрементальні чи диференційні), а також визначати місце збереження резервних копій (локальні сервери, зовнішні носії чи хмарні сервіси). Важливою перевагою автоматичних бекапів є їхня здатність працювати у фоновому режимі, не впливаючи на роботу основної системи і без потреби в додаткових ресурсах від кінцевих користувачів. Це дозволяє забезпечити безперервність бізнес-процесів і своєчасне оновлення резервних копій у разі зміни даних.

2. **Хмарні системи зберігання даних.** Хмарні технології відіграють важливу роль у резервному копіюванні, оскільки вони забезпечують високу доступність, масштабованість та безпеку даних, зберігаючи їх у віддалених дата-центрах, що надають сервіси резервного копіювання. Хмарне резервне копіювання дає можливість зберігати резервні копії без фізичної прив'язки до конкретного місця або обладнання, що зменшує ризик втрати даних через фізичні uszkodження серверів або ж природні катастрофи, такі як пожежі чи повені. Системи хмарного зберігання також дозволяють автоматизувати процес резервного копіювання, забезпечуючи регулярне оновлення даних без необхідності втручання користувача. Крім того, хмарні сервіси дозволяють зберігати резервні копії на кількох географічно розподілених серверах, що підвищує рівень захисту від втрат або пошкоджень через локальні аварії.

Запровадження ефективної стратегії резервного копіювання дозволяє організаціям не лише знизити ризики втрати даних, але й забезпечити безперервність їхньої діяльності у разі виникнення надзвичайних ситуацій. Всі методи резервного копіювання сприяють підвищенню рівня надійності та цілісності інформаційних ресурсів, оскільки створення резервних копій забезпечує швидке відновлення даних після пошкоджень чи втрат. Автоматизація бекапів знижує ймовірність людської помилки, а хмарні рішення дозволяють скоротити витрати на інфраструктуру та підвищити доступність даних. У сукупності ці методи створюють комплексний підхід до управління даними, який забезпечує ефективне зберігання, захист і відновлення інформації в умовах сучасних кіберзагроз.

Навчання персоналу є важливою складовою системи кібербезпеки, що полягає в підвищенні обізнаності працівників щодо сучасних кіберзагроз та методів їх нейтралізації. Це включає організацію семінарів і тренінгів, де співробітники отримують знання

про актуальні загрози, такі як фішинг, соціальна інженерія, віруси та інші шкідливі програми, а також вчать застосовувати ефективні методи для їх попередження. Регулярні перевірки знань дозволяють оцінити рівень усвідомлення співробітниками політик безпеки та виявити потенційні прогалини в обізнаності, що сприяє своєчасному коригуванню підходів до навчання та зміцненню кіберграмотності в організації. В результаті, навчання персоналу сприяє створенню культури безпеки, яка є критично важливою для збереження конфіденційності, цілісності та доступності даних організації.

Забезпечення безпеки і конфіденційності даних є невід’ємною частиною функціонування сучасних інформаційних систем, оскільки гарантує захист від різноманітних загроз, таких як кібератаки, витоки даних і технічні збої. Впровадження комплексних заходів, зокрема резервного копіювання, систем автентифікації, захисту від загроз, а також навчання персоналу, створює ефективну основу для захисту інформаційних ресурсів. Використання автоматизованих бекапів і хмарних технологій для зберігання даних, а також регулярний моніторинг і аудит дій користувачів сприяють мінімізації ризиків і забезпечують безперебійний доступ до критично важливої інформації. Підвищення рівня обізнаності працівників щодо актуальних кіберзагроз і методів їх нейтралізації допомагає створити культуру безпеки, що є ключовою для підтримки довіри між організаціями та їх клієнтами в умовах цифрового середовища та електронного документообігу.

3.3. Системи електронного документообігу

Системи електронного документообігу є важливим інструментом для сучасних організацій, оскільки вони сприяють оптимізації та поліпшенню управління електронними документами на кожному етапі їх життєвого циклу.

На рис. 3.7 представлено переваги систем електронного документообігу.

Системи електронного документообігу виявляються важливим інструментом для *швидкого, зручного та ефективного створення електронних документів*. Вони не лише дозволяють створювати документи, але й удосконалюють цей процес шляхом розширення функціоналу. За допомогою різноманітних інструментів для редагування, форматування та спільної роботи, ці системи спрощують

та роблять більш доступними операції над документами. Вони включають у себе не лише базові функції редагування, а й інструменти для колективної роботи, що дозволяють користувачам працювати над документами одночасно в режимі реального часу, об'єднуючи зусилля та полегшуючи комунікацію між учасниками процесу. Такий розширений спектр можливостей значно підвищує продуктивність та якість роботи з електронними документами.

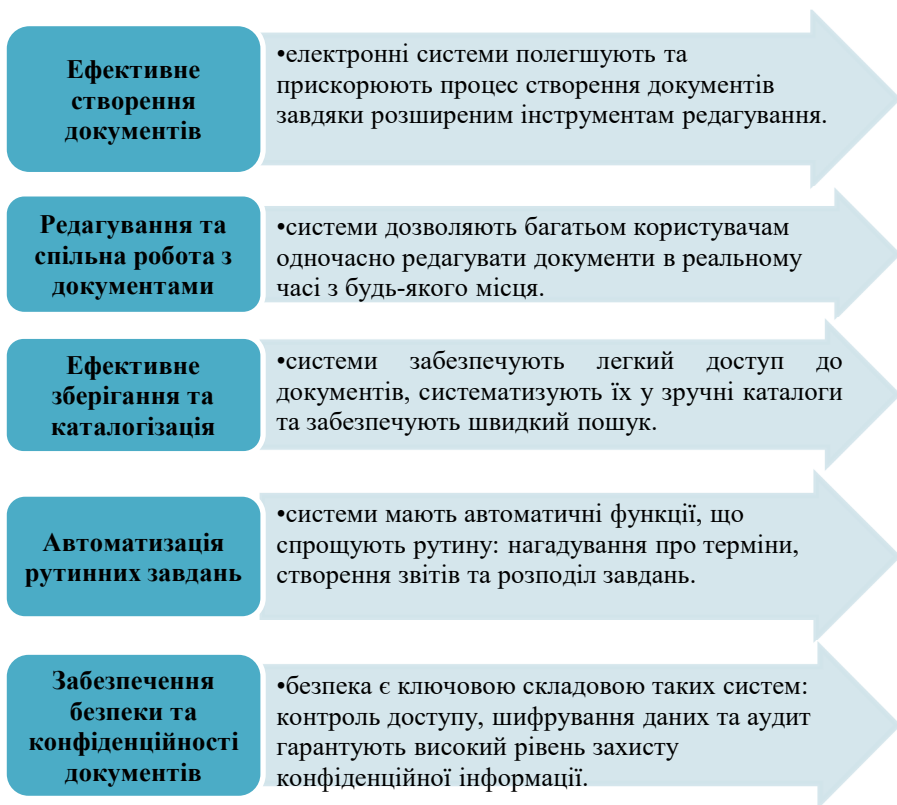


Рис. 3.7. Переваги систем електронного документообігу

Системи електронного документообігу дозволяють не лише зручно редагувати документи, а й сприяють спільній роботі без обмежень місця та часу. Вони створюють можливість одночасного редагування документів у режимі реального часу для користувачів з будь-якої локації, що дозволяє ефективно співпрацювати та вносити зміни до документів у колаборативному режимі. Такий підхід до

редагування робить комунікацію між учасниками процесу більш зручною, швидкою та ефективною, сприяючи спільній роботі над проектами та завданнями навіть у віддаленому режимі.

Системи електронного документообігу виявляються важливим інструментом для *ефективного зберігання та управління документами*. Вони не лише забезпечують зручний доступ до збережених документів, а й структурують їх у логічні каталоги чи бази даних, спрощуючи організацію та пошук необхідної інформації. Ці системи можуть автоматично класифікувати документи за різними параметрами, такими як тип, дата, автор чи тема, що робить їх легко знаходимими та доступними для користувачів. Швидкий пошук інформації в межах такої системи сприяє ефективній роботі, забезпечуючи не лише доступність документів, а й їхню швидку і точну локацію для поточних та майбутніх проектів чи завдань. Такий підхід спрощує взаємодію з документами та підвищує продуктивність користувачів у керуванні та використанні інформації.

Системи електронного документообігу вбудовують у себе *автоматизовані функції, що допомагають у спрощенні рутинних завдань*. Ці функції включають нагадування про терміни, автоматичне створення звітів та автоматизований розподіл завдань між співробітниками. Вони дозволяють автоматично встановлювати та виконувати ряд рутинних операцій, що звільняє час працівників для більш важливих та творчих завдань. Наприклад, система може автоматично нагадувати про наближення дедлайну, створювати стандартні звіти за заданими параметрами або автоматично розподіляти завдання між членами команди на основі певних критеріїв. Це допомагає оптимізувати час та ресурси, підвищує ефективність робочих процесів та сприяє швидшому виконанню завдань.

Системи електронного документообігу ставлять *особливий акцент на забезпеченні безпеки та конфіденційності*. Вони включають в себе комплекс заходів безпеки, які забезпечують високий рівень захисту конфіденційної інформації. Це включає контроль доступу, що регулює, хто має доступ до якої інформації та в який спосіб, шифрування даних для захисту їх під час передачі та зберігання, а також проведення аудиту, що дозволяє відстежувати та перевіряти дії з документами для виявлення потенційних загроз чи несанкціонованого доступу. Ці заходи забезпечують надійний захист від витоку чи несанкціонованого використання інформації, роблячи систему

безпечною та надійною для зберігання конфіденційних даних та документів.

Загалом, системи електронного документообігу відображають сучасні підходи до обробки та управління документами. Вони допомагають оптимізувати використання часу шляхом автоматизації рутинних завдань, забезпечують більш ефективне збереження ресурсів, оскільки зменшують необхідність у паперових носіях даних, і підвищують рівень співпраці в межах організації, створюючи зручні умови для спільної роботи над документами та обміну інформацією. Ці системи допомагають зробити робочі процеси більш організованими та продуктивними, сприяючи загальній ефективності та розвитку організації.

На рис. 3.8 наведено перелік семи високопродуктивних систем електронного документообігу, які активно використовуються на території України. Цей перегляд систем спрямований на охоплення широкого спектру потреб користувачів у сфері електронної обробки документів та взаємодії з інформацією в організаційному контексті.

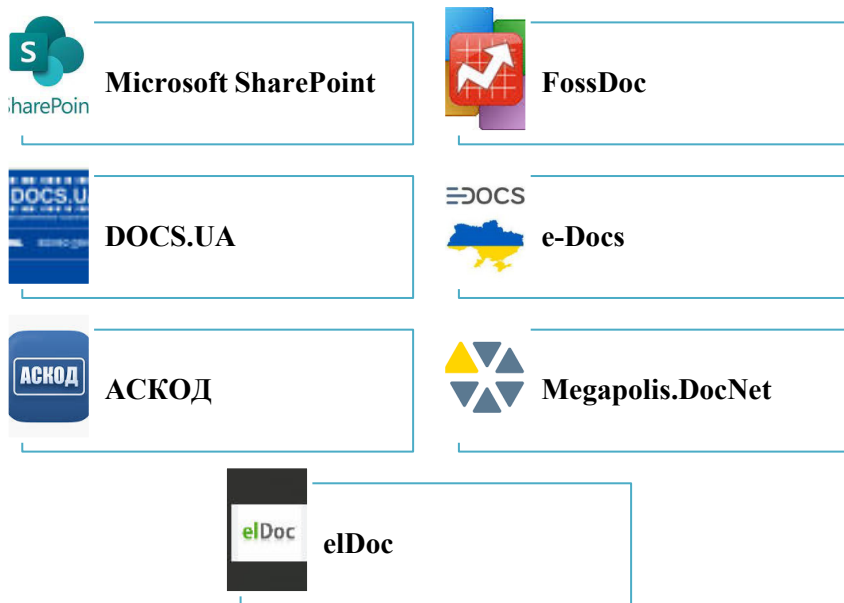


Рис. 3.8. ТОП–7 систем електронного документообігу для України на кінець 2023 року

Microsoft SharePoint – це комплексна платформа для управління корпоративним контентом та спільної роботи, яка може використовуватися як корпоративний портал. Ця система має розширений функціонал, включаючи безліч розширень та інтеграцію з іншими системами. Особливо важлива її тісна інтеграція з продуктами Microsoft, такими як MS Office та MS Exchange. Платформа може постачатися як послуга SaaS, що дозволяє зручно впроваджувати та використовувати її у корпоративному середовищі.

Microsoft в 2020 році представила сервіс SharePoint Syntex, який використовує штучний інтелект для автоматизації вилучення та класифікації даних із документів на основі наявних сервісів SharePoint. Цей сервіс тепер перетворився в самостійну платформу Microsoft Syntex, що включає набір інструментів для автоматизованого розпізнавання документів, включаючи анотування файлів та вилучення даних. Syntex зчитує, позначає та індексує вміст документів (чи то цифрових, чи то фізичних) та робить ці дані доступними для пошуку та використання в додатках Microsoft 365. Він також допомагає управляти життєвим циклом даних за допомогою інструментів безпеки та архівації.

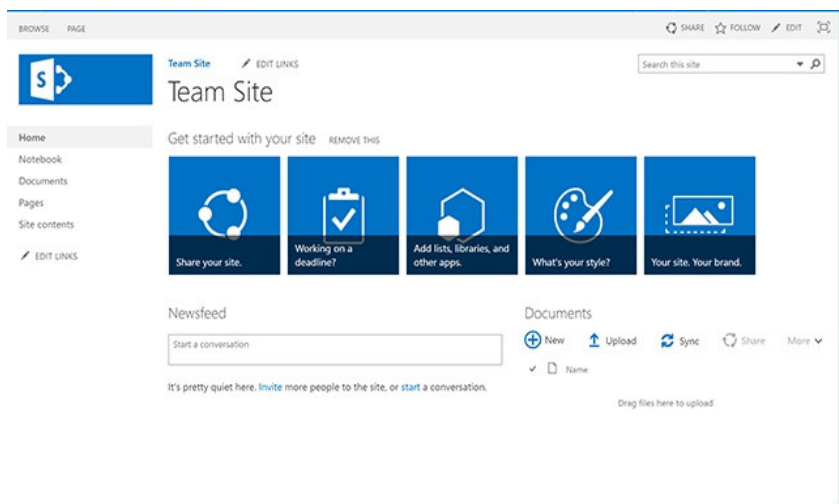


Рис. 3.9. Microsoft SharePoint [22]

DOCS.UA – це система електронного документообігу в категорії Enterprise Content Management (ECM), яка надає повнофункціональні механізми для ефективного управління документами та моделювання

бізнес–процесів. Ця платформа високого класу розроблена для оптимізації роботи з документацією та автоматизації бізнес–процесів у режимі реального часу.

DOCS.UA відрізняється відмінним функціоналом, який включає в себе не лише збереження та обмін документами, але і можливість створення та оптимізації робочих потоків. Система надає великий вибір інструментів для керування версіями документів, надання доступу до необхідної інформації в реальному часі та взаємодії користувачів в одній ефективній робочій області.



ФУНКЦІОНАЛЬНІ МОДУЛІ

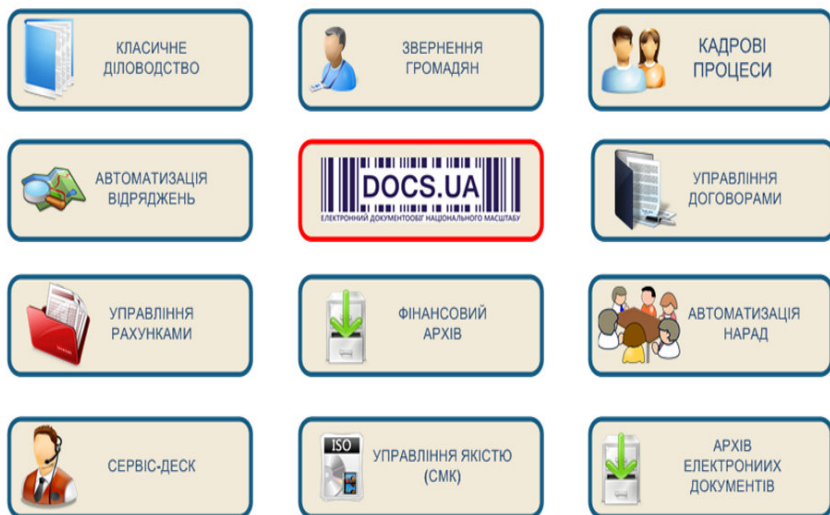


Рис. 3.10. DOCS.UA [5]

DOCS.UA також враховує вимоги сучасних бізнес–процесів, забезпечуючи можливість інтеграції з іншими корпоративними системами та додатками. Ця система стає важливим інструментом для підприємств, які прагнуть підняти ефективність свого документообігу та бізнес–процесів до нового рівня.

Платформа DOCS.UA здатна одночасно обслуговувати значну кількість користувачів та забезпечувати ефективне зберігання великого

обсягу документів. Її вражаючі характеристики масштабованості підтверджені успішними реальними проектами та випробуваннями, проведеними у технологічному центрі Microsoft.

Відкритість платформи робить її гнучкою, дозволяючи розробникам створювати індивідуальні технічні та інтеграційні рішення для вирішення специфічних викликів конкретної організації. Це надає платформі гнучкість, доступність та економічність використання, що робить її привабливою для державних організацій, установ влади та бізнесу.

АСКОД – Український розробник програмного забезпечення із досвідом роботи з 1992 року, спеціалізується на розробці та впровадженні програмних рішень. Зокрема, фахівець працює в сфері автоматизації ділових, управлінських та інших процесів.

Розроблена ним система електронного документообігу, АСКОД, відзначається створенням єдиного інформаційного простору та загального структурованого корпоративного сховища документів. Ця система дозволяє автоматизувати процеси обробки документів і контролю виконавчої дисципліни, сприяючи при цьому скороченню термінів проходження документів та покращенню ефективності роботи персоналу. АСКОД стає важливим інструментом для підвищення організаційної продуктивності та забезпечення ефективного управління документальним потоком.

АСКОД Корпоративний/

АСКОД Мобільний

АСКОД Портал

АСКОД Реєстр

АСКОД Проведення засідань

АСКОД Архів

АСКОД Адміністрування

АСКОД Чат

АСКОД Конструктор

АСКОД Договори

АСКОД Судові справи

АСКОД Кадри



АСКОД Корпоративний/WEB

АСКОД Корпоративний – забезпечує тип доступу до системи через desktop-клієнт та реалізує всі функції системи електронного документообігу, забезпечуючи при цьому створення єдиного інформаційного простору та загального структурованого сховища документів в організації.

АСКОД WEB - забезпечує тип доступу до функціональності АСКОД (web-клієнт) за допомогою Інтернет-браузерів Google Chrome, Mozilla Firefox, Opera та Safari.

Використання АСКОД Корпоративний/WEB забезпечить ефективну та безперерйну віддалену роботу співробітників, а завдяки гнучкості, система забезпечить автоматизацію практично будь яких бізнес-процесів організації.

[Дізнатися більше](#)

Рис. 3.11. АСКОД [26]

Проекти впроваджені із застосуванням СЕД «АСКОД»:

1. Автоматизована система документообігу Адміністрації Президента України.
2. Автоматизована система документообігу Національного Банку України.
3. Єдиний інформаційний простір територіальної громади м.Києва (Київська міська державна адміністрації, Київська міська рада, районні у м.Києві державні адміністрації, головне управління та департаменти, комунальні підприємства).
4. Єдина автоматизована система документообігу Волинської області (Волинська обласна державна адміністрація, Волинська обласна рада, районні державні адміністрації Волинської області).
5. Система управління електронною чергою і автоматизована система документообігу центру надання адміністративних послуг в місті Чернігові та Луцьку.
6. Автоматизована система документообігу в державній службі України з надзвичайних ситуацій.
7. Відомча автоматизована система документообігу в Державної агенції автомобільних доріг в Україні.
8. Автоматизована система документообігу міністерстві промислової політики України, Українського центру оцінювання якості освіти.
9. Автоматизована система документообігу Фонду гарантування вкладів фізичних осіб, Українського центру оцінювання якості освіти та Федерації профспілок України.

FossDoc – це передова система електронного документообігу, розроблена українською компанією ФОСС–Он–Лайн із штаб-квартирою у Харкові. Ця інноваційна система спеціально створена для оптимізації управління документами, ефективної організації корпоративного документообігу та автоматизації бізнес–процесів.

FossDoc вражає своєю унікальністю і високим рівнем функціональності. Основною метою цієї системи є створення електронного архіву документів, що дозволяє організації ефективно управляти своїми документами з використанням сучасних технологій. Завдяки FossDoc підприємства отримують можливість оптимізувати свої бізнес–процеси, раціоналізувати потоки інформації та прискорювати проходження документів.

Надійність та безпека FossDoc гарантують успішну і безпечну роботу з конфіденційною інформацією. Інтеграція цієї системи у

підприємство сприяє ефективній координації дій співробітників та полегшує керування багатьма аспектами документообігу. FossDoc – це крок у майбутнє, де технології взаємодіють із бізнес-процесами для досягнення максимальної продуктивності та якості управління.

FossDoc Server – це сервер додатків, який реалізує бізнес-логіку та забезпечує взаємодію клієнтських програм з сервером Системи Управління Базами Даних (СУБД). Модулі, що визначають функції системи, з'єднуються з сервером додатків, роблячи продукт унікальним за наявністю різних серверних компонентів.

Web-сервер дозволяє користувачам взаємодіяти із сервером додатків через звичайний веббраузер. Цей модуль, що використовується як зовнішній, приєднується до сервера додатків, забезпечуючи зручний доступ через вебінтерфейс.

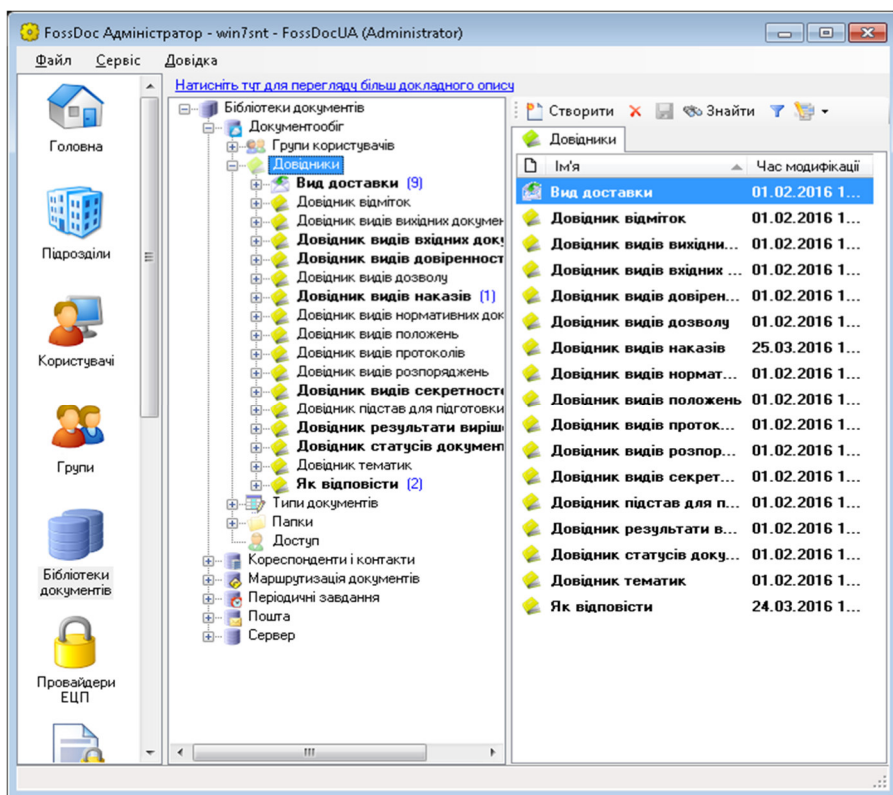


Рис. 3.12. FossDoc [12]

База даних керується сервером СУБД (таким як MySQL, Microsoft SQL Server або Oracle) і відповідає за зберігання різноманітної інформації, такої як документи, довідники, дані користувачів, налаштування та інше.

FossDoc Client представляє собою клієнтський windows–додаток, який служить автоматизованим робочим місцем для користувача. Він дозволяє користувачеві підключатися до сервера додатків через локальну мережу або Інтернет та вирішувати свої службові завдання, діючи як співробітник підприємства.

FossDoc Web Client – це вебінтерфейс, який реалізує ті ж функції, що і windows–програма FossDoc Client, за допомогою звичайного веббраузера. Взаємодія з цим клієнтом забезпечується вебсервером системи, дозволяючи використовувати систему в онлайн режимі.

FossDoc Адміністратор – це клієнтська програма, яка служить інструментом для адміністрування сервера додатків. Вона дозволяє адміністраторам ефективно керувати системою, вводити нових користувачів, налаштовувати права доступу, підключати додаткові функції, проектувати маршрути документів та інше.

e-Docs – це сучасна та надійна система для електронного документообігу, яка дозволяє автоматизувати бізнес–процеси та значно підвищити ефективність роботи організації.

e-Docs.Platform – це сучасна програмна платформа для створення простих та зручних у використанні рішень по управлінню документообігом та бізнес-процесами.

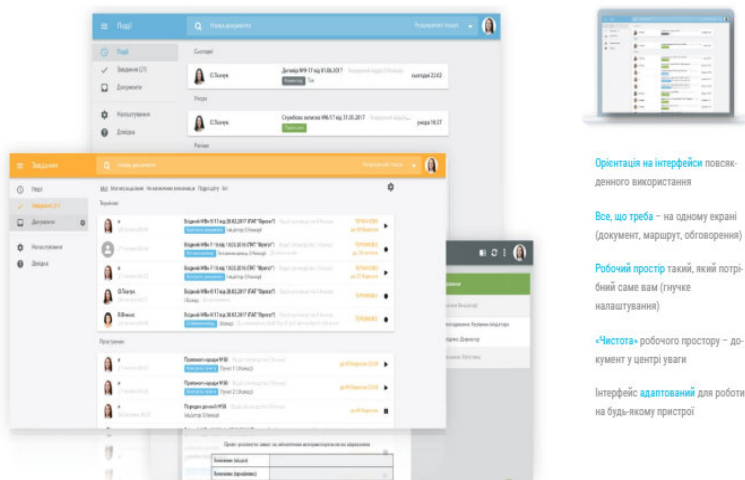


Рис. 3.13. e-Docs [8]

Система пропонує широкий набір функціональних можливостей, що включають готові прикладні рішення, які можна легко адаптувати до потреб вашого бізнесу. Інтуїтивно зрозумілий інтерфейс і зручність використання забезпечують швидку адаптацію користувачів, що дозволяє скоротити час на впровадження електронного документообігу. Завдяки досвіду і професіоналізму нашої команди, ви отримаєте комплексне рішення, яке забезпечить безперебійну роботу вашої організації, дозволяючи швидко перейти до цифрових процесів і зменшити залежність від паперових документів. Лише за кілька тижнів ви зможете оцінити всі переваги автоматизації, такі як зниження витрат на зберігання і обробку документів, підвищення оперативності прийняття рішень і поліпшення внутрішньої комунікації.

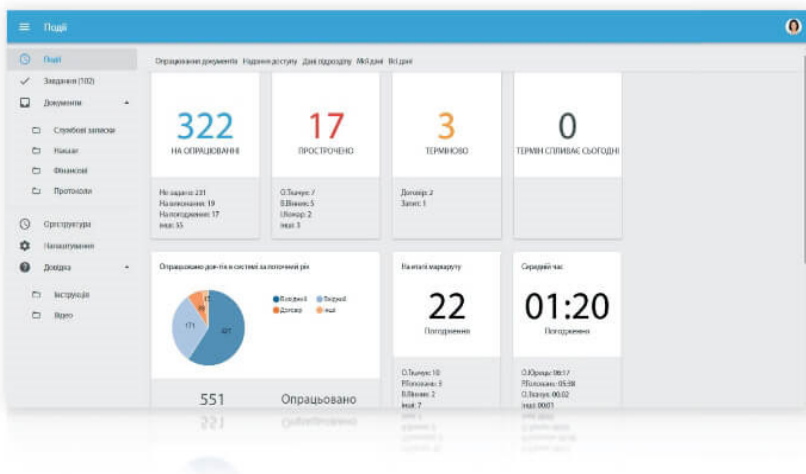


Рис. 3.14. Зведена інформація про стан опрацювання документів та завдань в e-Docs [8]

Унікальна архітектура системи e-Docs побудована на використанні передових технічних рішень від Microsoft, що відкриває практично необмежені можливості для задоволення потреб вашого бізнесу. Розроблені рішення дозволяють не лише швидко впроваджувати систему, а й досягати високого рівня продуктивності та ефективності в роботі з електронною документацією.

Команда розробників не лише надає технічну підтримку, але й готова поділитися своїм унікальним досвідом у створенні та впровадженні ефективних рішень для автоматизації бізнес-процесів.

E–DOCS пропонує передовий інструмент для управління документами та можливість оптимізації бізнес–процесів з метою досягнення кращих результатів.

Для управління внутрішнім документообігом було розроблено ECM–рішення *Megapolis.DocNet*. В його основу лягла інноваційна платформа UnityBase з відкритим вихідним кодом. Megapolis.DocNet забезпечує повний цикл управління документами: від їх підготовки до зберігання. Це серверне рішення, яке може бути розгорнуто на системах Windows Server, Linux або Unix. Доступ здійснюється за допомогою вебклієнта. Бази даних, що підтримуються: Oracle, MS SQL Server, PostgreSQL. Можливо паралельне використання ЕЦП українських АСЦК і ЕЦП RSI.

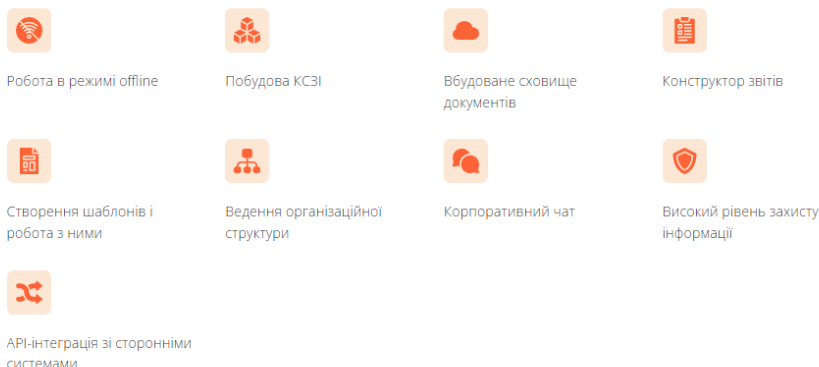


Рис. 3.15. Ключові особливості Megapolis.DocNet [19]

Megapolis.DocNet визначається як високоефективне та універсальне рішення, спроектоване для організації та управління системою електронного документообігу в різноманітних компаніях, незалежно від їхнього рівня та галузей діяльності. Ця інноваційна платформа також ідеально підходить для впровадження у державних установах.

У контексті Megapolis.DocNet виходить за рамки простої системи електронного документообігу. Вона створена для вирішення різноманітних завдань, забезпечуючи високий ступінь гнучкості та адаптивності. Інструменти цієї системи дозволяють ефективно керувати потоками документів, автоматизувати рутинні бізнес–процеси та забезпечувати безпеку і конфіденційність інформації.

Наявність різноманітних функціональних можливостей у Megapolis.DocNet дозволяє компаніям в будь-якій сфері діяльності ефективно вирішувати виклики, пов'язані з обробкою документів, а також підвищувати продуктивність та оптимізовувати робочі процеси. Для державного сектору це рішення може стати важливим інструментом удосконалення адміністративної ефективності та забезпечення швидкого обміну інформацією в системі управління документами.

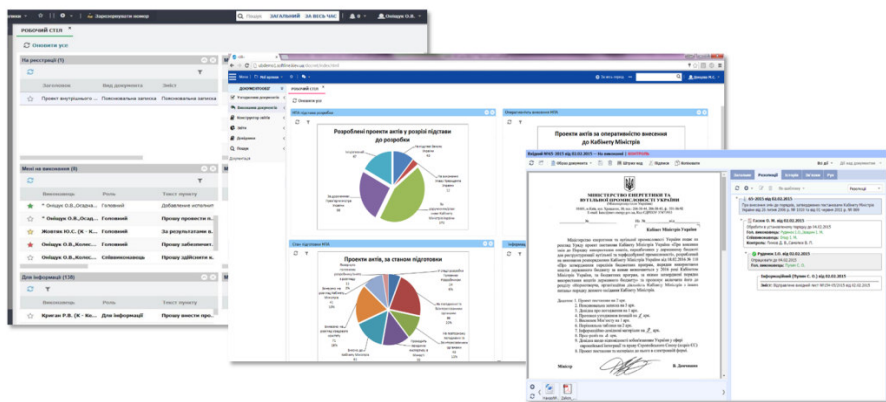


Рис. 3.16. Megapolis.DocNet [19]

Megapolis.DocNet, як інноваційне рішення в галузі управління документами, глибоко вписується у концепцію ECM (Enterprise Content Management), що підкреслює його важливість та відмінність. Ця платформа створена для повного обслуговування життєвого циклу документів в організації, а також для ефективної автоматизації різноманітних бізнес-процесів.

Megapolis.DocNet використовує передові принципи управління корпоративним контентом, забезпечуючи комплексний підхід до роботи з документами та інформацією в організації. Вона створена, щоб не лише оптимізувати зберігання та доступ до документів, але й активно впроваджувати сучасні практики ефективного управління корпоративним контентом.

Мегаполіс.DocNet встановлює нові стандарти управління документами, охоплюючи всі етапи їхнього життєвого циклу – від створення та затвердження до архівування та знищення. Система пропонує комплексний підхід до управління документацією, що дозволяє організаціям ефективно і зручно працювати з великими

обсягами інформації. Крім того, Megapolis.DocNet активно сприяє автоматизації бізнес-процесів, знижуючи людський фактор та забезпечуючи високу точність і швидкість у виконанні завдань. Це не просто інструмент для обробки документів, а потужне рішення, яке інтегрується в бізнес-процеси організації, оптимізуючи роботу на всіх рівнях і допомагаючи знизити витрати. Мегаполіс.DocNet стає невід’ємною частиною стратегічного розвитку сучасних підприємств, адже забезпечує стабільність, прозорість і контроль над інформацією, що є основою успішного управління в умовах цифровізації.

Компанія «DMS Solutions» є провідним розробником інтегрованої платформи «*elDoc*», що здійснює інтелектуальну автоматизацію обробки документів відповідно до концепції IDP (Intelligent Document Processing) та автоматизації робочих процесів. Окрім цього, компанія виступає лідером у впровадженні технологій роботизації бізнес-процесів (RPA) в Україні та розробці систем управління програмними роботами, а також інтелектуальної обробки документів, що є основою для оптимізації операційної діяльності організацій.



Рис. 3.17. elDoc [10]

Основні напрямки діяльності «DMS Solutions» включають:

– розробка та впровадження інтелектуальних рішень для обробки документів, що дозволяють значно підвищити ефективність та знизити

витрати на управління документами, а також оптимізувати внутрішні бізнес-процеси через інтеграцію платформи з іншими інформаційними системами організацій;

- застосування сучасних платформ, таких як UiPath та Automation Anywhere, для створення автоматизованих систем управління програмними роботами, які сприяють значному зменшенню часу на виконання рутинних завдань та зниженню людського фактору в процесах;

- надання комплексних консультаційних послуг у галузі роботизації бізнес-процесів та інтелектуальної автоматизації, зокрема шляхом впровадження таких передових технологій, як Computer Vision, Natural Language Processing (NLP) та Machine Learning, що дозволяють забезпечити гнучкість та інтелектуальність управлінських процесів.

«DMS Solutions» має міжнародне представництво, з головним офісом, розташованим у Гонконзі, що дозволяє компанії забезпечувати передові технологічні рішення, які відповідають найвищим світовим стандартам. Завдяки своєму стратегічно вигідному місцезнаходженню, компанія активно бере участь у глобальних процесах розвитку та інновацій, пропонуючи інноваційні продукти та послуги, що охоплюють широкий спектр галузей. «DMS Solutions» є важливим гравцем на ринку, забезпечуючи ефективні технологічні рішення, адаптовані до специфічних потреб підприємств різних секторів економіки. Постійна орієнтація на передові технології та високий рівень обслуговування дозволяють компанії залишатися на передовій хвилі інновацій та задовольняти вимоги сучасного бізнес-середовища.

Отже, системи електронного документообігу значно покращують ефективність роботи організацій, оскільки автоматизують низку ключових бізнес-процесів та забезпечують зручне і ефективне управління документами. Вони дозволяють не лише надійно зберігати та швидко обмінювати документи, а й підтримують спільну роботу між працівниками, забезпечуючи можливість редагування в реальному часі та гарантують підвищену безпеку даних. Завдяки впровадженню таких систем відбувається значна оптимізація процесів зберігання і пошуку інформації, що дозволяє значно знизити витрати на адміністративне управління, зменшити час на виконання рутинних операцій і підвищити загальну продуктивність. Всі ці фактори разом сприяють зміцненню позицій організації на ринку, підвищенню її конкурентоспроможності та сприяють реалізації стратегії довгострокового розвитку.

3.4. Інновації та новітні технології в електронному документообігу

Електронний документообіг є важливою складовою сучасних бізнес–процесів, який значно спрощує взаємодію між організаціями, установами та фізичними особами, забезпечуючи швидкість, ефективність і зручність у роботі з інформацією. З розвитком цифрових технологій, електронний документообіг не лише вдосконалюється, але й отримує нові можливості завдяки впровадженню інноваційних рішень, що радикально змінюють процеси створення, обміну, зберігання та обробки документів. Впровадження таких технологій дозволяє значно знизити адміністративні витрати, зменшити кількість помилок, покращити доступність даних та забезпечити високий рівень безпеки інформації.

Одними з найзначніших досягнень у сфері електронного документообігу є використання технологій блокчейн для забезпечення незмінності документів і автоматизації процесів підпису, а також застосування штучного інтелекту для автоматизації процесів обробки та аналізу документів. Блокчейн технології, завдяки своїй структурі, гарантують прозорість і безпеку електронних транзакцій, що стає критично важливим для юридичних, фінансових та державних установ, де надійність і відсутність змін у документах є обов’язковими умовами. Використання штучного інтелекту дозволяє зменшити ручне втручання в процеси обробки документів, автоматизуючи класифікацію, перевірку та аналіз, що значно збільшує ефективність і швидкість роботи.

Важливим кроком у розвитку електронного документообігу є також інтеграція з хмарними технологіями та системами управління інформацією, що дозволяє забезпечити збереження та доступність документів в будь-який час і з будь-якої точки світу. Хмарні сервіси забезпечують масштабованість, безпеку і зручність у зберіганні великих обсягів даних, а також дозволяють оптимізувати витрати на інфраструктуру.

Таким чином, інновації в електронному документообігу відкривають нові можливості для розвитку організацій, підвищуючи рівень безпеки, ефективності та доступності інформації, що в свою чергу сприяє підвищенню конкурентоспроможності на глобальному рівні. У цьому контексті, розгляд сучасних технологій, таких як блокчейн, ШІ, хмарні сервіси та інші інноваційні рішення, стає необхідним для ефективного впровадження та використання

електронного документообігу в умовах сучасної цифрової трансформації.

В табл. 3.2 представлено інноваційні технології в електронному документообігу.

Таблиця 3.2

Інноваційні технології в електронному документообігу

Назва технології	Опис	Приклад існуючих програм
Блокчейн	Технологія для забезпечення незмінності та автентичності електронних документів через дистрибуцію даних у розподіленій мережі.	Ethereum [11], Hyperledger [16], IBM Blockchain [17]
Штучний інтелект (AI) для обробки документів	Використання машинного навчання для автоматизації класифікації, розпізнавання тексту та пошуку в документах, а також для виявлення аномалій.	Google Cloud Vision [13], Amazon Textract [3], Microsoft Cognitive Services [20], ABBYY FlexiCapture [1]
Автоматизоване створення документів за допомогою AI	Використання ШІ для автоматичного створення шаблонів і документів, що забезпечує їх відповідність заданим стандартам і вимогам.	LawGeex [18], HotDocs [15], Contract Express [4]
Інтеграція блокчейн для аутентифікації та підпису	Використання блокчейн для автоматичного запису підписів та відстеження змін у документах, що забезпечує високу безпеку і верифікацію.	DocuSign [6], Adobe Sign [2], Signaturit [23]
Хмарні платформи для електронного документообігу	Використання хмарних технологій для централізованого зберігання та доступу до документів, що дозволяє покращити спільну роботу та знижує витрати на інфраструктуру.	Google Drive [14], Dropbox [7], Microsoft OneDrive [21]

Блокчейн є революційною технологією, яка забезпечує незмінність і автентичність електронних документів завдяки використанню дистрибуційної мережі, що складається з численних учасників, котрі підтримують та оновлюють спільний реєстр. У системі

блокчейн кожен запис або транзакція (яка, в контексті документообігу, є окремим документом або зміною в ньому) фіксується в «блоці», що поєднується з попереднім блоком за допомогою криптографії. Це гарантує, що будь-яка зміна в документах є прозорою і доступною для всіх учасників системи, що запобігає можливості фальсифікації або підробки даних.

Технологія блокчейн дозволяє створювати механізми забезпечення довіри в цифровому середовищі, де учасники можуть бути анонімними або не взаємодіяти один з одним безпосередньо, але, завдяки механізмам консенсусу, підтверджувати автентичність і цілісність документів. Вона також надає можливість вести журнал змін документів, що дозволяє в будь-який час повернутися до попередньої версії документа, що забезпечує високий рівень прозорості і контролю за змінами.

Нижче представлено більш ширше опис деяких платформ блокчейн для ефективного забезпечення документообігу.

Ethereum є однією з найвідоміших і найширше використовуваних платформ для створення і запуску смарт-контрактів, що також активно застосовуються для забезпечення автентичності електронних документів. У випадку з Ethereum, документи можуть бути збережені в блоках, а смарт-контракти забезпечують автоматичне виконання угод при виконанні певних умов. Цей процес може бути застосований до різноманітних юридичних і фінансових документів, де необхідно забезпечити незмінність і юридичну силу. Перевагою є те, що документи, закріплені в Ethereum, стають частиною дистрибуційної мережі, де кожен учасник має доступ до історії змін, що робить підробку або зміну документів неможливою без відома інших учасників.

Hyperledger, який є проєктом з відкритим кодом під керівництвом Linux Foundation, був розроблений для створення приватних і дозволених блокчейн-рішень, що можуть застосовуватись у корпоративних середовищах. Відмінною рисою Hyperledger є наявність розподілених реєстрів для зберігання даних, що дозволяють компаніям ефективно вести документообіг між різними сторонами. Hyperledger дозволяє легко налаштувати блокчейн-мережу для забезпечення інтеграції з існуючими інформаційними системами та застосування в різних сферах, таких як фінансові послуги, страхування і постачання товарів, де важливо забезпечити високий рівень безпеки і незмінності документів.

IBM Blockchain, як один із лідерів у сфері корпоративного блокчейну, пропонує рішення, яке надає підприємствам можливість інтегрувати технології блокчейн для відстеження та збереження електронних документів у реальному часі. Використовуючи цей блокчейн, організації можуть створювати надійні системи для перевірки автентичності документів, автоматизації процесів укладання угод і забезпечення прозорості в обміні даними. IBM Blockchain підтримує не тільки дистрибуцію і збереження документів, але й інтеграцію з іншими платформами для створення гнучких рішень у реальному часі для бізнесу.

Аргументація використання блокчейн у електронному документообігу:

- незмінність даних. Одна з найбільших переваг технології блокчейн для електронного документообігу – це забезпечення незмінності документів. Оскільки всі транзакції записуються в блоки і зв'язуються один з одним, будь-яка спроба змінити вже існуючий запис потребує зміни всіх наступних блоків. Це робить підробку або фальсифікацію даних практично неможливою;

- прозорість та доступність. Блокчейн дає змогу зберігати всі записи про зміни в документах в одному доступному для всіх учасників реєстрі. Кожен користувач, який має доступ до блокчейн-мережі, може переглядати всі зміни, що забезпечує високу прозорість і контроль за документообігом. Це особливо важливо в таких сферах, як фінанси та юридичні послуги, де довіра та надійність є основою для взаємодії;

- відстеження історії змін. Взаємодія з документами, які зберігаються в блокчейні, надає можливість не лише побачити поточний стан документа, але й відслідковувати історію його змін, хто і коли вносив корективи. Це забезпечує контроль над процесом редагування та дозволяє швидко виявляти підозрілі дії або несанкціоновані зміни;

- захист від несанкціонованого доступу. Оскільки блокчейн працює за принципом дистрибуційної мережі з високим рівнем шифрування та консенсусу серед учасників, це гарантує захист від несанкціонованого доступу до документів. Лише дозволені учасники можуть взаємодіяти з певними документами або вносити зміни, що забезпечує високий рівень конфіденційності.

Отже, технологія блокчейн пропонує потужне рішення для забезпечення автентичності, прозорості та безпеки електронних

документів, що робить її важливим інструментом у сучасному документообігу.

Штучний інтелект (AI) в обробці документів використовує машинне навчання для автоматизації рутинних завдань, таких як класифікація, розпізнавання тексту та пошук у документах. Застосування AI дозволяє значно підвищити ефективність роботи з великими обсягами інформації, автоматизуючи процеси, які традиційно вимагали великих затрат часу і людських ресурсів. Машинне навчання дозволяє системам «навчатися» на великих масивах даних, знаходити закономірності та покращувати свої алгоритми для точної та швидкої обробки документів.

Одним із важливих напрямів використання AI в обробці документів є класифікація документів. Це процес автоматичного визначення категорії документа на основі його вмісту. Наприклад, при обробці юридичних або фінансових документів, система штучного інтелекту може автоматично визначати тип документа (контракт, рахунок-фактура, акт, лист) і направляти його в відповідну категорію. Завдяки цьому, процес сортування документів значно пришвидшується і зменшується ймовірність людської помилки. Такі технології, як Google Cloud Vision та Amazon Textract, активно використовуються для автоматичного сканування та класифікації документів, що дозволяє зменшити обсяг рутинної роботи для співробітників компаній.

Другим важливим аспектом є розпізнавання тексту в документах. Технології оптичного розпізнавання символів (OCR) на основі AI дозволяють перетворювати відскановані або фотографовані документи у редаговані текстові файли. Для цього використовуються алгоритми машинного навчання, що можуть «читати» текст на зображеннях і перетворювати його в структуровані дані. Важливою характеристикою таких систем є їх здатність до адаптації: вони можуть коригувати свої алгоритми в залежності від якості зображення або шрифтів, що забезпечує високу точність розпізнавання. Програми, як Microsoft Cognitive Services та ABBYY FlexiCapture, застосовують такі технології для автоматизованої обробки великих обсягів документів, зокрема, для рахунків-фактур, договорів, медичних та юридичних документів.

Також важливим аспектом є пошук в документах. Сучасні системи на базі AI можуть здійснювати пошук не лише за ключовими словами, але й за змістом, що дозволяє знаходити потрібну інформацію навіть у великих масивах даних. Такий пошук включає в себе контекстуальний аналіз, що дає змогу не тільки знаходити окремі

фрази, а й розуміти зв'язки між термінами, що дає більш точні результати. Наприклад, Ross Intelligence, використовує AI для пошуку правових документів, де пошук здійснюється на основі юридичних контекстів, що дозволяє швидше знаходити необхідні матеріали для адвокатів чи юристів.

Ще однією важливою функцією є виявлення аномалій у документах. Машинне навчання може застосовуватись для виявлення підозрілих або аномальних змін у документах, що можуть свідчити про несанкціоновані редагування або потенційні помилки. Наприклад, в банківських і фінансових установах AI може виявляти аномалії у фінансових звітах або рахунках-фактурах, що може бути сигналом про шахрайство чи зловживання. Це є особливо важливим для захисту від внутрішніх загроз, де співробітники можуть несанкціоновано змінювати документи. Системи, що використовують AI для виявлення аномалій, надають можливість оперативно виявляти і реагувати на потенційні загрози.

Використання AI для обробки документів має значний вплив на оптимізацію робочих процесів. За допомогою цих технологій організації можуть значно зменшити витрати часу на ручну обробку, скоротити кількість помилок, підвищити точність та забезпечити високу швидкість обробки документів. Системи на основі машинного навчання здатні навчатися на великих обсягах даних, вдосконалювати алгоритми для більш ефективної роботи та адаптуватися до нових умов.

Загалом, впровадження AI для обробки документів є необхідним кроком для організацій, що прагнуть автоматизувати свої документообіг і підвищити ефективність своїх бізнес-процесів. Технології, як Google Cloud Vision, Amazon Textract, Microsoft Cognitive Services, ABBYY FlexiCapture та Ross Intelligence, є яскравими прикладами інструментів, які активно використовуються для автоматизації обробки документів та підвищення безпеки і точності обробки великих масивів даних.

Автоматизоване створення документів за допомогою штучного інтелекту (AI) є важливим напрямком у розвитку технологій, який сприяє значній оптимізації і стандартизації процесу створення документів. За допомогою ШІ, організації можуть автоматично генерувати шаблони документів, що відповідають певним стандартам і вимогам, знижуючи ризик людських помилок, прискорюючи процеси і забезпечуючи високий рівень відповідності всіх створених документів існуючим правовим і корпоративним нормам.

Процес автоматичного створення документів через AI включає використання алгоритмів машинного навчання та аналізу великих обсягів даних для автоматичного створення шаблонів, адаптованих під специфічні потреби організації. Цей підхід є особливо корисним у юридичних, фінансових та корпоративних сферах, де важлива точність формулювань і відповідність строгим стандартам. В результаті цього, документи можна створювати значно швидше та зменшити можливість неточностей, які можуть виникнути під час ручного процесу.

Одним із найбільш значних застосувань технології є юридична сфера, де автоматизація створення контрактів, угод і договорів є критично важливою для забезпечення точності та юридичної сили документів. Програми, як LawGeex, використовують AI для автоматичного перевірки контрактів на відповідність стандартам, виявлення неточностей або відсутності необхідних елементів, що можуть вплинути на юридичну силу документа. У цьому контексті AI не лише створює шаблони документів, але й допомагає визначити, чи відповідає кожен елемент контракту вимогам законодавства, що значно зменшує ризик помилок, пов'язаних з людським фактором.

HotDocs є ще одним прикладом програми, яка використовує AI для автоматизованого створення документів. HotDocs дозволяє створювати складні документи, використовуючи готові шаблони, на основі даних, введених користувачем. Це дозволяє швидко генерувати такі документи, як контракти, угоди або звіти, що вимагають повторюваного використання стандартних формулювань і умов. HotDocs автоматично адаптує ці шаблони під конкретні дані, зберігаючи їх відповідність правовим вимогам і корпоративним стандартам.

Contract Express – це ще один інструмент, який активно використовує технології штучного інтелекту для автоматизації процесів створення і перевірки контрактів. Ця платформа допомагає юридичним компаніям створювати стандартизовані контракти за допомогою простого інтерфейсу, де користувачі вводять необхідну інформацію, а система автоматично генерує документ, який відповідає заданим вимогам. Завдяки AI, Contract Express дозволяє компаніям значно скоротити час на підготовку документів і забезпечити їх відповідність стандартам.

На рис. 3.18 представлено аргументація використання автоматизованого створення документів через AI.



Рис. 3.18. Аргументація використання автоматизованого створення документів через AI

Технології автоматизованого створення документів, що базуються на штучному інтелекті, значно спрощують і прискорюють процес підготовки документації. Завдяки AI організації здатні створювати складні документи за лічені хвилини, що є суттєвим досягненням порівняно з традиційними методами, які вимагають значних витрат часу на ручну обробку. У високошвидкісних середовищах документообігу, де кожна затримка може призвести до серйозних фінансових та правових наслідків, автоматизація таких процесів стає необхідною умовою для ефективного функціонування організацій.

Одним з важливих переваг автоматизованого створення документів є зниження ймовірності помилок, які можуть бути спричинені людським фактором. AI використовує чітко визначені алгоритми для генерації документів, що мінімізує ризик пропусків важливих пунктів або невірнього формулювання, особливо в юридичних та фінансових документах. У цих сферах навіть незначна помилка може призвести до серйозних наслідків, таких як юридичні позови чи фінансові втрати, тому автоматизація створення таких документів забезпечує високий рівень точності та відповідності стандартам.

Крім того, автоматизація процесу створення документів сприяє значному підвищенню ефективності і зниженню витрат. Організації можуть зекономити значну кількість ресурсів, оскільки автоматичне генерування документів зменшує потребу в людському втручанні та

економить час, що зазвичай витрачається на ручне створення кожного документа. Цей підхід дозволяє компаніям не лише оптимізувати робочі процеси, але й зменшити адміністративні витрати, що в кінцевому підсумку підвищує загальну рентабельність бізнесу.

Не менш важливим є і аспект гнучкості та адаптивності, який надають технології AI в автоматизованому створенні документів. Системи AI здатні швидко адаптуватися до змін у законодавстві або внутрішніх політиках компаній, автоматично оновлюючи шаблони відповідно до нових стандартів. Це дозволяє організаціям своєчасно реагувати на правові зміни та зберігати відповідність вимогам без необхідності вручну змінювати кожен документ, що значно спрощує процеси управління та знижує ризики невідповідностей. Технології AI таким чином забезпечують стійкість бізнесу до змін та адаптацію до нових реалій.

Загалом, використання технологій штучного інтелекту для автоматизованого створення документів є потужним інструментом для організацій, що прагнуть підвищити ефективність своєї діяльності, знизити ризики помилок і забезпечити високий рівень відповідності своїх документів юридичним та корпоративним вимогам. Програми, як LawGeex, HotDocs і Contract Express, є яскравими прикладами того, як AI може допомогти організаціям створювати та перевіряти документи швидше, точніше і ефективніше.

Інтеграція блокчейн-технологій для аутентифікації та підпису документів є важливим кроком у розвитку систем електронного документообігу, що забезпечує високу безпеку, прозорість та можливість верифікації документів. Технологія блокчейн, яка є розподіленим реєстром, дозволяє зберігати записи про підписи та зміни в документах в захищеній та незмінній формі. Кожна транзакція (підпис або зміна) зберігається у блокчейні, що робить підробку або зміну інформації неможливою без виявлення спроби несанкціонованого втручання. Це забезпечує не лише збереження цілісності документа, але й гарантує, що кожен підпис чи зміна підтверджені відповідними учасниками мережі.

Використання блокчейн для автоматичного запису підписів має величезне значення для зниження ризиків фальсифікацій і підробок документів. Завдяки дистрибуційному характеру блокчейн-мережі, кожен підпис або зміна документа реєструється в блоках і зберігається на всіх учасників мережі. Це дозволяє створювати цифрові підписи, які є значно безпечнішими, оскільки вони можуть бути перевірені кожним

учасником системи і не потребують централізованого органу для підтвердження їх автентичності. Таким чином, підпис на документі стає не лише підтвердженням волевиявлення сторін, але й гарантією того, що документ не був змінений після підписання.

Застосування блокчейн для аутентифікації та підпису особливо корисне в контексті юридичних та фінансових угод, де підписування документів повинно мати юридичну силу і не піддаватися оскарженню. У таких сферах блокчейн дає змогу забезпечити не лише неперервність документів, але й точну часову відмітку кожної зміни або підпису, що є важливим для підтвердження законності угод. Завдяки блокчейн-технології, кожен документ, підписаний в системах, таких як DocuSign або Adobe Sign, отримує додатковий рівень захисту, адже всі зміни, підписи та їхні автори фіксуються в блоках, що неможливо змінити або видалити без залишення слідів.

DocuSign, одна з найбільш відомих платформ для електронного підпису, інтегрує блокчейн для додаткової верифікації та захисту підписаних документів. Платформа забезпечує юридичну силу підписів, а також дозволяє відслідковувати статуси документів і зміни в реальному часі. З використанням блокчейн, DocuSign дозволяє створювати абсолютно надійні і незмінні цифрові підписи, які не піддаються оскарженню, що особливо важливо для міжнародних угод і контрактів.

Adobe Sign також активно інтегрує блокчейн для підвищення рівня безпеки підписаних документів. Вона дозволяє користувачам використовувати цифрові підписи, які підтверджуються за допомогою блокчейн-технологій, забезпечуючи повну верифікацію і збереження автентичності документів. Це значно підвищує довіру до підписаних документів і знижує ймовірність виникнення суперечок щодо їхнього змісту або підпису.

Signaturit є ще однією платформою, яка поєднує електронний підпис з блокчейн-технологією для додаткового рівня захисту. Платформа дозволяє здійснювати аутентифікацію та підписання документів у реальному часі, зберігаючи записи про кожну операцію в блокчейні, що дозволяє забезпечити їхню невідомість. Це робить систему надзвичайно корисною для компаній, що працюють з високими юридичними вимогами, де необхідно мати максимальний рівень захисту і прозорості.

Таким чином, інтеграція блокчейн для аутентифікації та підпису документів дозволяє значно підвищити рівень безпеки і верифікації в

системах електронного документообігу. Ця технологія забезпечує не лише високу захищеність від фальсифікацій, але й дає можливість ефективно відслідковувати та верифікувати кожну операцію з документами, що є важливим кроком у розвитку електронних підписів, особливо у юридичній та фінансовій сферах.

Хмарні платформи для електронного документообігу є важливим інструментом для зберігання та доступу до документів, що значно покращує ефективність спільної роботи та дозволяє знизити витрати на інфраструктуру. Використання хмарних технологій забезпечує централізоване зберігання даних, що дозволяє організаціям зберігати великі обсяги інформації без необхідності витрачати ресурси на створення та обслуговування локальних серверів. Водночас, хмарні платформи надають доступ до документів у будь-який час і з будь-якого місця, що є важливою перевагою для підприємств, які працюють на віддаленому або мобільному форматі.

Однією з ключових переваг хмарних платформ є їх здатність забезпечувати гнучкість і масштабованість. Організації можуть збільшувати або зменшувати обсяг зберігання даних залежно від потреб, що дозволяє ефективно управляти ресурсами та скорочувати витрати на інфраструктуру. Хмарні платформи також забезпечують високий рівень безпеки завдяки використанню сучасних методів шифрування та багаторівневої аутентифікації, що гарантує захист конфіденційних документів навіть при зберіганні їх на віддалених серверах.

Google Drive є однією з найпопулярніших хмарних платформ для зберігання документів, яка надає користувачам можливість зберігати, організовувати та обмінюватися файлами в реальному часі. Завдяки інтеграції з іншими сервісами Google, такими як Google Docs та Google Sheets, Google Drive дозволяє безперешкодно працювати з документами спільно з іншими користувачами, що значно підвищує ефективність командної роботи. Google Drive також пропонує різні рівні доступу до файлів, що дозволяє обмежити доступ до конфіденційних даних лише для уповноважених осіб.

Dropbox є ще однією популярною хмарною платформою, яка забезпечує централізоване зберігання документів і дозволяє здійснювати їх обмін серед користувачів. Dropbox надає можливість автоматично синхронізувати файли між різними пристроями, що дозволяє працювати з документами з будь-якого місця. Крім того, Dropbox забезпечує надійний контроль версій, що дозволяє

відновлювати попередні версії документів у разі помилок або несанкціонованих змін. Ця платформа також підтримує інтеграцію з іншими інструментами для колаборації, такими як Slack і Zoom, що дозволяє створювати ефективне робоче середовище для команд.

Microsoft OneDrive є частиною екосистеми Microsoft 365 і забезпечує зберігання і доступ до документів в хмарі. OneDrive інтегрується з іншими продуктами Microsoft, такими як Word, Excel і PowerPoint, що дозволяє працювати з документами безпосередньо в хмарі без необхідності завантажувати їх на локальні пристрої. Одна з ключових переваг OneDrive – це потужні функції для роботи в команді, включаючи спільне редагування документів в реальному часі, що забезпечує ефективну взаємодію між співробітниками незалежно від їхнього фізичного місцезнаходження.

Використання хмарних платформ для електронного документообігу має безліч переваг, зокрема забезпечення безперервного доступу до документів, зниження витрат на інфраструктуру, покращення співпраці між співробітниками та підвищення безпеки даних. Завдяки таким платформам, як Google Drive, Dropbox та Microsoft OneDrive, організації можуть забезпечити високу продуктивність і гнучкість в роботі з документами, знижуючи при цьому витрати на зберігання і обробку інформації. Хмарні платформи також дозволяють бізнесам бути більш адаптивними і швидко реагувати на зміни в умовах роботи, що є особливо важливим в умовах сучасного динамічного цифрового середовища.

Інновації та новітні технології в електронному документообігу стали основними чинниками, що визначають успіх сучасних організацій у цифровому світі. Завдяки впровадженню таких технологій, як блокчейн, штучний інтелект та хмарні сервіси, вдалося значно підвищити рівень безпеки, ефективності та швидкості обробки документів, що є критично важливим у сучасному бізнес-середовищі. Блокчейн, забезпечуючи незмінність та прозорість даних, дозволяє мінімізувати ризики фальсифікацій та підробок документів, що особливо важливо для сфер, де потрібна висока довіра, як юридична та фінансова галузь. Штучний інтелект, в свою чергу, автоматизує рутинні та часозатратні процеси, такі як класифікація, пошук та обробка документів, що дозволяє значно знижувати людські помилки та прискорювати робочі процеси. Використання хмарних платформ надає організаціям можливість зберігати і отримувати доступ до документів з будь-якої точки світу, забезпечуючи високу гнучкість,

масштабованість та безпеку даних. Ці технології не лише оптимізують документообіг, але й надають організаціям можливість швидко адаптуватися до змін у бізнес–потребах та вимогах законодавства. Автоматизація процесів створення, підписання та зберігання документів дозволяє компаніям значно скоротити витрати, підвищити ефективність управлінських процесів та забезпечити високу точність та відповідність усіх створених документів встановленим стандартам. Враховуючи розвиток цифрової трансформації та постійну потребу в інноваціях, організації повинні активно інтегрувати ці технології у свої стратегії для підвищення конкурентоспроможності та забезпечення безпеки в роботі з електронними документами.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які основні функції систем електронного документообігу (СЕД)?
2. Як автоматизація створення документів у системах електронного документообігу сприяє підвищенню ефективності роботи організації?
3. Які переваги має організація обігу документів в системах електронного документообігу?
4. Як системи електронного документообігу забезпечують безпеку та конфіденційність даних?
5. Чим важлива функція пошуку та фільтрації документів у СЕД?
6. Як інтеграція систем електронного документообігу з іншими інформаційними системами (CRM, ERP) покращує ефективність бізнес-процесів?
7. Які інноваційні технології в електронному документообігу ви знаєте, і як вони змінюють процеси обробки та зберігання документів?
8. Як технології блокчейн можуть змінити процеси аутентифікації та підпису документів в електронному документообігу? Наведіть приклади існуючих рішень.
9. Яким чином штучний інтелект сприяє обробки документів в системах електронного документообігу? Як це впливає на ефективність і точність роботи з великими обсягами документів?

РОЗДІЛ 4. ЕЛЕКТРОННЕ ВРЯДУВАННЯ

4.1. Основні етапи розвитку електронного врядування в Україні

Електронне урядування в Україні є одним з ключових напрямів реформування державного управління та модернізації суспільних процесів. В умовах глобалізації та стрімкого розвитку інформаційних технологій країна взяла на себе амбітне завдання інтеграції сучасних цифрових рішень для забезпечення ефективної взаємодії між державними інституціями, громадянами та бізнесом. Впровадження електронного урядування має на меті не лише підвищення ефективності управлінських процесів, а й створення умов для прозорості та відкритості державних органів, що сприяє боротьбі з корупцією та зміцненню демократичних інститутів.

Україна послідовно впроваджує електронні технології на всіх рівнях державного управління, що дозволяє підвищити оперативність прийняття рішень і полегшити доступ громадян до адміністративних послуг. Починаючи з перших кроків у впровадженні цифрових підписів і систем електронного документообігу, країна поступово перейшла до інтеграції більш складних систем, таких як онлайн-платформи для надання публічних послуг, цифрова ідентифікація громадян і бізнесу, а також мобільні додатки для взаємодії з державними установами.

Розвиток електронного урядування в Україні супроводжувався прийняттям важливих нормативно-правових актів, що регламентують впровадження і функціонування нових систем. Кожен етап впровадження електронних послуг ґрунтувався на світовому досвіді та відповідних потребах українського суспільства, а також був підкріплений міжнародною співпрацею, зокрема з країнами Європейського Союзу та іншими глобальними партнерами. Це дозволяє Україні бути серед лідерів у галузі впровадження цифрових рішень на пострадянському просторі та активно використовувати технології для забезпечення державного управління в умовах сучасних викликів.

Подальші етапи розвитку електронного врядування в Україні зумовлені як необхідністю удосконалення існуючих систем, так і прагненням інтеграції з європейськими цифровими стандартами. Це забезпечує країні можливість адаптації до сучасних викликів, включаючи кризові ситуації, та підтримання стабільної роботи державних інституцій. Основні етапи розвитку електронного

врядування в Україні демонструють послідовний підхід до створення ефективного, прозорого та зручного для громадян державного управління, який продовжує вдосконалюватися разом із впровадженням нових технологічних рішень.

В табл. 4.1 наведено ключові етапи цього процесу, що відображають розвиток електронного урядування в Україні.

Таблиця 4.1

Ключові етапи розвитку електронного урядування в Україні

Рік	Закон/Постанова	Основні зміни та досягнення
1	2	3
2003	Закон України «Про електронний цифровий підпис» (№ 852–IV, 22.05.2003). Втратив чинність у 2018 році, замінений Законом України «Про електронну ідентифікацію та електронні довірчі послуги» 05.10.2017 № 2155–VIII	Створення правової бази для використання електронного цифрового підпису (ЕЦП), що важливо для електронного документообігу.
2011	Закон України «Про доступ до публічної інформації» (№ 2939–VI, 13.01.2011)	Забезпечення прозорості діяльності органів влади через електронні системи, доступ громадян до публічної інформації онлайн.
2015	Постанова Кабінету Міністрів України №851 «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету» (21.10.2015)	Регламентує вимоги до реєстрації, супроводу та використання доменних імен державними органами в Україні, забезпечуючи їхню відповідність стандартам безпеки та використання офіційних доменних зон GOV.UA та .UKR для державних веб-сайтів і службової
2017	Постанова Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» (№ 649–р, 20.09.2017)	Визначення стратегічних напрямів розвитку електронного урядування, впровадження нових послуг.

продовження табл. 4.1

1	2	3
2018	«Цифровий порядок денний України 2020» (17.01.2018)	Визначення основних стратегічних напрямків розвитку цифрової економіки та суспільства в Україні.
2019	Постанова Кабінету Міністрів України. № 1137 «Питання Єдиного державного вебпорталу електронних послуг та Єдиного державного порталу адміністративних послуг» (від 04.12. 2019 р	Постанова регламентує створення Єдиного державного веб-порталу електронних послуг, який з 1 січня 2020 року також виконує функції Єдиного державного порталу адміністративних послуг для забезпечення поліпшеного доступу громадян і юридичних осіб до електронних послуг.
2020	Запуск порталу «Дія» (2 квітня 2020)	Створення порталу для інтеграції ключових державних послуг в онлайн-формат, на якому спочатку було доступно 27 послуг.
2021	Закон України «Про особливості надання публічних (електронних публічних) послуг» № 1689-IX (від 15.07.2021)	Розширення функціональності порталу «Дія» в межах концепції «Держава в смартфоні», коли всі основні державні послуги доступні онлайн.

Розвиток електронного урядування в Україні є важливим компонентом процесу реформування державного управління, спрямованим на підвищення ефективності, прозорості та доступності державних послуг для громадян та бізнесу. Електронне урядування відіграє вирішальну роль у модернізації управлінських процесів та інтеграції сучасних цифрових технологій у роботу органів державної влади. Аналіз основних етапів розвитку електронного урядування свідчить про поступове впровадження інноваційних рішень, що відповідають світовим стандартам та потребам суспільства.

На початку розвитку електронного урядування в Україні важливим кроком стало ухвалення Закону України «Про електронний цифровий підпис» у 2003 році. Цей закон заклав основу для використання електронного підпису як правового інструменту для забезпечення юридичної сили електронних документів. Впровадження електронного підпису стало важливим кроком на шляху до автоматизації документообігу, зменшення бюрократичних процедур та підвищення ефективності державного управління. Згодом, у 2018 році

цей закон був замінений Законом «Про електронну ідентифікацію та електронні довірчі послуги», що підкреслило необхідність подальшого розвитку технологій у сфері електронного урядування та надання електронних послуг.

Прийняття Закону «Про доступ до публічної інформації» у 2011 році стало ключовим моментом для забезпечення прозорості державного управління. Цей закон відкрив нові можливості для громадян щодо отримання публічної інформації через електронні платформи, що стало важливим інструментом підвищення довіри до державних інституцій та боротьби з корупцією. Впровадження електронних інструментів для доступу до інформації дозволило значно спростити взаємодію між громадянами та державою, що сприяло демократизації державного управління.

Додатковим важливим кроком стало прийняття постанови Кабінету Міністрів у 2015 році, яка регламентує використання доменних імен державними органами в українському сегменті Інтернету. Ця постанова встановила стандарти безпеки для державних веб-ресурсів і забезпечила єдині правила для державних органів у сфері використання інтернет-інфраструктури. Використання офіційних доменних зон, таких як GOV.UA та .УКР, стало важливим елементом у забезпеченні безпеки та надійності державних інтернет-сайтів, що також сприяло зміцненню довіри громадян до електронного урядування.

Особливо важливим етапом у розвитку електронного урядування в Україні стало затвердження у 2017 році Концепції розвитку електронного урядування. Цей документ визначив стратегічні напрями розвитку електронних послуг, впровадження інноваційних технологій у державне управління та створення умов для інтеграції України у світовий цифровий простір. Концепція передбачала розширення доступу громадян і бізнесу до електронних адміністративних послуг, підвищення ефективності державного управління та створення інфраструктури для підтримки цифрової економіки.

Важливим кроком у реалізації цих стратегічних цілей стало затвердження «Цифрового порядку денного України 2020» у 2018 році. Цей документ став дороговказом для впровадження цифрових технологій у різні сфери суспільного життя та економіки. Він визначив основні напрямки розвитку цифрової економіки, електронного урядування та суспільства в цілому, що дозволило Україні продовжити інтеграцію в глобальні процеси цифровізації.

Одним з найбільш значущих досягнень стало створення у 2020 році порталу «Дія», який об'єднав на єдиній платформі ключові державні послуги. Завдяки цьому portalу громадяни отримали можливість користуватися багатьма державними послугами онлайн, що значно спростило доступ до адміністративних процедур. Запуск portalу «Дія» став кульмінацією багаторічних зусиль з розвитку електронного урядування та сприяв підвищенню оперативності надання послуг.

Прийняття у 2021 році Закону «Про особливості надання публічних (електронних) послуг» закріпило досягнення у сфері електронного урядування та забезпечило подальше розширення функціональності portalу «Дія». Це дозволило ще більше наблизити Україну до реалізації концепції «Держава в смартфоні», коли всі основні державні послуги доступні онлайн для громадян і бізнесу.

Отже, резюмуючи вище описане дослідження етапів розвитку електронного урядування в Україні, можна зробити висновок, що розвиток електронного урядування в Україні є складним і багатоступеневим процесом, який забезпечує перехід держави до нових стандартів управління, сприяє інтеграції у світовий цифровий простір та дозволяє державі ефективніше реагувати на потреби громадян і бізнесу. Кожен етап розвитку електронного урядування відображає прагнення держави до впровадження сучасних технологій, покращення якості надання послуг та підвищення ефективності державного управління в цілому.

Електронне урядування в Україні, зокрема завдяки платформі «Дія», на сьогоднішній день визнане одним з найкращих у світі та є прикладом для наслідування багатьма країнами. Ця платформа дозволяє громадянам України отримувати понад 14 цифрових документів, включно з першим у світі цифровим паспортом, що має таку саму юридичну силу, як і паперовий. «Дія» надає можливість швидко та зручно отримувати державні послуги через смартфон, включно з реєстрацією бізнесу, оформленням будівельних дозволів, виплатами субсидій, а також поданням заявок на компенсацію за пошкоджене майно під час війни.

Значним фактором успіху є те, що «Дія» зменшує корупційні ризики, мінімізуючи особисту взаємодію громадян з бюрократами та роблячи процес отримання державних послуг повністю прозорим і автоматизованим. Це не лише спрощує адміністративні процедури, але й підвищує довіру громадян до державних установ. Крім того,

Україна активно ділиться своїм досвідом з іншими країнами. Наприклад, Естонія, визнаний світовий лідер у галузі електронного урядування, почала впроваджувати технології та дизайн «Дії» для розробки власної мобільної платформи. Також кілька інших країн, серед яких США та Мексика, висловили зацікавленість у впровадженні українських технологій для модернізації своїх систем електронного урядування.

Важливо зазначити, що розвиток «Дії» не зупинився навіть під час повномасштабної війни. В умовах військової агресії Росії платформа відіграла ключову роль у забезпеченні громадян необхідними документами для евакуації, реєстрації статусу внутрішньо переміщених осіб, а також отримання фінансової допомоги. Унікальні функції, такі як можливість повідомляти про пересування ворожих військ через додаток, підтверджують інноваційність та адаптивність цієї платформи до нових викликів.

Завдяки своїм технічним можливостям, масштабованості та здатності швидко впроваджувати нові рішення, Україна змогла не лише утримувати високий рівень надання державних послуг під час кризових ситуацій, але й стати глобальним лідером у цій сфері. Ці успіхи роблять електронне урядування в Україні одним із найбільш розвинених у Європі, а платформа «Дія» – взірцем для наслідування на міжнародному рівні.

4.2. Переваги електронного врядування

Електронне врядування є ключовим інструментом сучасного управління, що забезпечує ефективну та зручну взаємодію між державними інституціями, громадянами та бізнесом. Завдяки застосуванню інформаційно–комунікаційних технологій у державному управлінні, цей процес сприяє підвищенню прозорості та підзвітності органів влади, а також оперативності прийняття рішень. Використання таких технологій зменшує корупційні ризики і значно спрощує доступ громадян до різних державних послуг. Впровадження електронного врядування дозволяє оптимізувати внутрішні процеси державних структур, забезпечуючи раціональне використання ресурсів та підвищення ефективності їх діяльності. Це, в свою чергу, сприяє розвитку інноваційних економік і зміцненню демократичних інститутів, створюючи умови для сталого соціально–економічного розвитку.

В табл. 4.2 представлено переваги електронного врядування.

Таблиця 4.2

Переваги електронного урядування

Перевага	Опис
Прозорість і підзвітність	зниження рівня корупції через відкритий доступ до інформації та публічний контроль.
Оперативність і ефективність	автоматизація процесів, що скорочує час виконання адміністративних процедур.
Зручність для громадян	спрощення доступу до послуг через електронні сервіси без черг і візитів до установ.
Економія ресурсів	оптимізація використання фінансових та людських ресурсів державних органів.
Покращення комунікації	забезпечення швидкого зворотного зв'язку між громадянами, бізнесом і державними органами.
Доступність інформації	швидкий пошук та отримання необхідної інформації через державні електронні ресурси.
Участь громадян у прийнятті рішень	активна участь громадян у процесах прийняття рішень через електронні платформи.
Міжнародна інтеграція	спрощення співпраці з міжнародними організаціями та впровадження передових практик.
Зменшення бюрократії	скорочення паперової роботи та спрощення адміністративних процесів.
Стійкість до криз	безперебійна робота державних служб під час надзвичайних ситуацій завдяки цифровим інструментам.

Електронне урядування має низку суттєвих переваг, які сприяють підвищенню ефективності державного управління, покращенню комунікації між урядом і громадянами та модернізації управлінських процесів. У сучасних умовах цифровізація державного сектору стає необхідною не лише для ефективного функціонування державних установ, а й для забезпечення прозорості та відкритості процесів управління. Це особливо важливо в контексті глобальних викликів, таких як цифрова трансформація, збільшення обсягу інформації та зростання очікувань громадян щодо якості послуг.

Однією з ключових переваг електронного урядування є **прозорість і підзвітність**. Використання цифрових технологій у державному управлінні дозволяє значно знизити рівень корупції через відкритий доступ до інформації про діяльність урядових установ. Громадяни мають змогу відслідковувати, як витрачаються бюджетні кошти, які рішення ухвалюються державними органами, та як ці

рішення впливають на суспільство. Наприклад, відкриті реєстри, онлайн-платформи для звітності та електронні портали для участі громадян у прийнятті рішень забезпечують прозорість процесів і підвищують довіру до органів влади. Крім того, можливість громадського контролю за діяльністю державних установ робить їх підзвітними, змушуючи діяти більш ефективно та в інтересах суспільства.

Прозорість сприяє також боротьбі з корупцією, оскільки зменшує можливості для несанкціонованих і прихованих дій державних посадовців. Наприклад, електронні тендери та публічні закупівлі дозволяють уникнути «тіньових» схем та зловживань, оскільки кожен етап процесу є доступним для громадського огляду. Це підвищує ефективність витрачання державних коштів та сприяє розвитку здорової конкуренції серед підприємств.

Важливою складовою є те, що громадяни отримують можливість не лише пасивно спостерігати за діями уряду, але й активно брати участь у процесах прийняття рішень. Електронні платформи для громадських обговорень, онлайн-консультацій та петицій надають громадянам реальний інструмент для впливу на державну політику. Це сприяє підвищенню рівня довіри до влади, оскільки громадяни бачать, що їхні думки враховуються, а держава відкрита до діалогу.

Отже, електронне урядування не лише модернізує державні процеси, а й сприяє створенню більш прозорого та підзвітного управління, що позитивно впливає на відносини між урядом і суспільством.

Ще однією важливою перевагою електронного урядування є **оперативність і ефективність управлінських процесів**. Сучасні цифрові технології дозволяють автоматизувати значну частину адміністративних процедур, що значно скорочує час на їх виконання. Раніше процес ухвалення рішень у державних установах міг бути тривалим і включати численні етапи перевірок, погоджень і затверджень. Впровадження електронних систем управління значно оптимізує цей процес, дозволяючи ухвалювати рішення швидше та з мінімальною участю людини, що зменшує кількість помилок і знижує ймовірність людського фактору.

Це особливо важливо в умовах стрімкого зростання кількості запитів з боку громадян і бізнесу, що ставлять перед державою високі вимоги до якості й швидкості надання послуг. Електронні сервіси забезпечують доступ до послуг у режимі 24/7, що дає змогу громадянам

і компаніям вирішувати питання, не чекаючи відкриття фізичних офісів державних установ. Наприклад, подача заяв на отримання довідок, реєстрація підприємств або податкові платежі можуть здійснюватися онлайн, що суттєво скорочує витрати часу та ресурси, які були б необхідні для таких дій у паперовому форматі.

Автоматизація також зменшує кількість етапів обробки документів, що скорочує ризик затримок у прийнятті рішень. Це підвищує ефективність роботи державних структур, оскільки звільняє час для вирішення більш складних і важливих завдань. Наприклад, системи електронного документообігу дозволяють відслідковувати статус кожного запиту в реальному часі, що знижує навантаження на державних службовців і покращує якість послуг.

Крім того, впровадження електронного урядування дозволяє оптимізувати не лише процеси надання послуг, але й управлінські рішення в цілому. Аналітичні інструменти, що використовуються в електронних системах, дають можливість уряду більш оперативно аналізувати дані та прогнозувати наслідки ухвалених рішень. Це сприяє ефективнішому управлінню державними ресурсами та підвищенню загальної продуктивності урядових установ.

Таким чином, електронне урядування дозволяє значно підвищити оперативність і ефективність державного управління, забезпечуючи швидке та якісне надання послуг громадянам і бізнесу, що позитивно впливає на загальний рівень розвитку держави.

Важливу роль відіграє **зручність для громадян**, оскільки електронне урядування суттєво спрощує процес взаємодії з державними органами. Однією з основних переваг є можливість отримання державних послуг без необхідності особисто відвідувати установи, що знижує адміністративні бар'єри та робить процес отримання послуг більш доступним і ефективним. Громадяни та представники бізнесу можуть скористатися різноманітними послугами, такими як реєстрація підприємств, подача документів, отримання довідок чи ліцензій через онлайн-платформи, що суттєво економить час і знижує витрати, пов'язані з фізичними візитами до установ.

Особливо важливим цей аспект є для мешканців віддалених регіонів або громадян з інвалідністю, для яких доступ до державних послуг традиційно ускладнений через географічні або фізичні бар'єри. Використання електронних платформ дозволяє їм отримувати ті самі послуги, що й мешканці великих міст, незалежно від місця проживання, оскільки такі сервіси доступні в будь-який час і з будь-якого місця. Це

не лише покращує рівень обслуговування, але й сприяє соціальній рівності, забезпечуючи рівні можливості доступу до державних сервісів для всіх громадян.

Онлайн-платформи електронного урядування надають *цілодобовий доступ* до послуг, що є важливим чинником для підвищення рівня задоволення користувачів. Громадяни можуть самостійно обирати зручний для них час для подачі заяв, отримання інформації або здійснення платежів, що усуває необхідність пристосовуватися до робочих годин державних установ. Це особливо важливо для тих, хто має обмежений час через роботу або інші зобов'язання. До того ж, можливість використання електронних сервісів з мобільних пристроїв ще більше підвищує зручність для користувачів.

Крім того, електронні сервіси часто пропонують можливість відстеження статусу заяв або документів в режимі реального часу, що знижує потребу в додаткових запитах або дзвінках до державних органів. Це не лише економить час громадян, але й зменшує навантаження на державні служби, покращуючи ефективність їх роботи.

Отже, зручність для громадян є однією з найважливіших переваг електронного урядування, яка дозволяє значно спростити доступ до державних послуг, скоротити часові та матеріальні витрати, а також підвищити загальний рівень задоволення користувачів завдяки цілодобовому та віддаленому доступу до послуг.

Економія ресурсів є ще однією вагомою перевагою електронного урядування, яка робить державне управління більш раціональним та ефективним. Впровадження цифрових технологій дозволяє суттєво знизити фінансові витрати на утримання державних структур завдяки оптимізації процесів і скороченню обсягів паперової роботи. Раніше більшість адміністративних процедур вимагала значних матеріальних та часових витрат на обробку документів, архівування, зберігання та інші пов'язані з ними операції. Електронне урядування дозволяє перевести ці процеси в цифровий формат, що знижує потребу у витратах на папір, зберігання документів та інші матеріальні ресурси.

Крім того, економія ресурсів відбувається за рахунок скорочення часу на виконання адміністративних завдань. Оперативність і ефективність електронних сервісів дозволяє обробляти більшу кількість запитів за короткий проміжок часу, що знижує загальні витрати на обслуговування громадян, це також сприяє *зниженню*

навантаження на державні установи, оскільки електронні сервіси працюють без перерв і поза межами традиційних робочих годин, дозволяючи автоматизовано обслуговувати громадян і бізнес у будь-який час.

Додатково, *оптимізація управлінських процесів* через цифрові інструменти сприяє раціональному розподілу ресурсів усередині державних установ. Вивільнені ресурси можуть бути перенаправлені на стратегічно важливіші напрямки, такі як інновації, покращення умов праці державних службовців або розвиток нових цифрових послуг. Це також сприяє підвищенню загальної продуктивності державних органів і їхньої здатності швидко адаптуватися до нових викликів і потреб суспільства.

Таким чином, економія ресурсів, що досягається завдяки впровадженню електронного урядування, дозволяє державним установам оптимізувати свої витрати, підвищити продуктивність і забезпечити більш ефективне управління за рахунок раціонального використання фінансових і людських ресурсів.

Не менш важливим аспектом є покращення комунікації між державними органами, громадянами та бізнесом. Впровадження цифрових платформ значно спрощує процес обміну інформацією та забезпечує оперативний і ефективний зворотний зв'язок, що сприяє більш прозорому та відкритому урядуванню. У минулому комунікація з державними органами часто була ускладнена через бюрократичні перепони, повільну обробку звернень та обмежені можливості для громадян висловити свої думки або запити. Електронне урядування дозволяє вирішити ці проблеми завдяки використанню технологій, що забезпечують двосторонню комунікацію в режимі реального часу.

Цифрові платформи, такі як електронні портали, мобільні додатки та соціальні мережі, дозволяють уряду швидко та ефективно відповідати на запити громадян, оперативно інформувати їх про актуальні питання та здійснювати моніторинг громадської думки. Це зменшує відстань між державними структурами та населенням, роблячи комунікацію більш відкритою та доступною для всіх соціальних груп. Завдяки електронним системам громадяни можуть звертатися до державних органів безпосередньо через електронну пошту, форми зворотного зв'язку або онлайн-консультації, отримуючи відповіді швидше, ніж у традиційній паперовій формі.

Особливе значення має те, що електронне урядування сприяє швидкому вирішенню проблем і зменшенню соціальної напруги.

Оперативний зворотний зв'язок дозволяє державним органам своєчасно реагувати на запити громадян, що є важливим фактором у ситуаціях криз або надзвичайних подій. Наприклад, під час природних катастроф або соціальних конфліктів електронні платформи можуть використовуватися для оперативного надання інформації та координації дій громадян, що сприяє зниженню рівня тривоги та швидшому вирішенню проблем.

Для бізнесу електронне урядування відкриває нові можливості для взаємодії з державою. Онлайн-платформи дозволяють підприємствам подавати документи, звіти та інші матеріали без необхідності витрачати час на фізичні візити до державних установ. Це не тільки підвищує ефективність бізнес-процесів, але й зменшує ризики втрат, пов'язаних з бюрократією. Більш того, цифрові канали комунікації спрощують участь бізнесу в законодавчих обговореннях та інших важливих процесах, що дозволяє уряду отримувати актуальну інформацію безпосередньо від ключових економічних гравців.

Загалом, покращення комунікації через електронне урядування забезпечує прозорість, оперативність і відкритість державних процесів. Це дозволяє уряду швидше реагувати на зміни, підвищує рівень довіри громадян до влади і сприяє формуванню активної взаємодії між державою, суспільством та бізнесом.

Значущою перевагою електронного урядування є **доступність інформації**. Завдяки цифровим платформам, громадяни та підприємства мають можливість швидко та легко отримувати доступ до державних реєстрів, баз даних та іншої важливої інформації, що значно спрощує процес прийняття рішень. Це дозволяє громадянам бути краще обізнаними про свої права, обов'язки та можливості в рамках взаємодії з державними органами. Для бізнесу доступність інформації з державних ресурсів також є ключовим фактором, оскільки вона сприяє ефективнішому плануванню діяльності, швидшому отриманню ліцензій та дозволів, а також доступу до ринкової інформації, що підвищує конкурентоспроможність компаній.

Цифрові платформи надають можливість оперативного доступу до інформації в режимі реального часу, що зменшує кількість запитів до державних органів та прискорює вирішення адміністративних питань. Така відкритість сприяє зниженню бюрократичних бар'єрів та підвищенню прозорості роботи державних органів, оскільки громадяни можуть самостійно отримати інформацію про роботу урядових

установ, процеси прийняття рішень та надання послуг. Це також сприяє зростанню рівня довіри громадян до влади.

Крім того, електронне урядування відіграє ключову роль у забезпеченні **активної участі громадян у процесах прийняття рішень**. Використання цифрових платформ, таких як онлайн-опитування, обговорення законодавчих ініціатив та проведення консультацій, дозволяє громадянам бути активними учасниками демократичного процесу. Це створює нові можливості для зворотного зв'язку з урядом, надаючи громадянам голос у вирішенні важливих питань на національному та місцевому рівнях.

Важливим аспектом є те, що електронні платформи дозволяють залучати до обговорень ширше коло людей, включаючи тих, хто раніше не мав можливості брати участь через географічні чи соціальні бар'єри, це підвищує рівень **демократичності процесів** і сприяє розвитку громадянського суспільства, оскільки громадяни відчувають свою причетність до формування державної політики. Цей підхід також покращує якість рішень, оскільки вони ухвалюються з урахуванням думок широкої громадськості та експертів у різних галузях.

Отже, доступність інформації та активна участь громадян у прийнятті рішень є одними з ключових переваг електронного урядування. Розглянуті аспекти сприяють підвищенню рівня прозорості, демократичності та ефективності державного управління, що має позитивний вплив на розвиток суспільства в цілому.

Міжнародна інтеграція є ще однією суттєвою перевагою електронного урядування, яка сприяє ефективнішій взаємодії держав із зовнішніми партнерами та організаціями. Впровадження передових практик і технологій у галузі електронного урядування дає можливість країнам покращити свою репутацію на міжнародній арені, підвищуючи прозорість та ефективність державного управління. Цифровізація управлінських процесів сприяє більшій відкритості урядів для іноземних інвесторів і міжнародних організацій, що значно спрощує співпрацю в економічній, політичній і соціальній сферах.

Завдяки електронному урядуванню держави можуть легко інтегруватися в глобальні процеси управління та брати участь у міжнародних ініціативах з обміну інформацією та досвідом. Цифрові платформи дозволяють швидко і безперешкодно обмінюватися даними між країнами, що сприяє більш тісній співпраці у сферах боротьби з корупцією, протидії міжнародній злочинності, управління міграційними потоками та забезпечення глобальної безпеки. Завдяки

уніфікації стандартів електронного урядування, держави можуть ефективніше взаємодіяти з міжнародними фінансовими установами, торгівельними партнерами та організаціями ООН, ЄС, СОТ тощо.

Інтеграція електронного урядування також сприяє економічному розвитку. Вона дозволяє країнам брати участь у міжнародних торговельних угодах і проектах, що вимагають прозорості, надійності та швидкості обміну інформацією. Це відкриває нові можливості для залучення інвестицій і розвитку міжнародної торгівлі, оскільки інвестори віддають перевагу країнам із високим рівнем прозорості та надійним правовим середовищем. Електронне урядування також полегшує процес підписання міжнародних угод та їх подальшого виконання, що зміцнює позиції держави в глобальній економіці.

Отже, міжнародна інтеграція завдяки електронному урядуванню допомагає державам не лише підвищити ефективність співпраці з міжнародними організаціями та партнерами, але й сприяє їх успішній участі в глобальних процесах управління та економічного розвитку, це робить держави більш конкурентоспроможними на міжнародній арені та забезпечує сталість економічного зростання.

Скорочення бюрократії є ще однією із складових позитивних наслідків впровадження електронного урядування. Традиційна бюрократія вимагає великої кількості паперових документів, складних адміністративних процедур та часто призводить до затримок у прийнятті рішень. Електронне урядування дозволяє суттєво скоротити обсяг паперової роботи завдяки цифровізації документів і автоматизації процесів, це не лише знижує навантаження на державні установи, але й значно підвищує швидкість і точність обробки даних.

Одним із найважливіших аспектів скорочення бюрократії є *спрощення адміністративних процедур*. Електронні платформи забезпечують громадянам і бізнесу можливість подавати заявки, реєструвати документи та отримувати необхідні дозволи в онлайн-режимі, що усуває необхідність фізичної присутності в державних установах і значно скорочує час на виконання адміністративних дій. Це також знижує ймовірність людських помилок, оскільки багато процесів автоматизовані, що сприяє більш точній і своєчасній обробці запитів.

Для громадян і підприємств скорочення бюрократії робить *державне управління більш доступним і зручним*. Онлайн-сервіси дозволяють користувачам взаємодіяти з урядовими установами з будь-якого місця та в будь-який час, що особливо важливо для жителів віддалених регіонів та малих підприємств, які часто стикалися з

труднощами через необхідність особистої присутності в державних органах. Зниження адміністративного тягаря стимулює розвиток бізнесу, оскільки компанії можуть швидше отримувати необхідні ліцензії та дозволи, що прискорює започаткування та розвиток підприємницької діяльності.

Скорочення бюрократичних процедур також сприяє зменшенню корупції, оскільки усувається необхідність у неформальних зустрічах чи особистих контактах із державними службовцями, що традиційно створювало передумови для корупційних практик. Автоматизація процесів забезпечує прозорість і контроль на кожному етапі, зменшуючи можливість для зловживань.

Таким чином, впровадження електронного урядування призводить до значного скорочення бюрократії, роблячи державне управління не лише ефективнішим, але й більш доступним, прозорим і зручним для громадян і бізнесу, що створює умови для розвитку демократичного суспільства та економічного зростання.

Нарешті, **стійкість до криз** є однією з ключових переваг електронного урядування, яка забезпечує безперебійну роботу державних інституцій у надзвичайних ситуаціях. Використання цифрових інструментів дозволяє урядам підтримувати функціонування критичних систем навіть у разі природних катастроф, соціальних криз або інших непередбачуваних подій. Це особливо важливо в умовах, коли традиційні форми управління можуть бути паралізовані через фізичні або організаційні обмеження. Електронне урядування забезпечує доступ до ключових державних послуг, зберігання та обмін інформацією, а також підтримку комунікацій між урядом і громадянами.

Ця перевага стала надзвичайно актуальною в умовах війни в Україні, коли традиційна інфраструктура була пошкоджена або недоступна через бойові дії. В таких умовах електронні платформи стали критичним інструментом для забезпечення управління та надання послуг. Завдяки впровадженню цифрових технологій уряд України зміг продовжувати надавати адміністративні послуги, такі як реєстрація, подача документів та виплати, забезпечуючи при цьому оперативне реагування на нові виклики. Наприклад, державні системи дозволяли громадянам подавати заявки на фінансову допомогу, переміщення в безпечні регіони, а також отримувати інформацію про надзвичайні ситуації в режимі реального часу.

Більше того, електронне урядування сприяло підтримці стабільності державних інституцій, що є критично важливим у період конфліктів і криз. Уряду вдалося зберегти ефективність управління на всіх рівнях, від місцевого до національного, завдяки безперервній комунікації та координації дій через цифрові платформи. Це дозволило зменшити вплив кризи на економіку та соціальну сферу, забезпечуючи підтримку функціонування критичної інфраструктури, медичних установ і логістичних ланцюгів.

Таким чином, електронне урядування відіграє вирішальну роль у підвищенні стійкості державних інститутів до кризових ситуацій, дозволяючи державі не лише підтримувати безперервність управління, але й адаптуватися до нових викликів у надзвичайних умовах. В умовах війни в Україні цей аспект набув особливого значення, продемонструвавши можливості електронного урядування як важливого інструменту для забезпечення стабільності і безпеки держави та її громадян у найскладніші часи.

4.3. Безпека електронного урядування

Безпека електронного урядування є однією з найважливіших складових сучасних цифрових трансформацій в державному управлінні. В умовах активного розвитку інформаційних технологій та збільшення залежності від електронних систем управління, забезпечення їх безпеки стає критичним для збереження цілісності державних інститутів, захисту персональних даних громадян і запобігання кібератакам. Надійність та безпека електронних сервісів безпосередньо впливають на рівень довіри громадян до органів влади, а також на ефективність роботи державних установ. У цьому контексті важливим завданням є створення ефективних механізмів для захисту електронного середовища від потенційних загроз, забезпечення конфіденційності, доступності та цілісності інформації, а також підвищення рівня кіберзахисту в державному секторі.

Загрози для електронного урядування становлять виклики для державних органів, які відповідають за забезпечення безпеки та ефективності цифрових сервісів. В умовах стрімкого розвитку інформаційних технологій та зростання залежності від електронних систем управління, важливо розуміти, які саме небезпеки можуть вплинути на цілісність та конфіденційність інформації. Своєчасне виявлення та розуміння основних загроз дозволяє вжити ефективних

заходів для їх попередження та зменшення ризиків. В табл. 4.3 представлені основні загрози для електронного врядування, їх опис та можливі наслідки для державних інститутів і громадян.

Таблиця 4.3

Основні загрози для електронного врядування

Загроза	Опис	Можливі наслідки
Кіберзлочинність	Незаконні дії, здійснені через Інтернет (фішинг, віруси, атаки типу «відмова в обслуговуванні» тощо).	Втрата або пошкодження даних, фінансові збитки, порушення роботи системи.
Несанкціонований доступ до даних	Проникнення в інформаційні системи державних установ з метою отримання доступу до конфіденційної інформації.	Викрадення особистих даних, витік конфіденційної інформації, порушення прав громадян.
Вразливості в програмному забезпеченні	Помилки в коді або слабкості в системах, які можуть бути використані хакерами для злому системи.	Уразливість до атак, втручання в роботу систем, компрометація даних.
Втрата або знищення даних	Невипадкове або навмисне видалення, пошкодження даних у системах електронного врядування.	Втрата важливої інформації, відновлення після інциденту, порушення надання послуг.
Інсайдерські загрози	Небезпечні або шахрайські дії з боку співробітників організацій, які мають доступ до систем.	Зловживання правами доступу, витік інформації, саботаж.
Кібертероризм	Використання інформаційних технологій для дестабілізації державних інститутів або порушення нормальної діяльності.	Порушення функціонування критичних інфраструктур, загроза національній безпеці.
Фізичні загрози інфраструктурі	Пошкодження або руйнування серверів, мережевого обладнання через стихійні лиха, технічні збої або терористичні акти.	Знищення або пошкодження даних, припинення роботи сервісів.
Загроза від соціальної інженерії	Маніпулювання людьми для отримання доступу до важливої інформації або систем.	Витік конфіденційної інформації, несанкціонований доступ до систем.
Атаки типу «відмова в обслуговуванні» (DDoS)	Атаки, що перевантажують систему з метою її блокування чи недоступності для користувачів.	Зупинка або сповільнення роботи системи, недоступність онлайн-послуг.

Безпека електронного врядування є однією з основних умов ефективного функціонування сучасної держави, оскільки від її забезпечення залежить не лише цілісність інформації, але й рівень довіри громадян до державних органів та інститутів. Зважаючи на технологічний прогрес, зростає кількість загроз, здатних серйозно вплинути на стабільність електронних систем управління. Аналіз основних загроз дозволяє визначити найбільш критичні фактори ризику, які потребують термінового вирішення для захисту інформаційних ресурсів та інфраструктури.

Однією з головних загроз є кіберзлочинність, яка охоплює широкий спектр злочинних дій, таких як фішинг, вірусні атаки, хакерські вторгнення. Вони можуть призвести до значних фінансових втрат, знищення або викрадення даних, а також до порушення нормального функціонування систем. Кіберзлочинці постійно вдосконалюють свої методи, що робить боротьбу з цими загрозами особливо складною. Урахування цих викликів вимагає постійного вдосконалення захисних заходів, таких як використання новітніх антивірусних програм, систем виявлення вторгнень і забезпечення моніторингу безпеки в реальному часі.

Несанкціонований доступ до даних є ще однією серйозною загрозою, особливо в контексті обробки персональних і конфіденційних даних громадян. Така загроза може виникнути як в результаті зовнішніх атак, так і через зловживання з боку співробітників організацій. Для мінімізації цього ризику необхідно розробляти та впроваджувати жорсткі політики доступу, забезпечення конфіденційності та використання високоякісного шифрування даних, що дозволяє обмежити доступ лише авторизованим користувачам.

Крім того, важливим є виявлення вразливостей у програмному забезпеченні. Програмні продукти, які використовуються для управління інформаційними системами, можуть містити помилки або слабкі місця, що можуть бути використані зловмисниками для здійснення атак. Ці вразливості можуть стати джерелом серйозних порушень у роботі системи. Тому важливо проводити регулярні оновлення програмного забезпечення, тестування на вразливості та аудит систем безпеки.

Атаки типу «відмова в обслуговуванні» (DDoS) також становлять значну загрозу для електронного врядування. Такі атаки спричиняють перевантаження серверів та інфраструктури, що призводить до тимчасової недоступності електронних послуг для користувачів.

Враховуючи зростаючу популярність онлайн-сервісів, критичними стають методи захисту від таких атак, включаючи використання спеціалізованих мереж для балансування навантаження та систем фільтрації трафіку.

Однією з найбільш важливих складових ефективної безпеки є запобігання інсайдерським загрозам. Загроза, що виникає зсередини організації, є не менш серйозною, оскільки вона часто пов'язана з використанням довірених ресурсів для незаконних цілей. Тому особлива увага має бути приділена моніторингу поведінки користувачів, обмеженню прав доступу, а також постійному навчанню співробітників про можливі загрози та способи їх уникнення.

Врахування цих загроз є необхідним для створення комплексної системи безпеки електронного врядування, яка б ефективно протидіяла наявним ризикам і забезпечувала захист як державних структур, так і інтересів громадян. Це вимагає постійної адаптації до змін у технологічному середовищі та взаємодії з міжнародними організаціями для обміну досвідом та вдосконалення методів захисту.

Забезпечення безпеки в електронному врядуванні є ключовим елементом для ефективного функціонування державних органів та інститутів у цифровому середовищі. В умовах зростаючої кіберзагрози та постійно змінюваного технологічного ландшафту, держави повинні впроваджувати комплексні та ефективні методи захисту, щоб забезпечити стабільність і безпеку своїх інформаційних систем. Для цього необхідно створювати національні стратегії кібербезпеки, впроваджувати відповідні стандарти та законодавчі ініціативи, а також сприяти розвитку технологій, здатних захистити важливі інфраструктури та персональні дані громадян. У цьому контексті важливо розглянути основні методи, які використовуються на рівні держави для забезпечення безпеки електронного врядування, адже тільки так можна ефективно протидіяти сучасним кіберзагрозам і забезпечити довіру громадян до державних установ.

На рис. 4.1 представлено методи забезпечення безпеки електронного врядування на рівні держави.

Національна система кібербезпеки є основою для забезпечення безпеки інформаційних технологій і даних на рівні держави. Її завдання полягає в створенні та підтримці центральної організації, яка здійснює координацію всіх заходів з кібербезпеки на державному рівні. Оскільки цифрові технології стали невід'ємною частиною роботи всіх державних інститутів, а також для забезпечення стабільного функціонування

економіки, енергетики, транспорту та інших важливих секторів, необхідно створити ефективну систему захисту від різноманітних кіберзагроз.

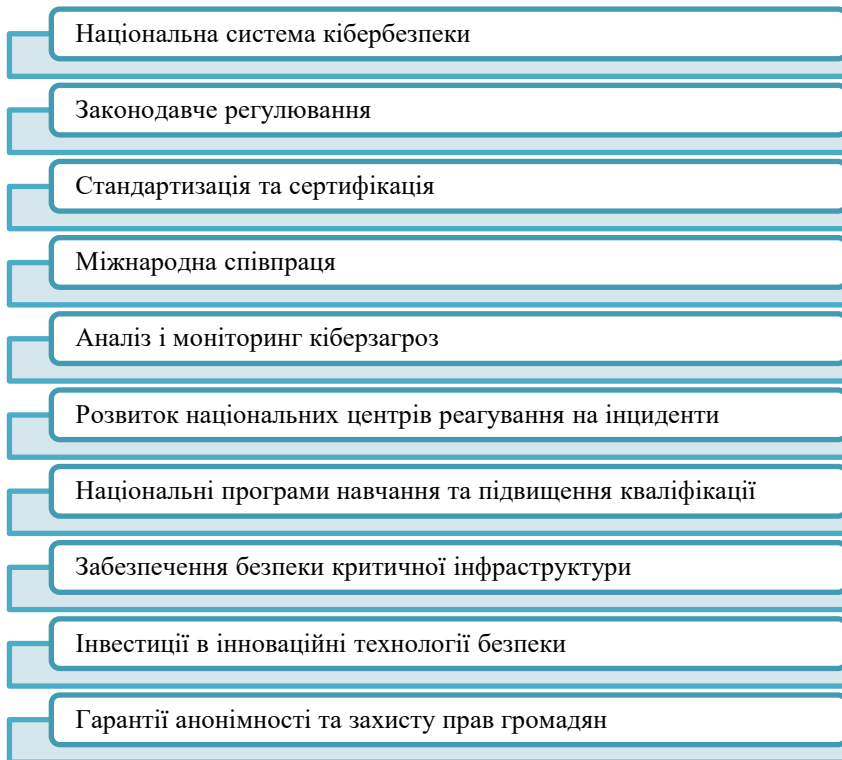


Рис. 4.1. Методи забезпечення безпеки електронного врядування на рівні держави

Центральна організація з кібербезпеки повинна виконувати роль координатора національних зусиль для боротьби з кіберзлочинністю, захисту інформаційних систем і критичної інфраструктури країни. Вона повинна мати повноваження для встановлення стандартів безпеки, розробки стратегій реагування на кіберінциденти, а також для моніторингу поточної ситуації в кіберпросторі. Це дозволить не тільки оперативно реагувати на наявні загрози, а й прогнозувати можливі ризики, що виникають унаслідок розвитку технологій і змін в глобальній кіберсфері. Стратегії та стандарти, визначені такою організацією, мають охоплювати всі аспекти кібербезпеки – від захисту

даних громадян і конфіденційної інформації до збереження цілісності державних інформаційних систем. Це важливо не лише для безперебійної роботи державних органів, а й для підтримки національної безпеки. Створення чітких, уніфікованих правил і стандартів забезпечить не тільки належний рівень захисту, але й полегшить інтеграцію нових технологій в інфраструктуру країни.

Крім того, національна система кібербезпеки повинна включати механізми співпраці між різними державними установами, а також між державами на міжнародному рівні. Враховуючи глобальний характер кіберзагроз, важливо, щоб національні стратегії кібербезпеки синхронізувалися з міжнародними ініціативами та стандартами. Це дозволить швидко реагувати на загрози, які можуть мати міжнародний характер, а також ефективно обмінюватися інформацією та досвідом з іншими країнами.

Одним із важливих аспектів національної системи кібербезпеки є забезпечення захисту критичної інфраструктури. До цієї інфраструктури належать енергетичні, транспортні, фінансові та інші системи, що мають важливе значення для функціонування держави та її економіки. Уразливість цих систем перед кіберзагрозами може призвести до серйозних наслідків, включаючи збої у наданні основних послуг населенню та економіці, а також порушення національної безпеки. Тому створення ефективних заходів для захисту цих критичних секторів є ключовим завданням національної системи кібербезпеки.

В результаті, національна система кібербезпеки повинна бути складною та багаторівневою структурою, що охоплює не тільки технічні засоби захисту, а й організаційні заходи, стандарти, стратегії та міжнародну співпрацю. Лише завдяки такому комплексному підходу можна забезпечити надійний захист від сучасних кіберзагроз та забезпечити стабільність і безпеку країни в цифрову епоху.

Законодавче регулювання є критично важливою складовою системи кібербезпеки на рівні держави. Це процес, що включає розробку, прийняття та постійне оновлення законів і нормативно-правових актів, які забезпечують належний рівень захисту цифрової інфраструктури, персональних даних громадян та запобігають кіберзлочинності. Враховуючи швидкий розвиток інформаційних технологій і глобалізацію цифрових загроз, постійне вдосконалення законодавчої бази є необхідним для забезпечення ефективної протидії кіберзагрозам.

Основним завданням законодавчого регулювання є створення правової основи для захисту від кіберзлочинності. Закони повинні визначати, що таке кіберзлочинність, які її види, а також передбачати відповідальність за порушення правил користування електронними системами та зловживання інформацією. Зважаючи на природу цифрових технологій, важливо, щоб закони охоплювали не лише традиційні форми злочинів, такі як шахрайство чи крадіжка даних, а й нові загрози, як-от кібертероризм або атаки на критичну інфраструктуру.

Захист персональних даних є ще однією важливою складовою законодавчого регулювання. У сучасному світі, де інформація стає одним із основних активів, захист особистих даних громадян стає пріоритетним завданням для держави. Закони повинні встановлювати чіткі правила щодо збору, зберігання, обробки та передачі персональних даних, а також визначати права громадян щодо контролю за своїми даними. Для цього необхідно впроваджувати жорсткі вимоги до організацій, які збирають або обробляють персональні дані, та створювати механізми для нагляду за їх виконанням.

Одним із важливих аспектів є визначення відповідальності за порушення безпеки в електронному середовищі. Законодавство повинно чітко прописувати наслідки для осіб, які вчиняють кіберзлочини або не дотримуються норм безпеки в електронних системах. Це включає кримінальну відповідальність за кібератаки, доступ до конфіденційної інформації без дозволу, а також за недотримання стандартів захисту інформації. Крім того, необхідно передбачити адміністративну та цивільну відповідальність для організацій, що порушують вимоги щодо безпеки даних або не вживають належних заходів для захисту своїх систем від кіберзагроз.

Законодавче регулювання також має сприяти створенню єдиного правового простору для міжнародної співпраці в боротьбі з кіберзлочинністю. Оскільки кіберзлочини часто носять транснаціональний характер, важливо, щоб законодавство забезпечувало механізми для екстрадиції злочинців, обміну інформацією між країнами та спільної боротьби з кіберзагрозами. Це дозволить ефективно реагувати на глобальні виклики і забезпечити справедливість у боротьбі з кіберзлочинністю.

Таким чином, законодавче регулювання в сфері кібербезпеки є основою для забезпечення правового захисту як громадян, так і державних установ від кіберзагроз. Це дозволяє формувати надійну

правову основу для боротьби з кіберзлочинністю, захисту персональних даних і забезпечення безпеки в електронному середовищі. Постійне вдосконалення законодавчої бази є необхідною умовою для успішного розвитку цифрового простору та забезпечення кібербезпеки в сучасному світі.

Стандартизація та сертифікація є важливими складовими забезпечення кібербезпеки на національному рівні. У сучасному цифровому середовищі, де інформаційні системи займають ключове місце в діяльності державних органів та бізнесу, створення єдиних стандартів безпеки та впровадження системи сертифікації є необхідною умовою для ефективного захисту інформації. Стандартизація визначає єдині вимоги та норми для безпеки інформаційних систем, забезпечуючи їх відповідність міжнародним та національним стандартам, а сертифікація служить механізмом підтвердження того, що ці вимоги виконуються.

Розробка національних стандартів безпеки для інформаційних систем є важливим етапом у створенні системи кіберзахисту в країні. Стандарти безпеки визначають чіткі правила та критерії для побудови, експлуатації та захисту інформаційних систем. Це включає в себе вимоги до архітектури систем, захисту даних, а також до програмного та апаратного забезпечення, що використовується в цих системах. Встановлення таких стандартів дозволяє забезпечити узгодженість дій усіх учасників процесу – від державних органів до приватних компаній, що використовують або надають інформаційні послуги.

Один із основних аспектів стандартизації полягає в забезпеченні відповідності інформаційних систем міжнародним стандартам. Це дозволяє не лише забезпечити високий рівень захисту, але й інтегрувати національні системи в глобальний цифровий простір, що є важливим для розвитку міжнародної торгівлі, співпраці в сфері науки та технологій, а також для боротьби з транснаціональними кіберзагрозами.

Сертифікація є процесом підтвердження відповідності інформаційної системи національним або міжнародним стандартам безпеки. Це важливий інструмент, що дозволяє перевірити, чи виконуються встановлені вимоги до захисту інформації. Процес сертифікації включає в себе тестування і аудит систем, перевірку їх вразливостей, а також оцінку рівня захисту даних. Важливо, що сертифікація не є одноразовою процедурою – вона повинна проводитися регулярно для перевірки, чи відповідають системи

актуальним вимогам та стандартам, оскільки кіберзагрози постійно еволюціонують.

Забезпечення відповідності вимогам щодо захисту інформації через стандартизацію та сертифікацію дає низку переваг. По–перше, це сприяє підвищенню рівня довіри з боку громадян та міжнародних партнерів, адже сертифікація гарантує, що організації дотримуються високих стандартів безпеки. По–друге, це дозволяє знижувати ризики кіберінцидентів, пов'язаних з уразливостями в системах, що не відповідають встановленим вимогам. І, по–третє, стандартизація допомагає уникати дублювання зусиль і забезпечує ефективне використання ресурсів при розробці та впровадженні заходів з кіберзахисту.

У результаті, стандартизація та сертифікація не лише підвищують рівень безпеки в електронному середовищі, а й сприяють розвитку ефективної та надійної інфраструктури для захисту інформації в країні. Це забезпечує не тільки захист державних та приватних інформаційних систем, але й допомагає створювати стабільне і безпечне цифрове середовище для розвитку економіки, науки та технологій.

Міжнародна співпраця в галузі кібербезпеки є важливим аспектом сучасної боротьби з кіберзагрозами та кіберзлочинністю, оскільки кіберпорушення не обмежуються кордонами окремих країн. Ураховуючи глобальний характер цифрових загроз, ефективна протидія їм вимагає тісної взаємодії між державами, міжнародними організаціями та приватними підприємствами. Участь у міжнародних ініціативах і угодах щодо кібербезпеки є необхідною для забезпечення глобальної безпеки та ефективного реагування на кіберзагрози, що постійно змінюються.

Одним із основних напрямків міжнародної співпраці є участь у міжнародних угодах і ініціативах, які спрямовані на боротьбу з кіберзлочинністю. Такі угоди забезпечують створення єдиних стандартів і принципів для боротьби з кіберзлочинцями, дозволяють країнам узгоджувати свої зусилля, а також обмінюватися інформацією про потенційні загрози та методи боротьби з ними. Прикладом таких угод є Конвенція про кіберзлочинність, яка визначає спільні правила для країн щодо боротьби з кіберзлочинністю і обміну доказами між країнами. Подібні угоди забезпечують юридичну основу для міжнародної співпраці в сфері кібербезпеки та створюють умови для ефективного реагування на кіберзагрози.

Обмін досвідом є ще одним важливим аспектом міжнародної співпраці. Оскільки кіберзагрози постійно еволюціонують, обмін інформацією та кращими практиками між країнами дозволяє швидко адаптувати стратегії захисту та запобігання атакам. Участь у міжнародних форумах, конференціях та робочих групах дає можливість державам і організаціям зібрати інформацію про новітні загрози, обговорити ефективні методи їх подолання та обмінятися досвідом у сфері кібербезпеки. Зокрема, міжнародні організації, як—от Інтерпол або Європейська агенція з кібербезпеки (ENISA), активно підтримують такі ініціативи, надаючи платформу для обміну знаннями і розвитком спільних підходів до кібербезпеки.

Спільна боротьба з глобальними кіберзагрозами та кіберзлочинністю також включає в себе створення спільних механізмів реагування на великомасштабні кіберінциденти. Це може бути як обмін інформацією про виявлені уразливості в системах, так і спільні дії з нейтралізації кіберзагроз, таких як атаки на критичну інфраструктуру або поширення шкідливого програмного забезпечення. Важливою частиною міжнародної співпраці є спільні навчання та тренування з реагування на кіберінциденти, які дозволяють країнам розробляти та вдосконалювати методи колективного реагування та відновлення після атак.

Крім того, міжнародна співпраця у сфері кібербезпеки має важливе значення для підвищення рівня довіри між країнами та зниження ризику політичних і економічних наслідків, пов'язаних з кібернападами. Це особливо актуально в умовах геополітичних конфліктів, коли кіберзагрози можуть бути використані як інструмент тиску або дестабілізації. Міжнародна співпраця дозволяє створити механізми для ефективного реагування на такі загрози та знижує ймовірність ескалації конфліктів через кібернапади.

Таким чином, міжнародна співпраця в сфері кібербезпеки є необхідною умовою для успішної боротьби з глобальними кіберзагрозами. Вона дозволяє країнам об'єднати зусилля, обмінюватися досвідом, створювати єдині стандарти та механізми реагування, що в свою чергу сприяє зміцненню глобальної безпеки в цифровому просторі.

Аналіз і моніторинг кіберзагроз є важливою складовою частиною системи національної кібербезпеки, оскільки дає змогу своєчасно виявляти потенційні загрози, розуміти їх природу і швидко реагувати на них. Оскільки цифрові технології розвиваються стрімко,

з'являються нові уразливості в інформаційних системах, а кіберзлочинці постійно удосконалюють свої методи, регулярний моніторинг кіберзагроз є необхідністю для забезпечення стабільності й безпеки національних інформаційних систем.

Розбудова інфраструктури для моніторингу кіберзагроз повинна передбачати створення централізованої платформи або системи, яка дозволяє здійснювати постійний нагляд за станом кібербезпеки на рівні держави. Такі системи повинні включати засоби для збору та аналізу даних з різних джерел: від інформаційних систем державних органів до комунікаційних мереж та критичної інфраструктури. Важливим аспектом є використання спеціалізованих інструментів для виявлення аномальних або підозрілих дій, що можуть свідчити про кібератаку чи спроби несанкціонованого доступу до систем.

Моніторинг кіберзагроз включає в себе кілька ключових етапів: виявлення вразливостей, аналіз інцидентів і оперативне реагування на нові загрози. Виявлення вразливостей є процесом, при якому постійно проводяться перевірки інформаційних систем на наявність слабких місць, які можуть бути використані зловмисниками. Це може бути як автоматичне сканування систем на наявність відомих уразливостей, так і оцінка нових загроз, що виникають у зв'язку з технологічними змінами або розвитком кіберзлочинності.

Аналіз інцидентів є важливою частиною цього процесу. Коли кіберінцидент, як—от кібератака, вже стався, необхідно швидко і ефективно провести його розслідування, з'ясувати, яким чином була порушена безпека, які саме дані були зкомпрометовані або пошкоджені, а також оцінити масштаби впливу інциденту. Цей етап дозволяє не лише мінімізувати негативні наслідки для організацій, а й забезпечити надійне відновлення систем після інциденту.

Оперативне реагування на нові загрози є наступним важливим етапом. Оскільки кіберзагрози постійно змінюються, необхідно мати гнучку та швидку систему реагування, яка дозволить оперативно впроваджувати заходи для нейтралізації загроз. Це може включати автоматичне блокування шкідливих дій у реальному часі, оновлення програмного забезпечення для усунення виявлених вразливостей, а також координацію дій між різними органами влади, правоохоронними органами та іншими зацікавленими сторонами.

Розбудова такої інфраструктури має на увазі також забезпечення комплексного моніторингу всіх аспектів інформаційної безпеки в державі. Це дозволяє не лише своєчасно виявляти загрози, але й

прогнозувати їх на майбутнє, вживаючи необхідних превентивних заходів. Моніторинг також допомагає оцінювати ефективність існуючих заходів безпеки, що дає змогу своєчасно коригувати стратегії захисту.

Важливою складовою є міжнародне співробітництво в рамках моніторингу кіберзагроз. Оскільки кіберзлочинність є глобальною проблемою, країни повинні обмінюватися інформацією про нові загрози, уразливості та методи боротьби з ними. Спільна робота з міжнародними організаціями та партнерами дозволяє забезпечити більш широкий захист і реагування на кіберзагрози.

Отже, аналіз і моніторинг кіберзагроз є невід’ємною частиною стратегії національної кібербезпеки, що забезпечує не лише виявлення і нейтралізацію загроз, а й допомагає формувати ефективну політику захисту від кіберзлочинності. У сучасному цифровому середовищі важливо постійно вдосконалювати інфраструктуру для моніторингу, щоб бути готовими до нових викликів і забезпечити стабільний захист національних інформаційних систем.

Розвиток національних центрів реагування на інциденти є одним із елементом стратегії кібербезпеки для забезпечення швидкої та ефективної протидії кіберзагрозам, які можуть поставити під загрозу державні установи та критичну інфраструктуру країни. Такі центри виконують важливу роль у системі кіберзахисту, оскільки вони спеціалізуються на виявленні, аналізі та ліквідації наслідків кіберінцидентів, що дозволяє оперативно реагувати на будь-які загрози, пов’язані з інформаційною безпекою.

Основною метою створення національних центрів реагування є забезпечення централізованої координації всіх дій з боротьби з кіберінцидентами. Центри мають забезпечити постійний моніторинг інформаційних систем, що дає змогу виявляти аномальні активності, які можуть свідчити про кібератаки або спроби несанкціонованого доступу. Оскільки кіберзагрози часто мають невизначений характер і можуть виникнути в будь-який час, національні центри повинні бути оснащені найсучаснішими технологіями для виявлення, швидкого реагування і зменшення негативних наслідків від кіберінцидентів.

Ключовими функціями таких центрів є:

1. ***Виявлення кіберзагроз.*** Центри повинні мати системи, які дозволяють автоматично виявляти аномальні або підозрілі дії в державних та приватних інформаційних системах. Це можуть бути спроби вторгнення, виявлення вірусів, шкідливого програмного

забезпечення або іншої небажаної активності в системах, що можуть загрожувати безпеці.

2. *Аналіз інцидентів.* Після виявлення загрози центри мають здійснити ретельний аналіз інциденту для з'ясування його природи, масштабу та можливих наслідків. Це включає ідентифікацію вразливостей, шляхів проникнення зловмисників, а також оцінку того, які саме дані були зкомпрометовані або пошкоджені.

3. *Оперативне реагування.* Після аналізу інциденту важливо забезпечити швидке реагування на загрозу. Це може включати тимчасове відключення уражених систем для мінімізації збитків, блокування атакуючих IP-адрес або доменів, застосування оновлень для усунення виявлених вразливостей, а також відновлення даних і нормалізацію роботи систем.

4. *Ліквідація наслідків.* Після вжиття заходів для нейтралізації загрози наступним кроком є відновлення інформаційних систем до нормального робочого стану. Це також включає в себе проведення комплексного аудиту системи для переконання в тому, що інцидент не призвів до пошкодження важливих даних або несанкціонованого доступу до інформації.

5. *Підготовка звітності та обмін інформацією.* Національні центри повинні не тільки реагувати на інциденти, але й збирати інформацію про їх характеристики, типи загроз і методи боротьби з ними. Ці дані використовуються для покращення стратегії кіберзахисту, а також для обміну досвідом з іншими країнами та міжнародними організаціями.

Важливим аспектом розвитку національних центрів реагування є забезпечення їх інтеграції з іншими органами державного управління, правоохоронними структурами та критичними інфраструктурами. Центри мають працювати в тісній взаємодії з іншими підрозділами, щоб ефективно координувати дії та мінімізувати потенційні загрози для національної безпеки. Крім того, центри повинні мати доступ до міжнародних ресурсів і баз даних, що дозволяє швидко обмінюватися інформацією про нові кіберзагрози та методи боротьби з ними.

Розвиток таких центрів є необхідною умовою для захисту критичних інфраструктур, таких як енергетичні мережі, фінансові системи, транспортні шляхи та інші важливі сектори, що становлять основу економіки країни. Оскільки загрози з кіберпростору можуть мати серйозні наслідки не тільки для окремих установ, але й для всього

суспільства, національні центри реагування є важливим елементом загальної стратегії кібербезпеки на рівні держави.

Таким чином, створення та розвиток національних центрів реагування на інциденти дозволяє забезпечити ефективний захист інформаційних систем від кіберзагроз, швидко ідентифікувати потенційні атаки, мінімізувати їх наслідки та забезпечити безперебійне функціонування критичної інфраструктури країни.

Національні програми навчання та підвищення кваліфікації є невід’ємною складовою системи кібербезпеки країни, оскільки вони сприяють підвищенню обізнаності та кваліфікації не лише серед державних службовців, а й серед широкого кола спеціалістів у сфері кібербезпеки, а також серед населення. Враховуючи постійну еволюцію кіберзагроз та зростаючу залежність від цифрових технологій, необхідність в підготовці та освіті стає ще більш очевидною.

Розробка освітніх програм для державних службовців та спеціалістів у сфері кібербезпеки є однією з основних задач для забезпечення належного рівня захисту інформаційних систем державних органів і критичної інфраструктури. Спеціалісти повинні мати глибокі знання з технічних аспектів кібербезпеки, включаючи виявлення загроз, їх аналіз та реагування на кіберінциденти. Однак знання повинні охоплювати також і управлінські аспекти, такі як розробка політик безпеки, управління ризиками, стратегічне планування у сфері кібербезпеки, а також ефективна взаємодія з іншими державними органами та міжнародними партнерами.

В рамках освітніх програм для державних службовців особливу увагу слід приділити вивченню міжнародних стандартів і норм кібербезпеки, а також правових аспектів, пов’язаних із захистом персональних даних та боротьбою з кіберзлочинністю. Такі програми повинні включати як теоретичні знання, так і практичні навички, що дозволяють швидко реагувати на кіберзагрози та ефективно вживати заходи для захисту державних інформаційних систем.

Особлива увага повинна приділятися підготовці населення до ризиків в онлайн-середовищі, адже кіберзагрози не лише впливають на державні органи чи бізнес, але й можуть завдати шкоди кожному користувачеві Інтернету. Програми навчання для громадян повинні включати основи кіберграмотності, знання про те, як захищати свою особисту інформацію, як виявляти фішингові атаки, уникати шкідливих програм та вживати заходів для безпеки під час

використання інтернет–сервісів. Кожен користувач повинен розуміти важливість паролів, двофакторної аутентифікації та інших засобів захисту для забезпечення власної безпеки в мережі.

Програми підвищення кваліфікації повинні включати регулярні тренінги та курси для підтримки знань на актуальному рівні. Оскільки кіберзагрози постійно змінюються, важливо, щоб державні службовці та спеціалісти з кібербезпеки мали можливість освоювати новітні методи і технології захисту інформаційних систем. Підвищення кваліфікації через семінари, вебінари та інші форми навчання допомагає постійно оновлювати знання про нові інструменти, техніки і стратегії боротьби з кіберзлочинністю.

Забезпечення освітніх ініціатив у сфері кібербезпеки на національному рівні не лише підвищує рівень обізнаності серед усіх категорій населення, а й створює здорове кіберсередовище, де кожен, від державного службовця до простого користувача, усвідомлює важливість дотримання норм безпеки в онлайн–просторі. Це, в свою чергу, дозволяє значно знизити кількість кіберінцидентів та ефективно протидіяти потенційним загрозам.

Важливим аспектом є також співпраця з міжнародними організаціями для обміну знаннями та досвідом у сфері кіберосвіти. Це дозволяє адаптувати національні програми до міжнародних стандартів і забезпечити найкращі практики для ефективного навчання та підвищення кваліфікації в галузі кібербезпеки.

Таким чином, національні програми навчання та підвищення кваліфікації є необхідною умовою для розвитку ефективної системи кібербезпеки, забезпечення захисту інформаційних ресурсів і створення свідомого та захищеного цифрового середовища на рівні держави.

Забезпечення безпеки критичної інфраструктури є однією з найбільш важливих складових національної кібербезпеки, оскільки це захист тих систем і ресурсів, які є основою для стабільного функціонування держави та її економіки. Критична інфраструктура включає в себе різноманітні об'єкти та мережі, які забезпечують життєдіяльність держави, серед яких енергетичні, транспортні, фінансові, водні, телекомунікаційні та інші системи. У разі порушення їхньої роботи можуть виникнути серйозні наслідки як для безпеки країни, так і для її економічної стабільності.

Одним із основних аспектів забезпечення безпеки критичної інфраструктури є її кіберзахист. Сучасні енергетичні та транспортні

системи, фінансові установи, а також інші ключові сектори економіки все більше залежать від інформаційних технологій, що збільшує їх уразливість перед кібератаками. Наприклад, хакери можуть здійснити атаки на енергетичні мережі, зупинити постачання електроенергії, чи здійснити кібератаки на фінансові установи, що призведе до краху банківської системи. Тому важливо створювати захищені інформаційні системи та інфраструктуру для кожної з цих сфер.

Ідентифікація та захист уразливих точок в критичній інфраструктурі є важливим етапом у забезпеченні її безпеки. Відповідні заходи повинні включати у себе захист від атак, які можуть бути спрямовані на ключові елементи інфраструктури, такі як енергетичні станції, транспортні вузли, фінансові системи та інші важливі об'єкти. Ризики включають не лише кібератаки, а й фізичні загрози, такі як природні катастрофи чи терористичні акти. Для цього необхідно постійно моніторити стан безпеки та проводити регулярні оцінки ризиків для виявлення потенційних уразливих місць і розробки відповідних стратегій захисту.

Найважливішою частиною забезпечення безпеки є розробка планів реагування на інциденти, що дозволяють ефективно і швидко реагувати на будь-які порушення в роботі критичної інфраструктури. Це включає в себе визначення процедур для відновлення роботи після атаки чи іншого інциденту, а також готовність організацій до швидкого відновлення нормальної діяльності. Наявність таких планів дає змогу знизити час, необхідний для ліквідації наслідків інцидентів, і скоротити економічні збитки.

Забезпечення безпеки критичної інфраструктури також включає розробку і впровадження національних стандартів та вимог щодо безпеки. Ці стандарти повинні стосуватися не лише технічних аспектів, таких як захист інформаційних систем, але й організаційних заходів, включаючи навчання персоналу, створення відповідних органів для моніторингу та контролю за безпекою, а також постійну оцінку та вдосконалення існуючих заходів безпеки. Підтримка високих стандартів захисту допомагає забезпечити стабільність критичної інфраструктури та знижує ризики від можливих загроз.

Ще одним важливим аспектом є міжнародне співробітництво в сфері кібербезпеки критичної інфраструктури. Оскільки загрози можуть носити транснаціональний характер, співпраця між державами дозволяє ефективно обмінюватися інформацією та реагувати на глобальні кіберзагрози. Міжнародні ініціативи, такі як співпраця в

рамках Організації Об'єднаних Націй, Європейського Союзу чи інших міжнародних структур, можуть допомогти у створенні спільних стандартів та політик щодо безпеки критичних інфраструктур.

Забезпечення безпеки критичної інфраструктури є складним і багатогранним процесом, що вимагає як технічних, так і організаційних заходів. Важливо, щоб держави активно працювали над удосконаленням своїх систем захисту, відповідно до нових загроз та викликів, адже саме від стану безпеки цих ключових об'єктів залежить стабільність і безпека всієї країни.

Інвестиції в інноваційні технології безпеки є критичним напрямом для забезпечення ефективного захисту інформаційних систем і критичної інфраструктури в умовах сучасних кіберзагроз. Сучасні загрози, які постійно еволюціонують, вимагають використання найновіших технологій для боротьби з кіберзлочинністю, атакою на інформаційні системи та іншими кібернебезпеками. Впровадження інноваційних технологій дозволяє підвищити рівень кіберзахисту, забезпечити більшу швидкість реагування на загрози і зменшити вразливість до атак.

Однією з найперспективніших технологій є штучний інтелект (ШІ). Завдяки здатності ШІ до обробки великих обсягів даних та виявлення закономірностей, ця технологія дозволяє автоматизувати процеси виявлення загроз, аналізу поведінки користувачів, а також швидкого реагування на кіберінциденти. Штучний інтелект може забезпечити ефективний моніторинг мереж, виявлення аномальних активностей, що може свідчити про кібератаки, а також реалізувати механізми для автоматичного блокування шкідливої діяльності. Інвестиції в розробку та впровадження систем штучного інтелекту для кібербезпеки дозволяють значно знизити людський фактор і підвищити швидкість виявлення та нейтралізації загроз.

Машинне навчання є ще однією інноваційною технологією, яка має величезний потенціал для підвищення рівня кібербезпеки. Використовуючи алгоритми машинного навчання, системи можуть аналізувати та запам'ятовувати дані про попередні кіберзагрози і на їх основі розпізнавати нові аномалії в системах. Це дозволяє створювати адаптивні системи безпеки, які здатні ефективно реагувати на нові й невідомі загрози. Машинне навчання допомагає не лише виявляти атакуючі дії, але й передбачати можливі загрози, що дозволяє організаціям проактивно реагувати та запобігати інцидентам.

Блокчейн – це ще одна технологія, яка може значно посилити безпеку в цифровому середовищі. Завдяки своїй дистрибутивній природі і здатності забезпечувати прозорість та незмінність даних, блокчейн може використовуватися для захисту від атак, зокрема у фінансовому секторі. Блокчейн дозволяє забезпечити надійний захист транзакцій, а також створювати безпечні реєстри для зберігання важливих даних, таких як особисті дані громадян або дані про транзакції в банках. Впровадження блокчейн-технологій в державні та приватні інфраструктури дає можливість підвищити рівень захисту інформації, що обробляється.

Інвестиції в ці інноваційні технології безпеки допомагають створити не лише більш захищене цифрове середовище, а й ефективно протидіяти новим видам кіберзагроз, зокрема таким, що вимагають використання складних аналітичних методів для виявлення. Технології ШІ та машинного навчання дозволяють не лише оперативно реагувати на загрози, але й прогнозувати їх появу, що значно знижує ризики. Водночас блокчейн створює додатковий рівень захисту даних і транзакцій, що особливо важливо для сфер, де безпека є пріоритетом.

Крім того, інвестиції в ці технології сприяють розвитку національної кіберінфраструктури, забезпечуючи підвищення рівня захисту як на рівні державних установ, так і на рівні приватних організацій. Враховуючи глобальну природу кіберзагроз, такі інвестиції також створюють можливості для міжнародного співробітництва, обміну знаннями та досвідом у сфері кібербезпеки.

Отже, розвиток і впровадження інноваційних технологій у сфері кібербезпеки є важливим кроком для забезпечення надійного захисту критичної інфраструктури та даних, знижуючи вразливість до атак і покращуючи здатність держави і бізнесу швидко реагувати на нові виклики. Інвестиції в ці технології не тільки сприяють розвитку цифрової економіки, а й допомагають забезпечити національну безпеку в умовах сучасних глобальних загроз.

Гарантії анонімності та захисту прав громадян у цифровому середовищі є основою для забезпечення довіри до електронного врядування та розвитку цифрових послуг. У світі, де все більше даних передаються через Інтернет, важливо забезпечити, щоб особиста інформація громадян була належним чином захищена, а їх права на приватність не порушувались. Це стає ще більш важливим в контексті електронної взаємодії з органами влади, оскільки зростає кількість державних послуг, які надаються через онлайн-платформи.

Одним із основних завдань є забезпечення законодавчих гарантій приватності. Для цього країни повинні розробляти та впроваджувати закони, що регулюють захист персональних даних громадян та обмежують можливості їх несанкціонованого збору, зберігання і обробки. Зокрема, важливим є прийняття законів, що регулюють захист персональних даних, визначають права громадян на доступ до своїх даних, а також встановлюють обов'язки органів влади щодо забезпечення їх конфіденційності. Одним з таких прикладів є Загальний регламент захисту даних (GDPR) в Європейському Союзі, який став моделлю для багатьох країн щодо захисту особистої інформації.

Технічні заходи також відіграють важливу роль у забезпеченні гарантій анонімності. Використання захищених каналів комунікації є необхідною умовою для гарантування конфіденційності даних під час електронної взаємодії між громадянами та органами влади. Шифрування даних, використання протоколів HTTPS, електронних підписів та інших технологій дозволяють захистити інформацію від несанкціонованого доступу, зберігаючи при цьому цілісність і конфіденційність даних. Інструменти, такі як VPN (віртуальні приватні мережі) та блокчейн, можуть використовуватись для забезпечення безпеки та анонімності в процесах онлайн-взаємодії, що знижує ризики викрадення або маніпуляції даними.

Важливою складовою є також забезпечення анонімності користувачів в інтернет-просторі, особливо коли йдеться про доступ до чутливої або персональної інформації. Використання технологій, що дозволяють користувачам залишатись анонімними, допомагає захистити їх приватність. Для цього можуть застосовуватися спеціальні системи, такі як анонімні браузері (наприклад, Tor), а також методи, що дозволяють уникнути відслідковування онлайн-активності громадян, без втрати функціональності або доступу до послуг.

Окрім того, важливо забезпечити правовий захист громадян у разі порушення їхніх прав на приватність. Для цього необхідно створити механізми, через які громадяни можуть отримати доступ до інформації, що стосується їхніх персональних даних, а також ефективно захищати свої права в разі порушення законодавства з боку державних органів чи інших суб'єктів. Це включає створення інституцій для нагляду та моніторингу за дотриманням законів, таких як уповноважений з прав людини або органи захисту персональних даних.

Прозорість і контроль за використанням даних є ще одним важливим елементом. Громадяни повинні мати чітке розуміння того, як і чому їхні дані збираються, використовуються і зберігаються, а також хто має доступ до цієї інформації. Для цього органи влади мають проводити регулярні аудити, публікувати звіти про використання даних та запроваджувати механізми, що дозволяють громадянам контролювати доступ до своїх персональних відомостей.

Отже, забезпечення гарантій анонімності та захисту прав громадян у цифрову епоху потребує як законодавчих, так і технічних заходів. Впровадження комплексної політики, що поєднує високий рівень захисту особистих даних з передовими технологіями для забезпечення анонімності та безпеки, є необхідною умовою для розвитку довіри громадян до електронного врядування та надання державних послуг в онлайн-середовищі. Це забезпечить не тільки захист прав громадян, а й зміцнить загальну кібербезпеку країни.

4.4. Електронні звернення та електронні петиції в Україні

Електронні звернення та електронні петиції стали важливим інструментом громадянської участі та демократичного процесу в Україні, що дозволяють громадянам безпосередньо взаємодіяти з органами державної влади, органами місцевого самоврядування та іншими державними інституціями. В умовах розвитку цифрових технологій та інтернет-комунікацій, електронні звернення і петиції стали невід’ємною частиною механізмів участі населення в прийнятті рішень і реалізації їхніх прав у суспільстві. Ці інструменти забезпечують більш прозорий, швидкий і зручний спосіб комунікації з державними органами, а також сприяють залученню громадян до процесу управління, посилюючи соціальний контроль і відповідальність влади перед населенням.

Електронні звернення дозволяють громадянам звертатися до державних органів через спеціалізовані онлайн-платформи, що спрощує процес подачі документів, скарг або запитів до органів влади, та забезпечує більшу доступність для осіб, що мають обмежений доступ до традиційних способів комунікації. Електронні петиції, своєю чергою, є засобом для ініціювання масових звернень до державних органів із конкретними вимогами або пропозиціями, які можуть бути розглянуті відповідними органами у разі збору достатньої кількості підписів.

В табл. 4.4 представлено механізм подачі петицій в Україні.

Таблиця 4.4

Механізм подачі петицій в Україні

Етап	Опис
1. Підготовка петиції	Громадянин або група осіб готують текст петиції, визначаючи тему, зміст і мету звернення.
2. Реєстрація петиції	Петиція подається через офіційний веб-портал, наприклад, на сайті Президента України або органів місцевого самоврядування.
3. Перевірка відповідності	Петиція перевіряється на відповідність вимогам: наявність підписів, правильність оформлення та дотримання норм.
4. Публікація петиції	Після реєстрації петиція публікується на сайті відповідного органу, щоб громадяни могли ознайомитися з її змістом.
5. Збір підписів	Для петиції необхідно зібрати мінімальну кількість підписів (наприклад, 25 000 для петиції до Президента). Підписи можуть збиратися через онлайн-платформу.
6. Розгляд петиції органом влади	Якщо петиція набирає достатньо підписів, орган влади зобов'язаний розглянути її та надати відповідь громадянам.
7. Рішення щодо петиції	Після розгляду орган влади приймає рішення щодо виконання або відмови від вимог петиції. Рішення публікується для громадськості.
8. Повідомлення ініціаторів	Ініціатори петиції отримують офіційну відповідь щодо результатів розгляду петиції, а також можливу реалізацію або відмову в її виконанні.

Механізм подачі петицій в Україні є важливою складовою демократичного процесу, що дозволяє громадянам безпосередньо взаємодіяти з органами влади та впливати на прийняття рішень на рівні держави та місцевого самоврядування. Він забезпечує прозорість, доступність та ефективність комунікації між громадянами та державними органами, сприяючи активному залученню населення до управлінських процесів.

Процес починається з підготовки петиції, коли громадяни або групи осіб формують свої вимоги та мету звернення. Це дозволяє чітко визначити тему петиції і забезпечити її відповідність інтересам громади. Після цього петиція реєструється через офіційні веб-платформи, що гарантує її доступність для громадськості та забезпечує прозорість збору підписів.

Згідно з положеннями статті 23-1 Закону України «Про звернення громадян», громадяни мають право подавати електронні петиції до різних органів державної влади, включаючи Президента України, Верховну Раду України, Кабінет Міністрів України, а також органи місцевого самоврядування. Для подачі таких петицій передбачено використання офіційних веб-сайтів органів, до яких вони звертаються, або веб-сайтів громадських об'єднань, що займаються збором підписів на підтримку петицій. Такий механізм забезпечує зручний і доступний спосіб для громадян висловлювати свої вимоги та пропозиції до органів влади, використовуючи електронні технології для реалізації своїх прав.

Основні вимоги до змісту електронної петиції в Україні чітко визначені законодавством. Петиція повинна містити конкретний опис питання, яке висувається на обговорення органу влади, а також інформацію про автора петиції, зокрема його прізвище, ім'я, по батькові та адресу електронної пошти. Крім того, веб-сайт органу, до якого подається петиція, або веб-сайт громадського об'єднання, що здійснює збір підписів, зобов'язаний публікувати дату початку збору підписів, а також надавати інформацію про кількість підписів, що були зібрані на підтримку петиції, та перелік осіб, які їх поставили.

У змісті електронних петицій в Україні існують певні заборони, які визначені законодавством для захисту національної безпеки та прав і свобод громадян. Зокрема, заборонено включати заклики до повалення конституційного ладу, порушення територіальної цілісності, терористичні акти, пропаганду насильства, розпалювання міжетнічної чи релігійної ворожнечі, а також інформацію, що принижує честь і гідність осіб або загрожує національним інтересам України. Такі петиції, що містять неправдиву інформацію або ненормативну лексику, підлягають відмові в публікації або видаленню з офіційного веб-сайту після перевірки та з'ясування обставин.

Процедура подачі електронної петиції починається з заповнення спеціальної форми на офіційному веб-сайті органу, до якого вона адресована, або на веб-сайті громадського об'єднання. Після заповнення форми та публікації тексту петиції, вона повинна бути

оприлюднена на сайті протягом двох робочих днів з моменту її подання автором (ініціатором). Це забезпечує швидке оприлюднення важливих громадських ініціатив і дозволяє громадянам оперативно долучитися до збору підписів.

У разі, якщо електронна петиція не відповідає встановленим вимогам, її публікація не здійснюється. Про це автор петиції має бути повідомлений не пізніше ніж у строки, передбачені для оприлюднення. Після того, як петиція оприлюднена на офіційному веб-сайті органу, відповідного Президента України, Верховної Ради України, Кабінету Міністрів України чи органу місцевого самоврядування, цей момент вважається початком збору підписів на її підтримку. Від цього моменту починається офіційний процес підтримки петиції громадянами, що може призвести до її розгляду відповідними органами влади.

Збір підписів є важливим етапом, адже він свідчить про рівень підтримки петиції серед громадян. Це дозволяє органам влади зрозуміти, чи є питання актуальним для широкої аудиторії. Після збору необхідної кількості підписів петиція розглядається органами влади, які зобов'язані прийняти рішення щодо її подальшого виконання або відмови. Це рішення, а також обґрунтування, чому було прийнято саме таке рішення, публікується для загального відома.

Щоб підтримати вже створену електронну петицію, необхідно спочатку увійти за допомогою інтегрованої системи електронної ідентифікації ID.GOV.UA, а після перейти на сторінку цієї петиції, ознайомитися з її текстом і натиснути кнопку «Підписатися». Зарахування голосу відбудеться одразу ж.

Завершальним етапом є офіційне повідомлення ініціаторів петиції про результати її розгляду. Це гарантує, що процес не лише прозорий, але й підзвітний. Ініціатори петиції отримують чітку відповідь, що дозволяє їм розуміти, чи була їх петиція реалізована, чи було відмовлено в її виконанні, і з якими обґрунтуваннями.

Згідно зі статтею 23-1 Закону України «Про звернення громадян», після розгляду електронної петиції орган, якому вона була адресована, зобов'язаний надати відповідь на порушені в петиції питання. Відповідь повинна бути публічно оприлюднена на офіційному веб-сайті органу в найкоротші терміни, але не пізніше наступного робочого дня після завершення розгляду. Це дозволяє забезпечити прозорість процесу та дає громадянам можливість швидко отримати інформацію щодо результатів розгляду їх ініціатив.

Крім того, відповідь на електронну петицію повинна бути надіслана в письмовому вигляді автору (ініціатору) петиції та громадському об'єднанню, яке організовувало збір підписів. Це гарантує, що всі зацікавлені сторони отримують необхідну інформацію і можуть далі діяти згідно з результатами розгляду петиції.

У разі, якщо пропозиції, викладені в петиції, визнані доцільними, орган, до якого була адресована петиція, має право реалізувати їх, прийнявши відповідне рішення з питань, що входять до його компетенції. Для пропозицій, що потребують більш широкого законодавчого вирішення, Президент України, Кабінет Міністрів України або народні депутати України можуть ініціювати розробку законопроектів. Ці законопроекти мають бути внесені до Верховної Ради України відповідно до встановленої процедури для вирішення питань, порушених у петиції.

Також важливо, що інформація про кількість підписів, зібраних на підтримку електронної петиції, а також про строки їх збору зберігається на офіційному вебсайті органу не менше трьох років з моменту публікації петиції. Це дає змогу забезпечити належний контроль за процесом збору підписів та дозволяє громадянам перевіряти, наскільки широко була підтримана петиція протягом цього часу.

Таким чином, механізм подачі петицій в Україні сприяє підвищенню участі громадян у державному управлінні, зокрема, на місцевому рівні. Це важливий крок до розвитку електронної демократії та зміцнення взаємодії між громадянами та державними органами, що позитивно впливає на демократичні процеси в країні.

Порядок розгляду *електронної петиції, адресованої Президентові України.*

Процедура подачі та розгляду електронних петицій до Президента України забезпечує громадянам ефективний інструмент для вираження своїх пропозицій та вимог до органів державної влади. Всі електронні петиції до Президента України подаються через спеціальний розділ на офіційному вебсайті Офіційного інтернет-представництва Президента України. Доступ до цього розділу можна отримати за адресою: <https://petition.president.gov.ua/>.

Щоб підтримати петицію або подати власну, користувач повинен пройти процес реєстрації або авторизації на зазначеному вебсайті. Для цього потрібно натискати кнопку «Вхід/Реєстрація», розташовану в верхньому правому куті сторінки. У результаті відкривається меню

інтегрованої системи електронної ідентифікації ID.GOV.UA, де користувач може вибрати один із способів входу, зокрема за допомогою електронного підпису або через онлайн-банкінг. У разі, якщо користувач вперше використовує сервіс електронних петицій, після успішної ідентифікації його реєстрація відбудеться автоматично, що забезпечує зручність і швидкість процесу.

Якщо петиція набирає не менш ніж 25 000 підписів протягом трьох місяців з дня її оприлюднення, вона підлягає розгляду відповідно до Порядку розгляду електронних петицій, затвердженого Указом Президента України від 28 серпня 2015 року № 523. У разі, якщо петиція отримала необхідну кількість підтримки, інформація про підтримку або відмову публікується на офіційному веб-сайті Президента України. Таке оголошення є публічним і сприяє забезпеченню прозорості процесу розгляду петицій.

Підтримати петицію можна, перейшовши на її сторінку на сайті, ознайомившись з її текстом і натиснувши кнопку «Підписатися». Якщо користувач вже авторизований на сайті, підпис буде зарахований негайно. Якщо ж користувач ще не авторизувався, він повинен увійти через систему ID.GOV.UA для того, щоб здійснити підпис. Це гарантує, що лише авторизовані користувачі можуть підтримати петицію, що забезпечує більшу точність збору підписів.

Електронні петиції, на яких триває збір підписів, доступні для перегляду на веб-сайті. Петиція, що не набрала необхідної кількості підписів до закінчення строку збору, після цього розглядається як звичайне звернення громадян відповідно до Закону України «Про звернення громадян». Це дає можливість органам влади враховувати звернення громадян навіть в разі недостатньої підтримки петиції.

Після розгляду петиції органи влади, зокрема Президент України, повинні надати офіційну відповідь щодо результатів розгляду порушених у петиції питань. Відповідь публікується на веб-сайті органу, якому петиція була адресована, не пізніше наступного робочого дня після завершення розгляду. Крім того, письмова відповідь надсилається автору петиції та громадському об'єднанню, яке проводило збір підписів.

У разі, якщо пропозиції в петиції визнані доцільними, Президент України має право реалізувати їх, прийнявши відповідне рішення з питань, що належать до його компетенції. За результатами розгляду петиції також можуть бути розроблені законопроекти, які будуть

внесені до Верховної Ради України для подальшого розгляду та вирішення питань, порушених у петиції.

Така система дозволяє громадянам активно впливати на державну політику, сприяє розвитку демократії та забезпечує прозорість і підзвітність органів влади. Водночас вона підвищує ефективність роботи державних органів, оскільки дозволяє враховувати думки громадян у процесі прийняття важливих рішень.

Порядку розгляду *електронної петиції, адресованої Кабінету Міністрів України*

Громадяни України мають можливість подавати петиції до Кабінету Міністрів України безпосередньо через офіційний веб-сайт Кабінету Міністрів, який є частиною Єдиного веб-порталу органів виконавчої влади (Урядовий портал). Крім того, петиції можуть подаватися через веб-сайти громадських об'єднань, що займаються збором підписів на підтримку електронних петицій. Такий механізм дозволяє забезпечити доступність петицій для широкої аудиторії та сприяє залученню громадян до процесу формування державної політики.

Порядок розгляду електронних петицій, адресованих Кабінету Міністрів України, регулюється відповідно до Порядку, затвердженого постановою Кабінету Міністрів України від 22 липня 2016 року № 457. Цей документ визначає основні етапи та правила розгляду петицій, зокрема, вимоги до формату подачі петиції, процес її оприлюднення та строки збору підписів.

Після збору необхідної кількості підписів на підтримку петиції, інформація про її підтримку або невідтримку публічно оголошується на офіційному вебсайті Кабінету Міністрів України. Це оголошення здійснюється Прем'єр-міністром України, що додає прозорості та забезпечує відкритість процесу прийняття рішень.

Збір підписів для підтримки петицій триває протягом визначеного періоду. Петиції, на яких триває збір підписів, можуть бути переглянуті на офіційному вебсайті. Це дозволяє громадянам ознайомитися з ініціативами інших осіб та приєднатися до підтримки тих, що вони вважають важливими.

Після завершення розгляду петиції органами Кабінету Міністрів України, на офіційному веб-сайті публікується відповідь щодо результатів розгляду порушених питань, з обґрунтуванням прийнятого рішення. Важливо, що відповідь повинна бути оприлюднена не пізніше наступного робочого дня після завершення розгляду петиції, що

забезпечує швидке реагування органів виконавчої влади на громадські ініціативи.

Крім того, письмова відповідь на електронну петицію надсилається не лише автору (ініціатору) петиції, а й громадському об'єднанню, яке проводило збір підписів на підтримку петиції. Це гарантує, що всі зацікавлені сторони отримують чітку інформацію про результати розгляду петиції.

Такий порядок розгляду електронних петицій сприяє розвитку діалогу між громадянами та органами влади, підвищує рівень прозорості та підзвітності державних інституцій і дозволяє громадянам безпосередньо впливати на процеси прийняття рішень у країні.

Розглянемо наступним кроком порядок розгляду електронної петиції, *адресованої органам місцевого самоврядування*.

Відповідно до внесених змін до Закону України «Про звернення громадян», що стосуються електронних звернень та петицій, було визначено нові вимоги щодо кількості підписів, необхідних для підтримки електронної петиції до органу місцевого самоврядування, а також строки збору підписів. Зокрема, ці зміни включають конкретні норми, які визначають, скільки підписів повинні зібрати громадяни на підтримку петиції для того, щоб орган місцевого самоврядування зобов'язаний був її розглянути.

Згідно з новими правилами, для подальшого розгляду електронної петиції необхідно зібрати підтримку серед жителів певної адміністративно-територіальної одиниці. Кількість підписів, яку потрібно зібрати для того, щоб петиція була розглянута органами місцевої влади, залежить від чисельності населення відповідної території. Збір підписів має відбуватись протягом трьох місяців з моменту публікації петиції на офіційному веб-сайті. Це означає, що кожен житель цієї території має можливість підписати петицію, тим самим виражаючи свою підтримку або незгоду з порушеними в ній питаннями.

Зокрема, вимоги до кількості підписів виглядають наступним чином:

1. У територіальних громадах з чисельністю до 1 тисячі жителів, для того щоб петиція була розглянута органом місцевого самоврядування, необхідно зібрати не менше ніж 50 підписів.

2. Для адміністративно-територіальних одиниць з чисельністю населення від 1 тисячі до 5 тисяч жителів на підтримку петиції має бути зібрано не менше ніж 75 підписів.

3. У громадах з чисельністю від 5 тисяч до 50 тисяч жителів кількість підписів, необхідних для розгляду петиції, становить не менше ніж 100 підписів.

4. Для територіальних одиниць, де проживає від 100 тисяч до 500 тисяч жителів, на підтримку петиції повинно бути зібрано не менше ніж 250 підписів.

5. У великих громадах з населенням від 500 тисяч до 1 мільйона жителів для того, щоб петиція була розглянута, необхідно зібрати не менше ніж 500 підписів.

6. Для територіальних одиниць, де проживає понад 1 мільйон жителів, мінімальна кількість підписів для підтримки петиції становить 1000 підписів.

Цей механізм збору підписів створює чітку систему для визначення важливості та підтримки петицій з боку громадян, забезпечуючи баланс між кількістю підписів і чисельністю населення в кожній адміністративно-територіальній одиниці.

Після того, як петиція набирає необхідну кількість підписів, орган місцевого самоврядування зобов'язаний оприлюднити результат її підтримки або не підтримки. Інформація про це публікується на офіційному вебсайті місцевої ради, де буде оголошено рішення голови відповідної ради щодо подальшого розгляду петиції. Це дозволяє громадянам бути в курсі всіх етапів процесу та дає змогу відстежувати, чи була петиція підтримана на рівні місцевої влади.

Крім того, в офіційному відповіді на петицію громадяни отримують інформацію про результати розгляду порушених у ній питань. Важливим аспектом є обґрунтування рішення, яке повинно бути надано органом місцевого самоврядування. Це дозволяє громадянам зрозуміти, чому було прийнято певне рішення і якими були мотиви його прийняття.

Таким чином, зміни в законодавстві України щодо електронних звернень та петицій сприяють полегшенню процесу громадянської участі, дозволяючи людям брати активну участь у вирішенні важливих для громади питань через онлайн-платформи.

Відповідно до законодавства України, **відповідальність за зміст електронної петиції несе автор або ініціатор петиції**. Це означає, що особа, яка подає петицію, зобов'язана забезпечити її відповідність чинному законодавству та уникати вмісту, який порушує правові норми або може завдати шкоди репутації інших осіб чи організацій.

Згідно зі статтею 26 Закону України «Про звернення громадян», громадянин, який подає звернення, що містить наклеп, образи або дискредитацію органів державної влади, органів місцевого самоврядування, об'єднань громадян, а також їх посадових осіб чи керівників підприємств, установ і організацій незалежно від форм власності, може бути притягнутий до відповідальності. Подібні звернення, що містять заклики до розпалювання національної, расової чи релігійної ворожнечі, або інші протизаконні дії, є підставою для застосування відповідних санкцій, передбачених чинним законодавством України.

Відповідно до статті 24 цього ж Закону, особи, які порушують вимоги цього закону, можуть нести цивільну, адміністративну або кримінальну відповідальність, залежно від тяжкості порушення. Це включає штрафи, позови про відшкодування завданої шкоди, або навіть кримінальне переслідування, якщо дія особи має ознаки злочину.

Таким чином, важливо, щоб подання петицій, звернень або інших громадських ініціатив не порушувало права та свободи інших осіб, а також відповідало нормам етики та законодавства, що регулює взаємодію громадян з органами державної влади та органами місцевого самоврядування.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які основні етапи розвитку електронного урядування в Україні?
2. Як впровадження електронного цифрового підпису сприяло розвитку електронного документообігу в Україні?
3. Які нормативно-правові акти є ключовими для впровадження електронного урядування в Україні?
4. Як портал «Дія» сприяв розвитку електронного урядування в Україні?
5. Які основні переваги електронного урядування виокремлюють в Україні?
6. Які заходи безпеки застосовуються для забезпечення захисту електронних послуг в Україні?
7. Як етапи розвитку електронного урядування в Україні інтегруються з європейськими цифровими стандартами?
8. Який механізм подачі електронних петицій в Україні, і як він сприяє громадянській участі в управлінні?

РОЗДІЛ 5. ЦИФРОВА ГРАМОТНІСТЬ

5.1. Важливість цифрової грамотності населення

В умовах стрімкого розвитку інформаційних технологій, глобалізації та інтеграції цифрових рішень у всі сфери життя, питання цифрової грамотності набуває особливої актуальності. Цифрова грамотність – це не лише здатність користуватися комп'ютерами та Інтернетом, а й важлива компетенція для ефективного функціонування в сучасному світі. Вона включає в себе розуміння основних принципів цифрових технологій, вміння критично оцінювати інформацію в Інтернеті, користуватися електронними сервісами, захищати свої особисті дані та зберігати кібербезпеку. Від рівня цифрової грамотності залежить успішність людини в різних сферах, від професійної діяльності до особистого життя.

Сучасне суспільство неможливо уявити без цифрових технологій. Вони стали невід'ємною частиною економіки, освіти, культури та адміністративних процесів. Інтернет, соціальні мережі, електронні комунікації, онлайн-банкінг та інші цифрові сервіси проникають у всі аспекти нашого життя, що робить цифрову грамотність необхідною умовою для повноцінної участі в суспільному житті. Особливо це важливо в контексті швидких змін на ринку праці, де навички роботи з цифровими інструментами стають вимогою до кожного працівника.

Незважаючи на все більше поширення цифрових технологій, рівень цифрової грамотності серед різних соціальних груп все ще залишається нерівномірним. Важливою задачею стає підвищення цифрових компетенцій серед різних верств населення, особливо серед осіб старшого віку, людей з інвалідністю та жителів віддалених регіонів. У цьому контексті держави та міжнародні організації активно розробляють програми та ініціативи для сприяння цифровій освіті, надаючи громадянам інструменти для адаптації до цифрового середовища.

Отже, важливість цифрової грамотності населення сьогодні не обмежується лише здатністю користуватися комп'ютером. Це комплекс знань і навичок, який забезпечує активну участь громадян у соціальних, економічних і культурних процесах, що відбуваються в умовах глобальної цифровізації.

У сучасному світі цифровізація стає основою трансформації суспільства, економіки та державного управління, створюючи умови для підвищення ефективності та конкурентоспроможності держави. Однак досягнення цих цілей безпосередньо залежить від рівня цифрової грамотності населення, яка є ключовим чинником успішного впровадження цифрових технологій. Незважаючи на зростаючу доступність цифрових інструментів, значна частина громадян все ще стикається з бар'єрами в оволодінні необхідними навичками, що призводить до цифрового розриву, соціальної нерівності та уповільнення загального процесу цифровізації.

Основні проблеми полягають у низькому рівні цифрових компетенцій серед певних соціальних груп, нерівномірному доступі до сучасної цифрової інфраструктури, відсутності системного підходу до цифрової освіти та недостатньому рівні інформаційної безпеки. Ці виклики вимагають розробки комплексних програм, спрямованих на підвищення цифрової грамотності через освітні ініціативи, поширення доступу до технологій та формування цифрової культури. Розвиток цифрових навичок населення є не лише основою для реалізації державної стратегії цифровізації, але й необхідною умовою для соціальної інтеграції та економічного зростання в умовах цифрової епохи.

Цифрова грамотність включає комплекс знань, умінь і навичок, які дозволяють людині ефективно, безпечно та відповідально використовувати цифрові технології в різних аспектах життєдіяльності. Цей феномен охоплює базові технічні навички, критичне мислення, розуміння принципів інформаційної безпеки, а також здатність до аналізу й використання цифрових ресурсів у професійній, освітній та особистій сферах. У сучасному світі, де цифрові технології стали невід'ємною частиною щоденного життя, цифрова грамотність перетворилася на одну з ключових компетенцій XXI століття [24].

Зростаючий темп технологічного прогресу зумовлює необхідність постійного вдосконалення цифрових навичок, адже їх рівень визначає здатність особистості інтегруватися в інформаційне суспільство. Завдяки високому рівню цифрової грамотності людина може ефективно працювати з інформацією, адаптуватися до технологічних змін і використовувати інноваційні рішення у своїй діяльності. Особливе значення ця компетенція має в умовах цифровізації професійної сфери та освітніх процесів, де від її рівня

залежать конкурентоспроможність працівника, здатність до навчання протягом життя та успішність у досягненні кар'єрних і освітніх цілей.

Окрім індивідуального значення, цифрова грамотність має вагомий вплив на розвиток суспільства та держави. Вона виступає фундаментом для забезпечення ефективного впровадження цифрових технологій у державному управлінні, економіці, освіті та інших важливих сферах. Рівень цифрової грамотності населення є індикатором готовності суспільства до використання новітніх технологій, зокрема в контексті глобальних викликів і трансформацій цифрового середовища. Таким чином, розвиток цифрової грамотності не лише сприяє особистісному зростанню, а й є визначальним чинником соціальної інтеграції та економічного зростання в умовах цифрової епохи.

В табл. 5.1 наведено основні категорії таких навичок та їх коротку характеристику.

Таблиця 5.1

Ключові навички цифрової грамотності населення

Категорія навичок	Опис
Технічні навички	Вміння використовувати комп'ютери, смартфони, планшети, периферійні пристрої.
Робота з програмним забезпеченням	Здатність працювати з текстовими редакторами, електронними таблицями, поштовими клієнтами, браузерами.
Робота з інформацією	Здатність знаходити, аналізувати, оцінювати та використовувати інформацію в інтернеті.
Комунікаційні навички	Використання цифрових інструментів для спілкування: електронна пошта, месенджери, відеозв'язок.
Кібербезпека	Знання основ інформаційної безпеки: створення паролів, розпізнавання шахрайських сайтів, захист персональних даних.
Критичне мислення	Здатність аналізувати достовірність інформації, розрізняти фейки та маніпулятивні матеріали.
Цифровий етикет	Правила поведінки в онлайн-середовищі, етичне спілкування та взаємодія з іншими користувачами.
Робота з даними	Вміння працювати з великими масивами даних, створювати таблиці, візуалізувати інформацію.
Адаптивність	Здатність швидко освоювати нові технології, пристрої та програми.
Творчі навички	Використання цифрових інструментів для створення контенту: фото, відео, графіка, текст.

Технічні навички є базовою складовою цифрової грамотності, адже вони забезпечують здатність користувачів працювати з різноманітними цифровими пристроями, такими як комп'ютери, планшети, смартфони та периферійні пристрої (принтери, сканери тощо). Володіння цими навичками є фундаментом для освоєння більш складних цифрових компетенцій. У контексті цифровізації держави, технічні навички населення забезпечують ефективний доступ до електронних послуг, зокрема адміністративних, освітніх і медичних. Наприклад, громадяни з високим рівнем технічної підготовки здатні самостійно користуватися системами електронного урядування, що зменшує бюрократичне навантаження та підвищує ефективність взаємодії з державними структурами.

Оволодіння програмним забезпеченням дозволяє використовувати сучасні інструменти для обробки інформації, управління проектами, комунікації та інших завдань, це включає роботу з текстовими редакторами, електронними таблицями, презентаційними програмами, браузером та поштовими клієнтами. Для цифровізації держави критично важливо, щоб населення вміло користуватися електронними платформами, такими як системи електронного документообігу чи портали державних послуг. Ці навички сприяють розвитку цифрової економіки, підвищуючи продуктивність праці та ефективність комунікації як між громадянами, так і між бізнесом та державою [2].

Здатність ефективно шукати, аналізувати та використовувати інформацію є основою для прийняття обґрунтованих рішень у цифровому середовищі. Ця навичка включає пошук релевантної інформації в інтернеті, оцінку її достовірності та критичний аналіз джерел. Для держави, яка прагне цифровізації, важливо, щоб громадяни були готові працювати з великими обсягами інформації, що генерується у цифрових системах. Наприклад, в освітньому середовищі це дозволяє учням і студентам ефективно використовувати онлайн-ресурси, а в професійній діяльності – приймати стратегічні рішення, базуючись на аналітиці та даних.

Комунікаційні навички включають вміння використовувати цифрові інструменти для спілкування, такі як електронна пошта, месенджери, відеоконференції та соціальні мережі. У контексті цифровізації держави це сприяє спрощенню взаємодії між громадянами, бізнесом і державними установами. Наприклад, використання цифрових платформ для подання заяв чи звернень значно

економить час і ресурси, водночас роблячи комунікацію більш прозорою, ці навички також відіграють важливу роль у побудові громадянського суспільства, оскільки дозволяють громадянам брати участь у суспільних дискусіях та ініціативах.

Знання принципів інформаційної безпеки та вміння захищати особисті дані є критично важливими у цифровому світі, це включає створення сильних паролів, розпізнавання фішингових атак, використання антивірусного програмного забезпечення та безпечну роботу з цифровими платформами. Для держави, яка розвиває електронне урядування, кібербезпека населення є гарантією захищеності даних та довіри громадян до цифрових інструментів. Недостатній рівень кібербезпеки може призвести до витоку інформації чи зловживань, що підриває зусилля з цифровізації.

Розвиток критичного мислення дозволяє громадянам аналізувати інформацію, розпізнавати маніпулятивні матеріали та протистояти дезінформації, це особливо важливо в умовах інформаційного перевантаження та ризиків цифрової пропаганди. Для цифровізації держави важливо, щоб громадяни були спроможні самостійно оцінювати якість інформації, з якою вони працюють, особливо якщо йдеться про прийняття рішень у сфері електронних послуг чи участь у суспільних ініціативах.

Цифровий етикет регулює правила поведінки у віртуальному середовищі, включаючи етичне спілкування, дотримання прав інших користувачів та уникнення конфліктів у мережі. У цифровізованій державі цифровий етикет забезпечує гармонійну взаємодію між користувачами в електронних системах, сприяючи зниженню рівня конфліктів та підвищенню ефективності спільних процесів. Знання норм цифрового етикету також сприяє створенню позитивного іміджу держави в глобальному інформаційному просторі.

Оволодіння навичками роботи з даними включає створення, аналіз, структурування та візуалізацію інформації. Для громадян цифрової держави ці навички є необхідними для роботи з різними типами даних, зокрема у сфері фінансів, управління чи освіти. Наприклад, здатність працювати з електронними таблицями чи платформами аналітики допомагає швидко приймати обґрунтовані рішення, що підвищує продуктивність як на особистому, так і на професійному рівнях.

Адаптивність визначає здатність людини швидко освоювати нові технології та пристосовуватися до змін у цифровому середовищі. Ця

навичка є особливо важливою в умовах динамічного розвитку цифрових інновацій. Для цифровізації держави адаптивність населення забезпечує оперативне впровадження нових інструментів та послуг, зокрема у сферах охорони здоров'я, освіти чи соціального захисту. Чим вищий рівень адаптивності громадян, тим швидше та ефективніше відбувається інтеграція нових рішень [2].

Творчі навички передбачають використання цифрових інструментів для створення та розвитку контенту, такого як фото, відео, графіка чи текстові матеріали. У контексті цифрової держави ці навички сприяють розвитку креативної економіки та підвищенню конкурентоспроможності країни. Наприклад, громадяни, які створюють якісний цифровий контент, можуть сприяти популяризації національної культури, освіти та бізнесу, використовуючи цифрові платформи для виходу на міжнародну аудиторію.

Розвиток ключових цифрових навичок є фундаментом для інтеграції громадян у цифрове середовище, забезпечуючи їхню активну участь у суспільному, економічному та культурному житті, ці навички сприяють ефективному використанню державних електронних сервісів, підвищують рівень соціальної взаємодії та стимулюють інноваційний розвиток. Успішна цифровізація держави можлива лише за умови системного підходу до формування цифрової грамотності всіх верств населення.

5.2. Аналіз цифрової грамотності населення України

Цифрова грамотність є важливою складовою сучасного суспільства, і в Україні спостерігається стійка тенденція до зростання рівня цієї компетенції серед населення. Згідно з дослідженнями, що проводяться Міністерством цифрової трансформації України (посилання на звіт під рисунком 5.1) можна побачити значне покращення в доступі до інтернет-послуг та вміннях користуватися цифровими технологіями. За останні роки частка інтернет-користувачів в Україні виросла на 8%, досягнувши 94%. Цей зріст є результатом не лише покращення інфраструктури, але й сприяння доступу до інтернету в різних регіонах країни. З кожним роком все більше українців отримують можливість скористатися цифровими технологіями, що дозволяє їм активно залучатися до глобальних процесів.



Рис. 5.1. Дослідження цифрової грамотності населення України за 2023 рік
https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Особливо слід відзначити, що цифрова грамотність охоплює не лише молоді та середні вікові групи, а й старші покоління. Це важливий аспект, оскільки раніше старші люди часто відставали у використанні технологій. Проте сьогодні ми можемо побачити значний прогрес і серед осіб віком 60–70 років. Зокрема, 71% людей цієї вікової групи активно користуються інтернетом, що свідчить про позитивні зміни в їхній цифровій грамотності. Найбільший відсоток користувачів спостерігається серед молоді віком 18–29 років, де інтернет використовує вже 96% осіб. Це підтверджує важливість цифрових навичок у сучасному світі, особливо для молоді, яка активно інтегрується в цифрове середовище.

Інтернет вже став базовою потребою для більшості населення, включаючи людей з інвалідністю. 91% дорослих громадян мають доступ до інтернету, а серед людей з порушеннями слуху цей показник складає 84%. Це показує, що інтернет є не лише інструментом комунікації, але й необхідною умовою для доступу до важливих послуг,

таких як освіта, медичне обслуговування, пошук інформації та багато інших. Крім того, інтернет дозволяє людям з інвалідністю інтегруватися в суспільство та брати активну участь у різних процесах, що значно покращує їхню якість життя.

Позитивна динаміка розвитку цифрових навичок є ще одним важливим фактором, який свідчить про зростання цифрової грамотності серед українців. Станом на 2023 рік, 93% дорослих громадян України віком 18–70 років мають базові цифрові навички, що на 8% більше, ніж у 2019 році. Особливо високі показники серед підлітків, де 95% осіб віком від 10 до 17 років володіють необхідними цифровими вміннями. Ці цифри свідчать про значні зусилля, спрямовані на розвиток цифрової освіти серед молоді, що допомагає їй швидше адаптуватися до вимог сучасного цифрового світу. Окремо варто відзначити успіхи серед людей з порушеннями слуху, де 99% осіб віком від 18 до 59 років володіють цифровими навичками, що сприяє їхній соціалізації та доступу до важливої інформації.

Однією з основних складових сучасного доступу до цифрових технологій є можливість підключення до інтернету вдома. За останні роки, рівень доступу до інтернету в домогосподарствах зріс на 5,4% і наразі складає 93,8%. Це створює умови для більш активного використання інтернет-ресурсів у повсякденному житті, дозволяючи громадянам вирішувати різноманітні завдання онлайн – від навчання до отримання медичних послуг або ведення бізнесу. Такий доступ забезпечує рівні можливості для людей з різних регіонів та соціальних груп і є важливим фактором у скороченні цифрового розриву.

Задоволення якістю інтернет-з'єднання також є важливою частиною цього процесу. Більше 83% українців висловлюють задоволення від якості інтернету, що свідчить про покращення інфраструктури та надання послуг. Відсутність технічних проблем з підключенням і стабільне з'єднання дозволяють користувачам більш ефективно використовувати цифрові ресурси для особистих і професійних цілей. Цей аспект є важливим для подальшого розвитку цифрової економіки та суспільства, оскільки стабільний доступ до інтернету відкриває нові можливості для всіх верств населення, забезпечуючи рівний доступ до знань, інформації та послуг.

Загалом, процес розвитку цифрової грамотності в Україні має позитивні тенденції. Зростання рівня доступу до інтернету та покращення цифрових навичок серед різних груп населення свідчать про поступове подолання цифрового розриву. Проте для забезпечення

повної інклюзивності та забезпечення рівних можливостей для всіх громадян необхідно продовжувати роботу над впровадженням нових програм, які сприятимуть розвитку цифрових компетенцій, зокрема серед старших поколінь та жителів віддалених регіонів.

В табл. 5.2 представлено зміна рівня цифрової грамотності населення України за роки моніторингу (2019–2023 роки).

Таблиця 5.2

Зміна рівня цифрової грамотності населення України за роки моніторингу

Назва	Роки			Абсолютне відхилення (+,-)	
	2019	2021	2023	2021/ 2019	2023/ 2022
Частка населення з рівнем цифрових навичок нижче базового	53%	47,80%	40,40%	-5,20%	-7,40%
Частка населення без цифрових навичок	15%	11%	7%	-4,00%	-4,00%
Частка населення з базовими та просунутими цифровими навичками	47%	52,20%	59,60%	5,20%	7,40%

Згідно з даними, представленими в таблиці, спостерігається позитивна динаміка змін у рівні цифрової грамотності населення України в період з 2019 по 2023 рік. Показники, що відображають різні категорії цифрових навичок серед українців, демонструють важливі тенденції розвитку цієї сфери. На основі отриманих результатів можна зробити висновки, що цифрові навички серед громадян зростають, а цифровий розрив поступово зменшується. Враховуючи значення цифрової грамотності для доступу до сучасних технологій та можливостей у всіх сферах життя, ці зміни є важливими для соціально-економічного розвитку країни.

Частка населення, яке має рівень цифрових навичок нижче базового, була однією з основних категорій, що підлягали аналізу в дослідженні. За період з 2019 по 2023 рік цей показник знизився з 53% до 40.40%, що свідчить про значне покращення. Зменшення частки таких осіб на 5.20% між 2021 та 2019 роками, а також на 7.40% між 2023 та 2022 роками, є важливим індикатором успіху в загальному

підвищенні рівня цифрової грамотності серед населення. Важливо зазначити, що цей процес має багато складових, зокрема покращення доступу до технологій, збільшення рівня освіти та цифрового навчання, а також впровадження нових цифрових послуг і інструментів, які стимулюють людей до освоєння нових навичок.

Іншим важливим аспектом є частка населення, яке не має жодних цифрових навичок. У 2019 році цей показник становив 15%, але до 2023 року він значно знизився до 7%. Зменшення на 4% за цей період є значним досягненням, оскільки це означає, що все більша кількість громадян долає бар'єри, пов'язані з відсутністю цифрових навичок, і отримує доступ до основних цифрових ресурсів. Для цього були створені різноманітні програми навчання, що дозволяють людям без досвіду вивчати основи роботи з інтернетом, комп'ютерами та мобільними пристроями. Така тенденція також свідчить про розширення доступу до освіти в цифровому форматі, що особливо важливо для людей старших вікових груп, які раніше мали обмежений доступ до технологій.

Найбільш виразним є збільшення частки населення з базовими та просунутими цифровими навичками. У 2019 році цей показник становив 47%, але до 2023 року він зріс до 59.60%. Це збільшення на 5.20% у 2021 році та 7.40% у 2023 році вказує на значний прогрес у розвитку цифрової грамотності серед українців. Такі зміни можуть бути обумовлені широким впровадженням цифрових технологій у всі сфери життя, що змусило громадян освоювати нові інструменти для комунікації, роботи та навчання. В результаті все більше людей володіють не лише базовими навичками, такими як користування інтернетом або офісними програмами, а й просунутими знаннями, що дозволяють їм ефективно працювати з новими цифровими рішеннями, використовувати онлайн-сервіси для здійснення фінансових операцій, дистанційного навчання чи розвитку кар'єри.

Загалом, тенденція до зростання рівня цифрової грамотності в Україні є важливим кроком до забезпечення рівних можливостей для всіх громадян незалежно від їхнього віку, освіти чи соціального статусу. Підвищення цифрових навичок має безпосередній вплив на можливості людей в професійній сфері, освіті, а також в особистому житті. З огляду на важливість цифрових технологій для майбутнього розвитку країни, важливо продовжувати підтримувати ініціативи, спрямовані на навчання громадян, і забезпечувати доступ до технологій для всіх верств населення, зокрема в сільських регіонах та серед

старших осіб, які можуть мати обмежений доступ до новітніх ресурсів і інструментів.

Отже, аналіз цих даних свідчить про позитивний розвиток цифрової грамотності серед населення, що є важливим і необхідним кроком у контексті сучасних викликів, які постають перед суспільствами в умовах глобалізації та стрімкого розвитку технологій. Зростання рівня цифрових навичок серед громадян означає, що більше людей стають активними користувачами сучасних цифрових інструментів, що значно полегшує їхнє повсякденне життя і сприяє інтеграції в глобальну економіку та культуру.

Позитивна динаміка в розвитку цифрової грамотності демонструє, що країна здатна адаптуватися до нових реалій, де цифрові технології стають основою для вирішення не тільки індивідуальних завдань, а й для розвитку цілого суспільства. Більш широке охоплення цифровими навичками значної частини населення дозволяє знижувати соціальну та економічну нерівність, забезпечуючи доступ до онлайн-освіти, дистанційної роботи та послуг, що раніше могли бути недоступними для певних груп людей. Таким чином, розвиток цифрової грамотності не лише покращує якість життя громадян, але й сприяє розвитку цифрової економіки, що є одним із головних напрямів розвитку держави в умовах 21 століття.

Це також має важливе значення для забезпечення рівних можливостей серед різних верств населення. Наприклад, значне зменшення частки людей без цифрових навичок свідчить про те, що більше людей, зокрема старшого віку та осіб із сільських регіонів, мають змогу долати бар'єри, які раніше заважали їхній цифровій інтеграції. Тому підвищення рівня цифрової грамотності серед цих груп є важливим елементом у зменшенні цифрового розриву і створенні більш інклюзивного суспільства. Водночас наявність базових та просунутих цифрових навичок серед більшої частини населення дозволяє забезпечити доступ до нових можливостей на ринку праці, де все частіше вимога до працівників включає вміння користуватися цифровими інструментами та технологіями.

У підсумку, позитивний розвиток цифрової грамотності не є лише технічним процесом освоєння нових технологій. Це соціальний процес, що тісно пов'язаний з усіма аспектами життя громадян. Це не лише зростання кількості користувачів інтернету або власників цифрових пристроїв, а й формування нового підходу до навчання, роботи та взаємодії між людьми в цифровому середовищі. Тому

подальше сприяння розвитку цифрових навичок серед всіх верств населення, особливо в сільських районах і серед старших людей, є необхідним кроком для забезпечення успішної адаптації країни до нових цифрових реалій.

В табл. 5.3 представлено рівень цифрових навичок серед дорослого населення, людей з порушеннями слуху та підлітків України (2023 рік).

Таблиця 5.3

Рівень цифрових навичок серед дорослого населення, людей з порушеннями слуху та підлітків України (2023 рік)

Категорія	Інформаційні навички	Комунікаційні навички	Навички вирішення життєвих проблем	Навички створення цифрового контенту
Цифрові навички дорослого населення (2023 рік)				
No skills	9,10%	8,70%	13,80%	39,80%
Basic skills	4,80%	3,40%	25,00%	19,00%
Above basic skills	86,10%	87,90%	61,20%	41,20%
Цифрові навички людей з порушеннями слуху (2023 рік)				
No skills	3,50%	2,00%	5,70%	7,40%
Basic skills	6,90%	4,40%	11,40%	9,70%
Above basic skills	89,10%	93,30%	82,80%	70,00%
Цифрові навички підлітків (2023 рік)				
No skills	7,20%	5,00%	5,80%	11,70%
Basic skills	7,20%	1,70%	11,40%	9,70%
Above basic skills	85,60%	93,30%	82,80%	78,60%

No skills: не застосовував жодну з навичок за останні 3 місяці.

Basic skills: застосовував одну навичку за останні 3 місяці.

Above basic skills: застосовував більше ніж одну навичку за останні 3 місяці

Дані: Дослідження цифрової грамотності населення України за 2023 рік
https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Згідно з наведеними даними, таблиця надає інформацію про рівень цифрових навичок серед дорослого населення, осіб з

порушеннями слуху та підлітків в Україні станом на 2023 рік. Всі ці категорії розподіляються за рівнем володіння різними цифровими навичками, такими як інформаційні, комунікаційні, навички вирішення життєвих проблем і створення цифрового контенту.

Перше, що привертає увагу, це високий рівень осіб з просунутими цифровими навичками серед дорослого населення. Зокрема, 86,1% дорослих осіб володіють рівнем навичок вище базового у сфері інформаційних навичок, що свідчить про добре розвинену цифрову грамотність серед більшості громадян України. У той же час, частка дорослих, які не мають жодних цифрових навичок, становить 9,1% у категорії інформаційних навичок, 8,7% у комунікаційних навичках і 13,8% у навичках вирішення життєвих проблем, що свідчить про наявність певного цифрового розриву в суспільстві, але в цілому рівень цифрової грамотності залишається досить високим.

Серед осіб з порушеннями слуху також спостерігається тенденція до зростання цифрових навичок. У цій категорії 89,1% мають просунуті цифрові навички в інформаційних технологіях, що є важливим для інтеграції цієї групи людей у сучасне цифрове середовище. Показник людей без цифрових навичок у групі з порушеннями слуху становить лише 3,5% в інформаційних навичках, що вказує на ефективність програм навчання і доступ до цифрових технологій для цієї групи осіб. Проте є певні категорії, де ще необхідно значно покращити рівень навчання та доступ до цифрових інструментів.

Що стосується підлітків, то більшість з них має високий рівень цифрових навичок, особливо в категорії інформаційних і комунікаційних навичок. У 2023 році 85,6% підлітків мають навички вище базового рівня в інформаційних навичках, а 93,3% – у комунікаційних навичках. Це свідчить про високий рівень цифрової освіти серед молоді, що є важливим чинником для подальшої адаптації до цифрового суспільства. Варто також відзначити, що лише 7,2% підлітків не мають цифрових навичок в інформаційних технологіях, що є досить низьким показником.

Загалом, ці дані демонструють позитивну тенденцію до покращення цифрової грамотності серед населення України в 2023 році. Рівень навичок, вищий за базовий, активно зростає, і більшість громадян, зокрема підлітки та люди з порушеннями слуху, набувають необхідних навичок для ефективної участі в цифровому середовищі. Проте все ще існують групи людей, зокрема деякі категорії дорослого населення, які мають обмежені цифрові навички. Це вимагає подальшої

роботи з підвищення рівня цифрової грамотності, зокрема серед старших верств населення та осіб з певними обмеженнями в доступі до технологій. Розвиток цифрових навичок є важливим кроком до створення більш інклюзивного та технологічно розвинутого суспільства.

В табл. 5.4 представлено динаміка цифрових навичок дорослого населення в розрізі сфер компетенцій.

Таблиця 5.4

Динаміка цифрових навичок **дорослого населення** в розрізі сфер компетенцій

Навички	2019 рік	2021 рік	2023 рік
Інформаційні навички			
No skills	18,60%	15,90%	9,10%
Basic skills	6,90%	5,10%	4,80%
Above basic skills	74,50%	78,90%	86,10%
Комунікаційні навички			
No skills	19,10%	15,60%	8,70%
Basic skills	5,60%	5,20%	3,40%
Above basic skills	75,30%	79,20%	87,90%
Навички розв'язання життєвих проблем			
No skills	20,10%	17,40%	13,80%
Basic skills	24,30%	26,70%	25,00%
Above basic skills	55,60%	55,80%	61,20%
Навички створення цифрового контенту			
No skills	52,20%	45,60%	39,80%
Basic skills	19,00%	19,70%	19,00%
Above basic skills	28,80%	36,80%	41,20%

Дані: https://osvita.diia.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Згідно з даними, представленими в таблиці, у період з 2019 по 2023 рік спостерігається поступове покращення рівня цифрових навичок серед дорослого населення України в різних сферах. Дані, що відображають зміни у сфері інформаційних, комунікаційних навичок, а також навичок вирішення життєвих проблем і створення цифрового контенту, свідчать про зростання рівня цифрової грамотності серед українців.

По-перше, у сфері інформаційних навичок частка осіб без будь-яких навичок зменшилася з 18,6% у 2019 році до 9,1% у 2023 році. Це значне зниження на 9,5% вказує на суттєве покращення ситуації, зокрема, завдяки різним ініціативам і програмам навчання, що сприяють підвищенню доступу до інформаційних технологій серед дорослого населення. У той же час, кількість людей, які мають навички на базовому рівні, також зменшилась з 6,9% до 4,8%. Це свідчить про тенденцію до розвитку більш просунутих цифрових навичок серед українців. Збільшення частки осіб з навичками вище базового рівня з 74,5% у 2019 році до 86,1% у 2023 році є важливим показником того, що значна частина дорослих громадян активно освоює новітні технології і стає все більш компетентною в інформаційних питаннях.

Щодо комунікаційних навичок, ситуація схожа. Частка осіб без комунікаційних навичок зменшилась з 19,1% у 2019 році до 8,7% у 2023 році, що також свідчить про позитивні зміни в рівні цифрової грамотності населення. Навички, які дозволяють здійснювати ефективну комунікацію в цифровому середовищі, є критичними для сучасного суспільства, тому зростання частки осіб з базовими навичками (з 5,6% до 3,4%) та навичками вище базового рівня (з 75,3% до 87,9%) є значним досягненням. Це свідчить про загальне покращення здатності українців користуватися цифровими каналами для зв'язку та обміну інформацією.

У сфері навичок вирішення життєвих проблем частка осіб без навичок зменшилася з 20,1% до 13,8%, а кількість осіб з базовими навичками залишалася стабільною, хоча і з невеликою зміною (з 24,3% до 25%). Водночас частка осіб з навичками вище базового рівня зросла з 55,6% до 61,2%. Це вказує на те, що все більше людей здатні ефективно вирішувати життєві проблеми з використанням цифрових технологій, що має особливе значення в умовах сучасного технологічного середовища, де розв'язання задач через інтернет, цифрові платформи і сервіси стає необхідним.

Відносно навичок створення цифрового контенту, дані показують, що хоча частка осіб без цих навичок була значною в 2019 році (52,2%), у 2023 році вона зменшилася до 39,8%, що є значним поліпшенням. Збільшення частки осіб з базовими навичками (з 19% до 19%) і вище базового рівня (з 28,8% до 41,2%) вказує на те, що населення поступово адаптується до нових вимог цифрового середовища, де створення контенту і вміння працювати з

мультимедійними матеріалами є важливими складовими цифрової грамотності.

Загалом, аналіз показує, що рівень цифрової грамотності серед дорослого населення України поступово зростає, і це є результатом ефективної політики у сфері цифрової освіти та надання доступу до новітніх технологій. Зменшення частки людей без цифрових навичок і зростання частки осіб з більш високим рівнем компетенцій у різних сферах є позитивними показниками того, що країна рухається в напрямку більш інклюзивного цифрового суспільства. Проте, для досягнення ще більших результатів необхідно зосередити зусилля на розвитку навичок серед старших верств населення та у віддалених регіонах, де доступ до цифрових ресурсів може бути обмежений.

В табл. 5.5 представлено динаміка цифрових навичок підлітків у розрізі сфер компетенцій.

Таблиця 5.5

Динаміка цифрових навичок підлітків у розрізі сфер компетенцій

Навички	2019 рік	2021 рік	2023 рік
Інформаційні навички			
No skills	7,30%	4,90%	7,20%
Basic skills	16,60%	16,80%	7,20%
Above basic skills	76,10%	78,30%	85,60%
Комунікаційні навички			
No skills	7,30%	6,80%	5,00%
Basic skills	6,50%	4,40%	1,70%
Above basic skills	86,20%	88,80%	93,30%
Навички розв'язання життєвих проблем			
No skills	0%	1,50%	5,70%
Basic skills	11,70%	18,00%	11,40%
Above basic skills	88,30%	80,50%	82,80%
Навички створення цифрового контенту			
No skills	7,30%	11,50%	11,70%
Basic skills	6,50%	11,50%	9,70%
Above basic skills	86,20%	77,00%	78,60%

Дані: https://osvita.diia.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Згідно з наданими даними, таблиця показує динаміку цифрових навичок серед підлітків в Україні за період з 2019 по 2023 рік у різних сферах компетенцій, таких як інформаційні навички, комунікаційні навички, навички вирішення життєвих проблем та створення цифрового контенту. Спостерігається значний прогрес у розвитку цифрових навичок серед підлітків, що свідчить про позитивні зміни в підготовці молоді до цифрового суспільства.

Перше, на що варто звернути увагу, це зменшення частки підлітків без інформаційних навичок. Якщо в 2019 році 7,3% підлітків не мали таких навичок, то до 2023 року цей показник знизився до 7,2%. Це свідчить про поступове підвищення рівня цифрової грамотності серед молоді, хоча проблема все ще існує, і необхідно продовжувати працювати над усуненням цифрового розриву. Частка підлітків з базовими інформаційними навичками залишалася на стабільному рівні: 16,6% у 2019 році, 16,8% у 2021 році та 7,2% у 2023 році, що вказує на тренд до освоєння більш просунутих навичок. У той же час, частка підлітків з навичками вище базового рівня зросла з 76,1% у 2019 році до 85,6% у 2023 році, що свідчить про зростання цифрових компетенцій серед молоді та здатність її активно використовувати новітні технології для вирішення різних завдань.

У сфері комунікаційних навичок спостерігається подібна тенденція. Якщо в 2019 році 7,3% підлітків не мали комунікаційних навичок, то до 2023 року цей показник зменшився до 5%. Це є важливим показником того, що все більше підлітків здатні ефективно використовувати цифрові інструменти для комунікації та взаємодії в цифровому середовищі. Частка осіб з базовими навичками у цій сфері зменшилася з 6,5% до 1,7%, що вказує на підвищення рівня володіння комунікаційними технологіями на більш просунутому рівні. Водночас частка підлітків з навичками вище базового рівня зросла з 86,2% до 93,3%, що є свідченням значного покращення їх здатності до ефективної комунікації через цифрові платформи.

У сфері навичок вирішення життєвих проблем спостерігається ще більший прогрес. У 2019 році 0% підлітків не мали навичок у цій сфері, однак до 2023 року цей показник збільшився до 5,7%. Частка підлітків з базовими навичками зросла з 11,7% до 11,4%, а частка з навичками вище базового рівня зменшилася з 88,3% до 82,8%. Це вказує на загальний тренд до зростання здатності підлітків використовувати цифрові технології для вирішення реальних життєвих задач і проблем, хоча є певні коливання в рівні базових навичок.

Що стосується навичок створення цифрового контенту, то також спостерігається поступовий прогрес. У 2019 році 7,3% підлітків не мали таких навичок, у 2023 році цей показник зменшився до 11,7%. Частка підлітків з базовими навичками залишалася стабільною – 6,5% у 2019 році та 9,7% у 2023 році, а частка з навичками вище базового рівня збільшилась з 86,2% до 78,6%, що вказує на покращення здатності підлітків створювати цифровий контент.

Загалом, аналіз цих даних показує, що підлітки в Україні поступово набувають все більших цифрових навичок. Це є важливим фактором для їхньої адаптації до швидко змінюваного цифрового середовища, а також для підготовки їх до майбутнього, де цифрові технології будуть невід'ємною частиною професійного та особистого життя. Проте для досягнення ще кращих результатів необхідно продовжувати працювати над розвитком цифрових навичок серед підлітків, зокрема в тих сферах, де спостерігається ще певна недосагнутість, таких як навички створення цифрового контенту.

В табл. 5.6 представлено динаміку цифрових навичок людей з порушеннями слуху у розрізі сфер компетенцій.

Таблиця 5.6

Динаміка цифрових навичок людей з порушеннями слуху у розрізі сфер компетенцій

Навички	2019 рік	2021 рік	2023 рік
Інформаційні навички			
No skills	22,40%	10,10%	3,50%
Basic skills	5,90%	37,20%	4,70%
Above basic skills	71,70%	52,70%	91,80%
Комунікаційні навички			
No skills	17,40%	42,10%	2,00%
Basic skills	2,70%	0,30%	1,20%
Above basic skills	79,90%	57,60%	96,80%
Навички розв'язання життєвих проблем			
No skills	24,70%	6,30%	5,70%
Basic skills	13,20%	46,70%	24,30%
Above basic skills	62,10%	47,00%	70,00%
Навички створення цифрового контенту			
No skills	34,20%	18,30%	37,40%
Basic skills	16,90%	17,50%	21,30%
Above basic skills	48,90%	64,20%	41,30%

Дані: https://osvita.diia.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Згідно з даними, наведеними в таблиці, спостерігається позитивна динаміка розвитку цифрових навичок серед людей з порушеннями слуху в Україні за період з 2019 по 2023 рік. Ці навички були оцінені в чотирьох категоріях: інформаційні навички, комунікаційні навички, навички вирішення життєвих проблем та створення цифрового контенту. Розглянемо докладно, як змінився рівень цифрової грамотності цієї групи населення.

У категорії інформаційних навичок частка людей без навичок зменшилась з 22,4% у 2019 році до 3,5% у 2023 році. Це є значним покращенням, яке вказує на зменшення цифрового розриву серед цієї групи. Водночас, частка осіб з базовими навичками збільшилась з 5,9% до 4,7%, що є ознакою того, що більш складні цифрові технології стають доступними для цієї групи. Частка осіб з навичками вище базового рівня зросла з 71,7% до 91,8%, що свідчить про зростання рівня цифрових компетенцій серед людей з порушеннями слуху і їх здатність користуватися складнішими цифровими інструментами для вирішення різних завдань.

Аналогічна позитивна динаміка спостерігається у сфері комунікаційних навичок. Якщо в 2019 році 17,4% людей з порушеннями слуху не мали таких навичок, то в 2023 році цей показник зменшився до 2%. Це означає, що все більше осіб здатні ефективно використовувати цифрові інструменти для комунікації. Частка людей з базовими комунікаційними навичками залишилась стабільною (з 2,7% до 1,2%), але зростання частки осіб з навичками вище базового рівня з 79,9% до 96,8% є вражаючим результатом. Це підтверджує високий рівень володіння комунікаційними технологіями серед цієї групи людей.

У сфері навичок вирішення життєвих проблем також спостерігається значне покращення. Частка осіб без таких навичок зменшилась з 24,7% у 2019 році до 5,1% у 2023 році. Водночас частка людей з базовими навичками зросла з 13,2% до 24,3%. Збільшення частки осіб з навичками вище базового рівня з 62,1% до 70% свідчить про те, що люди з порушеннями слуху дедалі більше здатні використовувати цифрові технології для вирішення життєвих проблем, таких як доступ до медичних послуг, освіти та комунікацій.

У категорії навичок створення цифрового контенту частка осіб без навичок зменшилась з 34,2% до 37,4%, що також є покращенням, але все ще залишається значним бар'єром для подолання. Зростання частки осіб з базовими навичками у цій сфері (з 16,9% до 21,3%) вказує

на позитивну динаміку, але найбільше покращення спостерігається серед осіб з навичками вище базового рівня, де частка збільшилась з 48,9% до 64,2%. Це означає, що все більше людей з порушеннями слуху здатні створювати цифровий контент, що є важливим аспектом для їх соціалізації та участі в сучасному цифровому світі.

Загалом, аналіз показує, що в Україні спостерігається значне покращення рівня цифрової грамотності серед людей з порушеннями слуху. Зменшення частки осіб без цифрових навичок і збільшення числа людей з просунутими навичками є свідченням успіху програм з цифрової освіти та доступу до новітніх технологій для цієї групи населення. Проте ще є сфери, в яких потрібно продовжувати роботу, зокрема у створенні цифрового контенту, де покращення рівня навичок потребує більш інтенсивних зусиль.

В табл. 5.7 представлено досвід користування українськими платформами для самоосвіти онлайн за останні 12 місяців (дослідження 2023 року).

Таблиця 5.7

Досвід користування українськими платформами для самоосвіти онлайн за останні 12 місяців (дослідження 2023 року)

Категорія	Так, є досвід користування	Ні, немає досвіду користування
Доросле населення	23,40%	76,60%
Люди з порушеннями слуху	16,60%	83,40%
Підлітки	42,30%	57,70%

Дані: https://osvita.diia.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Згідно з даними, наведеними в таблиці, у 2023 році було проведено дослідження, яке показало рівень використання українських платформ для самостійного онлайн-навчання серед різних груп населення за останні 12 місяців.

Зокрема, серед дорослого населення 23,4% осіб мають досвід користування українськими онлайн-платформами для самонавчання, в той час як 76,6% не користуються ними. Це свідчить про певний рівень відсутності цифрової грамотності або доступу до таких ресурсів серед дорослих громадян, що потребує подальшого розвитку інфраструктури та підтримки ініціатив з цифрового навчання.

Серед людей з порушеннями слуху лише 16,6% мають досвід користування українськими платформами для самостійного навчання

онлайн. Водночас, 83,4% не користуються такими платформами. Це може вказувати на існуючі бар'єри, пов'язані з доступністю таких платформ для цієї групи людей, що може бути спричинено обмеженим доступом до спеціалізованих ресурсів або недостатньою кількістю онлайн-курсів, адаптованих для людей з порушеннями слуху.

Що стосується підлітків, то 42,3% з них активно користуються українськими платформами для самонавчання онлайн, в той час як 57,7% не мають такого досвіду. Це вказує на значний потенціал для розвитку в цій категорії, оскільки молодь активно використовує онлайн-ресурси для освіти. Однак важливо зазначити, що частка підлітків, які не користуються такими платформами, все ж є досить значною, що вказує на необхідність подальшого розширення доступу до онлайн-освіти.

Загалом, ці дані свідчать про те, що хоча українські онлайн-платформи для самонавчання набувають популярності, все ще існують значні соціальні групи, де доступ до таких ресурсів є обмеженим. Це вимагає подальших зусиль з розширення доступу до онлайн-освіти, зокрема для людей з порушеннями слуху та серед старших поколінь.

В табл. 5.8 представлено причини некористування українськими платформами для самоосвіти онлайн серед цільових груп.

Таблиця 5.8

Причини некористування українськими платформами для самоосвіти онлайн серед цільових груп

Причини	Доросле населення	Люди з порушеннями слуху	Підлітки
1	2	3	4
Не знаю про наявність таких сервісів	42,00%	38,90%	55,90%
Мені не цікаві теми, які пропонують ці платформи	28,30%	21,40%	9,20%
Я використовую інші ресурси для освітніх цілей (Google, youtube, блог тощо)	14,20%	7,40%	19,20%
Відсутність потреби/бажання у навчанні	4,60%	1,30%	3,50%
Мене не цікавить онлайн навчання	3,50%	2,10%	9,10%
Не використовую інтернет	1,80%	0,90%	0,90%
Не маю достатніх коштів для навчання онлайн	3,40%	8,30%	3,50%

продовження табл. 5.8

1	2	3	4
У мене немає технічного обладнання для навчання онлайн	3,20%	2,10%	0,90%
Рівень моїх знань слабкий, якість інформації, яка подається на освітніх платформах не відповідає моїм потребам	1,60%	0,90%	2,00%
Відсутність часу для навчання	1,30%	1,00%	1,80%
Не довіряю розробникам платформ	0,70%	1,00%	0,90%
Мені не подобається формат подачі інформації	1,00%	0,70%	0,90%
Не сумісність цього професійного напрямку з моєю роботою або іншими зобов'язаннями	0,60%	0,30%	0,00%
Інше	1,30%	2,10%	1,80%
Важко відповісти	4,50%	25,50%	3,50%

Дані: https://osvita.dii.gov.ua/uploads/1/8800ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Аналіз причин некористування українськими онлайн-платформами для самоосвіти серед різних цільових груп дозволяє виявити кілька ключових факторів, які значно впливають на використання таких сервісів. Першою і найбільш поширеною причиною серед усіх груп є незнання про наявність таких платформ. Це вказує на недостатню інформованість населення щодо доступних освітніх можливостей. Особливо це стосується підлітків, де майже 56% з них не мають інформації про наявність онлайн-ресурсів для навчання. Така ситуація свідчить про необхідність активніших просвітницьких кампаній, спрямованих на інформування громадян, зокрема через школи, соціальні мережі та інші канали, які доступні для молоді.

Іншою важливою причиною є відсутність інтересу до тем, що пропонуються на цих платформах. Це є досить актуальним для дорослого населення, де 28,3% не зацікавлені у пропонованих темах. Люди, що не знайшли себе у цих платформах, можуть шукати більше індивідуальних або практичних курсів, що відповідають їхнім конкретним потребам, особливо в професійній сфері. Це може свідчити про те, що контент, який пропонується на платформі, може бути

занадто загальним або не достатньо спеціалізованим для деяких груп користувачів.

Ще однією причиною є використання альтернативних ресурсів для навчання, таких як Google, YouTube чи блоги, що є основним джерелом для 14,2% дорослих і 19,2% підлітків. Це свідчить про те, що ці користувачі вже мають доступ до безкоштовних і більш гнучких інструментів для навчання. Вони можуть використовувати ці ресурси для вивчення тем, що їх цікавлять, без необхідності реєстрації або структурованих курсів. Така тенденція вказує на потребу платформ для самоосвіти адаптувати свої пропозиції і зробити їх більш інтуїтивно зрозумілими та доступними.

Відсутність потреби чи бажання в навчанні також є фактором, який суттєво впливає на рівень користування платформами. Це може бути пов'язано з низьким рівнем мотивації серед певних груп, особливо дорослих, які можуть бути зайняті професійними або сімейними обов'язками і не знаходити часу на навчання. Однак для молоді ця причина не є такою актуальною, оскільки вони, як правило, мають більше часу для навчання, але, як показує статистика, часто не можуть знайти цікаві та актуальні курси на існуючих платформах.

Не менш важливим фактором є фінансова складова – для деяких категорій населення, особливо для людей з обмеженими фінансовими можливостями, плата за доступ до онлайн-освіти може бути суттєвою перешкодою. Це підтверджується тим, що 3,4% дорослих і 8,3% людей з порушеннями слуху відзначають, що не мають достатніх коштів для навчання онлайн. Платформи, які пропонують платні послуги, можуть бути недоступними для цих груп, тому розвиток безкоштовних або частково безкоштовних освітніх програм є важливим напрямом.

З технічної точки зору, проблема доступу до обладнання є важливою для деяких груп, зокрема для 3,2% дорослих і 2,1% людей з порушеннями слуху, які не мають необхідного технічного забезпечення для навчання онлайн. У цьому контексті забезпечення доступу до сучасних пристроїв і інтернет-ресурсів є критичним для того, щоб зробити онлайн-освіту доступною для більшої кількості людей.

Незважаючи на різноманітність причин, можна зробити висновок, що для подолання бар'єрів у користуванні українськими платформами для самоосвіти необхідно зосередити зусилля на кількох ключових аспектах: інформування населення про доступні ресурси, розширення тематики курсів, адаптація контенту до інтересів різних цільових груп, створення безкоштовних або доступних навчальних

платформ, а також забезпечення технічної доступності для всіх верств населення. Ці заходи допоможуть розширити доступ до освіти і зробити онлайн-навчання більш ефективним і привабливим для всіх категорій громадян.

5.3. Портал Дія для підвищення цифрової грамотності населення в Україні

В табл. 5.9 представлено опис національної онлайн-платформи для розвитку цифрової грамотності «Дія.Освіта».

Таблиця 5.9

Опис національної онлайн-платформи для розвитку цифрової грамотності «Дія.Освіта»

Параметр	Опис
1	2
Назва платформи	«Дія. Освіта» https://osvita.diia.gov.ua/
Опис	Платформа, що спрямована на розвиток цифрових навичок серед українців, надаючи доступ до онлайн-курсів з основних цифрових навичок, таких як безпека в інтернеті, використання електронних послуг, фінансова грамотність тощо.
Запуск	Платформа була запущена в 2020 році як частина державної ініціативи для підвищення цифрової грамотності в Україні.
Цільова аудиторія	Платформа орієнтована на широкий спектр користувачів: від школярів і студентів до пенсіонерів, а також на людей з обмеженими можливостями.
Основні функції	- онлайн-курси для різних рівнів цифрових навичок. - сертифікація навичок цифрової грамотності. - доступ до ресурсів для навчання використанню державних послуг. - різноманітні навчальні модулі з цифрової безпеки, роботи з е-урядами, електронними документами.
Курси	Платформа пропонує курси з різних тем, включаючи: - цифрова безпека та захист особистих даних. - як користуватися державними онлайн-послугами (платформами «Дія», електронними послугами тощо). - основи роботи з Інтернетом.
Доступність	Платформа доступна безкоштовно для всіх громадян України через інтернет. Курси можна проходити в будь-який час, без необхідності відвідувати навчальні заклади.
Методи навчання	Курси складаються з відеоуроків, тестів та інтерактивних завдань, що дозволяє користувачам вивчати матеріал в зручному темпі.

1	2
Сертифікація	Після проходження курсів учасники отримують сертифікат про проходження, що підтверджує рівень їхніх цифрових навичок.
Співпраця	Платформа співпрацює з провідними освітніми установами, державними органами та міжнародними організаціями для створення та оновлення навчальних матеріалів.
Підтримка	На платформі доступна підтримка у вигляді технічної допомоги та консультацій щодо проходження курсів.
Особливості	Платформа адаптована до потреб різних верств населення, включаючи осіб з обмеженими можливостями.
Партнери	Платформа «Дія. Цифрова освіта» є частиною ініціативи Міністерства цифрової трансформації України, а також співпрацює з різними державними органами та приватними компаніями для поліпшення цифрових послуг.
Досягнення	З моменту запуску платформа дозволила навчити сотні тисяч українців цифровим навичкам, що стало важливим кроком у розвитку цифрової економіки в Україні.

Дія.Освіта для всіх ▾



Рис. 5.2. «Дія. Освіта» <https://osvita.diia.gov.ua/>

Рис. 5.2 демонструє інтерфейс української онлайн-платформи для самоосвіти «Дія. Освіта», що пропонує різноманітні освітні ресурси

для користувачів, зокрема освітні серіали, тести, симулятори, гіді, вебінари, подкасти та події. Така структура платформи дозволяє користувачам обирати різні формати навчання, що робить її зручною та доступною для широкої аудиторії. Важливим є те, що платформа орієнтована на різні рівні навчання і надає інструменти для самостійного розвитку в різних сферах знань, що сприяє підвищенню цифрової грамотності та надає можливість отримати корисні знання у зручному форматі.

На сайті «Дія. Освіта» можна обирати напрямок навчання рис. 5.3.

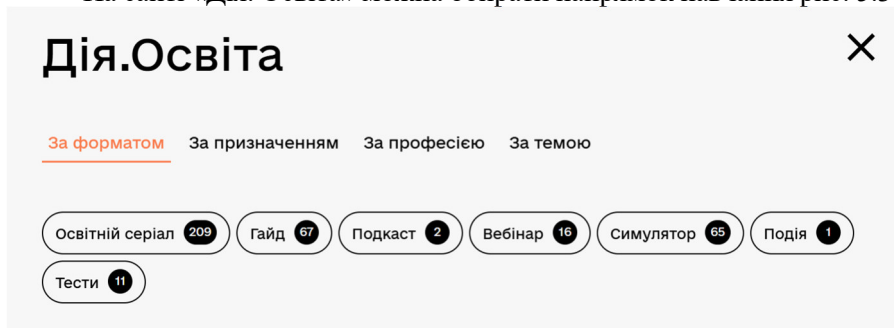


Рис. 5.3. «Дія. Освіта» за напрямком навчання <https://osvita.diia.gov.ua/>

Рис. 5.3 відображає інтерфейс платформи «Дія. Освіта», яка пропонує широкий спектр освітніх ресурсів для різних цільових груп громадян України. Цей сервіс надає можливість вибору курсів за напрямками навчання, що охоплюють безліч професійних та інтересових категорій, таких як курси для криптоентузіастів, державних службовців, медичних працівників, бізнесменів, учителів, школярів, активних громадян, батьків, підлітків та стартаперів. Платформа дозволяє користувачам обирати курси, які відповідають їхнім потребам та інтересам, що підвищує ефективність навчання та забезпечує гнучкість у виборі формату освіти. Така різноманітність курсів забезпечує доступність освіти для різних верств населення, сприяючи розвитку цифрових навичок, професійної кваліфікації та особистісного зростання в умовах сучасного інформаційного середовища. Платформа «Дія. Освіта» таким чином виступає важливим інструментом для саморозвитку громадян і підвищення їх професійної та цифрової грамотності.

На рис. 5.4 представлено напрямки навчання «за призначенням».

За форматом За призначенням За професією За темою

Рис. 5.4. «Дія. Освіта» навчання «за призначенням»

Розділ «За призначенням» на платформі «Дія. Освіта» представляє широкий спектр навчальних курсів, орієнтованих на різні категорії користувачів, що дає можливість кожній групі знайти відповідні ресурси для свого розвитку. Це дозволяє людям з різними професійними, соціальними та інтересовими спрямуваннями отримувати доступ до освітніх можливостей, які найкраще відповідають їхнім потребам.

Курси для криптоентузіастів орієнтовані на людей, які бажають глибше вивчити криптовалюту та технології блокчейн. Це включає вивчення основ криптографії, особливостей роботи з криптовалютами, а також безпеки в цій сфері. Це дуже актуальний напрямок, враховуючи зростаючий інтерес до криптовалют у всьому світі, зокрема в Україні.

Для державних службовців розроблені курси, які дозволяють покращити навички в управлінні, підвищити ефективність роботи органів влади та навчитися впроваджувати нові технології в державне управління. Курси включають питання електронного урядування, використання цифрових інструментів в адміністративних процесах, а також покращення комунікації з громадянами.

Медичні працівники мають можливість пройти курси, що охоплюють новітні досягнення в медицині, медичну етику, технології для покращення догляду за пацієнтами, а також вдосконалення навичок у використанні медичних технологій. Це особливо важливо для підвищення кваліфікації медичних працівників та їх здатності працювати з новими медичними інструментами і технологіями.

Курси для бізнесменів і підприємців орієнтовані на навчання сучасним бізнес-практикам, фінансовому менеджменту, маркетингу,

управлінню проектами та розвиткові стартапів. Підприємці можуть отримати корисні знання щодо ефективного ведення бізнесу, оптимізації витрат, використання інноваційних технологій для розвитку підприємств та вдосконалення стратегій маркетингу.

Освітні ресурси для вчителів дозволяють покращити педагогічні навички, включаючи новітні методики навчання, використання цифрових технологій у викладанні та вдосконалення інструментів для інтерактивного навчання. Це допомагає вчителям адаптувати свої методи до сучасних умов освіти, що є важливим для розвитку освіти в Україні.

Новачки можуть знайти курси, які допомагають освоїти базові навички у різних галузях. Це курси для тих, хто тільки починає свій шлях у професійному розвитку або вивчає нові для себе сфери. Такий підхід дає можливість швидко освоїти основи і забезпечити старт для подальшого розвитку.

Курси для школярів включають навчальні програми, спрямовані на підтримку учнів у їхньому навчанні, розвиток критичного мислення, освоєння нових технологій, а також доповнення шкільної програми, що дозволяє підготувати молодь до викликів майбутнього.

Тренери отримують доступ до спеціалізованих програм, які дозволяють удосконалити навички навчання, методики тренінгів, психолого-педагогічні аспекти роботи з різними групами. Це також включає вивчення новітніх підходів у сфері фізичного виховання та розвитку м'яких навичок.

Курси для батьків орієнтовані на виховання дітей, психолого-педагогічні методи, а також на підтримку родинного розвитку в умовах сучасних викликів. Це важливий напрямок, оскільки допомагає батькам стати кращими наставниками та підтримати дітей в їхньому особистісному розвитку.

Активні громадяни можуть знайти курси, що зосереджені на розвитку громадянської свідомості, участі в місцевих ініціативах, а також на формуванні навичок ефективної взаємодії з органами влади та іншими громадськими організаціями.

Для підлітків пропонуються курси, що допомагають їм зрозуміти свої професійні інтереси, освоїти базові навички для майбутнього навчання та кар'єрного росту, а також розвивати критичне мислення та здатність працювати в команді.

Стартапери можуть отримати корисні знання для запуску і розвитку власних бізнес-ідей, оптимізації процесів в стартапах та

залучення інвестицій. Це сприяє розвитку підприємницької ініціативи серед молоді та людей, які прагнуть реалізувати свої бізнес-проекти.

Ця структура курсу, орієнтованого на конкретні категорії користувачів, дозволяє кожному знайти саме те, що відповідає його професійним або особистим потребам, що є важливим для розвитку навичок і підвищення кваліфікації в сучасному цифровому світі.

На рис. 5.5 представлено навчання «за професією».

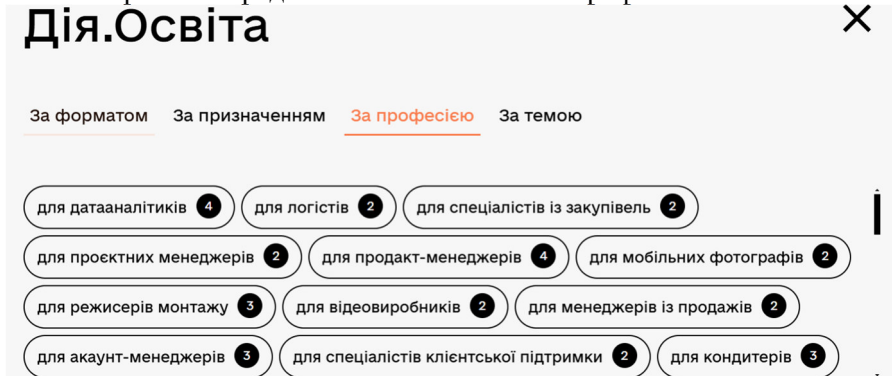


Рис. 5.5. «Дія. Освіта» навчання «за професією»

Рис. 5.5 показує розділ платформи «Дія. Освіта», де курси орієнтовані на конкретні професії. Користувачі можуть знайти навчальні програми для датааналітиків, логістів, спеціалістів з закупівель, проєктних менеджерів, продукт-менеджерів, мобільних фотографів, монтажників, відеовиробників, менеджерів з продажу, акаунт-менеджерів, спеціалістів клієнтської підтримки та консультантів. Це дозволяє професіоналам покращити навички у своїй галузі та адаптуватися до нових вимог на ринку праці.

На рис. 5.6 представлено навчання «за темою».

Зображення демонструє розділ платформи «Дія. Освіта» за темами, де користувачі можуть обирати курси, що відповідають їхнім інтересам або потребам у конкретних галузях. Доступні курси з таких тем, як Re/UpSkilling (перепідготовка та розвиток нових навичок), Open Data (відкриті дані), Підтримка ветеранів та реінтеграція, Працевлаштування, Онлайн-безпека, Громадянське суспільство, Урбаністика, Ментальне здоров'я, Військова служба, Туризм та дозвілля, Антикорупція, Безпека, Безбар'єрність, Вибори та Державні послуги.

За форматом За призначенням За професією За темою

Рис. 5.6. «Дія. Освіта» навчання «за темою»

Цей набір курсів охоплює важливі для суспільства теми, що дозволяють громадянам отримувати необхідні знання для покращення професійних навичок, особистісного розвитку та активної участі в житті країни. Платформа пропонує можливості для саморозвитку в різних сферах, що має велике значення для підвищення рівня освіти та громадської свідомості серед населення.

Для підвищення цифрової грамотності варто звертати увагу на освітні серіали, які є запропоновані для проходження навчання на порталі.

Навчання за допомогою освітніх серіалів на порталі «Дія. Освіта» проходить у вигляді структурованих відео-уроків, що охоплюють різноманітні теми та навички. Освітні серіали на платформі призначені для того, щоб допомогти користувачам отримувати знання у зручному та доступному форматі. Зазвичай вони поділяються на кілька серій, кожна з яких розкриває конкретну тему або аспект обраної галузі.

Процес навчання включає перегляд серій, де кожен етап подається у вигляді інформативних відео з поясненнями, прикладами та корисними порадами. Користувачі можуть проходити ці серії в будь-який час, у зручному для себе темпі. Після кожного уроку часто передбачені тести або практичні завдання, щоб перевірити засвоєні знання та навички. Це дозволяє не тільки слухати матеріал, але й активно включитися в навчальний процес.

Платформа дає можливість переглядати серії заново, якщо потрібно, або повертатися до важливих моментів для кращого засвоєння матеріалу. Такий формат навчання особливо підходить для

тих, хто хоче отримувати знання поступово, без необхідності відвідувати традиційні заняття або проходити складні курси.

Освітні серіали на «Дія. Освіта» зручні тим, що дають змогу навчатись у будь-який час, використовувати мобільні пристрої для доступу до матеріалів, а також дають можливість інтерактивного навчання через додаткові ресурси та інструменти, що забезпечують повну зануреність у тему.

У навчанні на платформі «Дія. Освіта», зокрема під час проходження освітніх серіалів, також можуть бути використані бали ЄКТС (Європейської кредитно-трансферної системи). ЄКТС – це система оцінювання, що використовується для стандартизації навчальних досягнень у рамках Європейського Союзу та забезпечує взаємне визнання освітніх результатів між навчальними закладами.

Бали ЄКТС на платформі «Дія. Освіта» зазвичай нараховуються за кожен успішно завершений курс чи серію, що дозволяє користувачам отримати офіційне підтвердження своїх досягнень у вигляді цифрового сертифікату. Кожен курс або серія оцінюються в певну кількість балів, що визначають загальний обсяг навчального навантаження для користувача.

Ця система балів забезпечує прозорість і узгодженість у вимірюванні досягнень учасників, а також дозволяє учасникам курсів більш чітко оцінювати рівень своїх досягнень у порівнянні з іншими освітніми програмами. Бал ЄКТС також може бути важливим інструментом при переведенні або визнаванні навчальних досягнень у інших освітніх установах або під час працевлаштування, оскільки це універсальна одиниця вимірювання результатів навчання.

Для прикладу одного із навчальних серіалів для підвищення цифрової грамотності можна виділити один із останніх серіалів а саме ***«Кібергігієна для молоді»***.

На рис. 5.7 представлено **приклад освітнього серіалу «Кібергігієна для молоді»**.

Освітній серіал на платформі «Дія.Освіта» допомагає молоді зрозуміти основні принципи кібербезпеки та захисту особистих даних від кіберзлочинців. Кожна серія містить корисні поради щодо безпечного користування інтернетом, зокрема електронною поштою, захисту акаунтів та уникання шахрайських сайтів. Освітній серіал був створений за ініціативи Мінцифри, Національного координаційного центру кібербезпеки та Національного університету «Києво-Могилянська Академія» за підтримки проєкту USAID.

продовження табл. 5.10

1	2	3	4
3.	Хто захищає нас від кіберзлочинців?	Огляд кіберзахисту в Україні, роль СБУ, Кіберполіції та Держспецзв'язку. Як реагувати на кіберінциденти.	4 хв
4.	Злам. Як діють кіберзлочинці	Методи зламу, включаючи технічні і соціальну інженерію, приклади атак, такі як DDoS на Telegram.	4 хв
5.	Безпека гаджетів	Як захистити свої гаджети від крадіжки або втрати, важливість паролів, шифрування, блокування.	3 хв
6.	Як софт забезпечує кібергігієну	Вплив програмного забезпечення на безпеку, важливість оновлення і використання перевірених додатків.	4 хв
7.	(Анти) Віруси	Різні види вірусів і їх вплив на пристрої. Як антивіруси допомагають захистити дані.	4 хв
8.	Зберігайся. Резервні копії	Важливість резервних копій, метод 3-2-1, автоматичне резервування та шифрування для захисту файлів.	4 хв
9.	Все про паролі	Як створювати надійні паролі, використання менеджерів паролів і загрози, пов'язані з простими паролями.	4 хв
10.	Подвійний захист	Як двофакторна аутентифікація забезпечує додатковий рівень захисту акаунтів. Різні види аутентифікації.	3 хв
11.	Безпека мережі	Захист від загроз в публічних Wi-Fi мережах, шифрування, використання VPN, налаштування DNS-серверів.	5 хв
12.	Фішинг: як хакери крадуть ваші дані	Різновиди фішингу та методи захисту від них: електронний, смс-фішинг, вебфішинг, дїпфейк-фішинг.	7 хв
13.	Захисти свій e-mail	Як захистити свою пошту від фішингових атак, використання резервних скриньок, плюс-адресація.	3 хв
14.	Не давай свій номер хакеру	Як захистити номер телефону від шахраїв, важливість PIN-коду для SIM-карти, заходи захисту.	3 хв
15.	Безпека банківських карток	Як захистити картки від шахраїв під час онлайн-покупок, важливість CVV-коду, використання 3-D Secure.	3 хв
16.	Контент під твоїм контролем	Як налаштувати приватність в інтернеті, контролювати геолокацію, захищати особисту інформацію.	5 хв
17.	FOMO – небезпека знати все	Як обирати надійні новинні джерела, перевіряти інформацію і уникати інформаційного перевантаження.	3 хв

Цей серіал допомагає молоді засвоїти основи кібербезпеки, навчаючи їх захищати свої персональні дані та уникати загроз в інтернеті. Навчання на освітньому серіалі «Кібергігієна для молоді» завершується фінальним тестом, який допомагає перевірити засвоєні знання та навички. Тест охоплює основні теми серіалів, дозволяючи учасникам оцінити рівень розуміння матеріалу та перевірити, як добре вони засвоїли правила кібербезпеки та захисту особистих даних. Після успішного проходження тесту учасники отримують сертифікат, який підтверджує їхню кваліфікацію в галузі кібергігієни.

Для отримання сертифікату необхідно виконати наступні кроки. Спочатку потрібно переглянути всі серії освітнього серіалу. Під кожною серією розміщено міні-тест, який слід пройти. По завершенню навчання буде доступне фінальне тестування. Для отримання сертифікату необхідно успішно пройти це тестування.

Отже, портал «Дія» став важливим інструментом для підвищення цифрової грамотності населення в Україні, забезпечуючи доступ до різноманітних освітніх ресурсів та сервісів, спрямованих на розвиток навичок користування цифровими технологіями. Через платформу «Дія. Освіта» громадяни можуть отримати знання у сферах кібербезпеки, цифрової грамотності, особистої безпеки в інтернеті та багатьох інших актуальних темах. Платформа також пропонує курси, що орієнтовані на конкретні професії, дозволяючи користувачам удосконалювати професійні навички, покращувати кар'єрні перспективи та інтегруватися в цифровий простір.

Завдяки зручному формату навчання, що включає освітні серіали, тести та інтерактивні завдання, платформа дозволяє досягати високих результатів навіть тим, хто тільки починає свій шлях у світі цифрових технологій. Зокрема, серіали з кібергігієни є важливим етапом у боротьбі з кіберзлочинністю та шахрайством, допомагаючи молоді і дорослим краще розуміти загрози в інтернеті і як захистити свої дані.

У зв'язку з глобальними викликами цифровізації та швидкими змінами в інформаційних технологіях, платформа «Дія» є не лише інструментом для підвищення цифрової грамотності, а й важливим ресурсом для розвитку суспільства, що здатне ефективно взаємодіяти з новітніми технологіями та адаптуватися до умов цифрового світу. Вона робить освіту доступною для кожного громадянина, підтримуючи принципи інклюзивності та рівного доступу до знань.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Що таке цифрова грамотність і чому вона є важливою для кожної людини?
2. Які основні компоненти входять у цифрову грамотність, крім вміння користуватися комп'ютером та Інтернетом?
3. Як рівень цифрової грамотності впливає на успішність людини в професійному та особистому житті?
4. Чому важливо підвищувати цифрові навички серед старшого покоління та людей з обмеженими можливостями?
5. Які основні проблеми заважають високому рівню цифрової грамотності в Україні?
6. Яка роль цифрової грамотності у забезпеченні ефективного впровадження цифрових технологій у державному управлінні та економіці?
7. Які навички охоплюють основи цифрової грамотності?
8. Як розвиток цифрової грамотності допомагає зменшити цифровий розрив між різними соціальними групами?
9. Яким чином платформи, такі як «Дія. Освіта», сприяють розвитку цифрової грамотності серед громадян України?
10. Як освітні серіали на платформі «Дія. Освіта» сприяють підвищенню рівня цифрової грамотності та захисту персональних даних?

ЗАВДАННЯ ДЛЯ ПРАКТИЧНИХ ЗАНЯТЬ

1. Створіть електронний документ у форматі PDF і підпишіть його за допомогою електронного підпису. Поясніть процес підписання та надайте зразок підписаного документа.
2. Дослідіть різні формати електронного підпису (XAdES, PAdES, CAdES) і створіть приклад підпису в кожному з них.
3. Ознайомтесь із платформою для петицій, що використовуються в Україні і створіть петицію щодо актуальної проблеми.
4. Зареєструйтесь в електронній системі документообігу або державних послуг (наприклад, у системі «Дія»), створіть профіль користувача та збережіть дані.
5. Створіть налаштування для введення в систему електронного документообігу (наприклад, налаштування прав доступу користувачів, створення шаблонів документів).
6. Порівняйте процеси обробки документа в традиційному паперовому вигляді та в електронній формі. Створіть таблицю з порівнянням плюсів і мінусів.
7. Використовуючи статистику, проаналізуйте рівень цифрової грамотності населення України. Оцініть необхідні навички для використання електронного врядування.
8. Напишіть електронне звернення через державний портал (наприклад, портал «Дія») і опишіть процес обробки такого звернення в системі електронного врядування.
9. Створіть модель електронного документообігу для умов малих організацій, враховуючи специфіку роботи з документами в електронному форматі.
10. Оцініть безпеку електронного документообігу в організації, досліджуючи існуючі вразливості в програмному забезпеченні.
11. Створіть план для розробки електронного архіву документів, враховуючи вимоги до безпеки та збереження даних.
12. Побудуйте схему процесу затвердження електронного документа (від його створення до підписання), вказуючи етапи та ролі користувачів.
13. Оцініть, як забезпечується захист персональних даних у системах електронного документообігу, і розробіть план заходів для підвищення безпеки.

14. Досліджуйте, як електронний документообіг може бути інтегрований із іншими інформаційними системами організації, такими як CRM, ERP тощо.

15. Створіть політику доступу для користувачів системи електронного документообігу в організації, включаючи різні рівні доступу до документів та їх обробки.

16. Ознайомтесь з актуальними законодавчими ініціативами щодо електронного документообігу в Україні (наприклад, закони про електронний підпис) та оцініть їх вплив на організації.

17. Проведіть тестування системи електронного документообігу в організації, оцініть її ефективність, швидкість обробки документів і надайте рекомендації для покращення.

18. Розробіть концепцію та алгоритм роботи електронного журналу для реєстрації вхідних та вихідних документів, а також для їх подальшої обробки.

19. Створіть детальний план впровадження електронного врядування в невеликій громадській організації, включаючи вибір програмного забезпечення, налаштування доступу, підготовку співробітників до роботи з новими технологіями.

20. Проведіть порівняльний аналіз популярних платформ для електронного документообігу оцініть їх переваги та недоліки для різних типів організацій.

21. Створіть реальний документ і застосуйте до нього електронний підпис, використовуючи систему електронного підпису. Поясніть, як цей процес підвищує довіру до електронного документа.

ПАКЕТ СИТУАЦІЙНИХ ВПРАВ

Ситуаційне завдання № 1

Уявіть, що ви працюєте в департаменті ІТ компанії, яка впроваджує електронний документообіг. Ваша задача – допомогти керівництву вибрати та впровадити систему для організації електронного документообігу в компанії, яка відповідатиме вимогам сучасного інформаційного суспільства і забезпечить безпеку обміну інформацією.

Вибір системи повинен базуватися на таких критеріях:

- інтеграція з існуючими корпоративними системами;
- можливість автоматизації обробки документів;
- забезпечення конфіденційності та безпеки через електронні підписи та контроль доступу;
- легкість використання для співробітників і підвищення ефективності внутрішнього документообігу.

Ваше завдання – розробити рекомендації для керівництва компанії щодо вибору системи електронного документообігу та зазначити основні кроки для її впровадження.

Ситуативне завдання № 2

Ваша компанія розпочала перехід до використання електронних документів для внутрішнього документообігу. Всі документи будуть створюватися, підписуватися та зберігатися в електронному форматі. Однак, перед впровадженням цієї системи потрібно забезпечити юридичну силу електронних документів і відповідність нормативним вимогам. Тому вам потрібно організувати процес створення, обробки та збереження електронних документів у компанії.

Запитання до завдання:

1. Яким чином ви забезпечите юридичну силу електронних документів у відповідності до вимог українського законодавства?
2. Які заходи слід вжити для збереження і архівації електронних документів?
3. Як ви будете використовувати електронний підпис для забезпечення автентичності та цілісності електронних документів?
4. Які законодавчі акти та нормативні документи слід врахувати при реалізації електронного документообігу?

Ситуаційне завдання № 3

Ви працюєте в управлінні електронного документообігу великої державної установи. Нещодавно ваша організація вирішила перейти до повного впровадження електронного документообігу з використанням кваліфікованих електронних підписів (КЕП). Вашим завданням є організація процесу підписання важливих адміністративних актів і договорів, а також налаштування процедури автентифікації підписувачів.

Під час запуску проекту виявлено, що деякі працівники організації не володіють необхідними знаннями щодо роботи з електронними підписами та методами їх зберігання. Крім того, є зацікавлені сторони, які вимагають гарантії щодо безпеки та юридичної сили підписаних документів.

Завдання:

1. Проаналізуйте ситуацію з точки зору правової значимості електронного підпису. Які форми електронного підпису повинні використовуватись для різних видів документів в організації? Які критерії визначають вибір підпису (простий, удосконалений, кваліфікований)?

2. Розробіть план навчання для працівників організації щодо використання кваліфікованих електронних підписів (КЕП) та організації процесу автентифікації.

3. Яким чином організація може забезпечити безпеку зберігання електронних підписів та документів на різних етапах їхнього життєвого циклу?

4. Оцініть правові та практичні ризики, які можуть виникнути при використанні електронних підписів і як можна знизити ці ризики за допомогою законодавчих норм або технічних засобів.

5. Опишіть можливі наслідки для організації, якщо буде виявлено підробку електронного підпису або порушення цілісності електронного документа.

Додаткове завдання:

Підготуйте презентацію для керівництва організації, яка міститиме огляд всіх необхідних процедур для забезпечення ефективного та безпечного використання електронних підписів в установі.

Ситуаційне завдання № 4

Ви працюєте в команді, яка відповідає за впровадження системи електронного документообігу (СЕД) у великій державній організації. Ваша організація має понад 1000 співробітників, і вже зараз зіштовхується з проблемами в управлінні великими обсягами документів, високими витратами на зберігання паперових документів та повільною обробкою даних. Більш того, документообіг часто відбувається вручну, що веде до неефективності та збоїв у роботі.

Ваша задача – вибрати та впровадити систему електронного документообігу, яка б оптимізувала робочі процеси, підвищила ефективність роботи співробітників, і водночас забезпечила б надійну безпеку та конфіденційність документів.

Завдання:

1. Аналіз і вибір системи:

– ознайомтесь з переліком систем електронного документообігу (Microsoft SharePoint, DOCS.UA, АСКОД, FossDoc, e-Docs, Megapolis.DocNet);

– визначте, яка з цих систем найкраще відповідає потребам вашої організації. Розгляньте різні аспекти, такі як інтеграція з іншими системами, безпека, зручність користування та можливості масштабування.

2. Опишіть, які методи безпеки будуть використовуватися для забезпечення конфіденційності та захисту інформації в новій системі (контроль доступу, шифрування даних, аутентифікація користувачів, аудит дій з документами).

3. Після впровадження системи, запропонуйте метрики для оцінки її ефективності. Як ви будете вимірювати покращення у роботі організації, скорочення часу на обробку документів, зниження кількості помилок чи витрат на зберігання документів?

Додаткове завдання:

Підготуйте презентацію для керівництва організації, в якій поясніть обрану систему, її переваги та етапи впровадження. Вкажіть, як нова система дозволить організації зекономити час і гроші та поліпшити взаємодію між співробітниками.

Ситуаційне завдання № 5

Ви працюєте в команді, яка розробляє стратегію цифрової трансформації для однієї з державних установ України (наприклад, Міністерство охорони здоров'я, Пенсійний фонд України або Державна фіскальна служба). Ця організація стикається з проблемами, пов'язаними з повільним документообігом, великим обсягом паперової документації, високим рівнем адміністративних витрат та ризиками несанкціонованого доступу до конфіденційних даних.

Ваша задача – розробити концепцію впровадження технологій блокчейн та штучного інтелекту в процеси електронного документообігу у державному органі. Враховуючи виклики, з якими стикаються державні установи (повільний документообіг, безпека даних, бюрократія), вам потрібно:

1. Оцініть, як існуюча система електронного документообігу може бути покращена за допомогою нових технологій.
2. Поясніть, як блокчейн та AI можуть вирішити ці проблеми. Обґрунтуйте, яку з технологій доцільніше впроваджувати в першу чергу.
3. Як впровадження цих технологій змінить процеси в установі? Як це вплине на час обробки документів і рівень безпеки?

Ситуаційне завдання № 6

Ви – консультант для державного органу, який намагається впровадити електронне урядування в своїй діяльності. Вашим завданням є розробити план для покращення комунікації та підвищення ефективності роботи органу через цифрові технології. Ви повинні вивчити переваги електронного урядування та запропонувати конкретні кроки для їх впровадження.

Завдання:

1. Оцініть існуючі проблеми в управлінні, які можна вирішити за допомогою електронного урядування (наприклад, складність доступу до послуг, корупційні ризики, затримки в процесах).

Як ці проблеми впливають на ефективність і довіру громадян до органу?

2. Ви повинні вибрати три ключові переваги електронного урядування (наприклад, прозорість і підзвітність, зручність для громадян, зменшення бюрократії) та обґрунтувати їх важливість для обраної установи.

Як ці переваги можуть покращити взаємодію з громадянами і підприємствами?

3. Окресліть етапи впровадження електронного урядування, починаючи з вивчення потреб і до впровадження першої електронної платформи для надання послуг.

Як ви плануєте залучити громадян до використання електронних послуг та забезпечити їхній доступ до цієї платформи?

Ситуаційне завдання № 7

Ваш університет отримав грант на створення системи електронного врядування для одного з регіонів країни. Ваша команда відповідальна за розробку та впровадження цього проєкту, який включає:

- реєстрацію та управління заявами на отримання адміністративних послуг (податкова реєстрація, реєстрація бізнесу, отримання довідок);

- створення електронних платформ для участі громадян у державних процесах, таких як голосування на місцевих виборах, петиції та опитування;

- впровадження нових цифрових інструментів для зручного доступу до інформації та послуг.

Однак, під час тестування системи, виявлено серйозні уразливості, які можуть призвести до витоку персональних даних користувачів.

Завдання:

1. Як би ви описали основні загрози безпеці цієї електронної платформи? Визначте ключові уразливості системи, на які потрібно звернути увагу. Оцініть, якими можуть бути наслідки для державного управління та довіри громадян у разі таких порушень безпеки.

2. Як ви розробили б стратегію для забезпечення безпеки цієї системи? Які технічні рішення, такі як шифрування, багатофакторна аутентифікація або використання протоколів безпеки, ви б рекомендували впровадити? Які кроки ви б вжили для захисту персональних даних громадян, щоб уникнути витоків та атак?

3. Вивчіть приклади країн, які успішно запровадили систему електронного врядування. Які рішення вони застосували для захисту даних громадян і протидії кіберзагрозам?

Ситуаційне завдання № 8

Вашій команді доручено створення стратегії для подальшого розвитку електронного врядування в Україні. Вам потрібно взаємодіяти з Міністерством цифрової трансформації для підготовки проекту з удосконалення цифрових сервісів для громадян та бізнесу. Одним із завдань є інтеграція послуг, таких як податкові та соціальні пільги, в єдину систему для зручності користувачів.

Завдання:

1. Опишіть, які послуги повинні бути включені до системи, щоб забезпечити зручність та доступність для громадян України. Як Міністерство цифрової трансформації може забезпечити надійний доступ до цих послуг?

2. Як можна заохотити громадян активно користуватися новими цифровими послугами? Які кроки повинно вжити Міністерство для того, щоб мінімізувати бар'єри у використанні цифрових платформ?

Ситуаційне завдання № 9

Підвищення цифрової грамотності є ключовим аспектом для успішного функціонування електронного врядування. Ваша команда отримала завдання створити план підвищення цифрової грамотності серед певної групи населення (наприклад, пенсіонери, малозабезпечені верстви, сільське населення).

Завдання для студентів:

1. Опишіть особливості цільової групи. Які фактори впливають на низький рівень цифрової грамотності цієї групи? Як це може вплинути на доступ до електронних послуг?

2. Розробіть програму навчання, яка включає як теоретичну частину (пояснення основ цифрових технологій), так і практичну частину (навчання на реальних прикладах через онлайн-курси або майстер-класи).

3. Як можна залучити місцеві органи влади та бізнес до процесу підвищення цифрової грамотності населення? Розробіть рекомендації для взаємодії з партнерами.

МОДУЛЬНІ ТЕСТОВІ ЗАВДАННЯ

1. Електронне урядування:

а) забезпечує відкритість і прозорість діяльності органів влади всіх рівнів, а також підвищує довіру громадян до влади, забезпечує більш ефективне і менш витратне адміністрування;

б) це сукупність відомостей про внутрішній і зовнішній стан об'єкта керування, необхідна для формування й реалізації керуючого впливу на нього;

в) передбачає дотримання встановлених правил запису інформації, специфічних для кожного типу документів.

2. Електронний уряд – це:

а) система документації, що створена за єдиними правилами та вимогами і містить інформацію, необхідну для управління у певній сфері діяльності;

б) форма юридичного закріплення проведеної уніфікації;

в) система, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій;

3. Саме поняття – електронний уряд (з англ. e-government) почали активно вживати у:

а) 90-х роках XX ст.;

б) 80-х роках XX ст.;

в) 90-х роках XIX ст.;

4. Електронне урядування – це:

а) складова частина державної системи класифікації й кодування техніко-економічної й соціальної інформації;

б) форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян;

в) базова теоретична конструкція, яка відноситься до всього, що може бути збережене або представлене, щоб служити як доказ для певної мети.

5. Інформаційне суспільство – це:

а) теоретична концепція постіндустріального суспільства, історична фаза можливого еволюційного розвитку цивілізації, в якій інформація і знання продукуються в єдиному інформаційному просторі

та є фундаментальним в понятійній системі, де відбиває ознаки реальних предметів, які служать об'єктами практичної діяльності по створенню, збору, аналітико-синтетичній обробці, зберіганню, пошуку та ін.

б) суспільство, орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток, у якому кожен міг би створювати й накопичувати інформацію та знання, мати до них вільний доступ, користуватися та обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному й особистому розвитку та підвищуючи якість життя;

в) вибіркове відображення у формі документів результатів соціальної діяльності членів суспільства.

6. Характерними рисами теоретичного інформаційного суспільства, є:

а) наявність інформації, змісту; стабільну форму, що забезпечує довгострокове користування та зберігання документа; функціональне призначення передачі інформації в просторі і часі, тобто від використання в соціальних комунікаційних каналах.

б) збільшення ролі інформації і знань в житті суспільства; зростання кількості людей, зайнятих інформаційними технологіями, комунікаціями і виробництвом інформаційних продуктів і послуг, зростання їх частки у валовому внутрішньому продукті; зростання інформатизації та ролі інформаційних технологій в суспільних та господарських відносинах;

в) створення глобального інформаційного простору, який забезпечує ефективну інформаційну взаємодію людей, їх доступ до світових інформаційних ресурсів і задоволення їхніх потреб щодо інформаційних продуктів і послуг; пошук у базі даних, перегляд і редагування електронних реєстраційних карток і текстів документів у відповідності з правами доступу до них користувача; контроль за проходженням і виконанням документів, їх оформлення і передання до електронного архіву для подальшого зберігання.

7. Доступ до інформації та знань – це:

а) організування раціонального руху, організування їх пошуку як по атрибутах, так і за змістом та засіб інформаційних ресурсів, необхідних для повноцінної реалізації політичних і соціокультурних прав особи в суспільстві;

б) загальна доступність необхідних методів, засобів і навичок для ефективного використання знань; засіб, що дозволяє громадянам контактувати з релевантним зовнішнім середовищем;

в) діяльність окремих працівників або підрозділів щодо створення документаційно – інформаційної бази на різних носіях для використання управлінським апаратом у процесі реалізації його функцій в процесі здійснення управління підприємством.

8. Інформаційна система (ІС) – це:

а) взаємозалежна сукупність засобів, методів і персоналу, використовуваних для збору, збереження, обробки і надання інформації задля досягнення поставленої мети; програмно-технічна та організаційна система надання інформаційних послуг з використанням інформаційних технологій;

б) потік документів, які циркулюють між пунктами опрацювання і створення інформації (керівниками організації і структурних підрозділів, спеціалістами) і пунктами технічного опрацювання документів;

в) сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації.

9. Інформаційні мережі – це:

а) структурні підрозділи, не маючи інформації про діяльність один одного, ефективно працюють, маю своєрідну здатність організації підтримувати зовнішні контакти;

б) одна або кілька організацій, які спільно виконують певну місію і керуються спільними цілями і завданнями для надання продукту або послуги;

в) засновані на передових електронних технологіях глобальні комп'ютерні (Інтернет), космічні і телекомунікаційні канали зв'язку, обміну, виробництва і поширення інформації, організовані системно-мережевим чином між країнами (урядами), регіонами та ін.

10. Інформаційна технологія (ІТ) – це:

а) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розсередження даних, доступ до джерел інформації незалежно від місця їх розташування;

б) процес відображення змісту документа і/або смислового значення інформаційного запиту інформаційно-пошуковою мовою;

в) здатність виражати з необхідною повнотою та точністю смислове значення інформації, що обробляється.

11. Інформаційний портал – це:

а) здатність відображати з необхідною повнотою та точністю смисловий зміст документів та запитів визначеної предметної області);

б) єдина «точка входу» в Інтернет для користувачів, що цікавляться певною інформацією, на якому зібрані і подані систематизованому і зручному вигляді якомога більше релевантних інформаційних ресурсів або гіперпосилань;

в) відвернення, відсторонення від ряду несуттєвих для даного дослідження властивостей і якостей феномена і разом з тим виділення важливих для дослідження властивостей і відношень.

12. Електронні адміністративні послуги – це:

а) метод дослідження і спосіб міркування, в якому загальний висновок робиться на підставі окремих і часткових посилок;

б) вивчення об'єкта (оригіналу) шляхом створення і дослідження його копії (моделі), яка заміщає оригінал у певних аспектах, що цікавлять дослідника;

в) державні послуги, які надаються в електронному вигляді органами державної влади та органами місцевого самоврядування людині та громадянину, фізичним та юридичним особам.

13. Основними видами адміністративних послуг, які можуть надаватися

через систему електронного уряду є:

а) загальний відділ, філософія, релігія, суспільні науки, філологія;

б) семантична сила, лексична повнота та точність, парадигматична повнота та точність, синтагматична повнота та точність;

в) інформування, одностороння взаємодія, двостороння взаємодія, проведення трансакцій.

14. Прийнято розглядати наступні етапи створення е-урядування в більшості країн:

а) електронне управління, електронний уряд, електронне урядування;

б) електронна формалізація, електронний уряд, електронна аксіоматизація;

в) електронне управління, електронний уряд, електронний аналіз.

15. Перехід до е-урядування починається з того, що:

- а)** вони надають повну динамічну інформацію з можливістю пошуку за базами даних і службою відповідей на посилення електронною поштою;
- б)** органи влади починають використовувати Інтернет;
- в)** розчленування цілісного предмета на складові частини (сторони, властивості, відношення, ознаки тощо) з метою їх всебічного дослідження.

16. Теоретичні засади електронного урядування:

- а)** аналогія, класифікація, моделювання;
- б)** теорія нового державного менеджменту, теорія політичних мереж;
- в)** інформаційний портал, інформаційне суспільство, інформаційне урядування.

17. До основних характеристик політичної мережі відносяться:

- а)** ідентифікатор мовної групи або країни; ідентифікатор видавництва; використання системи узгоджень та контрактів, формальних та неформальних правил комунікації;
- б)** місцезнаходження мережі на межі держави та суспільства; реферативний аналіз змісту документа; використання системи узгоджень та контрактів, формальних та неформальних правил комунікації;
- в)** множинність та різнотипність елементів мережі; відсутність ієрархічного контролю, рівність усіх учасників мережі (при можливості наявності «координуючих» центрів); свобода входу до складу мережі та виходу з неї для всіх учасників; наявність у кожного з елементів мережі особистих інтересів та ресурсів.

18. Розвиток інформаційного суспільства та інформаційних технологій стимулює країни й органи державного управління до прийняття концепції «електронного уряду». Вона спрямована на досягнення таких цілей:

- а)** перебудувати відносини з населенням; забезпечити громадянам можливість навчатися протягом усього життя; створити форми управління з активним залученням громадськості;
- б)** розробляти ефективні нормативно-правові акти та здійснювати раціональну політику; сприяти розвитку економіки;

в) вивчення об'єкта (оригіналу) шляхом створення і дослідження його копії (моделі), яка заміщає оригінал у певних аспектах, що цікавлять дослідника.

19. Який етап впровадження електронного урядування включає розроблення відповідної нормативно-правової бази, стандартів, регламентів, приведення вітчизняного законодавства у відповідність з європейськими стандартами?

- а) третій етап;
- б) другий етап;
- в) перший етап.

20. На другому етапі впровадження електронного урядування планується?

а) упорядкування виписаних понять, які відносяться до даного ключового слова відповідно до смислових зв'язків між ними;

б) безпосередньо надання послуг у електронному вигляді; залучення громадян до управління; впровадження технологій інтерактивної взаємодії органів державної влади та місцевого самоврядування з громадянами та ін.;

в) передбачається створити єдину інформаційно-телекомунікаційну інфраструктуру органів державної влади та місцевого самоврядування, вдосконалення надання адміністративних послуг та ін.

21. На третьому етапі впровадження електронного урядування:

а) відбувається сукупність допоміжних показників, які виконують роль путівника по тексту огляду і забезпечують ефективність пошуку у ньому необхідної інформації;

б) передбачається розроблення відповідної нормативно-правової бази, стандартів, регламентів, приведення вітчизняного законодавства у відповідність з європейськими стандартами;

в) передбачається створити єдину інформаційно-телекомунікаційну інфраструктуру органів державної влади та місцевого самоврядування, вдосконалення надання адміністративних послуг та ін.

22. Пілотний проект:

а) є одним з ефективних інструментів пошуку таких підходів, в процесі виконання якого досліджуються, визначаються та впроваджуються нетрадиційні механізми розбудови інформаційного суспільства;

б) єсукупністю допоміжних показників, які виконують роль путівника по тексту огляду і забезпечують ефективність пошуку у ньому необхідної інформації;

в) є ризиком впровадження електронного урядування, які пов'язані насамперед з великими фінансовими інвестиціями, з питаннями безпеки, недостатньою вмотивованістю державних службовців щодо впровадження інновацій.

23. Головна мета пілотного проекту:

а) системне та ефективне об'єднання зусиль, ресурсів, передового досвіду органів державної виконавчої влади та органів місцевого самоврядування, громадських організацій та бізнесу;

б) широка інформатизація відносин органів державної влади з суспільством;

в) приватні компанії, що провадять електронну комерцію, орієнтуються не лише на місцевих споживачів, а виходять на нові ринки, що сприяє підвищенню рівня професійної підготовки і зайнятості населення на місцях.

24. Принципи створення і функціонування інформаційної системи «Електронний уряд»:

а) принцип системності, принцип розвитку (відкритості), принцип нових завдань, принцип надійності, принцип безпеки даних, принцип абстрагування та ін.;

б) принцип нових завдань, принцип надійності, принцип безпеки даних, принцип пристосування (адаптації), принцип толерантності, принцип абстрагування та ін.;

в) принцип системності, принцип розвитку (відкритості), принцип сумісності, принцип стандартизації, принцип ефективності та ін..

25. Переваги електронного урядування:

а) економія матеріальних і часових ресурсів, оптимізація корпоративного управління, електронна передача інформації для прискорення її доставки споживачам, прозорість та відкритість публічної адміністрації;

б) підвищення ефективності управлінської діяльності, електронна передача інформації для прискорення її доставки споживачам, прозорість та відкритість публічної адміністрації;

в) прозорість та відкритість публічної адміністрації, економія матеріальних і часових ресурсів, оптимізація корпоративного

управління, підвищення якості надання адміністративних послуг, зменшення корупції в органах влади.

26. Електронна демократія – це:

а) форма демократії, що характеризується використанням інформаційно- комунікаційних технологій (ІКТ) як основного засобу для колективних розумових адміністративних процесів (інформування, прийняття спільних рішень);

б) організаційно-технологічний комплекс методичних, технічних, програмних та інформаційних засобів, який забезпечує комплекс функцій для роботи;

в) процес створення, одержання, спільного використання, відслідковування, ревізії, розподілу та зберігання інформації, яку вони містять у межах певної інформаційної системи.

27. Сьогодні в Україні реалізовані наступні елементи електронної демократії:

а) електронні звернення, консультації та анкетування; загальна кількість та число рівнів структур, які відображають особливості внутрішньої організації підприємства; локальні портали адміністративних послуг;

б) електронне законодавство у частині публікування нормативно-правових актів після їх реєстрації та прийняття на офіційному сайті Верховної Ради; електронні звернення, консультації та анкетування; електронні портали, такі як «Електронна митниця» та «Вебпортал державних закупівель»; локальні портали адміністративних послуг;

в) електронне законодавство у частині публікування нормативно-правових актів після їх реєстрації та прийняття на офіційному сайті Верховної Ради; різноманітні онлайн ініціативи неурядових організацій; засоби регламентації доступу та криптографічного захисту; повна або часткова автоматизація бізнес-процесу, при якій документи, інформація або завдання передаються від одного учасника до іншого.

28. Е-демократія:

а) є системою, яка могла підтримувати будь-яку кількість користувачів з здатність системи нарощувати потужність визначалась тільки потужністю відповідного програмного забезпечення;

б) є атрибутом захисту громадянами своїх інтересів і визначення форм співпраці з державою за допомогою технологій е-урядування;

в) повинна складатись з окремих модулів, інтегрованих між собою, на випадок, якщо користувачу системи не потрібно одразу впровадження всіх компонентів системи документообігу.

29. Поняття «електронна демократія» включає «електронне» визначення базових понять політичного процесу:

а) Е-парламент, Е-законодавство, Е-правосуддя, Е-голосування, Е-консультація, Е-звернення, Е-агітація, Е-модульність, Е-розподіленість, Е-інтеграція, Е-уніфікація та ін.;

б) Е-голосування, Е-консультація, Е-звернення, Е-агітація, Е-підрахунок голосів та е-опитування, Е-охоплення, Е-включення, Е-партнерство та ін.;

в) Е-парламент, Е-законодавство, Е-правосуддя, Е-посередництво, Е-середовище, Е-вибори, Е-референдуми та Е-ініціативи та ін.

30. Електронний парламент – це:

а) використання ІКТ зібраннями вибраних представників (депутатами), а також політичними та публічними службовцями з метою активізації залучення громадян до законотворчої діяльності;

б) швидка автоматизація бізнес-процесів завдяки наявності вбудованих процесів опрацювання, які настроюються та модифікуються у відповідності з вимогами специфіки діяльності замовника;

в) використання ІКТ з метою пошуку засобів вирішення спорів без фізичної присутності сторін, що сперечаються: посередниками можуть служити електронні інструменти.

31. Електронне законодавство – це:

а) використання ІКТ задля аналізу й захисту оточуючого середовища, просторового планування та раціонального користування природними ресурсами;

б) використання ІКТ для коментування, обговорення, складання, структурування, форматування, виправлення, голосування та видання законів та нормативно-правових актів, прийнятих представницькими органами;

в) дозволяють громадянам розробляти та висувати політичні пропозиції за допомогою засобів ІКТ.

32. Електронне правосуддя – це:

а) дозволяють неформально здійснювати збір позицій певної сукупності громадян за допомогою електронних засобів по

відношенню визначеного питання та набору можливих варіантів громадської реакції на нього;

б) засіб збору поглядів визначених осіб або широкої громадськості з конкретного політичного питання без необхідності зобов'язувати їх діяти відповідно з його результатом;

в) використання ІКТ в юридичній сфері всіма зацікавленими сторонами з метою підвищення ефективності та якості державних служб, зокрема, для приватних осіб і підприємств.

33. Електронне голосування – це:

а) вибори або референдум, які передбачають використання електронних засобів;

б) електронна доставка зауважень чи рекомендацій;

в) засіб збору поглядів визначених осіб або широкої громадськості з конкретного політичного питання без необхідності зобов'язувати їх діяти відповідно з його результатом.

34. Електронна агітація – це:

а) це вибори або референдум, які передбачають використання електронних засобів як мінімум безпосередньо при проведенні голосування;

б) дозволяють неформально здійснювати збір позицій певної сукупності громадян за допомогою електронних засобів по відношенню визначеного питання та набору можливих варіантів громадської реакції на нього;

в) цілеспрямований вплив на переконання громадян за допомогою електронних засобів, а також їх безпосереднє залучення у виборчі та інші політичні кампанії, спрямовані на формування або реалізацію суспільної стратегії.

35. Процес становлення електронної демократії має декілька основних етапів:

а) Е-охоплення, Е-включення, Е-партнерство;

б) Е-охоплення, Е-включення, Е-застосування;

в) Е-збір, Е-включення, Е-партнерство.

36. Електронне партнерство – це:

а) поділяється на: е-консультування – уряд в режимі он-лайн звертається до громадян з метою отримання їхньої думки щодо вироблення відповідної державної політики чи обговорення прийнятих урядових рішень; е-участь – активна участь громадян на основі підтримки зворотного зв'язку за допомогою сучасних інформаційно-комунікативних технологій;

б) е-інформування, яке виступає передумовою зміцнення стосунків між владою та громадянами, має односторонній характер, тому що інформація надходить в режимі он-лайн від державних органів до громадян;

в) етап поглиблення взаємодії громадян з державною владою, де відповідальність за прийняття рішень покладається на обидві сторони, передбачає внесок кожного у розвиток громадянського суспільства. Основна передумова – взаємна довіра.

37. Електронне охоплення – це:

а) поділяється на: е-консультування – уряд в режимі он-лайн звертається до громадян з метою отримання їхньої думки щодо вироблення відповідної державної політики чи обговорення прийнятих урядових рішень; е-участь – активна участь громадян на основі підтримки зворотного зв'язку за допомогою сучасних інформаційно-комунікативних технологій;

б) е-інформування, яке виступає передумовою зміцнення стосунків між владою та громадянами, має односторонній характер, тому що інформація надходить в режимі он-лайн від державних органів до громадян;

в) етап поглиблення взаємодії громадян з державною владою, де відповідальність за прийняття рішень покладається на обидві сторони, передбачає внесок кожного у розвиток громадянського суспільства. Основна передумова – взаємна довіра.

38. Електронне включення – це:

а) поділяється на: е-консультування – уряд в режимі он-лайн звертається до громадян з метою отримання їхньої думки щодо вироблення відповідної державної політики чи обговорення прийнятих урядових рішень; е-участь – активна участь громадян на основі підтримки зворотного зв'язку за допомогою сучасних інформаційно-комунікативних технологій;

б) е-інформування, яке виступає передумовою зміцнення стосунків між владою та громадянами, має односторонній характер, тому що інформація надходить в режимі он-лайн від державних органів до громадян;

в) етап поглиблення взаємодії громадян з державною владою, де відповідальність за прийняття рішень покладається на обидві сторони, передбачає внесок кожного у розвиток громадянського суспільства. Основна передумова – взаємна довіра.

39. Звичайний виборчий процес відповідно до законодавства України проходить такі етапи:

- а)** підготовка до голосування, проведення голосування, підрахунок голосів, транспортування виборчих бюлетенів;
- б)** проведення голосування, підрахунок голосів, транспортування виборчих бюлетенів;
- в)** підготовка до голосування, проведення голосування, транспортування виборчих бюлетенів.

40. Парламент визначається як:

- а)** національний представницький орган державної влади, який діє постійно, повністю або частково формується шляхом прямих виборів;
- б)** включення у єдину інформаційну систему, які створюються в організації або надходять до неї у будь-якій формі на основі єдиних правил реєстрації;
- в)** інтегрована система управління організаційного типу, що забезпечує приймання, обробку, передачу та зберігання інформації в рамках корпоративної мережі.

41. Ознаки демократичного парламенту:

- а)** представницький, прозорий, доступний, підзвітний, ефективний;
- б)** представницький, прозорий, секретний, доступний, підзвітний;
- в)** інформаційний, прозорий, доступний, підзвітний, ефективний.

42. Ефективний – ознака демократичного парламенту:

- а)** забезпечує відповідальність парламентарів перед своїми виборцями за свою діяльність та чесність поведінки;
- б)** забезпечує відповідальність парламентарів перед своїми виборцями за свою діяльність та чесність поведінки;
- в)** організує діяльність відповідно до демократичних цінностей, ефективно виконуючи законотворчі і контрольні функції, які відповідають актуальним суспільним потребам.

43. Підзвітний – ознака демократичного парламенту:

- а)** відкритий для народу через засоби масової інформації, публічний у своїй повсякденній діяльності;
- б)** забезпечує відповідальність парламентарів перед своїми виборцями за свою діяльність та чесність поведінки;

в) організує діяльність відповідно до демократичних цінностей, ефективно виконуючи законотворчі і контрольні функції, які відповідають актуальним суспільним потребам.

44. Прозорий – ознака демократичного парламенту:

а) відкритий для народу через засоби масової інформації, публічний у своїй повсякденній діяльності;

б) забезпечує відповідальність парламентарів перед своїми виборцями за свою діяльність та чесність поведінки;

в) організує діяльність відповідно до демократичних цінностей, ефективно виконуючи законотворчі і контрольні функції, які відповідають актуальним суспільним потребам.

45. Принципи діяльності електронного парламенту:

а) прозорість, відкритість, укомплектованість, дієздатність, обов'язковість доступу, підзвітність, налагодження онлайн діалогу та ін.;

б) підзвітність, електронність, практичність, зобов'язання, налагодження онлайн діалогу, безпечність, приватність та ін..

в) прозорість, відкритість, обов'язковість доступу, підзвітність, налагодження онлайн діалогу, безпечність, приватність та ін..

46. Обов'язковість доступу:

а) оскільки Інтернет широко використовується парламентом для оприлюднення своїх дій, рішень та документів потрібно забезпечити як доступ до парламентської інформації так і доступ до комунікацій для всіх громадян, незалежно від їхнього місцезнаходження, стану чи можливостей;

б) подолання так званого «дефіциту звітності», коли електорат не завжди може зробити певний висновок про діяльність та чесність парламентарів, який забезпечують нові можливості ІКТ, що розширюють інформування про діяльність парламенту та парламентарів;

в) ІКТ уможливають обмін ідеями між парламентами, знання практичного досвіду законодавчих органів інших країн, надаючи парламентарям та виборцям змогу обмінюватися досвідом та ефективніше співпрацювати над схожими проблемами в Інтернеті.

47. Глобалізація законотворчої діяльності:

а) оскільки Інтернет широко використовується парламентом для оприлюднення своїх дій, рішень та документів потрібно забезпечити як доступ до парламентської інформації так і доступ до комунікацій для

всіх громадян, незалежно від їхнього місцезнаходження, стану чи можливостей;

б) подолання так званого «дефіциту звітності», коли електорат не завжди може зробити певний висновок про діяльність та чесність парламентарів, який забезпечують нові можливості ІКТ, що розширюють інформування про діяльність парламенту та парламентарів;

в) ІКТ уможливають обмін ідеями між парламентами, знання практичного досвіду законодавчих органів інших країн, надаючи парламентарям та виборцям змогу обмінюватися досвідом та ефективніше співпрацювати над схожими проблемами в Інтернеті.

48. Підзвітність:

а) оскільки Інтернет широко використовується парламентом для оприлюднення своїх дій, рішень та документів потрібно забезпечити як доступ до парламентської інформації так і доступ до комунікацій для всіх громадян, незалежно від їхнього місцезнаходження, стану чи можливостей;

б) подолання так званого «дефіциту звітності», коли електорат не завжди може зробити певний висновок про діяльність та чесність парламентарів, який забезпечують нові можливості ІКТ, що розширюють інформування про діяльність парламенту та парламентарів;

в) ІКТ уможливають обмін ідеями між парламентами, знання практичного досвіду законодавчих органів інших країн, надаючи парламентарям та виборцям змогу обмінюватися досвідом та ефективніше співпрацювати над схожими проблемами в Інтернеті.

49. Інформаційно-аналітичний простір парламенту – це:

а) можливість захисту від несанкціонованого доступу та розмежування прав доступу співробітників до інформації;

б) діяльність сучасного парламенту та рішення будуть вчасно та інформативно висловлені, що вимагає поєднання традиційних заходів;

в) середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації, інформаційна взаємодія підрозділів, дослідницької служби і користувачів систем аналітичної підтримки.

50. Інформаційно-аналітичний ресурс – це:

а) можливість захисту від несанкціонованого доступу та розмежування прав доступу співробітників до інформації;

б) діяльність сучасного парламенту та рішення будуть вчасно та інформативно висловлені, що вимагає поєднання традиційних заходів;

в) складова інформаційно-аналітичного простору, що поєднує в собі дані, їхнє місцезнаходження, взаємозв'язок між інформаційними елементами, системи аналітичного супроводженні і прийняття рішень та відомості про процеси надходження, зберігання, обробки тощо.

51. Процес залучення громадських організацій до політичного процесу державних структур має:

- а) п'ять етапів;
- б) чотири етапи;
- в) три етапи.

52. Перший етап – це:

- а) допомога у визначенні найбільш актуальних проблем для вирішення;
- б) політичне конструювання шляхів розв'язання проблеми;
- в) імплементація теорії у практику (безпосереднє вирішення проблеми).

53. Другий етап – це:

- а) допомога у визначенні найбільш актуальних проблем для вирішення;
- б) політичне конструювання шляхів розв'язання проблеми;
- в) імплементація теорії у практику (безпосереднє вирішення проблеми).

54. Третій етап – це:

- а) допомога у визначенні найбільш актуальних проблем для вирішення;
- б) політичне конструювання шляхів розв'язання проблеми;
- в) імплементація теорії у практику (безпосереднє вирішення проблеми).

55. Визначають чотири можливі шляхи впливу громадських організацій на державну політику:

- а) безпосередній вплив, консультативний, інноваційний, наглядовий;
- б) демонстративний, консультативний, інноваційний, наглядовий;
- в) безпосередній вплив, консультативний, інноваційний, завершальний.

56. Цифровий розрив (бар'єр), цифрова нерівність, інформаційна нерівність визначається як:

- а) висока швидкість пошуку і одержання інформації;
- б) підвищення ефективності управлінської діяльності;

в) обмеження можливостей соціальної групи через відсутність у неї доступу до сучасних засобів комунікації.

57. Причини виникнення та посилення цифрового розриву можуть бути розділені на наступні групи:

а) економічні, соціальні, результативні, адміністративні;

б) економічні, соціальні, культурні, пов'язані з контентом;

в) економічні, результативні, культурні, пов'язані з контентом.

58. Державна політика – це:

а) організаційно-технологічний комплекс методичних, технічних, програмних та інформаційних засобів, який забезпечує комплекс результатів;

б) курс дій, тобто не одне певне рішення, дія чи реакція, а ретельно розроблений підхід або стратегія;

в) процес створення, одержання, спільного використання, відслідковування, ревізії, розподілу та зберігання інформації, яку вони містять у межах певної інформаційної системи.

59. П'ять етапів вироблення державної політики:

а) ініціювання політики, формування, ухвалення, реалізація, оцінка;

б) ініціювання політики, формування, ухвалення, фінансування, вкладення;

в) вивчення політики, формування, ухвалення, реалізація, оцінка.

60. Формування політики:

а) здійснення та моніторинг державної політики, що передбачає комплекс заходів із впровадження прийнятих рішень і програм;

б) легітимізація та фінансування державної політики, що передбачають закріплення розробленої політики в низці рішень і програм;

в) розробка державної політики, що передбачає узгодження інтересів, цілей і засобів їх досягнення.

61. Ухвалення політики:

а) здійснення та моніторинг державної політики, що передбачає комплекс заходів із впровадження прийнятих рішень і програм;

б) легітимізація та фінансування державної політики, що передбачають закріплення розробленої політики в низці рішень і програм;

в) розробка державної політики, що передбачає узгодження інтересів, цілей і засобів їх досягнення.

62. Реалізація політики:

а) здійснення та моніторинг державної політики, що передбачає комплекс заходів із впровадження прийнятих рішень і програм;

б) легітимізація та фінансування державної політики, що передбачають закріплення розробленої політики в низці рішень і програм;

в) розробка державної політики, що передбачає узгодження інтересів, цілей і засобів їх досягнення.

63. Державне управління – це:

а) здійснення управлінського організуючого впливу шляхом використання повноважень виконавчої влади через організацію виконання законів, здійснення управлінських функцій з метою комплексного соціально-економічного та культурного розвитку держави, її окремих територій;

б) загальна доступність необхідних методів, засобів і навичок для ефективного використання знань; засіб, що дозволяє громадянам контактувати з релевантним зовнішнім середовищем;

в) діяльність окремих працівників або підрозділів щодо створення документаційно – інформаційної бази на різних носіях для використання управлінським апаратом у процесі реалізації його функцій в процесі здійснення управління підприємством.

64. Такі найхарактерніші ознаки державного управління:

а) законність, підзаконність, фінансування, масштабність та універсальність, ієрархічність, організуючий характер;

б) виконавчо-розпорядчий характер, підзаконність, масштабність та універсальність, ієрархічність, організуючий характер;

в) виконавчо-розпорядчий характер, підзаконність, масштабність та універсальність, ієрархічність, методологічний характер.

65. Сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та використанню інформації – це:

а) державне електронне урядування;

б) міжнародна політика;

в) державна інформаційна політика.

66. Серед завдань державної політики з впровадження електронного урядування передбачається:

а) провадження узгодженої цілеспрямованої діяльності всіма органами державної влади; удосконалення принципів державного

управління, структури і функцій органів державної влади та органів місцевого самоврядування; створення інформаційної інфраструктури електронного урядування та ін.;

б) навчання громадян і суб'єктів господарювання використанню технологій електронного урядування; можливість роботи за «вільною» схемою, без жорсткої фіксації маршрутів; створення системи мотивації державних службовців, громадян і суб'єктів господарювання щодо використання технологій електронного урядування та ін.;

в) підтримка роботи з кількома версіями документа, можливість інтеграції з іншими додатками; особливості настроювання програмного продукту на потреби конкретного замовника; підготовку кваліфікованих кадрів, які забезпечуватимуть впровадження елементів електронного урядування та надання адміністративних послуг; створення інформаційної інфраструктури електронного урядування та ін..

67. Суб'єкт управління, взаємодія та взаємо сприяння, суспільна система – це складові:

а) системи електронного урядування;

б) системи державного управління;

в) системи інформаційної політики.

68. Об'єкт управління – це:

а) система створення єдиного інформаційно-управлінського простору для організацій будь-якої складності;

б) координація людей, інформації, об'єктів та подій для виконання послідовності операцій і досягнення статусу, який призводить до досягнення встановлених цілей;

в) система, яка підпорядковується владній волі суб'єкта управління і виконує його рішення, тобто система, якою управляють.

69. Суб'єкт і об'єкт управління утворюють:

а) процес реалізації управління;

б) процес управління;

в) процес впровадження.

70. Управлінські відносини – це:

а) система управління для підвищення ефективності управлінської діяльності;

б) комплекс «уніфіковане клієнтське місце».

в) відносини людей стосовно здійснення функцій управління.

71. Функції державного управління:

а) загальні, спеціальні;

б) основні, додаткові;

в) загальні, службові.

72. Загальні функції державного управління:

а) планування, прийняття рішень, мотивація, організація, комунікація, контроль;

б) забезпечення прав, свобод людини і громадянина, адміністративно-політичні, економічні, соціальні, культурно-освітні, забезпечення екологічної безпеки та інші.

73. Спеціальні функції державного управління:

а) планування, прийняття рішень, мотивація, організація, комунікація, контроль;

б) забезпечення прав, свобод людини і громадянина, адміністративно-політичні, економічні, соціальні, культурно-освітні, забезпечення екологічної безпеки та інші.

74. Індикатори використовуються для:

а) оцінки запобіжного впливу на інформацію;

б) оцінки розвитку інформаційного розвитку;

в) оцінки розвитку результативності праці індикатора.

75. Система індикаторів SIBIS:

а) індикатори, що вимірюють Інтернет-готовність населення та комерційних підприємств, – характеристики інфраструктури та технічних можливостей доступу до Інтернет індивідуальними користувачами та компаніями;

б) важливість моніторингу та оцінки розбудови інформаційного суспільства та розробки відповідної методології вимірювання.

76. Система індикаторів WSIS:

а) індикатори, що вимірюють Інтернет-готовність населення та комерційних підприємств, – характеристики інфраструктури та технічних можливостей доступу до Інтернет індивідуальними користувачами та компаніями;

б) важливість моніторингу та оцінки розбудови інформаційного суспільства та розробки відповідної методології вимірювання.

77. Індекс готовності є комплексним показником і базується на таких трьох компонентах:

а) індекс вебпослуг, що визначає ступінь розвиненості вебпослуг з боку електронного уряду; індекс телекомунікаційної інфраструктури, що оцінює ступінь оснащення громадян засобами ІКТ; індекс створення єдиного інформаційно-управлінського простору для організацій будь-якої складності;

б) індекс вебпослуг, що визначає ступінь розвиненості вебпослуг з боку електронного уряду; індекс телекомунікаційної інфраструктури, що оцінює ступінь оснащення громадян засобами ІКТ; індекс людського капіталу, що показує, наскільки високий рівень освіти у громадян і чи готові вони користуватися інформаційними послугами;

в) індекс телекомунікаційної інфраструктури, що оцінює ступінь оснащення громадян засобами ІКТ; індекс людського капіталу, що показує, наскільки високий рівень освіти у громадян і чи готові вони користуватися інформаційними послугами; індекс організації спільного інформаційного простору з розподіленою структурою;.

78. Стадії надання вебпослуг:

а) початкова, основна, інтерактивна, інноваційна, мережева;

б) початкова, поліпшена, інтерактивна, транзакційна, мережева;

в) початкова, запозичена, інтерактивна, транзакційна, мережева;

79. На якій стадії в вебпросторі повинна бути доступна базова інформація про уряд?

а) четвертій;

б) першій;

в) другій.

80. На якій стадії через вебінтерфейс доступні не тільки архівні, але й поточні оперативні дані про нормативні акти, розпорядження, постанови, звіти, новини, завантажені бази даних?

а) п'ятій;

б) другій;

в) першій.

81. На якій стадії реалізована двостороння взаємодія між громадянами і державою?

а) третій;

б) четвертій;

в) п'ятій.

82. Основні складові інформаційної системи – електронний уряд:

а) електронний документообіг в державних структурах; розгалужена інформаційно-телекомунікаційна інфраструктура; електронний ключ; цифровий електронний підпис та ін.;

б) смарт-карти; електронний ключ; закрита спеціалізована інформаційна мережа (Інтранет) для внутрішньоурядових транзакцій; динамічна модифікація форми і змісту облікових даних і процедури реєстрації; робота з будь-якими електронними об'єктами та ін.;

в) електронний документообіг в державних структурах; спільна для різних урядових структур база даних, що дає змогу уникнути дублювання інформації та зайвих витрат; фіксація перебігу виконання, контроль виконання та ін.;

83. Портал є:

а) загальнодоступним державним веб-ресурсом, який забезпечує у зручній інтерактивній формі електронний діалог громадян, бізнесу та влади.

б) комплексом апаратно-програмних засобів і технологій електронного урядування;

в) завдання потокового використання інформації, коли найбільшого значення набуває оперативність доступу до неї.

84. Архітектурна модель центрального урядового порталу має три рівні:

а) клієнтська частина, програмне забезпечення, моніторингова частина;

б) клієнтська частина, серверна частина, програмне забезпечення;

в) персональна частина, серверна частина, програмне забезпечення.

85. Клієнтська частина:

а) основна точка входу урядового порталу;

б) рівень, на якому здійснюється інтеграція послуг;

в) окремі міністерства й відомства, місцеві органи влади та інші системи і процеси, залучені до надання послуг.

86. Програмне забезпечення проміжного прошарку:

а) основна точка входу урядового порталу;

б) рівень, на якому здійснюється інтеграція послуг;

в) окремі міністерства й відомства, місцеві органи влади та інші системи і процеси, залучені до надання послуг.

87. Серверна частина:

а) основна точка входу урядового порталу;

б) рівень, на якому здійснюється інтеграція послуг;

в) окремі міністерства й відомства, місцеві органи влади та інші системи і процеси, залучені до надання послуг.

88. Функції Інтернет-порталу органу державного управління: розміщення і структура одержання інформації?

а) спеціальний блок («торговельний майданчик») Інтернет-порталу за потреби може забезпечити проведення конкурсів серед

організацій і підприємств на виконання тих чи інших робіт для державних потреб;

б) представлена на Інтернет-порталі інформація має бути повною, точною й актуальною;

в) дана функція забезпечується набором сервісів, які дають змогу громадянам та організаціям запитувати й одержувати через Інтернет необхідні довідки або реєструвати дозволи.

89. Функції Інтернет-порталу органу державного управління: взаємодія громадян та організацій з органом державної влади?

а) спеціальний блок («торговельний майданчик») Інтернет-порталу за потреби може забезпечити проведення конкурсів серед організацій і підприємств на виконання тих чи інших робіт для державних потреб;

б) представлена на Інтернет-порталі інформація має бути повною, точною й актуальною;

в) дана функція забезпечується набором сервісів, які дають змогу громадянам та організаціям запитувати й одержувати через Інтернет необхідні довідки або реєструвати дозволи.

90. Функції Інтернет-порталу органу державного управління: проведення органами державної влади заходів для громадян та організаційна)? спеціальний блок («торговельний майданчик») Інтернет-порталу за потреби може забезпечити проведення конкурсів серед організацій і підприємств на виконання тих чи інших робіт для державних потреб;

б) представлена на Інтернет-порталі інформація має бути повною, точною й актуальною;

в) дана функція забезпечується набором сервісів, які дають змогу громадянам та організаціям запитувати й одержувати через Інтернет необхідні довідки або реєструвати дозволи.

91. Єдиний інформаційний простір – це:

а) сукупність стандартизованих технологій обміну інформацією і даними, ведення і використання інформаційних баз і банків даних, інформаційної безпеки, інформаційно-комунікаційних систем і мереж, які функціонують на основі єдиних принципів і за загальними правилами і стандартами,

б) форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням

інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян;

в) базова теоретична конструкція, яка відноситься до всього, що може бути збережене або представлене, щоб служити як доказ для певної мети.

92. Єдиний інформаційний простір України включає:

а) національні системи, міжгалузеві системи, відомчі системи;

б) національні системи, міжгалузеві системи, інформаційні системи;

в) міжнародні системи, національні системи, міжгалузеві системи.

93. Національні системи:

а) Електронний паспорт, Електронні ідентифікаційні картки: державні, регіональні, бізнес-вживання, Уніфіковані стандарти, Єдині реєстри;

б) Законодавча система, Комунікаційна інфраструктура, Інфраструктура цифрового підпису і документообігу, Електронний уряд;

в) Електронна податкова служба, Електронна митниця, Електронний земельний кадастр, Електронне право, Електронне голосування.

94. Електронний паспорт, Електронні ідентифікаційні картки: державні, регіональні, бізнес-вживання, Уніфіковані стандарти, Єдині реєстри – це:

а) національні системи;

б) відомчі системи;

в) міжгалузеві системи.

95. Електронна податкова служба, Електронна митниця, Електронний земельний кадастр, Електронне право, Електронне голосування – це:

а) національні системи;

б) відомчі системи;

в) міжгалузеві системи.

96. Єдиний державний портал адміністративних послуг повинен забезпечувати:

а) доступ до інформації про адміністративні послуги, що надаються суб'єктам звернення; доступ до інформації про центри та суб'єктів надання адміністративних послуг; пошук за ключовими

словами в полях опису адміністративної послуги; класифікацію та пошук послуг за життєвими ситуаціями та категоріями;

б) подання он-лайн заяви на одержання адміністративної послуги; внесення встановленої плати за надання адміністративної послуги з використанням електронних платіжних систем; забезпечення доступу до інформації практично з будь-якої територіально віддаленої точки за умови наявності відповідних прав доступу; підвищення надійності зберігання інформації, зменшення ризику втрати важливої інформації через недбалість персоналу або вплив зовнішніх факторів;

в) внесення встановленої плати за надання адміністративної послуги з використанням електронних платіжних систем; відстеження етапів проходження документів щодо надання адміністративної послуги; відстеження статистики відвідувань; 7) формування звітів про роботу користувачів з електронним архівом; 3) встановлення і підтримка логічних зв'язків між документами.

97. Функціонування електронного урядування базується на «трьох китах»:

а) законодавство, організаційна структура органів влади, інформаційно-технологічна інфраструктура;

б) законодавство, захист громадян та технологія державного управління;

в) організаційна структура органів влади, державна політика, інформаційно-технологічна інфраструктура.

98. Система електронного уряду має забезпечити вирішення таких завдань:

а) тісна співпраця фахівців ІТ-служб замовника та виконавця; чіткий розподіл обов'язків та повноваження всіх, хто залучений до впровадження системи; впровадження пілотного проекту для відпрацювання бізнес-процедур, які підлягають автоматизації; навчання співробітників на постійній основі та на всіх етапах впровадження та ін.;

б) підвищення ефективності використання інформації за рахунок зменшення часу на пошук необхідних документів; забезпечення доступу до інформації практично з будь-якої територіально віддаленої точки за умови наявності відповідних прав доступу; інтеграція з іншими інформаційними системами підприємства та ін.;

в) захист прав громадян на доступ до державної інформації; забезпечення конфіденційності та інформаційної безпеки; залучення громадян до участі в управлінні державними справами; удосконалення

технології державного управління; підвищення якості управлінських рішень та ін.

99. Загальна архітектура системи включає такі складові:

а) підсистеми телекомунікацій, веб-портал електронного уряду, виборчих процесів, адміністрування послуг, введення документування та ін;

б) підсистеми телекомунікацій, інформаційних ресурсів, вебпортал електронного уряду, ведення адресного домену, електронних розрахунків та ін.;

в) підсистеми телекомунікацій, інформаційних ресурсів, вебпортал електронного уряду, адміністрування послуг, введення документування та ін;

100. Інформаційний простір – це:

а) сукупність інформування та їх процесів для вдалого розвитку та розповсюдження ресурсів, а також задоволення їх інформаційних потреб.

б) сукупність інформаційної інфраструктури, інформаційних ресурсів, технологій та регламентів використання інформаційних ресурсів;

в) сукупність відкритості інформаційного простору для функціонування програмно-технічних засобів і організаційно-нормативних документів.

101. Єдиний інформаційний простір складається з таких головних компонентів:

а) інформаційні ресурси, організаційні структури, засоби інформаційної взаємодії громадян і організацій;

б) інформаційні ресурси, організаційні структури, ресурси обміну;

в) функціональні ресурси, організаційні структури, ресурси обміну.

102. Телекомунікаційна система – це:

а) система, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій;

б) система, яка могла підтримувати будь-яку кількість користувачів з здатність системи нарощувати потужність визначалась тільки потужністю відповідного програмного забезпечення;

в) організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів

шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином.

103. Інформаційна система – це:

а) організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

б) система, яка могла підтримувати будь-яку кількість користувачів з здатність системи нарощувати потужність визначалась тільки потужністю відповідного програмного забезпечення;

в) організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином.

104. Інтегрована система – це:

а) організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

б) система, яка могла підтримувати будь-яку кількість користувачів з здатність системи нарощувати потужність визначалась тільки потужністю відповідного програмного забезпечення;

в) сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як систему.

105. Основними напрямками розвитку телекомунікаційних мереж вважаються:

а) виявлення зацікавленості керівництва у реалізації проекту; відмова від розробки системи силами власного ІТ-підрозділу і застосування готових рішень від виробників; розробка і впровадження концепції розвитку документаційного забезпечення підприємства, планом впровадження системи електронного документообігу, вибір керівника проекту, формування робочої групи та ін.;

б) створення сучасних широкосмугових мультисервісних транспортних мереж на базі єдиних протоколів, сумісних з Інтернет-протоколами; розвиток широкосмугового абонентського доступу з використанням перспективних технологічних рішень, зокрема, волоконно-оптичних ліній, технологій оптичної мережі,

радіотехнологій доступу, технологій надширокосмугового радіодоступу та ін.;

в) розробка і впровадження концепції розвитку документаційного забезпечення підприємства, планом впровадження системи електронного документообігу, вибір керівника проекту, формування робочої групи; створення сучасних широкосмугових мультисервісних транспортних мереж на базі єдиних протоколів, сумісних з Інтернет-протоколами та ін.

106. Основними напрямками розвитку телекомунікаційних мереж вважаються:

а) тісна співпраця фахівців ІТ-служб замовника та виконавця; чіткій розподіл обов'язків та повноваження всіх, хто залучений до впровадження системи; впровадження пілотного проекту для відпрацювання бізнес-процедур, які підлягають автоматизації та ін.;

б) прискорення розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах з використанням найбільш ефективних технологій; приведення системи нумерації телекомунікаційних мереж у відповідність з європейськими стандартами; розвиток та оптимізація всіх елементів телекомунікаційної інфраструктури українського сегмента Інтернетз метою створення рівних умов для доступу споживачів до Інтернет та забезпечення розвитку в Україні інформаційного суспільства та ін.;

в) перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, заблоковані та поновлені сертифікати ключів; прискорення розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах з використанням найбільш ефективних технологій та ін.

107. Географічні інформаційні системи (ГІС) – це:

а) сучасна комп'ютерна технологія для картування та аналізу об'єктів реального світу, а також подій, що відбуваються в навколишньому середовищі, у нашому житті і діяльності;

б) діяльність підрозділів щодо створення документаційно-інформаційної бази на різних носіях для використання управлінським апаратом у процесі реалізації його функцій в процесі здійснення управління підприємством.

в) одна або кілька організацій, які спільно виконують певну місію і керуються спільними цілями і завданнями для надання продукту або послуги;

108. Апаратні засоби, програмне забезпечення, дані, виконавці, методи – це складові частини:

- а) географічно інформаційних систем;
- б) Геоінформаційної системи;
- в) Соціально-економічної системи.

109. Комп'ютер, на якому розміщена ГІС-складова?

- а) програмне забезпечення;
- б) дані;
- в) апаратні дані.

110. ГІС містить функції та інструменти, необхідні для зберігання, аналізу та візуалізації географічної (просторової) інформації – складова?

- а) виконавці;
- б) апаратні дані;
- в) програмне забезпечення.

111. Успішність та ефективність (зокрема економічна) застосування ГІС багато в чому залежить від правильно складеного плану і правил роботи, які мають відповідати специфіці завдань кожної організації – складова?

- а) виконавці;
- б) методи;
- в) дані.

112. Носій інформації або засіб закріплення інформації про факти, події, явища об'єктивної дійсності та розумової діяльності людини – це:

- а) документ;
- б) матеріальний носій (диск, флешка);
- в) архів.

113. Електронний документообіг – це:

а) 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;

б) форма документа, що характеризується використанням інформаційно-комунікаційних технологій як основного засобу для колективних розумових і адміністративних процесів (інформування, прийняття спільних рішень);

в) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розсередження даних, доступ до джерел інформації незалежно від місця їх розташування;

114. Система електронного документообігу (СЕД) – це:

а) впровадження автоматичного контролю, виконання всіх етапів роботи з документами для підвищення якості роботи виконавців, терміни роботи документів більш прогнозовані;

б) сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації;

в) програмно-технічний комплекс, який забезпечує (підтримує) здійснення електронного обміну документами в організаційних структурах та міжвідомчу взаємодію.

115. Переваги системи електронного документообігу:

а) нормативно-методична база діловодства; види документів та їх класифікація; стандартизація, уніфікація та трафаретизація управлінських документів; документування та документальне забезпечення управлінської діяльності установ державного управління та місцевого самоврядування та ін.;

б) використання шаблонів текстових атрибутів у системі; колективна робота під час розроблення і виконання документів; наочний і зручний контроль виконання встановлених доручень; автоматичне зняття завдань з контролю під час реєстрації документів, що скасовують їх виконання; підтримка завдань з циклічним періодом виконання та ін.;

в) підвищення оперативності роботи апарату управління і відповідальності виконавців шляхом розмежування функцій, структурних підрозділів і обов'язків виконавців, чіткого розподілу інформації; економія праці за рахунок використання інформаційно-довідкового апарату (предметно-тематичного каталогу) та ін..

116. Суб'єктами електронного документообігу є:

а) автор, підписувач, адресат;

б) книга, документ, носій;

в) документопотік, документообіг.

117. Електронний підпис – це:

а) дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації

підписувача цих даних;

б) ваше «Я» на будь-якому офіційному документі;

в) обов'язковий реквізит будь-якого документа, як службового, так і особистого.

118. Електронний цифровий підпис накладається за допомогою:

а) електронного цифрового ключа;

б) відкритого ключа;

в) особистого ключа.

119. Електронний цифровий підпис відкривається за допомогою:

а) електронного цифрового ключа;

б) відкритого ключа;

в) особистого ключа.

120. На першому етапі перевірки електронного цифрового підпису одержаного документу:

а) адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.

б) за допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток;

в) при перевірці ЕЦП порівнюються відбитки початкового і одержаного документів.

121. Другий етап перевірки електронного цифрового підпису одержаного документу:

а) адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.

б) за допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток;

в) при перевірці ЕЦП порівнюються відбитки початкового і одержаного документів.

122. Завершальний етап перевірки електронного цифрового підпису одержаного документу:

а) адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа;

б) за допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток;

в) при перевірці ЕЦП порівнюються відбитки початкового і одержаного документів.

123. До електронних інформаційних ресурсів належать:

а) дані, інформація, бази даних, документи, носії та ін.;

б) дані, інформація, бази даних, реєстри та ін.;

в) дані, інформація, документи, бази даних, реєстри та ін.

124. Персональні дані – це:

а) результати вимірювань, спостережень, логічних або арифметичних операцій, придатні для обробки та зберігання в інформаційно-телекомунікаційних системах;

б) інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їх бажанням відповідно до передбачених ними умов;

в) дані про особу, що у сукупності є унікальними даними конкретної фізичної особи, належать цій особі та дозволяють ідентифікувати особу.

125. Дані – це:

а) результати вимірювань, спостережень, логічних або арифметичних операцій, придатні для обробки та зберігання в інформаційно-телекомунікаційних системах;

б) інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їх бажанням відповідно до передбачених ними умов;

в) дані про особу, що у сукупності є унікальними даними конкретної фізичної особи, належать цій особі та дозволяють ідентифікувати особу.

126. Електронні інформаційні ресурси є:

а) системою, яка могла підтримувати будь-яку кількість користувачів з здатність системи нарощувати потужність визначалась тільки потужністю відповідного програмного забезпечення;

б) складовою національного інформаційного простору та інформаційної інфраструктури держави;

в) є атрибутом захисту громадянами своїх інтересів і визначення форм співпраці з державою за допомогою технологій е-урядування.

127. Державні реєстри, кадастри, електронні бази даних, портали та сайти органів влади – це:

- а)** інформаційні чинники органів державної влади;
- б)** інформаційні ресурси органів державної влади;
- в)** інформаційні відносини органів державної влади.

128. Національний реєстр – це:

а) державний реєстр договорів(контрактів) про спільну інвестиційну діяльність за участю іноземних інвесторів та ін.;

б) інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, обробки та зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів;

в) реєстр галузевих і регіональних угод, колективних договорів.

129. Адміністративна послуга – це:

а) підвищення оперативності роботи апарату управління і відповідальності виконавців шляхом розмежування функцій, структурних підрозділів і обов'язків виконавців, чіткого розподілу інформації;

б) встановлення єдиного комплексу видів і різновидів документів для аналогічних управлінських ситуацій, розробка єдиних форм і правил складання, оформлення і створення трафаретних текстів;

в) державна послуга, яка є результатом здійснення суб'єктом повноважень щодо прийняття згідно з нормативно- правовими актами на звернення фізичної або юридичної особи адміністративного акта, спрямованого на реалізацію та захист її прав і законних інтересів;

130. Надання державно управлінських послуг громадянам передбачається через єдиний портал, або «єдине вікно» – це:

а) організаційна форма надання адміністративних послуг, яка передбачає проведення всіх процедур, необхідних для надання адміністративної послуги посадовими особами суб'єкта, за умови отримання від одержувача всіх документів;

б) офіційний документ, що засвідчує особу та її права, обов'язки, службове або громадське становище і у ньому можуть бути також інші відомості біографічного характеру;

в) єдина комп'ютерна база даних про адміністративні послуги, які надаються відповідно до законодавства центральними органами виконавчої влади, їх територіальними органами.

131. Одержувач адміністративної послуги – це:

а) фізична або юридична особа, якій законом або за згодою

суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

б) фізична чи юридична особа (резидент або нерезидент), що звертається або звернулася за адміністративною послугою безпосередньо або через законного представника до адміністративного органу;

в) фізична або юридична особа, якій належить право власності на інформацію.

132. Орган виконавчої влади, орган місцевого самоврядування в межах делегованих їм органами виконавчої влади повноважень, підприємства, установи та організації, на які згідно з нормативно-правовими актами покладено повноваження надавати адміністративні послуги це:

а) собівартість адміністративної послуги;

б) суб'єкт надання адміністративних послуг;

в) стандарт адміністративної послуги.

133. У країнах Європейської співдружності надаються базові державні послуги для громадян в он-лайнному режимі:

а) прибутковий податок, пошук роботи через служби зайнятості, соціальна допомога, допомога на дитину, відшкодування витрат на медичні послуги, оплата навчання та ін.;

б) публічні бібліотеки, свідоцтва про народження, шлюб, подання заяви на вступ до вищого навчального закладу, інформування про зміну місця проживання, послуги, пов'язані з медициною, надання проживання, оплачування відпусток та ін.;

в) прибутковий податок, пошук роботи через служби зайнятості, соціальна допомога, інформування про зміну місця проживання, послуги, пов'язані з медициною, надання проживання, оплачування відпусток та ін.

134. Державна установа є:

а) об'єктом управління;

б) суб'єктом управління.

135. Юридична особа, що має власне майно, майнові права, певну незалежність від осіб в її складі та є відповідальною за свої дії – це:

а) об'єкт господарювання;

б) суб'єкт господарювання;

в) суб'єкт управління.

136. Розрізняють такі принципи управління:

а) структурний, адміністративний, фінансовий і розподільчий;

б) міжгалузевий, адміністративний, податковий та розгалужений;

в) структурний, адміністративний, податковий, розподільчий.

137. Структурний принцип управління:

а) передбачає, що реальна діяльність здійснюється на найнижчих рівнях ієрархії;

б) властивий великим ієрархічним структурам і характеризується переданням керівних впливів згори вниз чи уздовж вертикалі влади;

в) полягає в тому, що організацію розбито на кілька окремих центрів.

138. Адміністративний принцип управління:

а) передбачає, що реальна діяльність здійснюється на найнижчих рівнях ієрархії;

б) властивий великим ієрархічним структурам і характеризується переданням керівних впливів згори вниз чи уздовж вертикалі влади;

в) полягає в тому, що організацію розбито на кілька окремих центрів.

139. Фінансовий принцип управління:

а) передбачає, що реальна діяльність здійснюється на найнижчих рівнях ієрархії;

б) властивий великим ієрархічним структурам і характеризується переданням керівних впливів згори вниз чи уздовж вертикалі влади;

в) полягає в тому, що організацію розбито на кілька окремих центрів.

140. Категорійно-понятійний апарат з питань інформаційної безпеки та захисту інформації:

а) доступ до інформації, захист інформації, знищення інформації, користувач інформації в системі, обробка інформації в системі та ін.;

б) несанкціоновані дії, знищення інформації, порушення цілісності інформації, комплексна система захисту інформації, розповсюдження інформації, видалення інформації та ін.;

в) доступ до інформації, захист інформації, знищення інформації, користувач інформації в системі, обмеження інформації, відкладення інформації та ін.

141. Несанкціоновані дії щодо інформації в системі – це:

а) дії, що проводяться з порушенням порядку доступу до цієї інформації, встановленого відповідно до законодавства;

б) несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її зміст;

в) дії, внаслідок яких унеможлиблюється доступ до інформації в системі.

142. Аутентифікація – це:

а) результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

б) процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апіорної інформації про нього, яка сприймається системою;

в) процедура встановлення належності користувачеві пред'явленого ним ідентифікатора.

143. Об'єкти інформаційної безпеки:

а) особистісні, соціальні;

б) соціальні, технологічні;

в) соціальні, технічні.

144. Особа, суспільство, держава – це об'єкти:

а) соціальні;

б) технічні;

в) технологічні.

145. Інформаційні ресурси, інформаційна інфраструктура, інформаційні технології – це об'єкти:

а) соціальні;

б) технічні;

в) технологічні.

Ключ до тесту:

1а; 2в; 3а; 4в; 5б; 6б; 7б; 8в; 9в; 10а; 11б; 12в; 13в; 14а; 15б; 16б; 17в; 18а; 19в; 20б; 21в; 22а; 23а; 24в; 25в; 26а; 27б; 28б; 29в; 30а; 31а; 32в; 33б; 34в; 35а; 36б; 37б; 38а; 39а; 40а; 41б; 42в; 43б; 44а; 45в; 46а; 47в; 48б; 49в; 50в; 51в; 52а; 53б; 54в; 55а; 56в; 57б; 58б; 59а; 60в; 61б; 62а; 63а; 64б; 65в; 66а; 67б; 68в; 69б; 69в; 70в; 71а; 72а; 73б; 74б; 75а; 76б; 77б; 77б; 78б; 79б; 80б; 81б; 82а; 83а; 84б; 85а; 86б; 87в; 88б; 89в; 90а; 91а; 92а; 93б; 94в; 95б; 96а; 97а; 98в; 99б; 100б; 101а; 102в; 103а; 104в; 105б; 106б; 107а; 108а; 109в; 110в; 111б; 112а; 113а; 114в; 115б; 116а; 117в; 118в; 119б; 120а; 121б; 122в; 123б; 124в; 125а; 126б; 127б; 128б; 129в; 130а; 131б; 132б; 133а; 134а; 135б; 136а; 137б; 138а; 139в; 140а; 141а; 142в; 143в; 144а; 145б.

СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ

А

Адаптація – процес інтеграції нових технологій у державну систему.

Автентифікація – перевірка достовірності особи через електронні засоби.

Анонімність – забезпечення конфіденційності особистих даних користувачів.

Аналітика – використання статистичних методів для аналізу інформації.

Апаратне забезпечення – фізичні пристрої, що використовуються для електронного документообігу.

Аудит – перевірка відповідності системи або документа вимогам безпеки.

Б

Безпека даних – захист інформації від несанкціонованого доступу.

Блокчейн – технологія для забезпечення прозорості та незмінності даних.

Бюрократія – складні адміністративні процедури, що ускладнюють доступ до послуг.

Більші дані – обробка великих обсягів інформації для отримання цінних висновків.

Баланс даних – управління рівнем доступу до інформації для забезпечення безпеки.

В

Вебплатформа – інтерактивна інтернет-платформа для надання послуг.

Верифікація – процес підтвердження достовірності даних або документів.

Взаємодія – обмін інформацією між різними системами та користувачами.

Виконання електронних процедур – здійснення адміністративних дій через цифрові системи.

Відповідальність – обов'язок органів влади надавати якісні електронні послуги.

Візуалізація даних – представлення складних даних у графічній формі для кращого розуміння.

Вхід у систему – процес авторизації користувача для доступу до послуг.

Г

Гарантії безпеки – механізми для забезпечення захисту інформаційних систем.

Глобалізація – процес інтеграції цифрових технологій у світову економіку.

Групи користувачів – різні категорії людей, які використовують державні електронні сервіси.

Генерація документа – створення документа в електронній системі управління.

Гнучкість системи – можливість адаптації електронних систем до нових вимог.

Д

Дані – інформація, що обробляється в електронних системах.

Документування – процес створення, обробки та зберігання документів.

Дистанційне управління – можливість керувати процесами без фізичної присутності.

Доступність – можливість використання сервісів без обмежень.

Державна реєстрація – процес внесення даних у офіційні електронні реєстри.

Документи в реальному часі – документи, що створюються та редагуються без затримок.

Е

Електронна ідентифікація – перевірка особи за допомогою цифрових інструментів.

Електронна петиція – онлайн-звернення громадян до органів влади.

Електронний підпис – криптографічний засіб для підтвердження автентичності документа.

Електронне урядування – використання цифрових технологій для управлінських процесів.

Електронний документообіг – система для обміну документами в електронному вигляді.

Експертиза документів – перевірка точності та достовірності електронних документів.

Електронні платформи – вебсайти для надання цифрових послуг громадянам.

Ж

Життєвий цикл документа – етапи створення, обробки, зберігання та знищення документів.

Журнали реєстрації – записи для фіксації всіх операцій з електронними документами.

Живі дані – дані, які постійно оновлюються в реальному часі.

Життєвий цикл проекту – етапи планування та реалізації проектів у сфері електронного врядування.

З

Захист персональних даних – забезпечення конфіденційності особистої інформації.

Зовнішній доступ – доступ до системи чи інформації ззовні організації.

Завершення процесу – момент, коли всі дії щодо документа в системі завершено.

Запит – звернення або вимога на отримання інформації або послуг.

Захист від зловживань – механізми запобігання незаконному використанню електронних систем.

Забезпечення доступу – надання користувачам права на доступ до електронних послуг.

І

Ідентифікація користувача – визначення особи за допомогою логінів або цифрових засобів.

Інтеграція систем – з'єднання різних інформаційних технологій для ефективної роботи.

Інформаційна безпека – захист інформації від кіберзагроз та несанкціонованих доступів.

Інтерфейс – зовнішня частина програми, з якою взаємодіє користувач.

Інструменти моніторингу – засоби для відстеження роботи електронних систем.

Інновації – нові технології або методи, які покращують роботу електронного урядування.

Інтернет-сервіси – онлайн-системи для доступу до різних державних послуг.

К

Контроль доступу – система, яка визначає, хто може отримувати доступ до інформації.

Кіберзагрози – потенційні загрози для інформаційних систем з боку кіберзлочинців.

Криптографія – технологія захисту даних через їх шифрування.

Користувач – особа, що взаємодіє з електронними системами та послугами.

Координація процесів – узгодження дій між різними частинами електронного документообігу.

Класичний документообіг – обробка документів в паперовому вигляді.

Комп'ютерні мережі – система для з'єднання комп'ютерів і обміну даними між ними.

Л

Ліцензування – процес надання дозволу на використання програмного забезпечення.

Логування – процес запису дій користувачів та системних подій у журнал.

Логіка документів – структура і організація документів в електронному обігу.

Локалізація – адаптація системи або програмного забезпечення до місцевих умов.

Ліміт доступу – обмеження доступу до конкретних даних або послуг.

М

Модернізація – оновлення або поліпшення електронних систем чи технологій.

Мережеві технології – інструменти та стандарти для роботи в комп'ютерних мережах.

Моделі управління – концепції та стратегії управління електронним документообігом.

Моніторинг систем – процес спостереження за роботою електронних систем.

Міжнародна співпраця – взаємодія між державами для покращення електронного врядування.

Мобільні платформи – застосунки для доступу до послуг через мобільні пристрої.

Масштабованість – здатність системи адаптуватися до збільшення обсягу даних або користувачів.

Н

Надійність системи – здатність електронної системи працювати

без перебоїв.

Нормативно–правова база – система законів та регламентів, що регулюють електронний документообіг.

Налаштування доступу – визначення прав користувачів для доступу до інформації.

Неправомірний доступ – несанкціонований доступ до даних або систем.

Невизначеність даних – ситуація, коли інформація є неповною або неясною.

Налаштування системи – конфігурація параметрів електронних платформ для ефективної роботи.

О

Онлайн–сервіси – цифрові послуги, доступні через інтернет.

Обробка даних – аналіз та використання інформації в електронних системах.

Оперативність – здатність системи швидко реагувати на запити користувачів.

Офіційні електронні документи – документи, що мають юридичну силу та створюються в електронному вигляді.

П

Персональні дані – інформація, що ідентифікує особу в електронних системах.

Протокол безпеки – набір правил для захисту даних і забезпечення безпеки в мережах.

Підпис електронний – засіб для підтвердження автентичності електронних документів.

Платформа електронного врядування – технологічна інфраструктура для надання державних послуг через інтернет.

Процес документообігу – етапи створення, перевірки, зберігання та передачі документів.

Публічні послуги – послуги, що надаються громадянам державними органами через електронні платформи.

Підключення до системи – процес автентифікації та доступу користувача до електронної платформи.

Р

Розпізнавання документів – процес аналізу та інтерпретації даних з електронних документів.

Резервне копіювання – збереження даних на випадок втрати інформації.

Реєстрація користувача – процес створення облікового запису для доступу до системи.

Робоче середовище – набір інструментів для виконання завдань в електронному документообігу.

Ризики безпеки – потенційні загрози для інформаційних систем.

Реакція на загрози – дії, що вживаються для нейтралізації кіберзагроз.

Робочі процеси – внутрішні процедури, що визначають ефективність роботи електронної системи.

С

Системи електронного документообігу – програмні комплекси для управління документами в електронному вигляді.

Сигнатура електронна – криптографічний підпис для підтвердження автентичності.

Сервіс цифрових підписів – онлайн-інструмент для створення електронних підписів.

Система управління доступом – система, що контролює права доступу до інформації в електронних системах.

Секретність даних – захист особистої та конфіденційної інформації від розголошення.

Система збереження даних – інфраструктура для довготривалого зберігання інформації.

Складність документа – рівень деталізації та обсягу інформації в електронних документах.

Т

Технічні вимоги – стандарти, що визначають умови для функціонування електронних систем.

Технологія шифрування – методи захисту інформації шляхом перетворення її в зашифрований вигляд.

Технічна підтримка – допомога користувачам у випадку проблем з електронними системами.

Термін зберігання – час, протягом якого зберігаються електронні документи.

Трансфер даних – передача інформації з однієї системи в іншу.

У

Управління доступом – процес визначення, хто і на яких умовах може отримувати доступ до інформаційних ресурсів.

Узгодження документів – процес перевірки, коригування та погодження документів в електронному вигляді.

Уніфікація формату – стандартизація форматів документів для їх сумісності в електронних системах.

Управління даними – процес організації, обробки та збереження даних в інформаційних системах.

Уповноважений підпис – цифровий підпис, що надається органом влади чи організацією для підтвердження документів.

Уразливість системи – слабкі місця в інформаційній системі, які можуть бути використані для порушення її роботи або безпеки.

Участь громадян – залучення населення до процесів електронного врядування через петиції, голосування та інші механізми.

Ф

Фізична безпека – заходи захисту фізичних елементів інформаційної інфраструктури, таких як сервери, мережеве обладнання.

Формати файлів – стандарти для збереження та обміну даними у вигляді файлів у різних програмах.

Фільтрація інформації – процес обмеження доступу до певних даних або функцій на основі прав користувача.

Функціональність платформи – можливості, які надає система для користувачів і адміністраторів.

Формування звітності – процес створення звітів та аналізу даних для моніторингу результатів роботи системи.

Х

Хмарні технології – методи зберігання даних та обчислень, що базуються на віддалених серверах через інтернет.

Хакерські атаки – несанкціоновані спроби проникнення в інформаційні системи з метою викрадення або порушення їх роботи.

Хронологія документів – відображення послідовності змін і версій документів у системах електронного документообігу.

Хостинг – послуга з надання місця для зберігання вебсайтів або даних в інтернеті.

Характеристики безпеки – параметри системи, що визначають її захищеність від зовнішніх і внутрішніх загроз.

Хостинг-сервіс – компанія або платформа, що надає серверне середовище для зберігання даних або вебсайтів.

Ц

Цифрове підписання – використання криптографії для підтвердження автентичності та цілісності електронних документів.

Цифровий формат – спосіб збереження та обміну даними в цифровому вигляді.

Центр обробки даних – фізична або віртуальна інфраструктура для зберігання, обробки та моніторингу інформаційних систем.

Цифровий документообіг – обробка та управління документами у цифровому форматі з використанням електронних систем.

Цілісність системи – відсутність збоїв або втручань у роботу інформаційної системи.

Ч

Часова мітка – цифровий запис часу створення або підписання документа.

Частота оновлень – періодичність оновлення програмного забезпечення та інформаційних систем.

Читання та запис – операції з доступом до даних у системах збереження інформації.

Ш

Шифрування даних – процес перетворення інформації у вигляд, зрозумілий лише тим, хто має ключ для її дешифрування.

Швидкість обробки – час, необхідний для виконання операцій з даними в електронних системах.

Шаблони документів – стандартизовані форми для швидкого створення документів у системах.

Ю

Юридична сила електронного документа – правова значущість документів, створених та підписаних в електронній формі.

Юзабіліті – зручність використання інформаційних систем для кінцевого користувача.

Юридичний статус електронного підпису – визначення легітимності електронного підпису відповідно до законодавства.

Я

Якість обробки даних – рівень точності та ефективності обробки інформації в електронних системах.

Явне схвалення – чітке підтвердження згоди користувача або організації щодо використання даних або підписання документа.

Явна ідентифікація – процес однозначного визначення особи або сутності в системі.

СПИСОК ЛІТЕРАТУРИ

1. ABBYY FlexiCapture. URL: <https://www.abbyy.com/flexicaputure> (дата звернення: 20.03.2025).
2. Adobe Sign. URL: <https://acrobat.adobe.com/us/en/sign.htm> (дата звернення: 20.03.2025).
3. Amazon Textract. URL: <https://aws.amazon.com/textract>
4. Contract Express. URL: <https://legal.thomsonreuters.com/en/products/contract-express> (дата звернення: 20.03.2025).
5. DOCS.UA. URL: <https://docs.ua> (дата звернення: 20.03.2025).
6. DocuSign. URL: <https://www.docusign.com> (дата звернення: 20.03.2025).
7. Dropbox. URL: <https://www.dropbox.com> (дата звернення: 20.03.2025).
8. e-Docs. URL: <https://www.edoc.gov.ua> (дата звернення: 20.03.2025).
9. E-Government Survey 2024. United Nations. URL: <https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf> (дата звернення: 20.03.2025).
10. elDoc. URL: <https://eldoc.ua> (дата звернення: 20.03.2025).
11. Ethereum. URL: <https://ethereum.org> (дата звернення: 20.03.2025).
12. FossDoc. URL: <https://fossdoc.com> (дата звернення: 20.03.2025).
13. Google Cloud Vision. URL: <https://cloud.google.com/vision> (дата звернення: 20.03.2025).
14. Google Drive. URL: <https://www.google.com/drive> (дата звернення: 20.03.2025).
15. HotDocs. URL: <https://www.hotdocs.com> (дата звернення: 20.03.2025).
16. Hyperledger. URL: <https://www.hyperledger.org> (дата звернення: 20.03.2025).
17. IBM Blockchain. URL: <https://www.ibm.com/blockchain> (дата звернення: 20.03.2025).

18. LawGeex. URL: <https://www.lawgeex.com> (дата звернення: 20.03.2025).
19. Megapolis.DocNet. URL: <https://megapolisdocus.net> (дата звернення: 20.03.2025).
20. Microsoft Cognitive Services. URL: <https://azure.microsoft.com/en-us/services/cognitive-services> (дата звернення: 20.03.2025).
21. Microsoft OneDrive. URL: <https://onedrive.live.com> (дата звернення: 20.03.2025).
22. Microsoft SharePoint. URL: <https://www.microsoft.com/sharepoint> (дата звернення: 20.03.2025).
23. Signaturit. URL: <https://www.signaturit.com> (дата звернення: 20.03.2025).
24. Smirnova N. E-government and social media in Ukraine: global challenges for legal regulations. Lex Portus 1(1(2020)). URL: https://www.researchgate.net/publication/340018781_E-government_and_social_media_in_Ukraine_global_challenges_for_legal_regulations (дата звернення: 20.03.2025).
25. The Importance of Digital Literacy у 21st Century. URL: <https://aithor.com/essay-examples/the-importance-of-digital-literacy-in-the-21st-century> (дата звернення: 20.03.2025).
26. АСКОД. URL: <https://askod.com.ua> (дата звернення: 20.03.2025).
27. ДСТУ 4163:2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів : затв. наказом ДП «УкрНДНЦ» від 01.07.2020 р. № 144. [Чинний від 2021-09-01]. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90348 (дата звернення: 20.03.2025).
28. ДСТУ 9031:2020. Правила публікування інформації архівних документів : затв. наказом ДП «УкрНДНЦ» від 01.07.2020 р. № 144. [Чинний від 2021-09-01]. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90349 (дата звернення: 20.03.2025).
29. «Дія. Освіта». URL: <https://osvita.diia.gov.ua/> (дата звернення: 20.03.2025).
30. Дослідження цифрової грамотності населення України за 2023 рік. URL: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf (дата звернення: 20.03.2025).

31. Електронне урядування в публічному управлінні : словник основних термінів і понять. Львів : Растр-7, 2024. 128 с.
32. Електронне урядування : навч. посіб. / Семенченко А. І. та ін. ; за ред. А. І. Семенченка. Кабінет Міністрів України, Нац. ун-т біоресурсів і природокористування України, навч.-наук. ін-т післядиплом. освіти. Херсон : Грінь Д. С., 2014. 391 с.
33. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851–IV. URL: <https://zakon.rada.gov.ua/go/851-15> (дата звернення: 20.03.2025).
34. Про інформацію : Закон України від 02.10.1992 р. № 2657–XII. URL: <https://zakon.rada.gov.ua/go/2657-12> (дата звернення: 20.03.2025).
35. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94–ВР. URL: <https://zakon.rada.gov.ua/go/80/94-вр> (дата звернення: 20.03.2025).
36. Про державну таємницю : Закон України від 21.01.1994 р. № 3855–XII. URL: <https://zakon.rada.gov.ua/go/3855-12> (дата звернення: 20.03.2025).
37. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089–IX. URL: <https://zakon.rada.gov.ua/go/1089-20> (дата звернення: 20.03.2025).
38. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155–VIII. URL: <https://zakon.rada.gov.ua/go/2155-19> (дата звернення: 20.03.2025).
39. Про обов'язковий примірник документів : Закон України від 09.04.1999 р. № 595–XIV. URL: <https://zakon.rada.gov.ua/go/595-14> (дата звернення: 20.03.2025).
40. Про Національний архівний фонд та архівні установи : Закон України від 24.12.1993 р. № 3814–XII. URL: <https://zakon.rada.gov.ua/go/3814-12> (дата звернення: 20.03.2025).
41. Про електронну комерцію : Закон України від 03.09.2015 р. № 675–VIII. URL: <https://zakon.rada.gov.ua/go/675-19> (дата звернення: 20.03.2025).
42. Ковбасюк Ю. В. Державне управління : підручник. Дніпропетровськ : НАДУ, 2013. 324 с.
43. Лист Державної фіскальної служби України від 04.05.2016 р. № 9985/6/99-95-42-01-16-01-15 щодо можливості використання електронного цифрового підпису при оформленні

первинних облікових документів. URL:
<https://tax.gov.ua/baneryi/podatkovyi-konsultatsii/konsultatsii-dlya-yuridichnih-osib/print-67999.html> (дата звернення: 20.03.2025).

44. Лист Державної податкової служби України від 26.12.2011 р. № 10406/7/18-4017 «Про визнання органами ДПС електронних первинних документів». URL:
<https://www.tax.gov.ua/elektronna-zvitnist/platnikam-podatkiv-pro/povidomlennya-platnikam-pod/58692.html> (дата звернення: 20.03.2025).

45. Лист Державної фіскальної служби України від 03.03.2017 р. № 4451/6/99-99-14-03-03-15 щодо використання документів, створених в електронному вигляді. URL:
<https://buhgalter911.com/normativnaya-baza/pisma/gfsu/schodo-vikoristannya-dokumentiv-1027204.html> (дата звернення: 20.03.2025).

46. Матвієнко О. В. Основи організації електронного документообігу : навч. посіб. К. : Центр учбової літератури, 2008. 112 с.

47. Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання : наказ Міністерства юстиції України від 11.11.2014 р. № 1886/5. URL: <https://zakon.rada.gov.ua/laws/show/z1421-14> (дата звернення: 20.03.2025).

48. Про затвердження Типової інструкції з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві : Постанова Кабінету Міністрів України від 17.01.2018 р. № 55. URL: <https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF> (дата звернення: 20.03.2025).

49. Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг : Постанова Кабінету Міністрів України від 12.12.2023 р. № 1298. URL: <https://ips.ligazakon.net/document/KP231298> (дата звернення: 20.03.2025).

50. Семенченка А. І., Дрешпака В. М. Електронне урядування та електронна демократія : навч. посіб. Київ : ФОП Москаленко О.М., 2017. Ч. 2. 72 с.

51. Скібіцька Л. І. Діловодство : навч. посіб. для студ. ВНЗ 2–ге вид. Київ : Кондор, 2012. 219 с.

52. Тітенко Л. А. Діловодство з використанням комп'ютерної техніки : навч. посіб. Держ. вищ. навч. закл. «Київ. нац. екон. ун-т ім. Вадима Гетьмана». Київ : КНЕУ, 2014. 345 с.

53. Федусенко О. В., Доманецька І. М., Красовська Г. М. Проектування систем електронного документообігу : навч. посіб. для студ., які навч. за напрямом підгот. 6.050101 «Комп'ютерні науки». Київ. нац. ун-т буд-ва і архітектури. Київ : КНУБА, 2017. 287 с.

54. Цифрограм. Дія. Цифрова Освіта. URL: <https://osvita.diia.gov.ua/digigram> (дата звернення: 20.03.2025).

55. Чукут С. А., Загвойська О. В., Цимбаленко Я. Ю. Основи електронного урядування : навч. посіб. Електронне мережне навчальне видання. Київ : КПІ ім. Ігоря Сікорського, 2022. 248 с. URL: file:///C:/Users/User/OneDrive/Desktop/%D0%9A%D0%9D%D0%98%D0%93%D0%90/E-governance_Manual_KPI.pdf (дата звернення: 20.03.2025).

Навчальне видання

*Маланчук Лариса Олексіївна
Гонгадзе Яна Володимирівна*

Основи електронного документообігу та електронного урядування

Навчальний посібник

Друкується в авторській редакції

Технічний редактор

Г.Ф. Сімчук

*Видавець і виготовлювач
Національний університет
водного господарства та природокористування,
вул. Соборна, 11, м. Рівне, 33028.*

*Свідоцтво про внесення суб'єкта видавничої справи до
державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції РВ № 31 від 26.04.2005 р.*