МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ
ФАКУЛЬТЕТ ЕКОНОМІКИ ТА УПРАВЛІННЯ

Роман Януш

Алла Фатенок-Ткачук

ОСНОВИ ЦИФРОВОЇ ГРАМОТНОСТІ

Конспект лекцій

Луцьк 2026

УДК 657:[37.011.2:004(07)
Ф 27

Рекомендовано до друку науково-методичною радою Волинського національного університету імені Лесі Українки (протокол № 6 від «18» лютого 2026 р.)

Рецензент: ***Стащук О. В****., д. е. н., професор, завідувач кафедри фінансів ВНУ імені Лесі Українки*

Януш Р. І., Фатенок-Ткачук А. О.
Ф 27 Основи цифрової грамотності : конспект лекцій для здобувачів напрямку підготовки D «Бізнес, адміністрування та право» спеціальності D1 «Облік і оподаткування» освітніх програм «Облік і оподаткування» та «Цифровий облік та консалтинг» денної та заочної форм навчання / Роман Ігорович Януш, Алла Олександрівна Фатенок-Ткачук. Луцьк : Вежа-друк, 2026, 80 с. – для розміщення в електронному репозитарії ВНУ імені Лесі Українки

Анотація: Конспект лекцій містить теоретичні аспекти згідно тематики курсу, що відповідає силабусу освітнього компонента «Основи цифрової грамотності».

Рекомендовано здобувачам денної та заочної форми здобуття освіти у напрямках обліку та фінансів з метою засвоєння теоретичних основ та отримання практичних навичок та soft skills зі спеціальності «Облік і оподаткування».

УДК 657:[37.011.2:004(07)

ЗМІСТ

ВСТУП

У сучасному світі цифрова грамотність стала основою, що визначає здатність людини ефективно орієнтуватися у цифровому інформаційному середовищі. Вона охоплює не лише базові технічні навички, як-от вміння користуватися таблицями чи текстовими документами, але й здатність критично мислити, аналізувати та безпечно використовувати інформацію.

Освітній компонент «Основи цифрової грамотності» належить до циклу загальної підготовки та спрямований на ознайомлення здобувачів освіти з основами інформаційних технологій сервісів, шляхів їх застосування здобувачів спеціальності «Облік і оподаткування», формування теоретичних знань та набуття компетенцій забезпечення інформаційними технологіями процесу обліку, аналізу, оподаткування, контролю.

Вивчення освітнього компонента базується на знаннях, уміннях і навичках, які здобувачі освіти отримали під час вивчення освітніх компонентів «Групова динаміка та комунікації (тренінг)», «Культура та етика ведення бізнесу», «Інформаційно-комунікаційні технології».

Вивчення освітнього компонента сприятиме кращому засвоєнню таких освітніх компонентів, як: «Навчальна практика з використання цифрових інструментів в бухгалтерському обліку», «Спеціалізовані інформаційні системи в обліку», «Цифрові інструменти в обліку бюджетних установ», «Бізнес-аналітика в цифровому просторі», «Цифрові технології в оподаткуванні суб'єктів господарювання», «Звітність підприємств у цифровій економіці» тощо.

Метою освітнього компонента є формування у майбутніх фахівців за професійним спрямуванням з обліку і оподаткування системних знань практичних навичок в користуванні інформаційними ресурсами, що спрощують роботу бухгалтера.

Основними завданнями освітнього компонента є ознайомлення здобувачів освіти інноваціями у сфері інформаційних технологій та шляхів їх використання в обліково-аналітичних процесах та збереженні облікових цифрових даних.

Згідно з освітньо-професійною програмою здобувачі освіти в результаті вивчення освітнього компонента «Основи цифрової грамотності» набудуть таких компетентностей та програмних результатів навчання:

Інтегральна компетентність – Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності у сфері обліку, аудиту та оподаткування або в процесі навчання, що передбачає застосування теорій та методів економічної науки і характеризується комплексністю й невизначеністю умов.

Загальні компетентності (ЗК):

ЗК01. Здатність вчитися і оволодівати сучасними знаннями.

ЗК02. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК04. Здатність працювати автономно.

ЗК06. Здатність діяти на основі етичних міркувань (мотивів).

ЗК08. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК10. Здатність спілкуватися іноземною мовою.

ЗК11. Навички використання сучасних інформаційних систем і комунікаційних технологій.

ЗК12. Здатність діяти соціально відповідально та свідомо.

ЗК14. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні (фахові) компетентності (СК):

СК06. Здійснювати облікові процедури із застосуванням спеціалізованих інформаційних систем і комп'ютерних технологій.

СК10. Здатність застосовувати етичні принципи під час виконання професійних обов'язків.

Програмні результати навчання (ПРН):

ПР02. Розуміти місце і значення облікової, аналітичної, контрольної, податкової та статистичної систем в інформаційному забезпеченні користувачів обліково-аналітичної інформації у вирішенні проблем в сфері соціальної, економічної і екологічної відповідальності підприємств.

ПР09. Ідентифіковувати та оцінювати ризики господарської діяльності підприємств.

ПР12. Застосовувати спеціалізовані інформаційні системи і комп'ютерні технології для обліку, аналізу, контролю, аудиту та оподаткування.

ПР17. Вміти працювати як самостійно, так і в команді, проявляти лідерські якості та відповідальність у роботі, дотримуватися етичних принципів, поважати індивідуальне та культурне різноманіття.

ПР20. Виконувати професійні функції з урахуванням вимог соціальної відповідальності, трудової дисципліни, вміти планувати та управляти часом.

ПР22. Розуміти і реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності вільного демократичного суспільства, верховенства права, прав і свобод людини і громадянина в Україні.

Soft skills

Критичне мислення та цифрова гігієна: здатність розрізняти достовірну інформацію від маніпуляцій, оцінювати ризики в цифровому просторі.

Цифрова адаптивність (Lifelong Learning): готовність до швидкого опанування нових інтерфейсів та оновлень ПЗ.

Цифровий тайм-менеджмент: вміння використовувати цифрові календарі, таск-менеджери та сервіси автоматизації для планування робочого часу бухгалтера.

Стійкість до цифрового стресу: навичка зберігати продуктивність при технічних збоях, зміні алгоритмів роботи або в умовах кіберзагроз.

Цифровий етикет (Netiquette): культура ділового листування в месенджерах, електронній пошті та через системи ЕДО.

Колаборація у віртуальному середовищі: навички ефективної командної роботи в хмарних сервісах (Google Workspace, Microsoft 365) та спільне редагування документів.

Етичне використання ШІ: розуміння меж відповідальності при використанні ChatGPT чи інших ШІ-інструментів у професійній діяльності.

Цифрова відповідальність: усвідомлення наслідків за розголошення персональних даних або порушення конфіденційності клієнтів.

У межах конспекту лекцій буде розглянуто широке коло питань: від поняття хмарних технологій та основ кібербезпеки до використання штучного інтелекту та Big Data у професійній діяльності бухгалтера. Опанування цих тем дозволить майбутнім фахівцям не лише ефективно використовувати сучасні ІТ-інструменти, а й адаптуватися до стрімких змін цифрової епохи.

ТЕМА 1. ЦИФРОВА ГРАМОТНІСТЬ: ПОНЯТТЯ, АКТУАЛЬНІСТЬ, РОЛЬ У ПОВСЯКДЕННІЙ ТА ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ

1. ***Поняття цифрової грамотності***
2. ***Роль цифрової грамотності у повсякденній діяльності***
3. ***Роль цифрової грамотності у професійній діяльності***

1.1 Поняття цифрової грамотності

У сучасному світі цифрова грамотність стала фундаментальною компетенцією, що визначає здатність людини ефективно орієнтуватися у цифровому інформаційному середовищі. Вона охоплює не лише базові технічні навички (вміння користуватися Excel таблицями чи Google документами), але й уміння критично мислити, аналізувати та безпечно використовувати інформацію. Сьогодні розглянемо поняття цифрової грамотності, її актуальність, а також роль у повсякденній та професійній діяльності.

Щоб більш точніше відобразити сутність поняття, наведемо визначення цифрової грамотності із декількох джерел:

Цифрова грамотність – це набір знань, умінь та навичок, які необхідні для безпечного та ефективного використання цифрових технологій та ресурсів інтернету [1].

Цифрова грамотність – здатність людини знаходити, оцінювати та передавати інформацію за допомогою друку або цифрових медіаплатформ *[2].*

Американська бібліотечна асоціація (ALA) визначає цифрову грамотність як «здатність використовувати інформаційні та комунікаційні технології для пошуку, оцінки, створення та передачі інформації, що вимагає як когнітивних, так і технічних навичок» [3]. Згідно із порталом UNESCO, де розширюється дане поняття, додаються аспекти безпечного і відповідального використання, керування та інтеграції інформації за допомогою цифрових технологій [4].

Підсумовуючи, вона поєднує в собі як технічні, так і когнітивні здібності, та використовується для створення, оцінки та обміну інформацією. До технічних навичок можна віднести вміння користуватися комп’ютерами, смартфонами,

програмним забезпеченням та іншими пристроями тощо. Когнітивні навички включають здатність критично аналізувати інформацію, розпізнавати достовірні дані та уникати фейків.

В ході розвитку, технології стали невід'ємною частиною існування кожної особи, а світовий ринок все більше інтегрує використання цифрових технологій, від можливості отримувати знання, до використання сервісів надання державних послуг тощо.

Частка населення України, яке використовує інтернет у своєму повсякденному житті з кожним роком зростає. Дані наведено у табл. 1.

Таблиця 1

Частка населення України, яке використовує інтернет

Рік	Кількість осіб (млн)
2013	18.6
2014	20.9
2015	22
2016	23.8
2017	26.4
2018	27.9
2019	31.1
2020	33.1
2021	34.6
2022	28.6

Також, можна спостерігати суттєві зміни за віковою групою. Дані наведено у табл.2.

Таблиця 2

Статистика частки населення за віковою групою

Вік (роки)	2022	2023	2024
0-4	4.5%	3.7%	3.5%
5-12	9%	9.3%	9%
13-17	5.4%	5.4%	5.9%
18-24	6.5%	4.3%	4.4%
25-34	13.3%	10.8%	9.7%
35-44	16.4%	16.8%	17%
45-54	13.8%	15.1%	15.4%
55-64	13.5%	15.1%	15%
65+	17.6%	19.5%	20.1%

Цифрові технології зробили освіту доступною та інтерактивною. Епідемія

SARS COVID-19 дала вагомий поштовх для розвитку онлайн-платформ з метою опанування іноземних мов, нових навичок та навіть професій. Онлайн-курси, електронні бібліотеки та дистанційне навчання дозволяють людям постійно підвищувати свою кваліфікацію. Сьогодні, ви можете стати студентом найкращих університетів світу не виходячи з дому чи слухати всесвітньовідомих вчених сидячи на дивані. Організація UNESCO наголошує на необхідності інтеграції цифрових навичок у всі рівні освітньої системи, щоб забезпечити конкурентоспроможність на глобальному ринку праці.

У цифрову епоху інформаційні потоки та соціальні мережі стали основними каналами комунікації. Вони формують суспільну думку, впливають на політичні процеси та визначають поведінку людей. Цифрова грамотність дозволяє критично оцінювати інформацію, розпізнавати фейки, захищати особисті дані та брати активну участь у суспільному дискурсі.

Це особливо важливо в умовах інформаційних воєн та масової дезінформації, коли маніпулятивні технології використовуються для впливу на свідомість громадян. Високий рівень цифрової грамотності сприяє розвитку медіакультури, відповідальному використанню онлайн-ресурсів і здатності перевіряти факти з надійних джерел. Опанування навичок аналізу інформації допомагає формувати свідому громадянську позицію та протистояти маніпуляціям.

За даними Європейської комісії, 90% робочих місць уже вимагають базових цифрових навичок. В умовах цифрової трансформації ринку праці знання технологій стає не лише перевагою, а й необхідністю.

Цифрова грамотність сприяє розвитку інновацій, оптимізації бізнес-процесів та відкриває нові можливості для підприємництва. Вона дозволяє автоматизувати рутинні завдання, підвищувати продуктивність праці та створювати конкурентоспроможні продукти. Для малих та середніх підприємств цифрові інструменти дають змогу виходити на глобальні ринки, ефективніше взаємодіяти з клієнтами та адаптуватися до змін.

Окрім економічних аспектів, цифрова грамотність є ключем до економічного зростання та соціальної мобільності. Вона допомагає людям отримувати доступ до

онлайн-освіти, розвивати кар’єру, працювати віддалено та використовувати новітні технології для самореалізації. У сучасному суспільстві рівень цифрових навичок визначає можливості для професійного та особистісного розвитку, а також сприяє зменшенню цифрового розриву між різними соціальними групами.

1.2 Роль цифрової грамотності у повсякденній діяльності

Сучасні технології забезпечують миттєвий доступ до великої кількості інформації, що сприяє самоосвіті та прийняттю обґрунтованих рішень. Провідні платформи для навчання можна поділити на декілька груп, зокрема:

1. Загальна освіта.

- Khan Academy (www.khanacademy.org) – охоплює математику, природничі науки, економіку, історію тощо з інтерактивними вправами;
- Coursera (www.coursera.org) – пропонує безкоштовні курси в університетах;
- edX (www.edx.org) – надає курси університетського рівня в таких закладах, як Гарвард і MIT;
- FutureLearn (www.futurelearn.com) – надає безкоштовні курси з бізнесу, здоров’я та технологій;
- Дія.Освіта (osvita.diia.gov.ua) – освітня платформа від Мінцифри, що пропонує курси з цифрової грамотності, підприємництва та кар’єрного розвитку;
- Prometheus (prometheus.org.ua) – платформа масових відкритих онлайн-курсів від провідних університетів України;
- EdEra (www.ed-era.com) – освітня студія, яка пропонує інтерактивні курси, навчальні матеріали та відеоуроки;
- На Урок (naurok.com.ua) – онлайн-платформа для учнів і вчителів з тестами, матеріалами та інтерактивними завданнями;
- Всеукраїнська школа онлайн (lms.e-school.net.ua) – безкоштовні онлайн-курси для учнів 5-11 класів;

- Оптіма Академія (optima.school) – онлайн-освіта для здобувачів із доступом до інтерактивних уроків.

2. Програмування та інформатика.

- freeCodeCamp (www.freecodecamp.org) – навчає програмуванню через практичні проекти та сертифікації;
- Codecademy (www.codecademy.com) – пропонує інтерактивні уроки кодування;
- CS50 by Harvard (cs50.harvard.edu) – безкоштовний вступний курс інформатики;
- MIT OpenCourseWare (ocw.mit.edu) – безкоштовний доступ до курсів MIT з інформатики;
- ITVDN (itvdn.com) – Курси програмування та IT-навичок українською мовою;

3. Наука та техніка.

- OpenStax (openstax.org) – безкоштовні підручники для коледжів з фізики, біології тощо;
- NASA STEM (www.nasa.gov/stem) – ресурси для студентів, які цікавляться космосом та технікою;
- Stanford Online (online.stanford.edu) – безкоштовні наукові та інженерні курси.

4. Бізнес і менеджмент

- Harvard Online Courses – безкоштовні курси з бізнесу, підприємництва тощо;
- Saylor Academy – безкоштовні курси з бізнесу, економіки та лідерства.

5. Мови та гуманітарні науки.

- Duolingo – платформа для вивчення мов;
- BBC Languages – безкоштовні ресурси для вивчення мов;
- OpenLearn – безкоштовні курси від The Open University;
- Lingva.Skills (lingva.ua) – безкоштовні курси з вивчення англійської

мови.

6. Особистий розвиток і навички.

- TED-Ed – навчальні відео на різні теми;
- Skillshare – наявні безкоштовні курси творчості та продуктивності;
- УМІТИ (umity.in.ua) – освітня платформа з навчальними курсами для розвитку професійних навичок.

У багатьох країнах, зокрема в Україні, впроваджуються цифрові сервіси для отримання державних послуг (наприклад, застосунок «Дія» тощо), що значно полегшує бюрократичні процеси. Завдяки таким платформам громадяни можуть швидко та зручно оформлювати документи, сплачувати податки, отримувати довідки та користуватися іншими послугами без необхідності відвідувати державні установи. Це не лише економить час, а й сприяє прозорості та ефективності роботи органів влади.

Перелік сервісів, які дозволяють зручно користуватися послугами в повсякденному житті:

Єдиний державний вебпортал електронних послуг (portal.diia.gov.ua) – надає доступ до електронних документів, довідок, витягів, реєстрації бізнесу тощо;

Система електронного судочинства «Електронний суд» – дозволяє подавати позови, отримувати судові рішення та відстежувати хід судових справ онлайн;

Є-Малятко – сервіс, що об’єднує кілька послуг для новонароджених (реєстрація народження, оформлення допомоги, прописка тощо);

Електронна черга до держустанов (наприклад, МВС, ДМС) – дозволяє записуватися на прийом до органів влади онлайн;

Електронний кабінет водія (e-driver.hsc.gov.ua) – перевірка штрафів, замовлення водійського посвідчення, реєстрація транспортних засобів;

Єдиний державний реєстр боржників (erb.minjust.gov.ua) – перевірка інформації про борги, судові рішення щодо заборгованості;

Державний земельний кадастр (map.land.gov.ua) – інформація про земельні ділянки, їх власників та межі;

Електронний кабінет споживача (послуги від енергопостачальних компаній, водоканалів) – онлайн-оплата комунальних послуг, подача показників.

1.3 Роль цифрової грамотності у професійній діяльності

Сучасний ринок праці вимагає від співробітників володіння цифровими технологіями. Це не лише базові навички, а й уміння працювати з аналітичними інструментами, програмним забезпеченням та сучасними комунікаційними платформами. Цифрова грамотність сприяє впровадженню нових технологій у бізнес, оптимізації процесів та створенню інноваційних продуктів. За даними Організації економічного співробітництва та розвитку (ОЕСР), здатність адаптуватися до цифрових змін є вирішальним фактором конкурентоспроможності. У швидкозмінному світі цифрових технологій, володіння цими навичками дозволяє професіоналам швидко реагувати на нові виклики та використовувати нові можливості для зростання.

Перелік сервісів, які дозволяють зручно користуватися послугами у професійній діяльності:

Електронний кабінет платника податків (cabinet.tax.gov.ua) – надає можливість подавати податкову звітність, отримувати довідки та вести взаємодію з податковою службою;

Електронний лікарняний (eHealth) – система обліку медичних даних, яка дозволяє отримувати електронні рецепти, лікарняні та взаємодіяти з медичними закладами;

Єдиний державний реєстр юридичних осіб та ФОП (usr.minjust.gov.ua) – перевірка реєстраційної інформації про компанії та підприємців;

Опендатабот (opendatabot.ua) – моніторинг судових рішень, боргів, змін у реєстрах компаній;

Портал «Дія.Бізнес» (business.diia.gov.ua) – консультації, гранти, можливості для підприємців;

Система Prozorro.Продажі – електронні аукціони з продажу державного та

комунального майна;

Платформа електронних державних тендерів Prozorro – для участі в держзакупівлях;

Електронний кабінет пенсійного фонду (portal.pfu.gov.ua) – перегляд пенсійного стажу, подача заявок на перерахунок пенсії.

Контрольні запитання до теми

1. Яке комплексне визначення поняття «цифрова грамотність» дає Американська бібліотечна асоціація (ALA)?

2. Які три основні чинники зумовлюють актуальність вивчення цифрової грамотності в сучасних умовах?

3. Як пандемія COVID-19 вплинула на розвиток цифрової грамотності в освітньому процесі?

4. Чому цифрова грамотність є критично важливою для захисту від інформаційних воєн та дезінформації?

5. Які цифрові сервіси державних послуг в Україні надають спрощення бюрократичних процесів?

6. У чому полягає роль цифрової грамотності у повсякденній діяльності сучасної людини?

7. Як знання цифрових технологій впливає на конкурентоспроможність фахівця на ринку праці?

8. Як UNESCO обґрунтовує необхідність інтеграції цифрових навичок в освітню систему?

9. Які переваги дає використання онлайн-платформ для самоосвіти?

10. Як цифрова грамотність допомагає в оптимізації бізнес-процесів?

11. Чому вміння користуватися смартфонами та комп'ютерами є лише частиною цифрової грамотності?

ТЕМА 2. ХМАРНІ ТЕХНОЛОГІЇ ЗБЕРЕЖЕННЯ ДАНИХ

1. Поняття хмарних технологій

2. Класифікація хмарних сервісів

4. Класифікація моделей розгортання хмарних технологій

5. Практичні застосування хмарних технологій

2.1 Поняття хмарних технологій

У сучасному світі інформаційні технології стрімко розвиваються, змушуючи підприємства, організації та окремих користувачів шукати нові способи оптимізації управління даними. Одним з найбільш інноваційних підходів у цій сфері є хмарні

обчислення, які дозволяють користувачам отримувати віддалений доступ до обчислювальних ресурсів без необхідності утримувати власну інфраструктуру.

Хмарні технології надають доступ до потужних серверів, сховищ даних, програмного забезпечення та інших IT-ресурсів через Інтернет. Як наслідок, це дозволяє бізнесу зменшити витрати на обладнання та обслуговування, підвищити безпеку даних і швидко розширювати функціональність відповідно до поточних потреб. Крім того, хмарні рішення широко використовуються в освіті, охороні здоров'я, фінансах, промисловості та повсякденному житті, забезпечуючи користувачам легкий доступ до інформації.

Сьогодні хмарні сервіси пропонують широкий спектр можливостей, включаючи зберігання та обробку великих обсягів даних (big data), машинне навчання (AI та ML), віддалену роботу та співпрацю, а також розгортання програмних додатків.

У цій лекції буде розглянуто поняття хмарних технологій, їх основні особливості та переваги, доцільність їх використання в різних сферах діяльності та практичні аспекти застосування цих рішень у бізнесі та повсякденному житті.

Хмарні технології (англ. cloud computing) – це модель надання обчислювальних ресурсів, таких як сервери, сховища даних, мережеві компоненти, програмне забезпечення та аналітичні інструменти, через інтернет, з оплатою за фактичне використання. *[10]*

Хмарні обчислення – це модель, яка забезпечує повсюдний, зручний, мережевий доступ на вимогу до спільного пулу налаштовуваних обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків та сервісів), які можуть бути швидко надані та звільнені з мінімальними управлінськими зусиллями або взаємодією з провайдером послуг. *[11]*

Підсумовуючи, це модель, яка забезпечує повсюдний та зручний доступ на вимогу, використовуючи ресурси всесвітньої павутини. Дана модель є досить гнучкою, оскільки ресурси, які вона надає, можуть бути оперативно надані та звільнені без залучення провайдера послуг, а затрати на такі ресурси є мінімальними.

Це можна порівняти з офісним центром, наприклад коворкінгом, де можна орендувати місце для роботи за фактичним часом використання, якщо є потреба працювати локально, або працювати дистанційно безоплатно. Кожне робоче місце є ізольованим середовищем, із власними умовами та потребами використання.

Кінцевим результатом, користувач отримує умовний налаштований провайдером «майданчик» яким він може керувати, хоча він може розташовуватися в будь якому місці на сервері в центрі обробки даних.

Враховуючи зростаючий обсяг даних, хмарні рішення стають не просто трендом, а невід'ємною частиною сучасного суспільства.

Стрімкий розвиток цифрових технологій у сучасному світі збільшив потребу в ефективному управлінні інформаційними ресурсами. Такі сектори, як бізнес, освіта, охорона здоров'я та наука, активно впроваджують нові методи обробки, зберігання та передачі даних. У цьому контексті хмарні обчислення стали важливим інструментом забезпечення доступності, безпеки та гнучкості у використанні інформаційних ресурсів.

Однією з головних причин інтересу до хмарних технологій є їхня здатність оптимізувати витрати на IT-інфраструктуру. Віддалені ресурси можна використовувати на умовах оплати за фактом використання, а це означає, що компаніям не потрібно робити великі інвестиції в серверне обладнання та його обслуговування. Ця особливість важлива для малих і середніх підприємств, які можуть отримати доступ до потужних технологій без необхідності робити великі інвестиції.

Також, до переваг можна віднести те, що хмарні рішення пропонують гнучкість і масштабованість. Даний аспект неймовірно важливий в умовах нестабільної економічної ситуації та сезонних змін навантаження. Хмарні технології також використовуються для віддаленої роботи та глобальних проектів, оскільки вони забезпечують безперебійний доступ до даних з будь-якої точки світу.

Безпека та надійність також є невід’ємними елементами хмарних технологій. Сучасні хмарні провайдери пропонують багаторівневий захист даних, механізми резервного копіювання та аварійного відновлення, які значно знижують ризик

втрати даних через технічні збої чи кібератаки тощо.

Розвиток штучного інтелекту, великих даних (big data) та Інтернету речей (IoT) безпосередньо пов'язаний з хмарними обчисленнями. Завдяки хмарним платформам компанії та дослідники можуть аналізувати великі обсяги інформації, використовувати машинне навчання та створювати інноваційні рішення, не маючи у власності потужних обчислювальних ресурсів.

Хмарні технології також відіграють важливу роль в освітньому процесі. Зокрема, дистанційне навчання, інтерактивні курси та спільна робота над проєктами стали можливими з розвитком хмарних платформ. Навчальні заклади та корпоративні університети використовують хмарні сервіси для доступу до навчальних матеріалів, організації відеоконференцій та перевірки знань.

2.2 Класифікація хмарних сервісів

Хмарні сервіси поділяються на декілька основних категорій залежно від функціональності, яку вони пропонують. Вони дозволяють користувачам отримувати доступ до обчислювальних ресурсів без підтримки власної інфраструктури, що значно скорочує витрати і спрощує управління ресурсами.

Основними категоріями хмарних сервісів є [12] [13]:

Інфраструктура як сервіс (IaaS) – надає обчислювальну потужність та ресурси інфраструктури. Користувачі можуть використовувати віртуальні машини, сховища, балансувальники навантаження та інші ресурси інфраструктури за потребою. Це ідеальне рішення для компаній, які хочуть мати повний контроль над своїм середовищем, але не бажають інвестувати в фізичні сервери. Прикладами є Amazon EC2, Google Compute Engine, Microsoft Azure Virtual Machines;

Платформа як сервіс (PaaS) – надає середовище для розробки, тестування та розгортання додатків. Всі технічні аспекти автоматизовані, тому користувачам не потрібно встановлювати сервери або керувати інфраструктурою. Це значно пришвидшує процес розробки та зменшує витрати на підтримку. Прикладами є Google App Engine, Microsoft Azure App Services, Heroku тощо;

Програмне забезпечення як сервіс (SaaS) – це послуга, що надає доступ до готового до використання програмного забезпечення через Інтернет. Вона набуває все більшої популярності серед бізнесу та кінцевих користувачів, оскільки користувачі можуть використовувати програми без необхідності встановлювати, оновлювати чи підтримувати їх. Прикладами є Google Workspace (Docs, Sheets, Drive), Microsoft Office 365, Dropbox;

Функції як сервіс (FaaS) – це модель, яка дозволяє програмному коду запускатися у відповідь на події без необхідності керувати інфраструктурою. Цей підхід широко використовується в безсерверних архітектурах. Прикладами є AWS Lambda, Google Cloud Functions та Azure Functions.

Додатково можна це виділити наступні категорії:

Інтеграція як сервіс (iPaaS) – це набір інструментів і сервісів для інтеграції різних додатків, даних і систем, що працюють у хмарних і локальних середовищах [14]. Вона автоматизує процеси між різними платформами і додатками, забезпечуючи безперебійну взаємодію між ними. Такий підхід дозволяє компаніям знизити витрати на розробку інтеграційних рішень і спростити процеси обміну даними. Прикладами є Dell Boomi, MuleSoft, Microsoft Azure Logic Apps;

Ідентифікація та доступ як сервіс (IDaaS) – це рішення для управління ідентифікацією користувачів і доступом до корпоративних систем і хмарних додатків [15] [16]. Вона централізує управління користувачами і правами доступу, забезпечуючи зручність при збереженні функціональності, безпеки і функціональності. Цей тип послуг важливий для компаній з великою кількістю користувачів і систем, які потребують розширеного контролю доступу. Прикладами є Okta, OneLogin, Microsoft Entra ID (Azure Active Directory), Amazon IAM;

Хмарні сервіси обробки даних – це сервіси, які дозволяють обробляти, аналізувати та візуалізувати дані в хмарі. Вони використовуються для обробки великих обсягів інформації (великих даних), машинного навчання, штучного інтелекту та аналітики. Прикладами є Google BigQuery, Amazon Redshift, Microsoft Azure Synapse Analytics.

Усі сервіси володіють унікальними особливостями та сферою застосування,

проте, Національний інститут стандартів і технологій США (NIST) визначає п'ять основних характеристик хмарних сервісів:

1. **Самообслуговування на вимогу (On-demand self-service)** – користувач може самостійно виділити та керувати обчислювальними ресурсами (за необхідності автоматизувати цей процес) без комунікації з провайдером;
2. **Широкий доступ по мережі (Broad network access)** – ресурси мають бути доступні в мережі;
3. **Об'єднання ресурсів (Resource pooling)** – загальний пул ресурсів одночасно можуть використовувати декілька користувачів, мультиарендність;
4. **Швидке масштабування (Rapid elasticity) –** хмарна модель повинна вміти оперативно і за необхідності автоматично масштабуватися відповідно до навантаження;
5. **Вимірюваний сервіс (Measured service)** – відстеження та вимірювання використання хмарних послуг дозволяє розрахувати та стягнути плату за послугу;

2.3 Класифікація моделей розгортання хмарних технологій

Хмарні технології сьогодні можна поділити на декілька типів, враховуючи спосіб організації обчислювальних ресурсів для їхнього надання користувачам: публічні, приватні, гібридні, спільні, мультихмари.

Публічна хмара – це модель хмарних обчислень, в якій обчислювальні ресурси, такі як сервери та сховища, надаються сторонніми провайдерами через Інтернет і стають доступними широкому колу користувачів. [17] [18]

Ці ресурси є спільними і загальнодоступними, що знижує витрати і спрощує доступ до потужних обчислювальних можливостей.

Переваги публічної хмари [19]:

Економічність – користувачі платять лише за ті ресурси, які вони фактично використовують, тому їм не потрібно робити великі початкові інвестиції у власну інфраструктуру;

Масштабованість – ресурси можуть бути швидко збільшені або зменшені в міру зміни потреб бізнесу;

Доступність – доступ до ресурсів з будь-якої точки світу через Інтернет підвищує мобільність і гнучкість.

Недоліки публічної хмари [19]:

Безпека та конфіденційність – розміщення даних на сторонніх серверах може викликати занепокоєння щодо захисту конфіденційної інформації;

Обмежений контроль – складніше контролювати інфраструктуру та ресурси порівняно з приватними хмарними або локальними рішеннями.

Приклади провайдерів публічних хмар: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

Публічні хмари є оптимальним рішенням для багатьох організацій, які хочуть використовувати хмарні технології без значних капітальних витрат на інфраструктуру. Однак, перш ніж обрати цю модель хмарних обчислень, важливо ретельно оцінити бізнес-потреби та потенційні ризики, пов'язані з безпекою та управлінням даними.

Приватна хмара – це модель хмарних обчислень, в якій хмарна інфраструктура використовується лише однією організацією. Вона може бути розгорнута на власному обладнанні компанії або в сторонніх дата-центрах і забезпечує високий рівень безпеки та контролю над даними. [17] [18]

Переваги приватної хмари:

Підвищена безпека – хмарні ресурси не поділяються між кількома клієнтами, що зменшує ризики, пов'язані з доступом до конфіденційної інформації;

Кращий контроль – організації мають повний контроль над конфігурацією та управлінням своєю інфраструктурою, що дозволяє їм краще реагувати на конкретні бізнес-вимоги;

Індивідуальна оптимізація – ресурси можуть бути налаштовані відповідно до конкретних потреб, забезпечуючи оптимальну продуктивність та ефективність;

Недоліки приватної хмари:

Вищі витрати – можуть бути дорожчими за публічні хмари через

необхідність інвестувати в обладнання та його обслуговування;

Обмежена масштабованість – на відміну від публічних хмар, розширення ресурсів обмежене і може вимагати додаткових інвестицій;

Приклади приватної хмари: IBM Cloud Private, Facebook, SAP.

Гібридна хмара – це модель IT-інфраструктури, яка поєднує елементи приватних і публічних хмар та забезпечує інтеграцію між ними. Це дозволяє підприємствам ефективно керувати даними і додатками та використовувати переваги обох середовищ. [17] [18]

Переваги гібридної хмари:

Гнучкість – можливість обирати найбільш підходящу платформу для кожного робочого навантаження, забезпечуючи оптимальну продуктивність та відповідність вимогам бізнесу;

Масштабованість – легке масштабування ресурсів від змінних потреб, що дозволяє ефективно реагувати на бізнес-запити.

Економічна ефективність – оптимізація витрат шляхом стратегічного використання ресурсів публічної хмари для менш критичних навантажень, одночасно зберігаючи конфіденційні дані в приватній хмарі;

Безпека – забезпечення захисту даних шляхом зберігання конфіденційної інформації в приватній хмарі, з одночасним використанням публічної хмари для менш чутливих даних;

Недоліки гібридної хмари:

Складність інтеграції – об'єднання різних хмарних середовищ може вимагати значних зусиль для забезпечення їх безперебійної взаємодії та сумісності;

Управлінські виклики – необхідність керувати гібридною інфраструктурою може бути складною, вимагаючи додаткових ресурсів та спеціалізованих знань;

Потенційні проблеми з продуктивністю – залежно від конфігурації, можуть виникати затримки або інші проблеми з продуктивністю при передачі даних між приватною та публічною хмарами;

Приклади гібридної хмари: BMW Group, Volkswagen, Dell Technologies.

Спільна хмара – це модель хмарних обчислень, в якій обчислювальні ресурси використовуються спільно кількома організаціями, які мають спільні інтереси або спільні вимоги. [17] Ця модель може бути побудована для обслуговування певної галузі або спільноти користувачів з подібними потребами та вимогами.

Переваги спільної хмари:

Спільне використання ресурсів – організації можуть ділитися інфраструктурою та сервісами, що знижує витрати на розгортання та обслуговування окремих систем;

Спеціалізовані рішення – можливість налаштувати хмару відповідно до специфічних потреб галузі або спільноти, забезпечуючи відповідність нормативним вимогам та стандартам;

Покращена безпека – спільна хмара може бути розроблена з урахуванням специфічних вимог безпеки учасників, що забезпечує високий рівень захисту даних.

Недоліки спільної хмари:

Обмежена гнучкість – оскільки ресурси спільні, можливості для індивідуальної настройки можуть бути обмежені;

Залежність від інших учасників – проблеми або зміни в потребах інших організацій можуть впливати на загальну ефективність та доступність хмари;

Приклади спільних хмар: Microsoft Azure Government, Google Cloud for Healthcare, IBM Cloud for Financial Services, Amazon Web Services (AWS) GovCloud (US).

Мульти-хмара – це стратегія використання декількох хмарних сервісів від різних постачальників для розміщення додатків, даних та інших ресурсів. Такий підхід дозволяє уникати залежності від одного постачальника, підвищувати надійність та гнучкість інфраструктури, а також оптимізувати витрати.

Переваги мульти-хмари:

Підвищена надійність – розподіл ресурсів між кількома хмарами зменшує ризик відмови сервісів через проблеми у одного постачальника;

Оптимізація витрат – можливість обирати найбільш вигідні умови у різних

постачальників та адаптувати використання ресурсів відповідно до потреб;

Гнучкість та масштабованість – легке масштабування ресурсів та адаптація до змінних бізнес-вимог завдяки різноманіттю доступних хмарних сервісів;

Недоліки мульти-хмари:

Складність управління – необхідність керувати різними хмарними середовищами може вимагати додаткових ресурсів та спеціалізованих знань;

Проблеми з інтеграцією – забезпечення сумісності та інтеграції між різними хмарними платформами може бути складним;

Безпека та відповідність вимогам – управління безпекою та відповідність нормативним стандартам можуть бути ускладнені через використання кількох хмар;

Приклади мульти-хмар: Netflix, Airbus, Spotify.

2.4 Практичні застосування хмарних технологій

Хмарні технології широко використовуються в різних галузях завдяки своїй гнучкості, масштабованості та здатності знижувати витрати.

Хмарні сервіси зберігання даних (наприклад, Google Drive, Dropbox, Microsoft OneDrive) дозволяють користувачам і організаціям зберігати великі обсяги інформації без потреби в локальних серверах або фізичних носіях. Зокрема, для бізнесу можливість централізовано зберігати та обмінюватися даними підвищує ефективність роботи та зменшує ризик втрати важливої інформації.

Таким чином, у хмарі зручно зберігати:

- файли та документи (тексти, таблиці, презентації, PDF);
- фото, відео, музику, фільми;
- резервні копії даних з комп'ютерів, телефонів і серверів, які допомагають відновити інформацію в разі поломки пристрою;
- бази даних;
- проєкти та розробки.

Хмарні технології широко використовуються установами, що проводять

онлайн-курси та дистанційне навчання, а такі платформи, як Google Classroom, Microsoft Teams чи Moodle дозволяють створювати інтерактивні курси та проводити відеоконференції, отримувати доступ до навчальних матеріалів.

У сфері охорони здоров'я хмарні технології використовуються для зберігання медичних записів, обміну даними між лікарями і пацієнтами та організації дистанційної медичної допомоги. Це дозволяє пацієнтам отримувати медичну допомогу дистанційно, а лікарям – мати доступ до актуальних медичних даних.

Хмарні технології також застосовуються і в аграрному секторі. Збір та обробка даних про стан ґрунту, погодні умови та врожайність сільськогосподарських культур, а також автоматизація фермерських процесів стало можливим завдяки хмарним платформам. Наприклад, системи моніторингу фермерських господарств, такі як PrecisionHawk і AgroSmart, використовують хмару для обробки даних з дронів, датчиків та інших пристроїв.

Медіакомпанії та творці контенту використовують хмарні платформи для створення, обробки та доставки цифрових медіа, а за допомогою хмарних сервісів для редагування відео та аудіо, таких як Adobe Creative Cloud та Avid Media Composer компанії можуть співпрацювати над контентом у режимі реального часу, зберігати великі файли без потреби в потужних локальних серверах, а також ефективно відстежувати та контролювати процес від виробництва до доставки.

Хмарні технології допомагають компаніям автоматизувати та оптимізувати внутрішні логістичні процеси. Хмарна платформа дозволяє компаніям відстежувати відправлення в режимі реального часу, автоматизувати процеси складування та управління запасами, а також прогнозувати потреби в матеріалах. Це дозволяє значно скоротити витрати на логістику та ефективніше використовувати ресурси.

Також, є великий потенціал у сфері обліку та оподаткування з точки зору автоматизації процесів, простоти використання та покращення взаємодії з податковими органами. Хмарні системи дозволяють компаніям ефективно відстежувати доходи та витрати, створювати фінансові звіти та баланси без необхідності розгортання складних і дорогих локальних рішень. Хмарні платформи

дозволяють автоматично розраховувати податки та подавати податкову звітність в електронному вигляді. Це зменшує ризик помилок при підготовці та поданні податкової звітності, а також скорочує робочий час. Такі системи, як M.E.Doc, дозволяють інтегрувати податковий облік безпосередньо з податковими органами, що значно спрощує взаємодію з державними установами.

Контрольні запитання до теми

1. Що таке хмарні технології?
2. Які є основні характеристики хмарних обчислень?
3. У чому полягає різниця між моделями сервісу SaaS, PaaS та IaaS?
4. Які переваги та недоліки мають «Публічні хмари», «Приватні хмари», «Гібридна хмара» та «Спільна хмара»?
5. Які найбільш популярні хмарні сховища використовуються для повсякденних потреб та бізнес процесів?
6. Які ключові переваги хмарних технологій для бізнесу?
7. Які ризики безпеки пов'язані з використанням хмарних сервісів?
8. Як хмарні технології сприяють забезпеченню спільної роботи над документами в режимі реального часу?
9. Яким чином хмарні обчислення допомагають у професійній діяльності бухгалтера?
10. Які практичні приклади використання хмарних технологій у навчальному процесі можна навести?

ТЕМА 3. ОСНОВИ КІБЕРБЕЗПЕКИ

1. Поняття кібербезпеки.

2. Види кіберзагроз.

3. Запобігання кіберзагрозам.

Є два типи компаній: ті, які були зламані, і ті, які ще не знають, що їх зламали
Джон Чамберс, колишній генеральний директор Cisco

3.1 Поняття кібербезпеки

За останні кілька десятиліть інформаційні технології кардинально змінили спосіб ведення бізнесу, спілкування та обробку даних. Світову економіку формують люди, які спілкуються в різних часових поясах і отримують доступ до важливої інформації з будь-якої точки світу. Сучасне суспільство стає все більш залежним від цифрових технологій, що приносить з собою багато переваг, але також і нові виклики.

Одним із таких викликів є забезпечення кібербезпеки, тобто захисту інформаційних систем, мереж і даних від несанкціонованого доступу, пошкодження та крадіжки.

Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи й мережу від кібератак *[20]*

Кібербезпека – це комплекс заходів, спрямованих на захист інформації в комп'ютерних системах і мережах від несанкціонованого доступу, використання, розкриття, порушення цілісності, модифікації або знищення *[21]*

Кібербезпека – стан захищеності даних в електронному вигляді від їх несанкціонованого використання або кримінальних дій з цими даними, а також набір заходів для досягнення такого стану захищеності даних *[22]*

Підсумовуючи, це комплекс заходів, основною метою яких є забезпечення трьох основних частин:

конфіденційність – інформація буде доступна лише уповноваженим на це особам, запобігання несанкціонованому використанню даних;

цілісність – збереження достовірності та повноти даних, запобігання її фальсифікації;

доступність – забезпечення безперебійного доступу до ресурсів (протидія DoS, DDoS тощо);

Поняття захисту не обмежується лише цифровими формами інформації; інформаційний простір існував задовго до появи перших комп'ютерів. Водночас, загрози для інформації в цифровому просторі є найбільш безпосередніми та масштабними. Тому організаціям необхідно застосовувати сучасні підходи та заходи для захисту інформації [22].

Загальним терміном для захисту інформації в комп'ютерних технологіях є «кібербезпека». Дане поняття має початки формування у далекі 1960-1970-ті роки, час коли почали з'являтися перші комп'ютери та їх мережі. Історія становлення кібербезпеки як самостійної дисципліни є досить цікавою, тому варто звернути увагу на причини, які дали поштовх даній галузі.

Одним з перших вірусів був вірус «Creeper», який був створений у 1971 році

на комп'ютерах мережі Arpanet. Цей вірус був здатний ширитися мережею, хоч і був практично нешкідливим, оскільки відображав лише повідомлення «I'm a creeper, catch me if you can!» (переклад «Я привид, спіймай мене, якщо зможеш!»). Як наслідок, був розроблений перший антивірус Reaper для боротьби з цим вірусом [23].

У 1988 році аспірант Корнельського університету Роберт Морріс створив хробака «Morris Worm» і запустив його у вищезгадану мережу, щоб дослідити масштаби поширення цього шкідливого програмного забезпечення, проте експеримент вийшов з-під контролю та спричинив серйозні проблеми. Як наслідок, 6000 комп’ютерних вузлів із 60000 були заражені та уповільнили роботу багатьох наукових і військових установ США [24]. Це подія вважається першим кіберзлочином та надала поштовх до розвитку кібербезпеки, оскільки показала що навіть прості програми можуть нанести великої шкоди.

З початком XXI століття тема кібербезпеки набула нового значення, оскільки комп’ютери та їх мережі починають поширюватися по всьому світу. Кількість кіберзлочинів зростає, а їх способи стають все більш небезпечними та хитрими, і тепер жертвою може стати будь-хто – від простої людини, до державної організації.

Яскравими прикладами цієї епохи є такі кіберзлочини:

1. **Вірус «ILOVEYOU»** – шкідливе ПЗ, яке поширювалося через електронну пошту і при відкритті запускало шкідливий код, що перезаписував особисті файли, викрадав паролі, копіював себе та відправляв усім контактам, спричиняючи подальше зараження;
2. **Витік даних компанії Target –** методом фішингу було атаковано підрядника, що мав доступ до внутрішньої мережі та скомпрометовано 40 млн платіжник карток та викрадено 70 млн персональних даних;
3. **Хробак «WannaCry»** – програмне забезпечення-вимагач (ransomware) яке при приникненні на комп’ютер шифрувало файли користувачів із подальшим повідомленням викупу;
4. **Кібератака на SolarWinds –** атака на компанію, яка розробляє ПЗ для управління ІТ-інфрактруктурою, в якій було отримано доступ до вихідного коду ПЗ

Orion із доданням до нього бекдору SUNBURST, в результаті якого отримано доступ до мереж урядів, корпорацій та важливий організацій;

5. **Вірус «NotPetya» –** програмне забезпечення-вимагач (ransomware), проте хоч мав вигляд простого шифрувальника, але основною метою було знищення даних;

6. **Кібератака на «Київстар»** – потужна хакерська атака спрямована на ядро мережі оператора мобільного зв'язку, яке відповідало за обробку та маршрутизацію трафіку, яка спричинила збій та перебої у наданні послуг по всій країні;

Із зростанням популярності соціальних мереж (Facebook, Twitter/X тощо) і мобільних пристроїв зросли і складнощі забезпечення хорошого рівня кібербезпеки. Втрата доступу до облікового запису та поширення повідомлень із переказом коштів та посиланням для наступного зараження є чи найбільш частою проблемою сьогодення.

Хоч і кібератаки мають різноманітну природу, проте цілі та мотиви можна поділити на 3 категорії [25]:

1. **Кримінальні** – злочинно мотивовані, зловмисники прагнуть отримати фінансову вигоду, зокрема викрадення коштів чи даних;

2. **Політичні** – привернення уваги громадськості чи отримання переваги над конкурентами;

3. **Особисті** – особисто мотивована причина задля отримання вигоди.

3.2 Види кіберзагроз

Кіберзагрози можуть мати різну форму, проте розуміння основних видів є ключовим елементом для захисту особистої інформації, бізнесу тощо. Більшість кіберзагроз можна поділити на такі види [25]

Шкідливе ПЗ – ПЗ, основна мета якого є пошкодження чи порушення роботи системи: криптомайнери; інфокради; трояни; руткіти.

Програми-вимагачі – шкідливе ПЗ, яке блокує або шифрує дані, вимагаючи

плату за дешифрування.

DoS/DDoS атаки – атаки на відмову в обслуговуванні, оскільки перевантажують системи, роблячи їх недоступними для користувачів.

Фішинг – отримання доступу чи інформації шахрайським способом, маскуючись під надійне джерело.

MitM («Людина посередині») атаки – атака, в якій зловмисник перехоплює, змінює чи підробляє дані у інтернет з'єднанні.

- Перехоплення незашифрованих з'єднань (HTTP, Telnet);
- Створення фальшивих точок доступу Wi-Fi (Evil Twin);
- Підробка доменів (DNS-spoofing);
- Підміна MAC-адреси в локальній мережі (ARP-spoofing).

Безфайлові атаки – атака, процес якої є експлойт легітимних процесів ОС, її вбудованих інструментів (PowerShell, Registry) чи запущених в памяті процесів;

- **PowerShell Exploits** – виконання шкідливих команд через PowerShell без створення файлів;
- **WMI Attacks** – використання Windows Management Instrumentation для збору даних або виконання команд;
- **Memory Injection** – впровадження шкідливого коду безпосередньо в пам'ять процесу;
- **Registry-Based Malware** – зберігання шкідливого коду в реєстрі Windows для запуску під час завантаження ОС;

Zero-day вразливості – вразливості, в основі яких є невідомі чи невиправлені прогалини в ПЗ;

Особливу увагу варто приділити соціальній інженерії – методу маніпуляції людьми з метою отримання конфіденційної інформації із використанням методів телефонних дзвінків, фішингових листів чи психологійчних маніпуляцій створення відчуття терміновості. Цей метод є ефективним завдяки зловживанню людської довіри.

3.3 Запобігання кіберзагрозам

Ефективний захист від кібератак вимагає комплексного підходу, що включає впровадження надійних заходів технічної безпеки, навчання користувачів основам кібергігієни та регулярне оновлення програмного забезпечення. У цьому розділі розглядаються основні способи запобігання кіберзагрозам, які можуть допомогти мінімізувати ризик атаки та забезпечити безпеку цифрових даних.

Заходами технічної безпеки є технічні засоби, які вже є готовим комплексом рішень. До них належать:

- Мережеві екрани;
- Антивірусне програмне забезпечення;
- Системи резервного копіювання;
- VPN-технології;

Мережевий екран (firewall) – система, в основі якої закладено контроль та фільтрацію вхідного та вихідного мережевого трафіку відповідно до визначених правил безпеки. Це своєрідний бар'єр між внутрішньою та зовнішньою мережею, що запобігає несанкціонованому доступу.

Основні методи роботи є фільтрація пакетів (зокрема перевірка заголовків, типу IP-адреси, порту та протоколу), станова перевірка (аналіз поточного стану з'єднання для визначення безпечності трафіку), проксі (може діяти як посередник між пристроями та приховувати реальну IP-адресу пристрою), аналіз додатків (використання штучного інтелекту для виявлення загрози на програмному рівні).

Фаєрволи поділяються на декілька типів:

1. Мережеві – встановлюються на рівні маршрутизаторів або серверів для контролю всього трафіку в мережі;
2. Персональні – програмне забезпечення для індивідуальних пристроїв (Windows Defender, ZoneAlarm);
3. Хмарні – забезпечують захист від атак через віддалені сервери (Cloudflare, AWS Shield);

Антивірусне програмне забезпечення – це ПЗ, призначене для виявлення,

блокування та видалення шкідливого програмного забезпечення (вірусів, троянів, шпигунських програм, програм-вимагачів та інших типів загроз), які потрапляють на комп'ютери та в мережі.

Зазвичай вони використовують декілька методів для виявлення та нейтралізації шкідливих програм:

1. **Використання бази даних підписів** – здійснюється порівняння файлів на комп’ютері з відомими підписами шкідливих програм, збережених в цій базі даних, і, якщо файл збігається з одним із записів, програма класифікує його як шкідливий;

2. **Аналіз поведінки** – вивчає поведінку файлів або програм у реальному часі. Якщо вони проявляють підозрілі дії (наприклад, намагаються змінити системні файли), антивірус блокуватиме ці дії;

3. **Ізоляція –** запуск програми у ізольованому середовищі (пісочниці), для того щоб побачити, як вона буде поводитися, не дозволяючи їй впливати на основну систему;

4. **Емулювання** – програма може імітувати виконання шкідливого коду в контролюваному середовищі для вивчення його поведінки без ризику для системи;

Антивірусне ПЗ поділяється на декілька типів:

1. **Індивідуальні** – розроблені для захисту окремих користувачів або малих бізнесів. Зазвичай включають функції сканування файлів, захист в реальному часі, захист веб-браузера, а також боротьбу з програмами-вимагачами. Приклади: Norton AntiVirus, McAfee Antivirus тощо;

2. **Рішення для бізнесу** – орієнтовані на захист підприємств та організацій від більш складних загроз. Включають централізоване управління, можливості моніторингу та аналізу, а також захист на рівні мережі. Приклада: Sophos Endpoint Protection, Trend Micro OfficeScan, ESET Endpoint Security;

3. **Інтернет-безпека та комплексні рішення** – пропонують повний набір інструментів для захисту комп’ютера, включаючи антивірус, брандмауер, захист від фішингу, захист банківських операцій та блокування небезпечних сайтів. Приклади: Bitdefender Internet Security, Avast Premium Security;

Хоч і антивірусне ПЗ є базовим для захисту, проте недоліками є певні обмеження виявлення загроз, оскільки якщо про них нічого невідомо, то і виявити такі загрози дане ПЗ не зможе, та може використовувати значну кількість ресурсів пристрою, тим самим сповільняючи його.

VPN (Virtual Private Network), або віртуальна приватна мережа – технологія, яка дозволяє створювати захищене і зашифроване з'єднання між пристроєм та мережею Інтернет.

За допомогою VPN користувачі можуть маскувати свою справжню IP-адресу, шифрувати передану інформацію і підключатися до інтернет-ресурсів, як ніби вони перебувають в іншому місці або в іншій мережі.

VPN активно використовується для забезпечення анонімності та захисту даних під час роботи в Інтернеті, особливо при підключенні до публічних або ненадійних мереж, наприклад, Wi-Fi мережі в кафе чи аеропортах. Дана мережа у своїй основі працює на технології тунелювання – створення захищеного каналу зв’язку.

Кроки роботи VPN:

1. **Шифрування даних** – дані шифруються, і, навіть при перехоплені не зможуть бути прочитані;
2. **Тунелювання** – передача зашифрованих даних зашифрованим каналом;
3. **Зміна IP-адреси** – при отримані даних на сервер VPN здійснюється підміна IP-адреси на свою власну, унеможливлюючи віднайти початкову фізичну адресу;
4. **Дешифрування** – кінцевий пристрій розшифровує отриману інформацію;

Хоч і маючи суттєві переваги, також існують і недоліки. Зокрема, можу знижуватися швидкість мережевого з’єднання, особлива при використанні складних ключів і протоколів шифрування. Також, деякі сервіси можуть виявляти використання VPN та обмежувати доступ до своїх ресурсів.

Основними аспектами кібергігієни є розробка політик безпеки, навчання та

підвищення обізнаності співробітників і аудит та моніторинг систем.

Кожна організація повинна розробити внутрішні політики, що регламентують порядок роботи з інформаційними системами, правила використання паролів, процедури реагування на інциденти та правила доступу до конфіденційних даних. Такий підхід дозволяє мінімізувати ризики людського фактора.

Часто найбільшу загрозу становить людський фактор, такі як помилки співробітників чи їх необізнаність. Регулярне навчання з питань кібербезпеки, проведення тренінгів та симуляцій кібератак є важливими заходами, що допомагають формувати культуру безпеки всередині організації.

Проведення регулярних аудитів безпеки дозволяє виявити слабкі місця в системах та швидко усунути їх. Використання систем моніторингу допомагає не лише відслідковувати поточний стан безпеки, але й прогнозувати можливі загрози завдяки аналізу відхилень у мережевій активності.

Для особистої безпеки дуже важливо використовувати двохфакторну автентифікацію та створювати складні паролі. При створенню паролю слід дотримуватися таких рекомендацій:

- Мінімальна довжина пароля не менше 12-16 символів;
- Використання різних символів (великі, малі літери, цифри, спеціальні символи);
- Уникання очевидних паролів (123456, qwerty, admin);
- Створювати унікальні паролі для різних облікових записів;
- Регулярно змінювати пароль;

В умовах стрімкого розвитку технологій та збільшення обсягу даних, що циркулюють в інформаційному просторі, важливість кібербезпеки лише зростатиме. Саме тому питання захисту інформаційних систем має стати пріоритетом не лише для IT-фахівців, а й для кожного, хто користується сучасними технологіями у повсякденному житті.

Контрольні запитання до теми

1. Дайте визначення кібербезпеки та її основної мети.
2. Які основні типи шкідливого програмного забезпечення існують?
3. У чому полягає сутність фішингу як методу кіберзагрози?
4. Що таке DoS та DDoS-атаки і як вони впливають на роботу систем?
5. Опишіть механізм «соціальної інженерії» та чому вона вважається небезпечною.
6. Які існують види програм-вимагачів?
7. Назвіть основні кроки для запобігання кіберзагрозам на персональному рівні.
8. Яку роль відіграє брандмауер у захисті мережі?
9. Чому регулярне оновлення програмного забезпечення є критичним для безпеки?
10. Які переваги використання антивірусного програмного забезпечення?
11. Чому навчання персоналу є одним із найважливіших елементів кібербезпеки організації?
12. У чому полягає перевага двофакторної автентифікації (2FA)?
13. Що таке «цифровий слід» і як він може бути використаний проти користувача?
14. Як безпечно користуватися публічними мережами Wi-Fi?
15. Назвіть основні правила створення надійних паролів.
16. Що таке VPN і як він забезпечує анонімність та захист даних?

ТЕМА 4. ЗАХИСТ ВЛАСНИХ ДАНИХ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

1. ***Персональні дані: класифікація та цифрова ідентичність.***
2. ***Правові аспекти захисту даних.***
3. ***Цифровий слід.***
4. ***Конфіденційність та приватність.***
5. ***Алгоритм дій у разі витоку даних.***

У сучасному світі інформаційні технології стали невід’ємною складовою життя людини. Ми щоденно користуємося інтернетом, соціальними мережами, мобільними застосунками, електронними сервісами держави та бізнесу. У процесі цього використання постійно відбувається збирання, обробка та зберігання персональних даних.

Саме тому питання захисту власних даних в інформаційному просторі є надзвичайно актуальним і безпосередньо пов’язаним із правами людини, її безпекою та свободою.

4.1 Персональні дані: класифікація та цифрова ідентичність

У цифровій епосі дані стали «новою нафтою». Але для користувача це

передусім його цифрова ідентичність. Персональні дані – це не лише ПІБ чи паспортні дані. Їх поділяють на дві основні категорії:

1. Загальні персональні дані: ім'я; адреса; номер телефону; електронна пошта; дані про місцезнаходження; IP-адреса; файли cookies тощо.

2. Чутливі дані: етнічне походження; політичні чи релігійні переконання; членство у профспілках; генетичні та біометричні дані; інформація про стан здоров'я; кримінальні записи тощо.

Захист даних – це не просто встановлення пароля, це контроль за тим, хто, як і з якою метою використовує інформацію про вас.

4.2 Правові аспекти захисту даних

Україна інтегрується в європейський цифровий простір, тому захист даних регулюється не лише національним законодавством, а й міжнародними стандартами:

Закон України «Про захист персональних даних» – визначає правила збору та обробки даних державними та приватними структурами;

GDPR (General Data Protection Regulation) – загальний регламент про захист даних ЄС.

Навіть якщо ви живете в Україні, GDPR захищає вас, якщо ви користуєтеся послугами європейських компаній (наприклад, Booking чи Ryanair). Він вводить «право на забуття» (можливість вимагати видалення своїх даних) та «право на портативність» (можливість забрати свої дані з одного сервісу в інший).

4.3 Цифровий слід

Кожен дія користувача в мережі залишає відбиток (слід). Його можна поділити на **активний** та **пасивний**.

Активний цифровий слід – це дані, які користувач передає в мережу свідомо та добровільно. Наприклад:

Соціальна взаємодія: пости, фотографії, коментарі, вподобайки та репости. Навіть видалений пост може залишитися в кеші пошукових систем або на серверах платформи;

Реєстрації та форми: створення облікових записів, підписка на розсилки, заповнення анкет для отримання знижок або участі в опитуваннях;

Професійна активність: публікація резюме на сайтах пошуку роботи, оновлення профілю в LinkedIn, участь у галузевих форумах;

Відгуки та транзакції: оцінювання товарів у маркетплейсах, публічні скарги на сервіси, підтвердження замовлень через електронну пошту.

Пасивний цифровий слід – це інформація, яка збирається автоматично та часто непомітно для користувача в процесі його взаємодії з веб-ресурсами. До прикладів можна віднести:

Технічні ідентифікатори: IP-адреса тип пристрою, операційна система та версія браузера;

Cookies: невеликі фрагменти даних, які сайти зберігають на вашому пристрої. Вони дозволяють сайтам «впізнавати» вас (наприклад для тощо щоб пам'ятати товари у кошику), але також відстежувати ваші переходи між різними ресурсами тощо;

Цифровий відбиток браузера (Fingerprinting): більш складна технологія збору даних про унікальні налаштування вашого браузера (встановлені шрифти, часовий пояс, роздільна здатність екрана тощо). Це дозволяє ідентифікувати особу навіть без використання cookies;

Геолокація: пошукові системи та додатки фіксують маршрути переміщення, якщо на пристрої увімкнено GPS або активний пошук мереж Wi-Fi;

Цифровий слід має властивість накопичуватися роками, формуючи так звану **цифрову ідентичність**, яка може суттєво відрізнятися від реальної людини. На основі цих даних алгоритми створюють психологічний профіль особи, який використовується для таргетованої реклами, маніпуляції вибором або навіть оцінки кредитоспроможності банками.

Найбільш розповсюдженими прикладами можуть бути:

1. **Алгоритмічне профілювання –** на основі пасивного сліду алгоритми популярних сервісів (наприклад YouTube, Facebook, Google) підбирають контент, який може «подобатися». Це обмежує доступ до альтернативних точок зору та формує викривлену картину світу;

2. **Динамічне ціноутворення** – деякі сервіси (авіакомпанії, готелі тощо) можуть змінювати ціну на послуги залежно від вашого цифрового сліду, як-от типу пристрою (користувачам дорожчих смартфонів можуть показувати вищі ціни) або історії пошукових запитів;

3. **Перевірка репутації –** сучасні роботодавці, банки та візові центри часто аналізують активний цифровий слід кандидата. Необережний коментар або фото 10-річної давності можуть стати причиною відмови;

4. **Тіньові профілі –** великі тех-гіганти збирають дані навіть про тих людей, які не зареєстровані в їхніх мережах, використовуючи інформацію з телефонних книг їхніх знайомих та трекери на сторонніх сайтах (наприклад застосунок GetContact, інші месенджери тощт).

4.4 Конфіденційність та приватність

Соціальні мережі за замовчуванням налаштовані на максимальну відкритість. Для захисту приватності необхідно:

- Закрити профіль від незнайомців, обмежити можливість позначати вас на фото без підтвердження.
- Перед завантаженням фото в мережу варто видаляти метадані, щоб не розкривати точну геолокацію вашого дому чи офісу.
- Використовуйте сервіси з наскрізним шифруванням (End-to-End Encryption).

1. Месенджер *Signal* вважається золотим стандартом приватності;
2. Месенджер *Telegram* має наскрізне шифрування лише у «секретних чатах», звичайні чати зберігаються на серверах компанії;

Смартфон перестав бути просто засобом зв'язку. Завдяки безперервному

телеметричному зв’язку, він акумулює дані, які виходять за межі усвідомленого вибору користувача. Тобто, у вашій кишені знаходиться об'єкт, який ідентифікує вашу особистість глибше та детальніше, ніж будь-хто інший. Тому, необхідно дотримуватися наступних рекомендацій, щоб знизити ризики втрати приватності:

Дозволи додатків – регулярно перевіряйте, до чого мають доступ ваші програми. Чи справді ліхтарику чи калькулятору потрібен доступ до контактів та мікрофона? Якщо ні – вимикайте.

Захист браузера:

1. Використовуйте режим "incognito" не для анонімності (оскільки в більшості він її не дає), а для того, щоб не зберігати історію на пристрої;
2. Встановіть розширення для блокування трекерів;
3. Використовуйте приватні пошукові системи (наприклад DuckDuckGo);

Найбільшою вразливістю є використання однакових паролів для різних сервісів. Менеджери паролів (такі як Bitwarden, 1Password чи KeePass) – це цифрові сейфи, що дозволяють генерувати унікальні та складні комбінації для кожного ресурсу. У такому разі вам необхідно пам'ятати лише один «майстер-пароль».

Проте з розвитком технологій навіть використання менеджерів паролів створює певні ризики, адже компрометація «майстер-пароля» відкриває доступ до всіх збережених даних. Для розв'язання цієї проблеми було впроваджено багатофакторну автентифікацію (MFA). Це критичний рівень захисту: навіть якщо зловмисник дізнається ваш пароль, він не зможе увійти в систему без підтвердження через другий фактор. Другим фактором може бути:

SMS-код – найменш безпечні (через ризик викрадення SIM-карти, перехоплення трафіку мережі тощо);

Додатки-автентифікатори – генерують тимчасові коди локально на пристрої, що значно надійніше (наприклад, Microsoft Authenticator або Google Authenticator);

Апаратні ключі – фізичні USB-пристрої, що забезпечують найвищий рівень захисту.

4.5 Алгоритм дій у разі витоку даних

Навіть за умови ідеальної цифрової гігієни, дані можуть опинитися у відкритому доступі через злам великих корпорацій, банків або державних реєстрів. У таких випадках швидкість вашої реакції визначає обсяг можливих збитків.

Етап 1. Моніторинг та ідентифікація витоку

Крім сервісу «**Have I Been Pwned»**, варто використовувати додаткові інструменти моніторингу:

Google One / Password Checkup – вбудовані інструменти Google, які сповіщають, якщо ваші паролі були знайдені в базах даних, які було викрадено;

Firefox Monitor – аналогічний сервіс від Mozilla, який надає детальні звіти про те, які саме дані (телефон, адреса, пароль) стали публічними;

Етап 2. Негайне технічне реагування

Якщо факт витоку підтверджено або ви помітили підозрілу активність, необхідно виконати наступні дії:

1. **Завершення всіх сеансів**. У налаштуваннях безпеки (Google, Facebook, Telegram тощо) оберіть функцію «Завершити всі активні сеанси». Це завершить всі активні сеанси та вилогінить зловмисника з вашого облікового запису, якщо він уже встиг увійти;

2. **Відкликання доступів сторонніх додатків**. Перевірте список сайтів та програм, яким ви надавали доступ до свого профілю через кнопки «Увійти за допомогою Google/Facebook». Видаліть усі підозрілі або застарілі дозволи.

3. **Зміна паролів за методом «доміно».** Починайте з основної електронної пошти, до якої прив'язані всі інші сервіси. Використовуйте тільки унікальні комбінації, згенеровані менеджером паролів.

Етап 3. Фінансова безпека (Критично для бухгалтерів та фінансистів)

Якщо витік стосується банківських даних або сервісів, де прив’язана платіжна картка:

1. **Тимчасове блокування карток.** Через мобільний банкінг заблокуйте картки або встановіть нульовий ліміт на операції в інтернеті;

2. **Перевипуск картки.** Якщо номер картки, термін дії та CVV-код могли потрапити до зловмисників, блокування недостатньо – необхідний повний перевипуск фізичної чи віртуальної картки;

3. **Моніторинг виписок.** Упродовж наступних 3-6 місяців уважно перевіряйте історію транзакцій на предмет дрібних списань (часто зловмисники «тестують» доступ малими сумами).

Етап 4. Звернення до правоохоронних органів та правовий захист

Злам облікового запису або викрадення персональних даних – це кримінальний злочин. Необхідно виконати дії за таким алгоритмом:

1. **Збір доказів.** Зробіть знімки екрану підозрілих повідомлень, сповіщень про вхід з невідомих IP-адрес, листів про зміну пароля, які ви не ініціювали. Збережіть логи (якщо сервіс їх надає);

2. **Подання заяви до Кіберполіції України.** Перейдіть на офіційний сайт cyberpolice.gov.ua та скористайтеся формою зворотного зв'язку для подання електронної заяви про злочин. У заяві детально опишіть: коли було виявлено злам, які дані могли бути викрадені, та чи було завдано матеріальної шкоди;

3. **Повідомлення Уповноваженого ВРУ з прав людини.** Якщо витік стався з вини компанії (наприклад, через недбале зберігання даних банком чи інтернет-магазином), ви можете подати скаргу до Секретаріату Уповноваженого, оскільки це порушує ваші конституційні права на приватність;

4. **Використання прав GDPR (для сервісів ЄС).** Ви маєте право вимагати від компанії офіційного пояснення причин витоку та інформації про те, які саме заходи були вжиті для захисту ваших даних надалі.

Етап 5. Репутаційне відновлення

- **Публічне сповіщення.** Якщо зловмисники отримали доступ до вашої електронної пошти або соцмереж, опублікуйте інформацію через друзів, родичів про даний злом та попередження про можливість інших зломів, вимагання коштів чи інших протиправних дій;
- **Професійна комунікація.** Якщо ви працюєте з клієнтськими даними (як бухгалтер чи аудитор), ви зобов'язані повідомити клієнтів про можливий

інцидент безпеки, щоб вони могли вжити власних заходів захисту.

Контрольні запитання до теми

1. *Як можна класифікувати дані? Наведіть приклади до кожного класу.*
2. *Як персональна інформація перетворюється на актив для бізнесу?*
3. *Як європейський регламент GDPR може захищати громадянина України?*
4. *У чому полягає різниця між «правом на забуття» та «правом на портативність» даних?*
5. *Чи може видалення допису в соцмережі повністю видалити ваш активний цифровий слід?*
6. *Які технічні ідентифікатори збираються автоматично, коли ви просто переглядаєте веб-сторінку?*
7. *Як технологічні гіганти можуть збирати дані про особу, яка не реєструється в соціальних мережах?*
8. *Яку небезпеку становлять метадані цифрових знімків, завантажених у мережу?*
9. *Чому доступ до мікрофона чи контактів для додатків типу «ліхтарик» є індикатором загрози приватності?*
10. *Які переваги та ризики використання менеджерів паролів (Bitwarden, KeePass тощо)?*
11. *Чому SMS-код вважається найменш надійним фактором у системі MFA порівняно з апаратними ключами?*
12. *Опишіть правильну послідовність зміни паролів у разі підтвердження витоку даних.*
13. *Куди саме і в якій формі потрібно звертатися в Україні, якщо ви стали жертвою кіберзлочину або несанкціонованого зламу облікового запису?*

ТЕМА 5. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОБЛІКУ І ОПОДАТКУВАННІ

1. ***Автоматизація системи бухгалтерського обліку***
2. ***Електронний документообіг***
3. ***Big Data та штучний інтелект у податковому обліку***
4. ***Блокчейн в обліку та оподаткуванні***
5. ***Стан сучасних інформаційних технологій в Україні***

Сучасні інформаційні технології відіграють важливу роль у бухгалтерському та податковому обліку, автоматизуючи процеси, підвищуючи ефективність та зменшуючи ризик помилок. Використання інформаційних систем не лише спрощує

ведення обліку, але й полегшує взаємодію між компаніями та податковими органами.

Розвиток цифрової економіки створив потребу у швидкій та ефективній обробці великих обсягів фінансових даних, а новітні інформаційні технології знайшли застосування в бухгалтерському обліку та оподаткуванні.

Крім того, глобалізація бізнес-процесів вимагає інтеграції різних облікових систем, що робить використання цифрових технологій незамінним інструментом для компаній будь-якого розміру.

Особливу увагу буде приділено автоматизованим системам бухгалтерського обліку, хмарним технологіям, електронному документообігу, штучному інтелекту, технології блокчейн та автоматизації податкового адміністрування.

5.1 Автоматизація системи бухгалтерського обліку

Автоматизація бухгалтерії – процес делегування частини функцій працівника бухгалтерії комп'ютерним програмам. Автоматизація бухгалтерського обліку стала можливою завдяки впровадженню спеціалізованого програмного забезпечення, яке не тільки спрощує фінансовий облік, але й підвищує його точність та ефективність.

Сюди можна віднести:

- обчислення податків, зборів, підсумкових сум;
- створення вибірок та зведень звітів;
- структурувати довідники та журнали;
- заповнювати накладні, реквізити, рахунки тощо;
- швидко обробляти велику кількість даних;
- формування діаграм для їх подальшого аналізу;
- обмінюватися даними між структурами чи підрозділами;
- своєчасне дотримання законодавчого регулювання та податкового законодавства.

Також, із використанням хмарних технологій з'явилася можливість вести облік та оподаткування дистанційно, без необхідності встановлення програмного

забезпечення на локальний пристрій. До основних переваг таких систем можна віднести:

- доступ з будь-якої точки світу;
- зменшення витрат на утримання IT-інфраструктури;
- своєчасне автоматичне оновлення та підтримка;
- більш вищий рівень захисту даних;

Найпоширенішими системами є SAP ERP, Xero, QuickBooks, FreshBooks, Microsoft Dynamics 365, Oracle NetSuite, Odoo, FinExpert, IT-Enterprise.

5.2 Електронний документообіг

Не менш важливим аспектом у бухгалтерському обліку є документообіг – рух первинних документів від моменту їх створення чи одержання до моменту передачі їх в архів. З розвитком технологій, електронний документообіг все більше витісняє традиційну модель, тим самим зменшуючи витрати на утримання паперової документації та прискорює процес обробки інформації.

Основними елементами електронного документообігу є:

накладання електронного підпису – забезпечення юридичної сили документів;

системи подання електронної звітності – подання звітності до податкових органів;

документообіг захищеними каналами зв'язку – забезпечення конфіденційності.

Щоб забезпечити юридичну силу документа необхідно накласти електронний підпис. Для того щоб краще зрозуміти що це таке, наведемо визначення із декількох джерел.

Електронний підпис – це електронні дані, які забезпечують цілісність документів та ідентифікують особу. *[26]*

Електро́нний цифрови́й пі́дпис *(ЕЦП)* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. [27]

Електронний підпис *(ЕЦП)* – це цифровий засіб підтвердження автентичності та цілісності електронних документів. Він дозволяє особі або організації підписувати електронні документи так, що будь-яка зміна в них буде помітна, і відтак, гарантує їхню недоторканість. *[28]*

На початках було поширене лише поняття електронного цифрового підпису (ЕЦП). Сфери застосування були різними, наприклад, бізнесові транзакції, електронна пошта, онлайн-банкінг, державні послуги, контракти тощо.

До переваг використання ЕЦП можна віднести: забезпечення автентичності; забезпечення цілісності; ефективність.

Проте має і свої недолік: складність налаштування; при викраденні ключа можливість несанкціонованого доступу; простота підробки; правові складнощі з його використанням відповідно до законодавства в різних країнах.

Проте із введенням у дію Закону України «Про електронні довірчі послуги» воно почало втрачати свою актуальність. [29]

Удосконалений електронний підпис (УЕП) – тип електронного підпису, що замінив старий варіант ЕЦП та є найпоширенішим варіантом. В його основі лежать процеси криптографічного перетворення даних. Важливою особливістю УЕП є можливість використання підпису, сертифікат якого зберігається на внутрішньому чи зовнішньому носії. [30]. Саме такого типу підписи використовуються в офіційних додатках, наприклад «Дія».

Кваліфікований електронний підпис (КЕП) – це аналог власноручного підпису, юридична сила якого підтверджена Законом України «Про електронний документообіг та електронні документи». З технічного погляду це електронні дані сформовані із вмісту документу, ключ підпису та часова позначка, які утворюють контейнер (архів чи окремий файл).

Цей підпис повинен зберігатися на відповідному захищеному апаратно-програмному носії, своєрідної «флешки», на якому не може зберігатися нічого крім цього ключа.

Також, із особливостей є використання кваліфікованого сертифікату, який може бути наданим надавачем довірчих послуг.

Як отримати ключ електронного підпису? На веб-ресурсі центрального засвідчувального органу (ЦЗО) надано перелік кваліфікованих надавачів ключів КЕП. Законодавство визначає єдиний для всіх надавачів послуг перелік документів для отримання ключа КЕП:

Для фізичних осіб та ФОП

- Заява на реєстрацію;
- Документ, що посвідчує особу;
- Ідентифікаційний код платника податків.

Для юридичних осіб

- Заява на реєстрацію;
- Документ, що посвідчує особу;
- Виписка з ЄДР;
- Ідентифікаційний код платника податків;
- Оригінал чи засвідчені копії документів, що підтверджують належність підписанта до юридичної особи та його повноваження.

Виданий сертифікат буде дійсний протягом 2 років, що убезпечує власника від компрометації ключа.

Найпоширенішими системами для ведення документообігу та звітності є M.E.Doc, СОТА, ПТАХ, Вчасно, FlyDoc, Fredo.

5.3 Big Data та штучний інтелект у податковому обліку

Із зростанням обсягу даних виникла проблема у ефективному методі їх опрацювання, яке зберегло якість та не дуже сповільнювало корпоративні процеси. Використання штучного інтелекту та машинного навчання може подолати дану проблему. Дані технології, зокрема, використовують для:

1. Аналізу ризиків та прогнозування (податкових надходжень, витрат);
2. Виявлення шахрайства (ухилення від сплати податків тощо);
3. Оптимізація податкового навантаження підприємства.

Зокрема, в Україні активно впроваджується система моніторингу податкових

ризиків – СМ КОР. Це новий механізм, який запроваджений Податковим кодексом України, для автоматичного аналізу податкових накладних на наявність ризиків задля підвищення ефективності боротьби з ухиленням від оподаткування. [31]

Також, штучний інтелект може використовуватися для автоматичного аналізу податкових декларацій, виявлення аномалій у фінансових звітах тощо. Наприклад, податкова служба у США (IRS) активно використовую таку технологію для аналізу податкових декларацій і виявлення схем ухилення від сплати податків, а у ЄС застосовуються алгоритми машинного навчання для аналізу транзакцій підприємств відповідно вимогам податкового законодавства.

На додачу, яскравим прикладом є ініціатива уряду Великої Британії – Making Tax DIgita (MTD), яка спрямована на цифровізацію податкової системи. Основними цілями даної системи є автоматизація та зменшення витрат на паперову документацію, підвищення точності податкових розрахунків, спрощення подання звітів та мінімізація помилок. Дана система вже має інтеграцію із такими сервісами, як QuickBooks, Xero, Sage Accounting, FreeAgent, ZohoBooks.

5.4 Стан сучасних інформаційних технологій в Україні

На початку 2000-х Україна активно впроваджувала інформаційні технології (ІТ) в різні сфери. Однак, через відсутність власного виробництва сучасних комп'ютерних систем, країна стала споживачем застарілих іноземних моделей обчислювальної техніки. [32] Це був період переходу до інформаційного суспільства, який передбачав розвиток інформаційної індустрії, пов'язаної з виробництвом технічних засобів і методів обробки інформації.

Протягом наступного десятиліття ІТ-індустрія України зазнала значного розвитку і стала важливою складовою економіки: зросла кількість ІТ-компаній та збільшився обсяг експортованих ІТ-послуг. Водночас зросло використання сучасних інформаційних технологій та систем в державі, що сприяло підвищенню адміністративної ефективності. [33]

Програмне забезпечення «1С:Бухгалтерія» – одна з найпоширеніших

бухгалтерських програм в Україні та країнах СНД. Протягом багатьох років вона є основним інструментом для ведення бухгалтерського обліку на малих і середніх підприємствах, оскільки вона забезпечувала простоту використання, доступність і широкий спектр функціональних можливостей.

У 2014 році Україна зіткнулася з серйозними політичними та економічними викликами, включаючи анексію Криму та початок військового конфлікту на сході країни. Це призвело до значних змін у податковій та фінансовій системах. Багато компаній відчули вплив на свої фінансові показники в цей період, що спонукало до розробки нових підходів до бухгалтерського обліку та звітності.

В травні 2017 року компанія «1С» була включена до санкційного списку України щодо російських компаній, що у свою чергу позначилося забороною щодо використання її продуктів в державних органах України. Для обходу заборони розробник продовжив роботу на українському ринку під торговельною маркою BAS.

Найпоширенішими системами бухгалтерського обліку в Україні є:

SAP Business One – це інтегроване програмне забезпечення для управління бізнесом (ERP-система), розроблене компанією SAP SE спеціально для малих та середніх підприємств. Ця система охоплює всі ключові аспекти управління підприємством, включаючи фінанси, продажі, закупівлі, складський облік, виробництво та управління персоналом [34];

QuickBooks – продукт компанії Intuit, який пропонує як десктоп, так і хмарні рішення для бухгалтерського обліку. Основні можливості включають управління продажами, витратами, виставлення рахунків, відстеження інвентарю та підготовку податкової звітності. Хмарна версія, QuickBooks Online, дозволяє користувачам отримувати доступ до даних з будь-якого місця та пристрою, забезпечуючи гнучкість та реальний час співпраці [35];

Xero – це хмарне бухгалтерське програмне забезпечення, розроблене для малого та середнього бізнесу. Воно пропонує функції для управління банківськими транзакціями, рахунками, витратами, проєктами та заробітною платою. Xero також інтегрується з понад 800 сторонніми додатками, що дозволяє розширити його

функціональність відповідно до потреб бізнесу. Користувачі відзначають інтуїтивно зрозумілий інтерфейс та потужні можливості звітності [36];

Zoho Books – є частиною екосистеми Zoho і пропонує комплексне рішення для бухгалтерського обліку. Серед основних можливостей це управління рахунками, витратами, проєктами, інвентарем та банківськими транзакціями. Zoho Books також підтримує автоматизацію робочих процесів та інтегрується з іншими додатками Zoho, такими як CRM та проєктний менеджмент, що забезпечує безшовну роботу між різними аспектами бізнесу [37];

IT-системи також допомагають інтегрувати різні аспекти бізнесу, забезпечуючи єдину платформу для бухгалтерського обліку, контролю запасів, розрахунку заробітної плати та інших функцій. Також, вони підвищують прозорість фінансових операцій, уможливлюють швидке прийняття рішень і дозволяють зберігати дані в захищених електронних форматах.

Контрольні запитання до теми

1. Які ключові переваги автоматизації бухгалтерського обліку для підприємства?
2. Чим відрізняються ERP-системи від спеціалізованих бухгалтерських програм?
3. Опишіть переваги впровадження електронного документообігу (ЕДО) у компанії.
4. Які програмні продукти для автоматизації обліку можна навести?
5. Як технологія Big Data використовується в податковому аудиті та контролі?
6. Що таке блокчейн і як він може гарантувати достовірність бухгалтерських записів?
7. Які переваги використання штучного інтелекту в процесі аналізу фінансової звітності?
8. Як цифровізація податкової служби впливає на взаємодію з бізнесом?
9. Який ефект від впровадження системи електронний чек?
10. Які виклики постають перед бухгалтерами у зв'язку зі швидким розвитком IT?
11. Як хмарні рішення змінюють підходи до ведення бухгалтерського обліку для малих підприємств?
12. Яка роль бізнес-аналітики у сучасному управлінському обліку?

ТЕМА 6. ЕЛЕКТРОННИЙ КАБІНЕТ ПЛАТНИКА ПОДАТКІВ

1. ***Структура кабінету платника податків***
2. ***Переваги використання кабінету платника податків***
3. ***Ризики роботи в кабінеті платника податків***

Електронний кабінет платника є захищеним, персоналізованим та багатофункціональним веб-сервісом ДПС України. Його впровадження стало революційним кроком у реформуванні податкової системи, перетворивши фіскальний орган на сервісну службу.

Правовий статус системи закріплений у Податковому кодексі України (стаття 42-1). Згідно із законом, ЕКП працює цілодобово, крім часу, необхідного для технічного обслуговування. Всі документи, отримані через кабінет, мають повну юридичну силу.

6.1 Структура кабінету платника податків

Як і більшість веб-ресурсів, електронний кабінет поділяється на відкриту (загальнодоступну частину) та приватну (особистий кабінет).

Відкрита частина доступна без ідентифікації користувача та дозволяє йому:

- переглядати податковий календар;
- користуватися реєстрами (наприклад дані про платників ПДВ, ЄП, неприбуткові організації тощо);
- завантажувати бланки податкової звітності
- отримати контакти підрозділів ДПС;
- переглядати новини ДПС.

Проте, більшість часу як користувач будете працювати із особистим кабінетом ресурсу. Навігаційну структуру наведено на рис. 1.

Отже, приватна частина кабінету складається із наступних розділів:

Новини – стрічка офіційних повідомлень ДПС, зміни в законодавстві та актуальні роз'яснення;

Опитування Пульс – сервіс зворотного зв'язку для оцінки якості обслуговування та повідомлення про труднощі у взаємодії з податковими органами;

ЕК для громадян – спеціалізований розділ для фізичних осіб (не підприємців), де можна переглянути нараховані податки на майно, подати декларацію про майновий стан та отримати довідку про доходи;

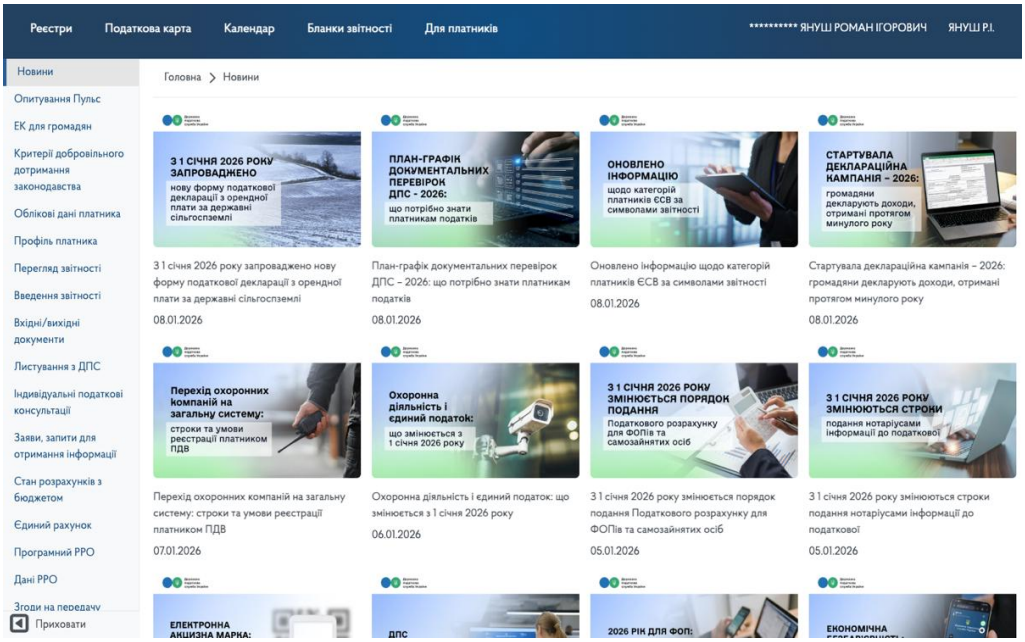

Рис. 1. Структура навігації приватної частини кабінету платника податків

Критерії добровільного дотримання законодавства – інформаційна система показників, за якими ДПС оцінює ризиковість платника та ймовірність включення його до плану перевірок.

Облікові дані платника – повна реєстраційна карта, в якій наведено:

1. **Ідентифікаційні дані –** наведено дані ПІБ, податковий номер;
2. **Реєстраційні дані –** наведено код та найменування ДПІ, дату взяття на облік платника податків чи його знаття, адресу, контактні дані, КВЕДи;
3. **Дані про реєстрацію платником ПДВ –** наведено дані про ІПН, дату та термін реєстрації, дату анулювання реєстрації та її причину та підставу;
4. **Дані про реєстрацію платником єдиного податку** – наведено дані про дату переходу на спрощену систему оподаткування, групу, ставку та можливу дату анулювання;
5. **Дані про реєстрацію платником ЄСВ** – наведено дані про дату взяття на облік чи зняття з обліку, реєстраційний номер платника єдиного внеску;
6. **Відомості про РРО** – наведено табличні дані про:

- Фіскальний номер РРО;

- Реєстраційний номер екземпляра РРО;
- Дата реєстрації РРО;
- Сфера застосування РРО;
- Номер останньої книги ОРО / журнала використання РРО;
- Дата реєстрації останньої книги ОРО / журнала використання РРО;
- Дата скасування реєстрації РРО.

7. **Інформація про книги ОРО** – наведено табличні дані про:

- Фіскальний номер книги ОРО;
- Ознака використання книги ОРО;
- Дата реєстрації книги ОРО;
- Дата скасування книги ОРО;
- Фіскальний номер останньої книги ОРО.

8. **Відомості про ПРРО** – наведено табличні дані про:

- Фіскальний номер ПРРО
- Локальний номер ПРРО
- Найменування ПРРО
- Статус ПРРО
- Дата реєстрації документа
- Адреса господарської одиниці, де використовується ПРРО.

9. **Відомості про об’єкти оподаткування** – наведено табличні дані про:

- Тип об'єкта оподаткування;
- Найменування об'єкта оподаткування;
- Ідентифікатор об’єкта оподаткування;
- Місцезнаходження об'єкта оподаткування
- Стан об'єкта оподаткування;;
- Вид права на об’єкт;
- Дата взяття на облік;
- Дата зняття з обліку;
- ДПІ обліку;

- Дата внесення змін;
- код КОАТУУ об’єкта оподаткування;
- Реєстраційний номер об’єкта оподаткування;
- Код КАТОТТГ.

10. **Інформація про неосновні місця обліку** – наведено табличні дані про:

- Код ДПІ за неосновним місцем обліку;
- Найменування ДПІ за неосновним місцем обліку.

11. **Дані про банківські рахунки у форматі IBAN** – наведено табличні дані про:

- МФО банку;
- Назва банку;
- Номер рахунку;
- Код банку;
- Валюта рахунку;
- Дата відкриття рахунку;
- Дата взяття на облік.

12. **Дані про укладені договори згідно з журналом договорів** – наведено табличні дані про:

- Податковий номер/серія та номер паспорта ЦСО;
- Назва/П.І.Б. ЦСО;
- Дата включення до Реєстру ЦСО РРО;
- Податковий номер/серія та номер паспорта власника РРО;
- Назва/П.І.Б. власника РРО;
- Номер договору;
- Період дії з;
- Період дії по;
- Дата анулювання договору;
- Модель (модифікація) РРО;
- Версія ПЗ РРО.

13. **Види діяльності** – наведено табличні дані про:

- Код ВЕД;
- Найменування ВЕД;
- Основна (логічне позначення основного виду діяльності).

14. **Дані з Реєстру платників, які використовують єдиний рахунок** – наведено табличні дані про:

- Дата включення платника до Реєстру;
- Дата виключення платника з Реєстру.

Перегляд звітності – реєстр усіх раніше поданих звітів незалежно від способу їх подання (паперово чи через стороннє ПЗ);

Введення звітності – основний робочий інструмент для створення, перевірки, підписання та відправки податкових декларацій, розрахунків та звітів;

Вхідні/вихідні документи – реєстр кореспонденції, де зберігаються отримані квитанції про прийняття звітів, відповіді на запити та офіційні повідомлення від ДПС;

Листування з ДПС – форма для надсилання листів довільної форми, заяв, скарг, консультацій, роз'яснень чи відповідь на лист ДПС;

Індивідуальні податкові консультації (ІПК) – розділ для подання запитів на отримання персональних роз'яснень щодо застосування норм податкового законодавства;

Заяви, запити для отримання інформації – функціонал для замовлення офіційних довідок (наприклад, про відсутність заборгованості чи довідки про доходи тощо);

Стан розрахунків з бюджетом – розділ із детальною інформацією по кожному податку: нарахування, фактичні сплати, наявність боргу, пені чи переплати в розрізі років;

Єдиний рахунок – розділ керування спецрахунком, з якого можна сплачувати більшість податків та зборів одним платежем (за винятком ПДВ та акцизу);

Програмний РРО – розділ із інструментарієм для реєстрації програмних кас, фіскалізації чеків та керування точками продажу;

Дані РРО – розділ інформація про всі зареєстровані за платником касові апарати (класичні та програмні) та історія переданих ними чеків (Z-звітів);

Згоди на передачу інформації – розділ налаштування дозволів на передачу особистих податкових даних третім особам;

Інформація про бізнес-партнера – розділ для перевірки контрагентів на предмет наявності податкового боргу;

Облік доходів і витрат для платників загальної системи оподаткування / Облік доходів і витрат для платників єдиного податку третьої групи платників ПДВ – розділ електронних книг обліку, де платник веде записи для подальшого автоматичного формування декларацій (доходи, витрати, амортизація);

Налаштування – розділ технічних налаштувань, оновлення інформації;

Допомога – розділ з інструкціями для користувача та відеоуроки;

Повідомити про помилку – форма для відправки знімків екрану з технічними збоями розробникам системи.

6.2 Переваги використання кабінету

Ключовою перевагою використання кабінету платника податків є автоматизація процесу, оскільки це не просто зручність, а комплексна трансформація взаємодії з державою, яка перетворює складне адміністрування на структурований цифровий процес.

Найбільш відчутна автоматизація відбувається у розділі «Введення звітності», зокрема:

Авто-заповнення реквізитів. При створенні будь-якого документа система автоматично підтягує дані з розділу «Облікові дані платника», включно із кодом ДПС, ПІБ / назви компанії та податкову адресу;

Контроль розрахунків. Кабінет містить вбудовані математичні алгоритми, та при введенні даних система автоматично розраховує підсумкові суми, податкове зобов'язання та перевіряє документ на відповідність логічним стандартам (наприклад, чи не перевищено ліміти для спрощеної системи);

Миттєвий статус. Розроблена система квитанцій. «Квитанція №1» генерується сервером автоматично при отриманні пакета даних, а «Квитанція №2» – після успішного автоматичного проходження контролю в базі даних ДПС;

Розділ «Стан розрахунків з бюджетом» є автоматизованою випискою, яка замінює ручні звірки з податковими інспекторами. Наприклад, синхронізація з казначейством – як тільки платіж проходить через банк, система автоматично відображає його в кабінеті, розподіляючи суми між основним платежем, пенею та штрафами. Також, напряму з картки особового рахунку можна згенерувати платіжний документ з уже вписаними актуальними реквізитами, що мінімізує ризик переказу коштів на неправильний рахунок.

На додачу, отримання офіційних документів стало безконтактним. Користувач підписує стандартну форму запиту (наприклад, витяг з реєстру платників ЄП), а система у відповідь автоматично формує електронний документ, що має таку ж юридичну силу, як і паперовий аналог. Це забезпечує значну економію часу та ресурсів.

Важливим є і те, що цей ресурс надає географічну свободу, оскільки використовувати його можна з будь-якої точки світу, де є доступ до мережі Інтернет. Це актуально для бізнесу, що працює за кордоном, або для релокованих компаній, оскільки ресурс доступний цілодобово, включ

аючи вихідні та святкові дні.

Інформація, яка відображається в картці платника в Кабінеті, є ідентичною тій, яку бачить податковий інспектор. Отже, цей ресурс можна вважати «єдиним джерелом істини».

Найбільш вагомим фактором на користь сервісу є його безкоштовність. ***Кабінет*** – це офіційний продукт, який не потребує ліцензій чи стороннього програмного забезпечення.

6.3 Ризики роботи в кабінеті

Використання цифрових сервісів у податковій сфері значно спрощує життя

бізнесу, проте воно супроводжується низкою ризиків, які варто враховувати для уникнення штрафів та правових проблем. Умовно їх можна поділити на технічні, безпекові, юридичні та суб'єктивні фактори.

Технічний ризик є найбільш непередбачуваним, оскільки він найменше залежить від дій платника. Головною проблемою тут залишається так званий «ефект останнього дня» – через надмірне навантаження на сервери ДПС у пікові періоди (наприклад, 20-го числа) система може працювати нестабільно або бути тимчасово недоступною. Крім того, графік платника може збігтися з регламентними технічними роботами на сервері. Якщо відкласти подання звіту на останню годину, існує висока ймовірність не встигнути через обслуговування системи або локальні проблеми, як-от зникнення інтернет-зв’язку чи вимкнення електроенергії.

Питання кібербезпеки тісно пов'язані зі збереженням КЕП (кваліфікованого електронного підпису). Оскільки підпис є ключем до всіх операцій, його компрометація (потрапляння файлу чи пароля до третіх осіб) дозволяє зловмисникам подавати фіктивну звітність або перереєструвати касові апарати від імені власника. Окрім прямої крадіжки даних, загрозу становить фішинг, коли шахраї створюють копії ресурсу. Також, не варто забувати про фізичну надійність носіїв: вихід флешки з ладу безпосередньо перед кінцевим терміном змушує витрачати дорогоцінний час на процедуру перевипуск ключа.

Юридичні та процедурні тонкощі часто стають причиною отримання штрафу через неуважність. Важливо пам'ятати, що отримання «Квитанції №1» про доставку документа ще не означає, що звіт успішно прийнято. Тільки «Квитанція №2» підтверджує відсутність помилок, тому ігнорування цього етапу може призвести до визнання звіту неподаним. Також, критичним є фактор часу. Юридично документ зафіксується лише тоді, коли він надійде на сервер ДПС, а будь-яка затримка в мережі може призвести до того, що звіт, надісланий о 23:59, отримає штамп часу 00:01 наступної доби, що вважатиметься порушенням термінів. Це стосується і автоматичних нарахувань, наприклад технічні збої в базах даних можуть спричинити появу неіснуючого боргу, про який платник дізнається вже під час

блокування рахунків, якщо не вчасно відслідковує стан розрахунків регулярно.

Зрештою, вагому роль відіграє людський фактор. Навіть в автоматизованому середовищі користувач може припуститися помилки, обравши неправильний код податку чи період. Хоча кошти зараховуються миттєво, процедура їх повернення або перенаправлення між рахунками є тривалою та складною.

Контрольні запитання до теми

1. Що таке «Електронний кабінет платника податків» та яка його мета?
2. Які сервіси доступні користувачу у відкритій (загальнодоступній) частині кабінету?
3. Як за допомогою кабінету можна перевірити стан розрахунків із бюджетом?
4. Які переваги надає листування з ДПС через електронний сервіс порівняно з паперовим?
5. Як скористатися сервісом «Податковий календар» в Електронному кабінеті?
6. Як функціонал «Критерії добровільного дотримання законодавства» допомагає бухгалтеру в податковому плануванні та превентивному захисті від перевірок?
7. Які юридичні наслідки для підприємства може мати компрометація КЕП, що використовується в Електронному кабінеті, та як алгоритм «Листування з ДПС» допомагає у вирішенні спірних питань?
8. У чому полягає різниця між Квитанцією №1 та Квитанцією №2?
9. Як за допомогою сервісу «Інформація про бізнес-партнера» бухгалтер може захистити підприємство від звинувачень у роботі з ризиковими контрагентами?
10. Які причини можуть призвести до ризику прострочення подання звітності навіть за умови її відправлення в останній день кінцевого терміну?

ТЕМА 7. ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ПОТРЕБ БУХГАЛТЕРА

1. ***Поняття штучного інтелекту***
2. ***Структура штучного інтелекту***
3. ***Чат-боти штучного інтелекту, моделі, платформи***
4. ***Переваги штучного інтелекту***
5. ***Недоліки штучного інтелекту***
6. ***Практичне використання штучного інтелекту***

Штучний інтелект безперечно, сьогодні ключова технологія, котра радикально перетворює звичні нам способи вирішення широкого спектру задач у різних галузях. Його вплив відчутний як у щоденних справах, так і у тонких професійних процесах, приводячи до збільшення продуктивності, пришвидшення

роботи та покращення її результатів. Зокрема, покращення вже можна побачити у медицині, фінансах, освітньому процесі, логістиці, промисловості тощо. Автоматизація, аналіз великих масивів інформації, розпізнавання зображень та мовлення, а також прийняття рішень на основі алгоритмів машинного навчання роблять ШІ незамінним інструментом сучасного світу.

Разом з тим, значні позитивні зміни, що їх приносить використання ШІ, супроводжуються низкою викликів, серед яких ключове місце посідають питання безпеки, етики та заміщення робочих місць. Значущим аспектом лишається його інтеграція в системи обліку та фінансів, зокрема, для автоматизації податкового обліку, керування бухгалтерськими процесами та прогнозування фінансових ризиків.

7.1 Поняття штучного інтелекту

Щоб більш точніше відобразити суть поняття, наведемо визначення штучного інтелекту із декількох джерел:

Штучний інтелект – розділ комп'ютерної лінгвістики й інформатики, який швидко розвивається і зосереджений на розробці інтелектуальних машин, здатних виконувати завдання, які зазвичай потребують людського інтелекту. *[38]*

Штучний інтелект – це технологія, яка дозволяє комп’ютерам і машинам імітувати людське навчання, розуміння, вирішення проблем, прийняття рішень, творчість і автономію. [39]

Підсумовуючи, це напрямок інформатики для створення інтелектуальних машин, здатних імітувати людські когнітивні здібності наприклад навчання, розуміння інформації, прийняття рішень, чи навіть творчість.

7.2 Структура штучного інтелекту

Структура штучного інтелекту визначається його класифікацією, цілями та підходами до реалізації. В основі функціонування ШІ лежать декілька ключових

складових:

- **Алгоритми та моделі.**

Машинне навчання (ML) – навчання на основі даних задля покращення результату без явного програмування;

Глибоке навчання (DL) – різновид машинного навчання, який використовує багаторівневі нейронні мережі;

Евристичні алгоритми – пошук оптимальних рішень у складних задачах;

- **Дані та сховища.**

Датасети – великі обсяги даних для навчання та тестування моделі;

Бази даних – місця зберігання даних для подальшої обробки;

Механізми збору даних – сенсори, API, веб-скрапінг тощо.

- **Обчислювальна інфраструктура.**

CPU, GPU, TPU;

Хмарні обчислення, мережеві ресурси.

- **Точки взаємодії (API тощо).**

Машинне навчання є одним із ключових елементів розвитку штучного інтелекту, оскільки воно дозволяє комп'ютерним системам самостійно розпізнавати закономірності в даних та підвищувати свою продуктивність.

Машинне навчання складається з таких концепцій:

1. **Тип машинного навчання**

Кероване навчання (Supervised Learning) – алгоритм навчається на основі розмічених даних, де кожному вхідному значенню відповідає правильний вихідний результат [40]. Приклади: розпізнавання облич, класифікація листів;

Некероване навчання (Unsupervised Learning) – алгоритм аналізує дані без явного надання правильних відповідей, знаходячи приховані закономірності. Приклади: кластеризація клієнтів у маркетингу, пошук аномалій у фінансових транзакціях;

Навчання з підкріпленням (Reinforcement Learning) – система навчається шляхом взаємодії із середовищем і отримання винагород за правильні дії [41]. Приклади: навчання роботів, стратегічні ігри;

2. **Алгоритми машинного навчання:**

- Лінійна регресія.
- Логістична регресія.
- Дерева рішень.
- Нейронні мережі.
- Метод опорних векторів (SVM).
- Кластеризація методом K-середніх тощо.

3. **Процес навчання моделі**

- Збір та підготовка даних.
- Вибір алгоритму.
- Навчання моделі.
- Оцінка якості моделі.
- Оптимізація та використання в реальних задачах.

Штучний інтелект можна поділити на декілька типів, зокрема [42]:

Слабкий штучний інтелект – тип штучного інтелекту, який обмежений певними завданнями та областями, алгоритми якого виконують конкретні завдання та не можуть здійснювати інтелектуальні дії поза цими межами. Приклади: гра в шахи, керування системами виробництва, рекомендації, рутинна справа;

Загальний штучний інтелект – тип штучного інтелекту, який має здатність розуміти, навчатися, адаптуватися до нових ситуацій та вирішувати різноманітні завдання, схожі на ті, які можуть виконувати люди. Приклади: чат-боти, віртуальні асистенти, навігація.

7.3 Чат-боти штучного інтелекту, моделі, платформи

1. **ChatGPT** – чат-бот від OpenAI для взаємодії, що може генерувати тексти, відповідати на запитання, підтримувати бесіду тощо;

2. **DALL·E** – модель від OpenAI, яка генерує зображення на основі текстових описів, що може бути використано для створення унікальних картин, ілюстрацій і навіть дизайнів, що відповідають заданим критеріям;

3. **Watson** – чат-бот від IBM для автоматизації служби підтримки клієнтів, надає аналітику і відповідає на питання;

4. **Google Assistant** – голосовий чат-бот, що допомагає з побутовими запитами, управлінням розумним будинком, пошуком інформації;

5. **Siri** – віртуальний помічник для пристроїв Apple, що виконує голосові команди;

6. **Alexa** – голосовий асистент від Amazon для управління пристроями в розумному домі, відповіді на запитання і запуск додатків;

7. **Replika** – чат-бот, створений для надання емоційної підтримки та розвитку соціальних навичок;

8. **Ada** – чат-бот для створення автоматизованих відповідей на запитання клієнтів, інтегрується з CRM-системами;

9. **Cleo** – особистий фінансовий помічник для управління коштами, створення бюджетів і отримання фінансових порад;

10. **Landbot** – візуальний чат-бот для автоматизації маркетингових кампаній, збору даних і комунікацій з клієнтами;

11. **SnatchBot** – чат-бот для автоматизації маркетингових стратегій, комунікацій і обробки запитів клієнтів;

12. **Runway ML** – платформа для генерації та редагування відео, а також створення зображень і анімацій за допомогою ШІ;

13. **Aiva Technologies** – платформа для створення музики в різних жанрах, допомагаючи музикантам і композиторам створювати нові твори;

14. **Writing AI** – генерує нові ідеї для написання коротких оповідань або романів, пропонуючи сюжети, персонажів і діалоги;

15. **GitHub Copilot** – помічник для програмістів, який допомагає писати код, надаючи пропозиції для автодоповнення, генерації функцій, і навіть цілих класів на основі коментарів та контексту.

7.4 Переваги штучного інтелекту

Штучний інтелект сприяє пришвидшенню та підвищенню ефективності виконання важких задач. Наприклад, у промисловості роботизовані комплекси здатні нарощувати обсяги виробництва, одночасно зменшуючи час простою. У розробці програмного забезпечення штучний інтелект допомагає автоматично виправляти помилки в програмному коді та надавати оптимальні рішення, що значно прискорює процес створення.

Банківські структури використовують штучний інтелект для автоматизованої обробки документів та перевірки фінансових операцій, що у свою чергу знижує навантаження на персонал і прискорює операційні процеси. Наприклад, у бухгалтерії програми, такі як Xero чи QuickBooks, самостійно обробляють рахунки-фактури та формують фінансові звіти.

Алгоритми штучного інтелекту зменшуються кількість помилок у фінансових звітностях, автоматично виявляючи невідповідності чи підозрілі транзакції. Наприклад, системи податкового моніторингу, що базуються на ШІ, допомагають знаходити помилки у поданих деклараціях та попереджають про можливі ризики неточної звітності.

Компанії, що спеціалізуються на Big Data, застосовують ШІ для аналізу колосальних масивів даних в режимі реального часу. Наприклад, у медичній сфері системи ШІ здатні швидко аналізувати історію хвороби пацієнтів та прогнозувати потенційні ризики. У фінансовому секторі алгоритми машинного навчання використовуються для аналізу ринку та прогнозування коливань вартості акцій.

ШІ-системи постійно вдосконалюються, навчаючись на основі отриманої інформації. Наприклад, чат-боти для клієнтської підтримки підвищують свою ефективність, аналізуючи попередні взаємодії з користувачами. У сфері обліку та оподаткування ШІ дозволяє автоматично аналізувати зміни у податковому законодавстві та надавати рекомендації щодо оптимізації рішень для підприємств.

7.4 Недоліки штучного інтелекту

ШІ потребує значних інвестицій на кожному кроці, від проектування до інтеграції. Для успішного та ефективного функціонування ШІ-систем необхідно не лише висококваліфіковані спеціалісти (інженери, вчені тощо), а й передове обладнання, спеціалізовані програмні продукти та інфраструктура. Навчання ШІ-моделей вимагає великих обсягів даних та обчислювальної потужності, що у свою чергу збільшує кінцеву вартість. Наприклад, розробка моделей, таких, як GPT-4 або DALL·E орієнтовно може коштувати від 10 млн доларів.

Штучний інтелект породжує чимало етичних та правових дилем, що стосуються недоторканності приватного життя, людських прав, упереджень та інших сфер. Зокрема, застосування ШІ для прийняття автоматизованих рішень, таких як оцінка платоспроможності або ідентифікація особистості, здатне спричинити непередбачувані результати через упередженість алгоритмів. Наприклад, у 2018 році компанія Amazon відмовилась від використання автоматизованої системи підбору кандидатів на роботу, оскільки алгоритм виявив упередженість проти жінок, оскільки навчався на історичних даних, де більшість програмістів були чоловіками.

Додатково, застосування технологій розпізнавання обличчя потенційно може порушити право на приватність і призвести до небажаного нагляду. У 2020 році в Китаї було запроваджено обов'язкові програми для використання цієї технології в публічних місцях, що спричинило занепокоєння щодо контролю та втручання в особисте життя громадян.

Штучний інтелект дуже чутливий до якості вхідних даних. Коли вхідні дані містять недоліки, зокрема помилки, упередження чи брак необхідних відомостей, це здатне призвести до хибних чи необ'єктивних наслідків. Зокрема, алгоритми машинного навчання залежні від того, наскільки добре вони навчені на репрезентативних даних. Наприклад, якщо модель штучного інтелекту, що розпізнає медичні зображення, навчається на даних низької якості або неповних (скажімо, на картинках, отриманих різними приладами або з технічними

дефектами), це здатне спричинити помилкові діагнози чи призначення лікування. Як наслідок, система, призначена для пошуку ракових утворень, може не ідентифікувати деякі різновиди пухлин через обмеженість представлених зображень.

ШІ може стати потужним інструментом у руках злочинців для кібератак, фінансових махінацій та інших протиправних дій. Так, застосування ШІ для підробки або зміни зображень та відеоматеріалів (глибинні підробки, deepfakes) веде до загрози спотворення фактів та використання довірливих відносин громадян.

Штучний інтелект здатен взяти на себе багато задач, звільнивши людей від певних обов'язків. Це може вплинути на багато професій, і в першу чергу – в промисловості, логістиці та сфері послуг. Наслідком може стати зменшення потреби у працівниках, що в свою чергу здатне викликати хвилювання у суспільстві та поглибити розрив у рівнях достатку.

Наприклад, розвиток технологій автономного транспорту зумовлює потенційне скорочення потреби у водіях різних категорій, включаючи вантажівки, таксі та автобуси. Експерти передбачають суттєве зменшення кількості робочих місць для водіїв, адже автономні машини з часом можуть замінити працю людей. За оцінками, автоматизація транспорту може призвести до втрати роботи мільйонами водіїв у найближчому майбутньому, що зумовлює необхідність адаптації та перекваліфікації працівників цієї сфери.

Додатково, впровадження автоматизованих систем на підприємствах, де переважають повторювані операції, може призвести до заміни людського ресурсу на виробничих лініях. Це потенційно може позначитися на скороченні кількості робочих місць у відповідних секторах економіки. Зокрема, у сфері автомобілебудування вже широко застосовуються роботи для складання транспортних засобів, що, у свою чергу, знижує потребу у ручній праці.

7.5 Практичне використання штучного інтелекту

Попри всі переваги і недоліки, все ж є користь у використанні ШІ в обліку та

оподаткуванні. Найпоширеніше використання:

Автоматизація ведення обліку – використання ШІ для розпізнавання та обробляння фінансових витрат (SAP, QuickBooks), прогнозування витрат та автоматична категоризація транзакцій (Xero, FreshBooks);

Податковий аудит та оптимізація – автоматичне заповнення податкових декларацій, аналіз можливих відрахувань (TurboTax, TaxSlayer), аналіз податкових ризиків та прогноз змін у податковому законодавстві (H&R Block);

Фінансова аналітика та прогнозування – аналіз бухгалтерських даних та фінансових показників (Microsoft Power BI, Tableau), автоматизація фінансового планування (Adaptive Insights);

Виявлення шахрайства та ризиків – аналіз транзакцій для виявлення підозрілих операцій (Kyriba, FICO Falcon Fraud Manager), автоматичний аудит фінансових даних для виявлення аномалій (MindBridge Ai Auditor);

Контрольні запитання до теми

1. Дайте визначення штучного інтелекту (ШІ) як галузі комп’ютерних наук.
2. Опишіть основні компоненти структури ШІ.
3. Які основні переваги використання ШІ у професійній діяльності бухгалтера?
4. Які недоліки та ризики використання ШІ існують у фінансовій сфері?
5. Як ШІ може допомогти в автоматизації розпізнавання первинних документів?
6. Опишіть роль ШІ в аналізі великих масивів даних для прогнозування фінансових показників.
7. Як чат-боти можуть використовуватися для консультацій клієнтів з питань оподаткування?
8. Які етичні виклики виникають при прийнятті рішень алгоритмами ШІ в обліку?
9. Як ШІ допомагає у виявленні аномалій та запобіганні фінансовому шахрайству?
10. Які навички повинен розвивати сучасний бухгалтер для ефективної роботи зі ШІ?
11. Як ШІ впливає на продуктивність праці в бухгалтерському відділі?

ТЕМА 8. КРИПТОВАЛЮТА ТА СМАРТ-КОНТРАКТИ В ОБЛІКУ

1. ***Технічна будова блокчейну для облікових процесів***
2. ***Криптовалюта як об'єкт обліку та управління***
3. ***Смарт-контракти: алгоритмізація та автоматичний облік***
4. ***Класифікація стандартів токенів в обліку***

5. ***Облік та оподаткування в умовах волатильності***
6. ***Цифрова безпека та Blockchain-аудит***

Поява цифрової економіки породила активи, які не мають фізичної форми та централізованого емітента, проте володіють ринковою вартістю. Для фахівця з обліку і оподаткування розуміння криптовалют та смарт-контрактів є критично важливим, оскільки ці інструменти трансформують традиційне уявлення про право власності, первинну документацію та автоматизацію договірних відносин.

Станом на 2026 рік інтеграція віртуальних активів у правове поле України вимагає від бухгалтера не лише знання проведень, а й розуміння технічної природи розподілених реєстрів.

8.1 Технічна будова блокчейну для облікових процесів

В основі всіх віртуальних активів лежить технологія блокчейн (Blockchain) – розподілений реєстр даних. Для обліку ця технологія приваблива насамперед своєю здатністю формувати середовище довіри без посередників

Кожна операція в блокчейні групується у блок, який підписується унікальним криптографічним кодом (хешем), а кожен наступний блок часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево. Така організація створює нерозривний ланцюг. Інформація про транзакції зазвичай надається відкритою, не зашифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку у наступний блок. З погляду аудиту це означає незмінність даних – будь-яка спроба змінити запис у минулому зруйнує весь ланцюг, що миттєво помітять усі учасники мережі. Таким чином, блокчейн виступає ідеальним основним реєстром де записи неможливо підробити, оскільки внесення змін в один з блоків вимагає відповідних змін в усіх блоках після нього, що зазвичай виявляється або дуже складно, або дуже коштовно. [43]

Важливим для бухгалтера є механізм консенсусу (наприклад, Proof-of-Stake). Це технічний протокол, який підтверджує, що транзакція є валідною. Саме в

момент підтвердження транзакції мережею актив вважається офіційно переданим, що є технічним тригером для визнання операції в обліку.

Основними перевагами використання даної технології в обліку та оподаткуванні:

- Прозорість – запис транзакцій у відкритий реєстр, унеможливлює підробку даних;
- Безпека – шифрування даних та розподіл між учасниками мережі;
- Автоматизація – самостійне податкове нарахування смарт-контрактами;
- Захист від помилок – автоматична перевірка;
- Спрощення аудиту – аудит незмінного реєстру фінансових операцій;

У деяких країнах блокчейн уже використовується для реєстрації податкових декларацій та ведення бухгалтерського обліку. Наприклад, Естонія впроваджує її для автоматизації податкових платежів (TaxChain).

Варто звернути увагу на бухгалтерську платформу «Acuity», яка базується на технології блокчейну та дозволяє підприємствам вести звітність без необхідності довіряти конкретному адміністраторові. Також, сервіс PwC використовує блокчейн для прискорення аудиторських перевірок, оскільки фінансові звіти автоматично оновлюються та є миттєвий доступ до незмінних даних.

Європейський Союз активно досліджує можливості впровадження технології блокчейн для вдосконалення системи податку на додану вартість (ПДВ), що спрямовано на спрощення процедур оподаткування та створення рівних умов для бізнесу. [44]

8.2 Криптовалюта як об'єкт обліку та управління

Криптовалюта – це цифровий актив, захищений криптографією, який використовується як засіб обміну або інвестиція. На відміну від фіатних грошей, доступ до криптоактивів регулюється через систему ключів.

Публічний ключ – це адреса у мережі, яку бухгалтер надає контрагентам

для отримання оплати.

Приватний ключ – це технічний інструмент доступу, який дозволяє підписувати транзакції та витрачати кошти. Втрата приватного ключа означає безповоротну втрату активу, що в обліку дорівнює повній втраті майна без можливості відновлення. У професійній діяльності ключовим є питання кастодіального зберігання.

Другим важливим аспектом є зберігання активів. Зокрема, можна виділити:

- гаряче зберігання – гаманці, постійно підключені до мережі, технічно зручні для операційної діяльності, але мають вищий ризик зламу;
- чолодне зберігання – апаратні пристрої, що зберігають ключі на диску чи іншому пристрої збереження інформації.

Підприємства часто використовують мультипідпис – це технічна архітектура, за якої рух коштів з корпоративного гаманця можливий лише за умови підтвердження операції кількома особами (наприклад, бухгалтером та фінансовим директором). Це створює цифровий аналог системи внутрішнього контролю та підпису платіжних доручень.

8.3 Смарт-контракти: алгоритмізація та автоматичний облік

Смарт-контракт – це програмний код, що зберігається та виконується у блокчейн-мережі. Він автоматично реалізує умови угоди між сторонами без необхідності участі посередників (банків, нотаріусів, арбітрів). Після розгортання смарт-контракт стає незмінним, а всі його дії є прозорими та перевіряються учасниками мережі.

Основними характеристиками смарт-контрактів є:

- автоматичність – виконання відбувається без людського втручання;
- прозорість – код і транзакції доступні для перевірки;
- незмінність – після публікації контракт не може бути змінений;
- надійність – результат виконання не залежить від волі окремої сторони.

Однак блокчейн за своєю природою є ізольованою системою, так званим «закритим контуром». Він не має прямого доступу до зовнішніх джерел інформації, таких як державні реєстри, банківські курси валют, метеодані або логістичні системи, а смарт-контракт може працювати лише з тими даними, які вже знаходяться всередині блокчейну. Для подолання цієї обмеженості використовуються оракули.

Оракули – це спеціальні програмно-апаратні або програмні сервіси, які виконують роль інформаційних посередників між реальним світом та блокчейном. Вони отримують дані з зовнішніх джерел і передають їх у смарт-контракти у форматі, придатному для обробки.

Оракули можуть передавати, зокрема:

- офіційні курси валют (наприклад, дані НБУ);
- інформацію про погодні умови;
- біржові котирування та ціни на енергоносії;
- статус доставки товарів або митного оформлення;
- результати спортивних подій чи фінансових індексів.

За способом роботи оракули поділяють на:

- централізовані (одне джерело даних);
- децентралізовані (кілька незалежних джерел, що підвищує надійність);
- вхідні (передають дані в блокчейн);
- вихідні (ініціюють дії у зовнішніх системах).

Смарт-контракт діє автономно, але лише на основі достовірних даних, отриманих від оракулів. Наприклад, у сфері міжнародної торгівлі смарт-контракт може автоматично перерахувати оплату постачальнику в той момент, коли вантаж перетнув державний кордон. Умова виконання буде активована лише після того, як оракул підтвердить отримання відповідних даних від митної або логістичної служби. Таким чином, оракули є критично важливим елементом екосистеми смарт-контрактів, адже саме вони забезпечують зв’язок між цифровим блокчейн-середовищем і реальними економічними, юридичними та соціальними процесами. Без оракулів практичне застосування смарт-контрактів було б суттєво обмеженим.

8.4 Класифікація стандартів токенів в обліку

У блокчейн-системах кожен цифровий актив описується стандартом токенів, який визначає правила його створення, передачі, зберігання та обліку. Такі стандарти забезпечують сумісність між смарт-контрактами, криптогаманцями, біржами та децентралізованими застосунками. Найбільш поширеними та універсальними є стандарти мережі Ethereum, які фактично стали світовим галузевим еталоном.

ERC-20 (взаємозамінні токени) – це базовий технічний стандарт для більшості криптовалют і утилітарних токенів. Кожна одиниця такого токена є ідентичною іншій та може бути поділена на менші частини. ERC-20 визначає стандартний набір функцій (переказ, перевірка балансу, дозвіл на списання), що забезпечує простоту інтеграції з платіжними системами та біржами. В бухгалтерському та фінансовому обліку такі токени розглядаються як подільні оборотні активи, функціонально подібні до грошових коштів або фінансових інструментів. Прикладами ERC-20 є стейблкоїни, внутрішні розрахункові токени підприємств та інвестиційні токени. [45]

ERC-721 (NFT – невзаємозамінні токени) – стандарт для унікальних цифрових активів, де кожен токен має власний ідентифікатор і не може бути замінений іншим без втрати його цінності. Такий токен зберігає інформацію про власника, походження та історію транзакцій, що робить його особливо цінним для підтвердження прав. В обліку ERC-721 ідеально підходить для фіксації прав власності або користування конкретними об’єктами, такими як нерухомість, транспортні засоби, предмети мистецтва, ліцензії, патенти або авторські права. Такі токени частіше відносяться до необоротних активів або нематеріальних активів підприємства. [46]

ERC-1155 (мультистандарт) – це універсальне технічне рішення, яке дозволяє одному смарт-контракту керувати одночасно як взаємозамінними, так і невзаємозамінними токенами. [47] На відміну від ERC-20 і ERC-721, цей стандарт підтримує масові операції з різними активами в межах однієї транзакції, що знижує

витрати на комісії та спрощує управління. У практиці обліку ERC-1155 є особливо корисним для складних структур активів, наприклад інвестиційних портфелів, цифрових сертифікатів, часткової власності або комбінованих фінансових продуктів, де поєднуються різні типи прав і зобов'язань.

8.5 Облік та оподаткування в умовах волатильності

Особливістю віртуальних активів є їхня висока волатильність, тобто значні та швидкі коливання ринкової вартості. Це створює суттєві виклики для їх балансової оцінки, визначення фінансового результату та коректного відображення у фінансовій звітності підприємства. Коливання цін можуть призводити як до значних нереалізованих прибутків, так і до втрат, що безпосередньо впливає на показники капіталу та ліквідності.

Згідно з міжнародними стандартами фінансової звітності (МСФЗ), криптовалюти не мають окремого спеціалізованого стандарту, тому їх облік здійснюється за аналогією з існуючими нормами.

Найчастіше вони класифікуються:

- як нематеріальні активи відповідно до **IAS 38**, якщо утримуються з метою довгострокового зберігання або використання як засобу розрахунків;
- як запаси згідно з **IAS 2**, якщо діяльність підприємства пов'язана з регулярною купівлею та продажем криптоактивів (трейдинг, маркет-мейкінг).

У випадку обліку за **IAS 38**, віртуальні активи первісно визнаються за собівартістю, а надалі можуть оцінюватися за:

- **моделлю собівартості** (з урахуванням зменшення корисності);
- **моделлю переоцінки**, якщо існує активний ринок і можливо достовірно визначити справедливу вартість.

При класифікації як запаси, криптовалюти оцінюються за меншою з двох величин: собівартістю або чистою вартістю реалізації, що особливо важливо в умовах різких падінь курсу.

Кожна операція в блокчейні потребує оплати за використання

обчислювальних потужностей мережі – так званих Gas fees. Такі витрати є невід'ємною частиною здійснення транзакції та, залежно від економічної суті, можуть:

- включатися до первісної вартості активу при його придбанні;
- відноситися на витрати періоду при реалізації або переказі активу;
- класифікуватися як операційні витрати, якщо транзакції мають регулярний характер.

Важливим аспектом обліку є також курсові різниці, оскільки більшість криптоактивів оцінюються у доларах США або інших іноземних валютах. Підприємства зобов'язані проводити переоцінку віртуальних активів на кожну дату балансу, застосовуючи курс, визначений на обраній криптовалютній біржі або агрегаторі цін, що має бути чітко зафіксовано в обліковій політиці підприємства.

Окрім цього, підприємства повинні забезпечити:

- належне документальне підтвердження володіння криптоактивами (ключі доступу, хеші транзакцій, виписки з блокчейн-оглядачів); [48]
- розкриття інформації про ризики волатильності та ліквідності у примітках до фінансової звітності; [49]
- внутрішній контроль доступу до цифрових гаманців як елемент фінансової безпеки. [50].

Таким чином, облік віртуальних активів потребує комплексного підходу, що поєднує вимоги МСФЗ, технічні особливості блокчейну та чітко сформовану облікову політику підприємства.

8.6 Цифрова безпека та Blockchain-аудит

Сучасний бухгалтер у роботі з віртуальними активами все частіше використовує блокчейн-експлорери як інструменти перевірки та контролю, що фактично формує новий напрям – блокчейн-аудит.

Такі сервіси дозволяють у режимі реального часу перевіряти транзакції, баланси адрес, комісії та історію руху активів без залучення третіх сторін. Технічна

особливість блокчейну полягає у можливості прослідкувати шлях кожної одиниці криптоактиву від моменту її створення (емісії або майнінгу) до поточного власника.

Завдяки цьому бухгалтер може:

- підтвердити факт отримання коштів;
- перевірити джерело їх походження;
- співставити дані блокчейну з внутрішніми обліковими регістрами підприємства.

Ця прозорість є ключовою для виконання процедур AML (Anti-Money Laundering) та KYC (Know Your Customer). Аналіз історії транзакцій дозволяє виявляти потенційні зв'язки з нелегальною діяльністю, санкційними адресами або високоризиковими сервісами, що є важливим елементом фінансового та податкового комплаєнсу.

Водночас головним технічним ризиком у роботі з криптоактивами є не злам самої блокчейн-мережі (яка має високий рівень криптографічного захисту), а викрадення доступу до приватних ключів. Найпоширенішими загрозами є фішингові атаки, підроблені вебсайти, шкідливе програмне забезпечення та компрометація електронної пошти або браузера.

У зв'язку з цим бухгалтер, який відповідає за цифрові активи, має дотримуватися суворих протоколів інформаційної та фінансової безпеки, зокрема:

- використовувати апаратні гаманці або апаратне підтвердження кожної транзакції;
- застосовувати багатофакторну автентифікацію;
- працювати лише з перевіреними шлюзами, біржами та кастодіальними сервісами;
- забезпечувати розмежування доступу між співробітниками (поділ повноважень).

Таким чином, роль бухгалтера в умовах цифрової економіки виходить за межі традиційного фінансового обліку та все більше поєднує облікові, аудиторські та кібербезпекові функції.

Блокчейн не лише змінює інструменти роботи, а й формує нові професійні компетенції, необхідні для забезпечення прозорості, безпеки та відповідності діяльності підприємства регуляторним вимогам.

Контрольні запитання до теми

1. Поясніть, як архітектура блокчейну (зв'язок блоків через хеш попереднього блоку) забезпечує концепцію незмінності даних та чому це є критично важливим для проведення фінансового аудиту?

2. Яким чином механізм консенсусу (наприклад, Proof-of-Stake) виступає технічним тригером для відображення операції в бухгалтерському обліку?

3. Проаналізуйте різницю між публічним та приватним ключами. Які наслідки для балансу підприємства має втрата приватного ключа?

4. Охарактеризуйте технологію «мультипідпису» (multisig). Чому її вважають цифровим аналогом системи внутрішнього контролю та розподілу повноважень у бухгалтерії?

5. Визначте основні характеристики смарт-контрактів. Як автоматичне виконання умов угоди впливає на формування первинної документації?

6. Хто такі «оракули» у блокчейн-мережі та чому без них неможлива автоматизація обліку операцій, що залежать від зовнішніх даних (наприклад, курсів валют НБУ чи статусу митного оформлення)?

7. Порівняйте стандарти токенів ERC-20 та ERC-721. У чому полягає принципова різниця в їхньому відображенні у складі активів (оборотні vs нематеріальні активи)?

8. За яких умов криптоактиви повинні обліковуватися як «Запаси» (IAS 2), а за яких — як «Нематеріальні активи» (IAS 38)?

9. Як у бухгалтерському обліку слід відображати витрати на сплату комісій мережі (Gas fees) при придбанні та реалізації віртуальних активів?

10. Як використання блокчейн-експлорерів змінює процедури підтвердження права власності та перевірки джерел походження коштів (AML/KYC) порівняно з традиційними банківськими виписками?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] «Цифрограм,» vseosvita.ua, [Онлайновий]. URL: https://vseosvita.ua/lp/cyfrogram.

[2] «Цифрова грамотність – Вікіпедія,» [Онлайновий]. URL: https://uk.wikipedia.org/wiki/Цифрова_грамотність.

[3] «Digital Literacy,» ALA, [Онлайновий]. URL: https://literacy.ala.org/digital-literacy.

[4] «TVETipedia Glossary,» UNESCO-UNEVOC, [Онлайновий]. URL: https://unevoc.unesco.org/home/TVETipedia%2BGlossary/lang%3Den/show%3Dterm/term%3Ddigital%2Bliteracy.

[5] «Ukraine: number of internet users 2024 | Statista,» Statista, [Онлайновий]. URL: https://www.statista.com/statistics/1376054/ukraine-number-of-internet-users/.

[6] Datum Intelligence, «Ukraine Online Population Forecast 2023-28,» Datumintell, 1 5 2024. [Онлайновий]. URL: https://www.datumintell.in/ukraine-online-population/.

[7] «Digital 2022: Ukraine — DataReportal – Global Digital Insights,» DataReportal – Global Digital Insights, [Онлайновий]. URL: https://datareportal.com/reports/digital-2022-ukraine.

[8] «Digital 2023: Ukraine — DataReportal – Global Digital Insights,» DataReportal – Global Digital Insights, [Онлайновий]. URL: https://datareportal.com/reports/digital-2023-ukraine.

[9] «Digital 2024: Ukraine — DataReportal – Global Digital Insights,» DataReportal – Global Digital Insights, [Онлайновий]. URL: https://datareportal.com/reports/digital-2024-ukraine.

[10] Microsoft, «What Is Cloud Computing? | Microsoft Azure,» [Онлайновий]. URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing.

[11] T. Grance та I. T. L. (. I. o. S. a. T. C. S. Division, The NIST definition of cloud computing, Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2011.

[12] «SaaS vs PaaS vs IaaS – Types of Cloud Computing – AWS,» Amazon Web Services, Inc., [Онлайновий]. URL: https://aws.amazon.com/types-of-cloud-computing/.

[13] «Types of Cloud Computing - Definition | Microsoft Azure,» Cloud Computing Services | Microsoft Azure, [Онлайновий]. URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/types-of-cloud-computing.

[14] «What is iPaaS? - Integration Platform as a Service Explained - AWS,» Amazon Web Services, Inc., [Онлайновий]. URL:

https://aws.amazon.com/what-is/ipaas/?nc1=h_ls.

[15] «Access Management- AWS Identity and Access Management (IAM) - AWS,» Amazon Web Services, Inc., [Онлайновий]. URL: https://aws.amazon.com/iam/?nc1=h_ls.

[16] «Microsoft Entra ID (formerly Azure Active Directory) | Microsoft Security,» Microsoft, [Онлайновий]. URL: https://www.microsoft.com/en-US/security/business/identity-access/microsoft-entra-id.

[17] «Про хмарні послуги,» Офіційний вебпортал парламенту України, [Онлайновий]. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text.

[18] «Публічна, приватна, гібридна чи мультиклауд: як вибрати потрібну хмару - GigaCloud,» GigaCloud, [Онлайновий]. URL: https://gigacloud.ua/articles/publichna-pryvatna-gibrydna-chy-multyklaud-yak-vybraty-potribnu-hmaru/.

[19] «Що таке публічна хмара, де використовується і чим буде корисною вашому бізнесу,» Colobridge, [Онлайновий]. URL: https://blog.colobridge.net/uk/2023/09/public-cloud-ua/.

[20] «Що таке кібербезпека? | Захисний комплекс Microsoft,» Microsoft, [Онлайновий]. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity.

[21] «Кібербезпека це комплекс заходів щодо захисту від кіберзагроз,» FoxmindEd, [Онлайновий]. URL: https://foxminded.ua/kiberbezpeka-tse/.

[22] «Основи кібербезпеки,» МОЗ України, [Онлайновий]. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2.

[23] «Історія кібербезпеки: від зародження ідеї до наших днів — стаття від «Cisco, мережна академія » — 🎓Education.ua,» Освіта в Україні. Education.ua, [Онлайновий]. URL: https://www.education.ua/blog/48055/.

[24] «Кібербезпека: найгучніші кібератаки в історії,» GoIT, [Онлайновий]. URL: https://goit.global/ua/articles/kiberbezpeka-nayhuchnishi-kiberataky-v-istorii/.

[25] «Дія.Освіта — IT-студії,» Дія.Освіта, [Онлайновий]. URL: https://it-osvita.diia.gov.ua/task/item/b3db5fff-d303-4cb9-89f9-57854968e438.

[26] «Що таке електронний підпис?,» Державні послуги онлайн | Дія, [Онлайновий]. URL: https://diia.gov.ua/faq/2.

[27] У. п. Вікімедіа, «Електронний цифровий підпис — Вікіпедія,» Вікіпедія, 29 10 2004. [Онлайновий]. URL: https://uk.wikipedia.org/wiki/Електронний_цифровий_підпис.

[28] «Що таке електронний цифровий підпис? | EDIN,» EDIN, [Онлайновий]. URL: https://edin.ua/shho-take-elektronnij-cifrovij-pidpis-ta-yak-vin-pracyuye/.

[29] «Що таке електронний підпис? — Блог,» Вчасно, [Онлайновий]. URL: https://vchasno.ua/shcho-take-elektronnyi-pidpys/.

[30] «Що таке електронний підпис (ЕП) та які його типи існують (УЕП, КЕП),» KONICA MINOLTA Ukraine, [Онлайновий]. URL: https://www.konicaminolta.ua/uk-ua/rethink-work/tools/what-is-an-electronic-signature#:~:text=%D0%A3%D0%B4%D0%BE%D1%81%D0%BA%D0%BE%D0%BD%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9%20%D0%BF%D1%9.

[31] «ЩО ТАКЕ СМ КОР?,» [Онлайновий]. URL: https://krliman.gov.ua/upload/files/o_1c1q237q6ov37kr6p87ivtvga.pdf.

[32] «Стан і розвиток інформатизації в Україні,» Освіта.UA, [Онлайновий]. URL: https://osvita.ua/vnz/reports/econom_pidpr/9299/.

[33] С. В. Устенко, «УЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ В УПРАВЛІННІ,» в *СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ В УПРАВЛІННІ*, Київ, КНЕУ, 2017.

[34] «SAP Business One,» SAP, [Онлайновий]. URL: https://www.sap.com/products/erp/business-one.html.

[35] «QuickBooks,» Intuit, [Онлайновий]. URL: https://quickbooks.intuit.com/online/.

[36] «Xero,» [Онлайновий]. URL: https://www.xero.com/.

[37] «Zoho Books,» Zoho, [Онлайновий]. URL: https://www.zoho.com/books/.

[38] У. п. Вікімедіа, «Штучний інтелект — Вікіпедія,» Вікіпедія, [Онлайновий]. URL: https://uk.wikipedia.org/wiki/Штучний_інтелект.

[39] IBM, «What Is Artificial Intelligence (AI)? | IBM,» IBM - United States, [Онлайновий]. URL: https://www.ibm.com/think/topics/artificial-intelligence.

[40] S. Russell та P. Norvig, Artificial Intelligence: A Modern Approach, Pearson, 2020.

[41] Y. Bengio, A. Courville та I. Goodfellow, «Deep Learning,» *MIT Press,* p. 800, 2016.

[42] Д. —. IT-студії, «Штучний інтелект,» Дія.Освіта, [Онлайновий]. URL: https://it-osvita.diia.gov.ua/educational-unit/1._shtuchnij_intelekt.

[43] У. п. Вікімедіа, «Блокчейн — Вікіпедія,» Вікіпедія, 17 5 2016. [Онлайновий]. URL: https://uk.wikipedia.org/wiki/Блокчейн.

[44] Державний податковий університет, Актуальні питання оподаткування в країнах ЄС: досвід для України, Ірпінь: Державний податковий університет, 2024.

[45] Ethereum, «ERC-20 Token Standard,» Ethereum, [Онлайновий]. URL: https://ethereum.org/developers/docs/standards/tokens/erc-20/.

[46] Ethereum, «ERC-721 Non-Fungible Token Standard,» Ethereum, [Онлайновий]. URL:

https://ethereum.org/developers/docs/standards/tokens/erc-721/.

[47] Ethereum, «ERC-1155 Multi-Token Standard,» Ethereum, [Онлайновий]. URL: https://ethereum.org/developers/docs/standards/tokens/erc-1155/.

[48] F. A. Foundation, «ACCOUNTING STANDARDS UPDATE 2023-08—INTANGIBLES—GOODWILL AND OTHER—CRYPTO ASSETS (SUBTOPIC 350-60): ACCOUNTING FOR AND DISCLOSURE OF CRYPTO ASSETS,» FASB, [Онлайновий]. URL: https://www.fasb.org/page/Document?pdf=ASU+2023-08.pdf&title=ACCOUNTING+STANDARDS+UPDATE+2023-08%E2%80%94Intangibles%E2%80%94Goodwill+and+Other%E2%80%94Crypto+Assets+(Subtopic+350-60):+Accounting+for+and+Disclosure+of+Crypto+Assets.

[49] Danielle MacKenzie, CPA, MSA, «Understanding the Standards Now in Effect for 2025 Reporting,» [Онлайновий]. URL: https://wsadvisors.com/understanding-the-2025-accounting-standards-for-crypto-assets-and-joint-ventures/.

[50] «Accounting for digital assets, including crypto assets,» Technical Line, [Онлайновий]. URL: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/technical/accountinglink/documents/ey-tl16494-221us-03-28-2025.pdf.

[51] UNESCO, “UNESCO’s Principles on Personal Data Protection and Privacy,” [Online]. URL: https://www.unesco.org/en/privacy-policy.

[52] OECD, «Digital Security Risk Management for Economic and Social Prosperity,» OECD, [Онлайновий]. URL: https://ccdcoe.org/uploads/2018/11/OECD-150917-digital-security-risk-management.pdf.

НАВЧАЛЬНЕ ВИДАННЯ

ЯНУШ РОМАН ІГОРОВИЧ

ФАТЕНОК-ТКАЧУК АЛЛА ОЛЕКСАНДРІВНА

Основи цифрової грамотності

Конспект лекцій

Друкується в авторській редакції