Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

СЕКЦІЯ 1 ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ

ЕЛЕКТРОННІ ФІНАНСОВІ ПОСЛУГИ ЯК ІНСТРУМЕНТ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

ELECTRONIC FINANCIAL SERVICES AS A TOOL FOR THE DEVELOPMENT OF THE DIGITAL ECONOMY

Кирило Каліновський, *студент*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н., доцент*
Сумський державний університет, Україна

Електронні фінансові послуги виконують важну роль у розвитку цифрової економіки, сприяючи ефективному управлінню грошовими потоками, здійсненню платежів, інвестуванню, отриманню кредитів та інших фінансових операцій. Вони надають можливість користувачам використовувати електронні канали зв'язку, такі як мобільні додатки, Інтернет-банкінг, електронні гаманці, цифрові платіжні системи та інші інноваційні технології.

Метою дослідження є аналіз електронних фінансових послуг, акцентування важливості цих послуг у забезпеченні доступу до фінансових ресурсів, стимулюванні інновацій, покращенні ефективності та прозорості фінансових операцій, а також сприянні росту цифрового сектору економіки.

Електронні фінансові послуги в Україні в останні роки зазнали значних змін і досягли значних успіхів. Ось найголовніші досягнення в цій сфері:

1. Впровадження електронних платіжних систем: Україна успішно впровадила ряд електронних платіжних систем, таких як ProZorro, ePayments та Дія. Ці системи сприяють електронному державному замовленню, забезпечують безпеку та зручність для користувачів та сприяють боротьбі з корупцією.

2. Впровадження електронного банкінгу: Українські банки активно впроваджують електронні банкінгові послуги, що дозволяють клієнтам здійснювати операції з рахунками, переказувати кошти, контролювати фінансовий стан та отримувати інші фінансові послуги.

3. Розширення електронного комерцію: зростання популярності електронної комерції сприяє розвитку електронних платіжних систем та онлайн-торгівлі. Україна поступово стає електронною торговельною платформою, де підприємства та споживачі можуть здійснювати електронні покупки та продажі швидко й безпечно.

4. Розширення фінансових технологій (FinTech): Україна стає все більш привабливою для стартапів і компаній, які працюють у сфері фінансових технологій. Це сприяє інноваціям і прогресу в електронних фінансових послугах, зокрема в галузях якісного аналізу даних, блокчейн-технологій, швидких платежів та інших фінтех-рішень.

5. Регуляторні зміни: Уряд та Національний банк України активно працюють над створенням сприятливого регуляторного середовища для розвитку електронних фінансових послуг. Це включає введення нових законодавчих актів та регуляторних стандартів, спрямованих на забезпечення безпеки та захисту прав споживачів в цифровому фінансовому просторі.

Ці та інші досягнення свідчать про поступовий розвиток електронних фінансових послуг в Україні. Вони сприяють ефективному управлінню фінансами, стимулюють економічний ріст і сприяють розвитку цифрової економіки країни.

Основні переваги електронних фінансових послуг для розвитку цифрової економіки:

1. Швидкість та ефективність. Електронні фінансові послуги дозволяють здійснювати миттєві фінансові транзакції без необхідності фізичної присутності або використання паперових документів.

2. Зручність та доступність. Електронні фінансові послуги доступні через Інтернет або мобільні пристрої, що робить їх доступними у будь-який час і будь-якому місці. Це надає зручність для користувачів і дозволяє їм здійснювати фінансові операції в зручний для них час і місце.

3. Зниження витрат. Використання електронних фінансових послуг дозволяє знизити витрати на проведення операцій, пов'язаних з фінансовими транзакціями. Наприклад, відмова від потреби утримувати фізичні офіси та персонал для обслуговування клієнтів може суттєво знизити загальні витрати.

4. Безпека. Електронні фінансові послуги, використовуючи передові технології шифрування та автентифікації, забезпечують високий рівень безпеки фінансових операцій, сприяючи виявленню та запобіганню шахрайству та зловживанню, що робить їх довіреними для користувачів. Безпека є ключовою складовою у забезпеченні довіри та успіху в цифровій економіці.

5. Покращення аналітики та прийняття рішень. Електронні фінансові послуги можуть збирати та аналізувати значні обсяги даних щодо фінансових транзакцій та поведінки клієнтів. Це дає змогу фінансовим установам та бізнесам отримувати цінні уявлення та здійснювати більш обґрунтоване прийняття рішень.

6. Стимулювання інновацій. Електронні фінансові послуги сприяють стимулюванню інновацій та прогресу нових технологій у фінансовому секторі. Наприклад, цифрові платіжні системи, блокчейн та

криптовалюти відкривають нові перспективи для фінансових інновацій. Вони сприяють виникненню нових бізнес-моделей, платіжних рішень та фінансових послуг, що сприяє зміцненню цифрової економіки.

7. Сприяння економічному зростанню. Електронні фінансові послуги спонукають до економічного росту, стимулюючи збільшення обсягів фінансових транзакцій та поліпшення доступу до фінансових послуг. Це в свою чергу сприяє розвитку бізнесу, привабленню інвестицій і створенню нових робочих місць. Збільшення ефективності фінансових операцій та розширення фінансових можливостей сприяють сталому економічному зростанню та процвітанню суспільства.

8. Можливість автоматизації фінансових операцій. Електронні фінансові послуги можуть бути інтегровані з автоматизованими системами управління, що дозволяє автоматизувати фінансові операції та процеси.

9. Підвищення прозорості та контролю. Електронні фінансові послуги можуть забезпечити більшу прозорість та контроль над фінансовими операціями. Користувачі мають можливість миттєво отримувати інформацію щодо стану своїх рахунків, транзакцій та фінансових зобов'язань.

10. Розширення інвестиційних можливостей. Електронні фінансові послуги дозволяють людям отримати доступ до різноманітних інвестиційних інструментів та ринків, що допомагає їм розширити свої можливості заробітку та зростання капіталу. Користувачі можуть здійснювати інвестиції в різні активи, такі як цінні папери, криптовалюти, фондові ринки тощо.

Існують деякі потенційні негативні наслідки електронних фінансових послуг для розвитку цифрової економіки. Наприклад, зростання кіберзлочинності може підірвати довіру користувачів до цифрових платформ та послуг, обмежуючи їх прийняття. Також можуть виникати питання щодо приватності та захисту персональних даних, що може вплинути на сприйняття електронних фінансових послуг користувачами. Важливо знайти баланс між зручністю та безпекою, щоб забезпечити стійкий розвиток цифрової економіки.

Отже, електронні фінансові послуги відкривають нові можливості для цифрової економіки, забезпечуючи швидкість, доступність, прозорість та безпеку фінансових операцій. Вони сприяють розвитку інновацій, розширенню фінансових можливостей та покращенню фінансової грамотності, що сприяє зростанню цифрового сектору економіки.

Електронні фінансові послуги є важливим інструментом розвитку цифрової економіки в Україні. Найголовніші досягнення включають впровадження електронних платіжних систем, розвиток мобільних платежів, електронного банкінгу, електронної комерції, фінтех і електронних гаманців. Ці зміни сприяють росту економіки, забезпечують зручність та безпеку для користувачів та створюють сприятливе регуляторне середовище.

ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ

DIGITAL TRANSFORMATIONS IN THE ECONOMY

Єлизавета Калюсенко, *студентка*
Сумський державний університет, Україна

Сучасне суспільство характеризується глибоким проникненням цифрових технологій у всі сфери життя. Ця нова ера інновацій, розвитку інформаційно-комунікаційних технологій та швидкі зміни потреб бізнесу та суспільства є невід'ємними компонентами сучасної реальності. Сьогодні, на тлі глобальних викликів і загроз, цифрова трансформація економіки стає особливо актуальною і наукові дослідження в цій галузі набувають значного значення. В цьому контексті, дослідження сутності та основних тенденцій цифрової трансформації економіки в умовах сучасних глобальних ризиків і загроз мають велике теоретичне і науково-практичне значення. [1]

Розглянемо трактування поняття «Цифрова трансформація». Цифрова трансформація представляє собою процес використання цифрових технологій з метою створення нових або модифікації існуючих бізнес-процесів, культури та клієнтського досвіду, щоб задовольнити змінні вимоги бізнесу та ринку. Ця трансформація відкриває перед малими підприємствами можливості поступового підвищення ефективності своєї діяльності, створення нових бізнес-моделей та поліпшення взаємодії з клієнтами. Вона також сприяє проривним підприємницьким інноваціям, які не були б можливими за допомогою традиційних або наявних операційних моделей. [2]

Для виробничих підприємств і компаній, що надають послуги, оптимізація операційних процесів стає ключовою характеристикою цифрової трансформації економіки. Це охоплює внутрішні процеси підприємства, підтримку персоналу та управління продуктивністю. У той же час, з точки зору держави, цифровізація економіки є каталізатором зростання ВВП, покращення комунікації з приватним сектором та вдосконалення секторальної структури економіки. [3]

Загальноприйнятою думкою є те, що цифровізація економіки має двозначний вплив на розвиток суспільства та економіки в цілому. Цифрові технології вже перетворили працю, управління, освіту, дозвілля та розваги, відкривши нові ринкові можливості й спричинивши значні соціально-економічні наслідки у різних галузях економіки та суспільства. Наприклад, упродовж останніх 30 років участь людини у виробництві по всьому світу зменшилася з 64% до 59%.[4] З прогнозів фахівців випливає, що до 2040 року автоматизація промисловості може призвести до скорочення робочих місць наблизько на 40%, переважно на рахунок низькооплачуваних посад у

виробництві.[5] Таким чином, цифровізація економіки може призвести до безробіття мільйонів людей у всьому світі. Прогнозується, що до 2030 року понад 60% професій будуть автоматизовані.

У майбутньому заводи та фабрики зможуть самостійно вдосконалюватися й модернізуватися без або з мінімальною участю людини. Бізнес-процеси, логістика та виробничі цикли будуть постійно оптимізовуватися в автономному режимі.

В цьому процесі значну роль відігратиме передбачувальна аналітика, що базується на аналізі великих обсягів даних. Це дозволить передбачати ймовірність несправності елемента системи або пристрою і замінювати компонент ще до того, як він повністю вийде з ладу. Siemens Electronic Works в Амберзі, Німеччина, є прикладом такого "розумного" заводу, де участь людини мінімізована завдяки впровадженню "розумної системи". Ця система самостійно відстежує функціонування 1,6 мільярда компонентів, встановлює норми виробництва і управляє логістичними потоками.

У таких умовах вартість робочої сили втрачає свою ключову роль у формуванні виробничих витрат, а головним фактором соціально-економічного розвитку стає технологічний потенціал національної економіки.

Узагальнюючи світовий досвід цифрової трансформації національних економік, можна виділити такі позитивні наслідки цих змін:

1. Створення нових можливостей для розвитку бізнесу шляхом використання передових технологій, таких як мобільні мережі, соціальні технології, аналітика великих обсягів даних. Ці технології підвищують потенціал для створення нових цінностей підприємств і організацій, залучення нових клієнтів та підвищення рівня продажів. [6]
2. Підвищення конкурентоспроможності національної економіки шляхом впровадження та розвитку нових бізнес-моделей і технологій, таких як аналітика великих обсягів даних, цифрові платформи, роботизація, 3D-друк, Інтернет речей, нейронні мережі, штучний інтелект, блокчейн тощо.
3. Збільшення прозорості у взаємодії корпоративного сектору і населення з державою та поліпшення ділового клімату в країні.
4. Збільшення обсягів державного фінансування в галузі освіти, науки та підготовки професійних кадрів у сфері ІТ.
5. Покращення якості і доступності медичних, освітніх, культурних, транспортних та послуг у сфері громадської безпеки.
6. Зменшення регуляторних обмежень, розробка єдиної нормативної бази для використання цифрових технологій і створення особливих правових режимів для пілотних проектів.
7. Стимулювання інтересу до використання цифрових інновацій та розвитку цифрової культури.

Водночас, серед негативних наслідків цифрової трансформації економіки можна виділити наступні аспекти:

1. Розширення розриву між освіченими та неосвіченими людьми в галузі цифрових навичок, що призводить до ризику недостатньої якості освіти та професійних знань, що вимагаються на ринку праці.
2. Поглиблення соціальної нерівності в суспільстві, зменшення можливостей для формування та розвитку середнього класу, обмеження соціальної мобільності та наявність соціальних бар'єрів. Особливу увагу слід приділити проблемам, пов'язаним з нестабільністю зайнятості серед економічно активного населення.
3. Виникнення соціально-психологічних проблем, які стосуються окремих осіб та суспільства в цілому, пов'язаних з загрозами сегрегації населення країни залежно від їх компетенцій у цифрових технологіях, погіршення функціональних можливостей та професійних навичок працівників, а також зміни мотиваційних орієнтацій. [7]

Список літератури

1. Вектори економічного розвитку 2030. Кабінет міністрів України. Центр економічного відновлення. 2020. 416 с.
2. Tapscott D. The Digital Economy: Promise and Peril in the Age of Networked Intelligence. McGrawHill, 1995. 342 p.
3. Струтинська І.В. Дефініції поняття "цифрова трансформація". Причорноморські економічні студії. 2019. Вип. 48 (2). С. 91—96.
4. Дєєва Н.Е., Делейчук В.В. Механізми залучення інвестицій емітентами в умовах розвитку цифрової економіки. Київ: Молодий вчений, 2018. С. 670.
5. Веретюк С.М., Пілінський В.В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. Наукові записки Українського науково-дослідного інституту зв'язку. 2016. № 2. С. 51—58.
6. Андрющенко К.А., Шергіна Л.А., Ковтун В.П. Аналіз особливостей та перспектив розвитку України в концепції "Індустрія 4.0". Технологічний аудит та ресурсозбереження.
7. Information communication technology policy. Hopestone Kayiska Chavula, Abebe Chekol, UNECA, 2011.

АНАЛІЗ РІВНЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ ТА КРАЇН ЄС

ANALYSIS OF THE LEVEL OF DIGITAL TRANSFORMATION OF THE ECONOMY OF UKRAINE AND THE EU

Сергій Миненко, доктор філософії
Сумський державний університет, Україна
Владислава Лук'янова, студентка
Сумський державний університет, Україна

Цифрова економіка базується на цифрових комп'ютерних технологіях та є прискорювачем соціально-економічного життя суспільства у сучасному світі. Цифровізація розвитку глобальної економіки проявляється різною мірою, проте місце кожної країни залежить від ступеня розвитку та впливу цифровізації на економічне та соціальне середовище. Для кожної країни підтримка промислового сектору та технологій є головною умовою економіки, сфери послуг і сприяння збільшенню рівня доходів і добробуту населення (*Аналіз концепцій напрямів цифрової трансформації економіки*, 2023).

Метою статті є аналіз основних тенденцій розвитку цифрової економіки країн ЄС та дослідження ключових аспектів цифровізації економіки України в умовах євроінтеграційних процесів з позиції практичного аспекту.

Як зазначено в «Концепції розвитку цифрової економіки та суспільства України», основною метою цифровізації є досягнення цифрової трансформації наявних і створення нових секторів економіки, а також трансформація сфер життєдіяльності на нові, більш ефективні та сучасні. Таке зростання можливе лише тоді, коли ідеї, заходи, ініціативи та програми, пов'язані із цифровізацією, інтегруються, зокрема, з національними, регіональними, галузевими стратегіями та програмами розвитку нашої країни (*Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*, б. д.).

Цифровізація державних сервісів, бізнесу та доступ до технологій відкривають безліч можливостей, важливо зрозуміти прогрес держави у цій сфері та покращувати цифровий досвід громадян. У цьому в країнах ЄС допомагає DESI (*Побудова екосистеми DESI в Україні - eu4digitalua*, б. д.).

Індекс цифрової економіки та суспільства (DESI) – це зведений індекс, який узагальнює показники цифрової ефективності Європи та відстежує еволюцію держав-членів ЄС в області цифрової конкурентоспроможності. Індекс DESI охоплює п'ять основних категорій: зв'язок, людський капітал, використання Інтернету, інтеграція цифрових технологій і цифрові державні

послуги (*Індекс цифрової економіки та суспільства (DESI) 2020 - EU4Digital*, б. д.).

Європейська комісія відстежує цифровий прогрес держав-членів за допомогою звітів Індексу цифрової економіки та суспільства (DESI) з 2014 року (рис.1). Щороку DESI включає профілі країн, які допомагають державам визначити напрями, що потребують першочергових дій, а також тематичні розділи, що пропонують аналіз у ключових цифрових областях, необхідний для підтримки політичних рішень.

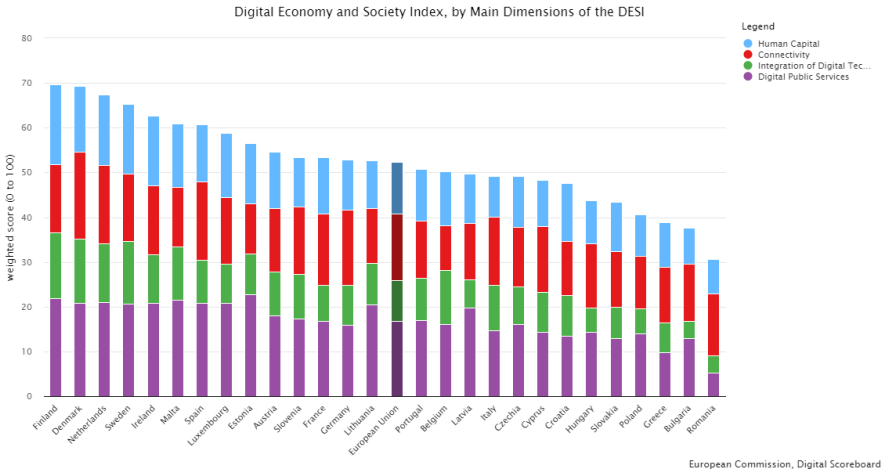

Рисунок 1. Індекс цифрової економіки та суспільства за основними параметрами DESI 2022 рік (*DESI composite index*, 2022)

Звіти DESI 2022 базуються переважно на даних за 2021 рік і відстежують прогрес, якого країни досягнули у сфері цифрових технологій. Під час пандемії COVID-19 темпи із цифровізації були уповільнені, але країни не стоять на місці та намагаються усунути прогалини в цифровій трансформації і розгортанні передових мереж 5G. ЄС виділив значні ресурси в розмірі 127 мільярдів євро на цифрові реформи та інвестиції в національні плани відновлення та підтримки цифрової трансформації. Це можливість прискорити цифровізацію, підвищити стійкість та зменшити зовнішню залежність за допомогою реформ та інвестицій. (*The Digital Economy and Society Index (DESI)*, б. д.-b).

Україна має серйозні передумови для приєднання до DESI, однак потрібна більш сучасна цифрова стратегія, узгоджена з останніми стратегіями ЄС. У листопаді проєкт EU4DigitalUA разом із місією технічної допомоги та обміну інформацією Європейської Комісії провів захід, щодо створення

передумов впровадження DESI в Україні. Участь брали Міністерство економіки України, Державна служба статистики, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, а також іноземні експерти країн ЄС. Проєкт EU4DigitalUA підтримує впровадження DESI в Україні, експерти аналізують нормативно-правову та політичну базу збору цифрових даних та допомагають створити підґрунтя для застосування DESI в Україні. Держава зможе не лише вимірювати та відстежувати, а й формувати політику цифрової трансформації на основі даних. За підтримки експертів EU4DigitalUA було підготовлено аналітичний звіт, який оцінює поточний стан та визначає необхідні кроки створення екосистеми DESI в Україні.

Впровадження DESI в Україні дозволить визначити динаміку та пришвидшити прогрес цифрового розвитку, порівнюючи з цифровими економіками ЄС, і таким чином сприятиме інтеграції до Єдиного цифрового ринку ЄС (*Побудова екосистеми DESI в Україні - eu4digitalua*, б. д.-b).

Як відомо, темпи цифровізації дещо поступаються передовим країнам світу, до того ж у 2022 р. ці процеси почали значно сповільнюватись через збитки і втрати, що зазнає бізнес від повномасштабної війни у країні. Саме ця причина актуалізує необхідність визначення основних тенденцій розвитку української національної економіки. Аналіз тенденцій розвитку цифрової економіки в Україні ускладнюється обмеженістю офіційної статистики. На відміну від європейської практики, вітчизняна статистична служба почала здійснювати моніторинг параметрів цифровізації діяльності економічних суб'єктів країни лише кілька років тому. Проте, незважаючи на наявність обмежень, аналіз актуальних тенденцій розвитку цифрової економіки в Україні може бути здійснений на належному науковому й аналітичному рівнях.

Цифрова трансформація бізнесу єдиний шлях його подальшого розвитку в умовах висококонкурентних ринків, карантинних обмежень, спричинених пандемією та проблем, викликаних повномасштабним воєнним вторгненням.

Список літератури

1. *Аналіз концепцій напрямів цифрової трансформації економіки*. (2023, 1 березня). Zenodo. https://zenodo.org/record/7688416

2. *Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*. (б. д.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/67-2018-р#Text

3. *Побудова екосистеми DESI в Україні - eu4digitalua*. (б. д.). eu4digitalua. https://eu4digitalua.eu/news/desi-escosystem-ukr/

4. *Індекс цифрової економіки та суспільства (DESI) 2020 - EU4Digital*. (б. д.). EU4Digital. https://eufordigital.eu/uk/library/digital-economy-and-society-index-desi-2020/

5. *DESI composite index*. (2022). https://digital-agenda-data.eu/. https://digital-agenda-data.eu/charts/desi-composite#chart=%7B"indicator":"desi_sliders","breakdown":%7B"desi_hc":5,"desi_conn":5,"desi_idt":5,"desi_dps":5%7D,"unit-measure":"pc_desi_sliders","time-period":"2022"%7D

6. *The Digital Economy and Society Index (DESI)*. (б. д.-a). Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/desi

7. *Побудова екосистеми DESI в Україні - eu4digitalua*. (б. д.-b). eu4digitalua. https://eu4digitalua.eu/news/desi-escosystem-ukr/

РОЗУМНІ МІСТА ТА ЇХ РОЛЬ У ЦИФРОВІЙ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

SMART CITIES AND THEIR ROLE IN THE DIGITAL TRANSFORMATION OF THE ECONOMY

Анастасія Самойленко, *студентка*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н, доцент*
Сумський державний університет, Україна

Концепція «Розумного міста» стала ключовим фактором сталого розвитку міст. У розумному місті сучасні технології у сферах енергетики, мобільності, міського планування, адміністрування та зв'язку об'єднані одна з одною, щоб зібрані дані допомагали краще приймати рішення та покращувати певні аспекти якості життя.

Метою даної роботи є дослідження поняття «розумне місто» та визначення його ролі у цифровій трансформації економіки.

«Розумні» міста – це міста, де цифрові рішення використовуються для покращення використання традиційних мереж і послуг. Таким чином, мета розумних міст полягає в тому, щоб підвищити якість життя мешканців, підвищити стійкість і принести користь бізнесу. Концепції розвитку розумних міст спрямовані на створення нових високотехнологічних міст завдяки розвитку інноваційної інфраструктури. За даними Центру світової конкурентоспроможності IMD у світовому рейтингу Smart City Index 2021 лідерами є Сінгапур, Цюріх та Осло. Київ зайняв 82 місце, піднявшись на 16 пунктів. Міста все більше поєднують потужність технологій обробки даних і силу людей, створюючи численні можливості.

Департамент з економічних і соціальних питань ООН прогнозує , що до 2050 року 68% населення світу проживатиме в містах. Технології «розумного міста» можуть допомогти успішно впоратися з деякими з цих викликів – завдяки численним технологіям, які входять в економіку та об'єднують людей. У розумному місті сучасні технології у сферах енергетики, мобільності, міського планування, адміністрування та зв'язку пов'язані для покращення рівня життя та комфорту мешканців.

Серед переваг розумних міст можна виділити:

- підвищення громадської безпеки;
- стійке довкілля та озеленення міст;
- покращення соціального спілкування;
- ефективне керування ресурсами;
- зменшення споживання енергії.

Розумне місто відіграє важливу роль у цифровій економіці. Головною ідеєю концепції «Розумне місто» є впровадження цифрових технологій в усі системи міста. У найближчі роки цифровізація стане головним фактором розвитку світової економіки. Для післявоєнної відбудови в Україні це стане важливою складовою розвитку економіки, адже цифрова економіка здатна стрімко підвищити ВВП країни. Рушійною силою розумних міст є такі тенденції, як машинне навчання, автоматизація, робототехніка. Яскравим прикладом є Сінгапур – найрозумніше місто світу. У цьому місті впроваджено робототехніку та чат-боти на основі штучного інтелекту, що спілкуються з літніми людьми, оцифрована система охорони здоров'я, мешканцям надані додатки, що дозволяють використовувати безпілотні транспортні засоби. Їхні проекти демонструють, наскільки важливу роль грає цифровізація в концепції розумного міста. Поєднання пристроїв і даних із фізичною інфраструктурою та послугами міста може скоротити витрати та підвищити стійкість. Цифрові технології надають право безмежного доступу до значного обсягу інформації, яка дозволяє забезпечувати відкрите інформаційне обслуговування населення на основі глобального інформаційного обміну. Розумне місто ґрунтується на використанні базових елементів, а саме Big Data, Open Data, Інтернету речей (IoT), п'ятого покоління мобільного зв'язку (5G), Wi-Fi, відеоспостереження і фотофіксації, єдиної диспетчерської служби тощо. Важливим фактором у розумному місці виступає оцифрування головних сфер економіки. У концепції розумного міста покладені такі основні технології:

– цифрові технології, що працюють на місто;

– інформаційно–цифрові технології для забезпечення трансформації житлових умов;

– технології для покращення взаємодії влади з суспільством.

В Україні тільки розпочинається шлях до впровадження концепції розумного міста. Найбільш розвиненим в Україні вважається Київ. У 2015 році Київрада затвердила концепцію «Kyiv Smart City 2020», яка за задумом має визначити базові принципи для подальшого інфраструктурного, технологічного та соціального розвитку столиці, а також новий вектор трансформації міського простору. У 2020 році в дію ввели застосунок «Київ Цифровий». Це значний крок в цифровій трансформації міста. Застосунок дозволяє поповнювати через мобільний телефон транспортну карту Kyiv Smart Card, купувати QR-квитки, здійснювати оплату за паркування, забирати евакуйовану автівку зі штрафмайданчика без черги. В перспективі концепція «Kyiv Smart City 2020» зосереджена в таких напрямках:

1) ефективно управління послугами ЖКГ (сортування відходів, водопостачання; збереження відновлюваних ресурсів);

2) розвиток електронних форм освіти, об'єднання мешканців та бізнесу до системи міських інновацій;

3) залучення громадян до управління містом, е-урядування;

4) якісна медицина та доступ всіх громадян до медичних послуг.

Проведене дослідження демонструє роль сучасних технологій у реалізації концепції розумного міста, їх важливу роль у формуванні цифровій економіці. В Україні є великий потенціал для впровадження даної концепції у міста.

ЦИФРОВІ ТРАНСФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ: ТЕНДЕНЦІЇ ТА МОЖЛИВОСТІ

DIGITAL TRANSFORMATIONS IN THE BANKING SECTOR: TRENDS AND OPPORTUNITIES

Аліна Сімановська, студентка
Сумський державний університет, Україна

Розвиток сучасного світу наразі не є можливм без використання цифрових технологій. Цифровізація вплинула на всі сфери життя: освіту, медицину, туризм тощо. Банківський сектор не є винятком. Цифровізація надає нові можливості для підвищення конкурентоспроможності банків, збільшення кількості клієнтів та прибутків установ.

Чимало дослідників та організацій присвятили свої праці розвитку цифрової трансформації. Серед актуальних досліджень можна виділити роботи Н. Азьмук, В. Апалькової, Дж. Кронка, Б. Кінга, П. Зиля, С. Волосовича, С. Циганова, статті Global Finance, The Economic Times та звіти Світового банку.

Мета роботи – проаналізувати поточний стан та особливості цифрової трансформації у вітчизняному та міжнародному банківському секторі.

Цифрова трансформація — це процес переходу до нових способів ведення бізнесу через впровадження цифрових технологій і послуг. Діджиталізація в теперішній час залежить від використання таких технологій як штучний інтелект, Інтернет речей, хмарні технології, блокчейн тощо. Їх застосування забезпечує широке коло охоплення аудиторії, скорочення операційних витрат, покращення якості обслуговування та швидкість надання банківських послуг.

Технічні можливості, які забезпечує цифрова трансформація у сфері фінансових технологій, значно зменшує потребу у відкритті банківських відділень. Цей процес почав набирати обертів ще з початку введення карантинних обмежень через COVID-19. Суттєво скоротилося фізичне відвідування клієнтами відділень, однак зріс попит на онлайн-банківські послуги. Таким чином у країнах ЄС було ліквідовано близько 25% банківських відділень за період пандемії.

Частина працівників вимушена була працювати дистанційно, користуючись гаджетами та новітніми технологіями. Клієнти отримували фінансові послуги через мобільні додатки, інтернет-банки та чат-боти (рис. 1).

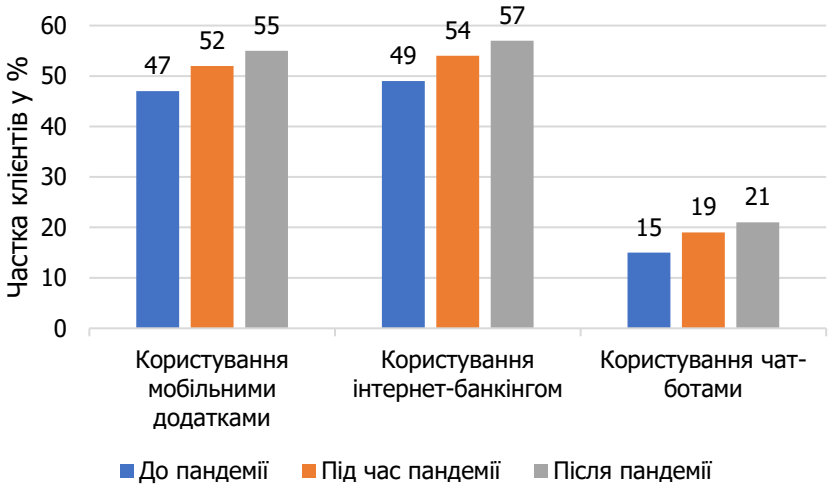

Рисунок 1. Вплив COVID-19 на розвиток цифрових банківських каналів (COVID-19, 2020)

За даними рис. 1 спостерігається помітне зростання користувачів, що користуються інтернет-технологіями для отримання банківських послуг. Більшість надає перевагу користуванню інтернет-банкінгом, трохи менше – мобільними додатками та п'ята частина клієнтів застосовує чат-боти.

Блокчейн є новою технологією, що покладається на фундаментальні інструменти з криптології та безпеки даних, особливо з точки зору автентифікації транзакцій. За допомогою використання криптографічних технологій, можна управляти регістром без централізованого управління. Серед переваг використання блокчейну виділяють: цілодобові транзакції, мінімальні ризики, відсутність посередніх осіб та контроль над власним веденням торгівельних справ і особистими даними.

Міжнародні та вітчизняні банки поступово надають перевагу використанню блокчейн-технологій. Наприклад, на криптовалютний спосіб оплати товарів та послуг були переведені японські Міжбанківські P2P перекази, завдяки впровадженню яких вдалося відмовитися від карткового еквайрингу, скоротити витрати та не платити комісію Visa і MasterCard (Халевський, О. І. та ін., 2019).

Українські банківські системи також використовують блокчейн. «ПриватБанк» першим з вітчизняних банків увів систему криптоплатежів у якості розрахункового інструменту.

Наразі штучний інтелект є однією з найперспективніших технологій у сфері фінансів. Чат-роботи надають клієнтам консультації з банківських

питань, фінансових операцій в режимі онлайн. З їх допомогою можна відкрити рахунок вдома, дізнатися актуальні новини банку, заключити фінансову угоду тощо. Штучний інтелект допомагає банківським установам здійснювати комплексний контроль ризиків, управляти корпоративною інформацією, автоматизовувати обслуговування клієнтів та роботу з документами та поповнювати інформацію про клієнтів.

Технології Big Data допомагають банкам ефективно розподіляти свої ресурси, приймати зважені рішення та підвищувати продуктивність. Machine learning ефективно виявляє та сприяє запобіганню шахрайства у використанні кредитних карток, бухгалтерському обліку, страхуванні тощо. З його допомогою вивчають CLV кожного сегмента клієнтів та виявляють найбільш та найменш цінний з них, створюють прості алгоритми, які аналізують та фільтрують діяльність користувача, щоб зробити найбільш актуальну для нього пропозицію.

Фінансові технології є одним з головних двигунів цифровізації банківської галузі, тому державі вигідно підтримувати їх діджиталізацію. З початку повномасштабної війни Національний банк України забезпечив можливістю фінансові установаи ще два роки надавати послуги, використовуючи хмарні серевери та обладнання на території європейських країн, США, Великобританії та Канади. Це дозволяє вітчизняним банкам не залежати від критичної інфраструктури всередині країни.

Отже, банківська галузь стрімко розвивається під впливом нових технологій. Забезпечується цілодобовий доступ користувачів до інформації, швидкість транзакцій, захищеність даних. Банкам надається можливість економити власні кошти за рахунок використання новітніх технологій та інвестувати їх у нові проєкти.

Вітчизняні банки не відстають від європейських за інноваціями. Вони аналізують перспективи від вровадження новітніх технологій іноземними компаніями та поступово реалізують їх у своєму функціонуванні. Таким способом забезпечується привабливість української фінансової сфери для громадян та іноземних клієнтів банку.

Список літератури

1. COVID-19 and the financial services consumer: Supporting customers and driving engagement through the pandemic and beyond. (2020). Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2020/05/COVID-19-and-the-financial-services-consumer_V5.pdf

2. Халевський, О. І., & Варламова, М. Л. (2019). Цифрова трансформація в міжнародній банківській сфері. Вісник студентського наукового товариства ДонНУ імені Василя Стуса, 226–230.

ЗРОСТАННЯ ЕКОНОМІЧНОЇ СТІЙКОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В СУЧАСНИХ УМОВАХ ДІЯЛЬНОСТІ

INCREASING THE ECONOMIC SUSTAINABILITY OF BUSINESS ENTITIES IN THE CURRENT OPERATING ENVIRONMENT

***Ігор Бараннік**, докторант*
Харківський національний економічний університет імені Семена Кузнеця, Україна
***Олексій Бударін**, аспірант*
Харківський національний економічний університет імені Семена Кузнеця, Україна

Воєнна російська агресія проти України призвела до колосальних економічних втрат, збитків та пошкоджень. Проте економіка України вистояла та адаптувалась в руйнівних умовах війни. Основним фактором забезпечення економічної стійкості в сучасних умовах є реалізації політики держави щодо перенесення тягаря воєнних наслідків з бізнесу та населення на бюджет (різноманітні програми підтримки, нова податкова політика, фіксація курсу гривні, заморожування тарифів для населення та інші), що стало можливим завдяки фінансовій допомозі від міжнародних партнерів, яка у 2022р. становила 32,7 млрд дол. США, з яких гранти – 14,3 млрд дол. США. Щодо глобального інноваційного індексу, то у 2022 році Україна погіршила свій рейтинг та посіла 57 позицію (у 2021 році посідала 49 позицію) в загальному рейтингу (набрала 31,0 бали зі 100), а також посіла 34 позицію серед 39 економік Європи [1].

Слід відмітити і істотні зміни у світовій економіці, а саме: відбуваються реальні зміни центрів економічної могутності, що в першу чергу проявляється через зміни розстановки сил країн G7. У світі відбуваються процеси посилення економічної фрагментації, що є противагою традиційним глобалізаційним процесам. Міжнародний валютний фонд попереджує про цей негативні наслідки процесу, оскільки він призводить до зниження інтеграції, веде до бідності. В таких умовах країни повинні диверсифікувати імпорт, чим убезпечити ланцюги поставок і зменшити втрати виробництва через перерви.

Суб'єктам господарювання в країні не зважаючи на складні воєнні умови, які призвели до розірвання логістичних ланцюжків, блокади морських портів, паливної кризи, вдалось подолати масштабну зупинку виробництва. Вони продовжують працювати і нарощувати свою економічну стійкість завдяки запровадження Урядом таких заходів як програма релокації підприємств на безпечну територію, нова податкова політика, спрямована на

зменшення фіскального навантаження на підприємства, фіскальні стимули для учасників індустріальних парків, кредитна підтримка тощо.

Протягом всіх засідань Діалогу Україна – ЄС розглядаються питання активізації співробітництва щодо укладення Угоди про оцінку відповідності та прийнятність промислових товарів (АСАА), співробітництва у сфері публічних закупівель, існуючих та потенційних інструментів ЄС для підтримки вітчизняних малих та середніх підприємств. Все це сприяє нарощуванню економічної стійкості суб'єктів господарювання [1]. Відомі вітчизняні вчені та практики вважають, що в умовах повоєнного відновлення і реконструкції економіки та соціальної сфери України можливим є досягнення суспільного консенсусу. Існування такого консенсусу буде необхідною умовою успішного переходу від війни до мирного розвитку. Достатність же умов досягатиметься політичною, економічною і культурною єдністю процесів соціалізації населення [2].

Важливим етапом забезпечення економічної стійкості суб'єктів господарювання є оцінювання її рівня. В оцінюванні економічної стійкості суб'єктів господарювання слід враховувати основний фактор її забезпечення, це – державну політику підтримки діяльності, формування умов нарощування стійкості. Аналітичну основу оцінювання економічної стійкості суб'єктів господарювання складають інструменти, методи, процедури здійснення процесу оцінювання, а також перелік визначених негативних та позитивних факторів впливу зовнішнього та внутрішнього середовищ на цю стійкість. Методичне забезпечення оцінювання економічної стійкості суб'єктів господарювання, яке передбачає встановлення мети, завдання, суб'єкту, об'єкту, предмету, принципів та методів оцінювання, має містити ієрархічну систему частинних та інтегральних показників, які відображають рівні складових та загальний рівень економічної стійкості [3]. Дієвість методичного забезпечення оцінювання економічної стійкості суб'єктів господарювання обумовлюється інформаційним, програмно-технічним та організаційним забезпеченням, які його підтримують.

Список літератури

1. Довідкові дані [Електронний ресурс]. – Режим доступу: https://www.me.gov.ua/?lang=uk-UA

2. Геєць В.М. До питання теорії і практики політики соціальної якості в повоєнній Україні // Економіка України. 2023. №4(737), с. 3 – 22. http://economyukr.org.ua/?page_id=723&lang=uk&aid=615

3. Малярець Л.М. Моделювання в оцінці та аналізі діяльності підприємства : монографія. Малярець Л.М., Мінєнкова О.В., Сабадаш Л.О. ХНЕУ ім. С. Кузнеця, 2018. 202 с.

РОЗВИТОК ФІНТЕХ-ІНДУСТРІЇ У СВІТІ: ТЕНДЕНЦІЇ ТА ВИКЛИКИ

DEVELOPMENT OF THE FINTECH INDUSTRY IN THE WORLD: TRENDS AND CHALLENGES

Анастасія Кузченко, *студентка*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н., доцент*
Сумський державний університет, Україна

Останнім часом ринок фінтех-послуг розвивається дуже швидко. Цьому сприяє стрімкий розвиток ШІ, блокчейну, хмарних обчислень та Інтернет речей (IoT), прогрес цих технологій дає змогу створювати нові фінансові продукти та полегшувати процеси. Кожен чув, а більшість вже використовувала цифрові платежі, цифрові інвестиції, цифрове кредитування, необанки. І це тільки невеликий перелік послуг та напрямів, що з'явилися та розвиваються у 2022 – 2023 році.

Дослідження фінтех-індустрії у світі, розгляд тенденцій та трендів, аналіз можливостей розвитку і викликів у майбутньому – основна мета дослідження.

Сфера інноваційних фінансів (фінтех) включає як компанії, що працюють у цій сфері, так і технології, які її підтримують: програми, вебсайти та цифрові рішення, які модернізують традиційні фінансові послуги та змінюють спосіб поводження з грошима. У 2022 році двома найбільшими були платіжні компанії Visa та Mastercard, їх ринкова капіталізація складала приблизно 465 і 345 мільярдів доларів. Третє місце посідала Tencent з ринковою капіталізацією 187,92 млрд доларів. Stripe, Klarna – європейські компанії, теж посідали високі місця у списку фінтех-компаній за високою ринковою капіталізацією.

Фінансові технології існують вже дуже давно, але тільки з 2014 року інвестиції в фінтех-стартапи почати зростати. Пандемія COVID-19 значно пришвидшила впровадження фінансових послуг онлайн і дала значний поштовх у розвитку технологій дистанційних фінансових послуг. 2022 рік був складним для індустрії фінансових технологій, на це вплинула інфляція, криптозима та повномасштабна війна в Україні. На фінтех-стартапи було залучено 79 млрд доларів, це на 38% менше ніж у 2021 році, але це майже у два рази більше ніж у 2019 році. Найбільше фінтех-стартапів в Америці – 11 651. США посідають перше місце за кількістю фінтех-єдинорогів. Китай також є домом багатьох найбільших фінтех-компаній.

Ситуація покращилася у 2023 році дохід почав зростати разом з інвестиціями. Світовий дохід від фінтеху склав 169,32 мільярда доларів США.

У 2027 році очікується, що загальний дохід світової фінтех-індустрії становитиме приблизно 294,5 мільярда доларів США. Ринок фінтех-послуг продовжує швидко зростати. Зростання відбувається в усіх секторах, включаючи електронні платежі, кредитування, інвестиції, краудфандинг, страхування та багато інших.

У всьому світі приблизно 5,62 мільярда користувачів фінтех. Найпопулярнішими є інтернет платежі. Мобільні платежі, цифрові гаманці та інші цифрові методи оплати стали повсюдними, що дозволяє швидко та легко здійснювати грошові операції. Суспільство в наш час прагне до зручності та швидкості, тому оплата за допомогою мобільних додатків та інтернету найкращий варіант. За даними Statista, одного з провідних світових статистичних інтернет-порталів, на сегмент цифрових платежів припало 4,4 мільярда користувачів на 2023 рік. Очікується, що ця цифра становитиме 5,48 мільярда до 2027 року.

Фінтех-платформи також пропонують альтернативні методи отримання кредитів і позик, нові можливості для інвестування та управління активами. Вони надають споживачам широкий спектр переваг, таких як швидкість, зручність, доступність, низькі витрати, інноваційні продукти та індивідуальний підхід – це все заохочує користувачів відмовлятися від послуг традиційних банків.

З переліченого вище можна побачити, що перспективи розвитку фінтех-індустрії у світі є дуже обіцяючими. Ринок фінтех-послуг розширює свою географічну присутність. Це дозволяє забезпечити доступ до фінансових послуг для раніше виключених шарів населення, покращує фінансову включеність і сприяє економічному розвитку. Цьому сприяє інтеграція новітніх технологій, такі як штучний інтелект, машинне навчання, блокчейн та аналітика даних, щоб поліпшити ефективність і зручність своїх послуг. Це включає розробку персоналізованих рішень, автоматизацію процесів та покращення кібербезпеки. Варто зауважити фінтех-індустрія співпрацює з іншими секторами, такими як технології "розумних міст", щоб створити інтегровані фінансові екосистеми. Це передбачає зв'язок між фінансовими послугами, транспортом, енергетикою, охороною здоров'я та іншими сферами для поліпшення якості життя мешканців. Але найбільшою перевагою є розширення продуктового спектра та фінансова включеність. Компанії безперервно розширюють свій асортимент послуг і пропонують нові інноваційні рішення. Наприклад, це можуть бути фінансові роботи-консультанти, криптовалюти, міжнародні платежі, розрахункові технології та багато інших. Це може допомогти покращити фінансову включеність та доступ до фінансових послуг для населення у країнах, що розвиваються, та малозабезпечених шарів населення. Мобільні платежі, мікрокредитування та інші інновації можуть розширити доступ до фінансових послуг. Ці

перспективи свідчать про те, що фінтех-індустрія продовжуватиме змінювати фінансовий ландшафт, розширювати доступ до фінансових послуг і пропонувати нові можливості для споживачів у всьому світі.

Незважаючи на всі переваги фінтех-індустрія може зазнати деяких складнощів. В різних країнах свої регуляторні вимоги та обмеження, тому потрібно розробляти ефективну регуляторну політику, щоб забезпечити інновації та захист прав споживачів. Управлінський апарат країни повинен спочатку добре зрозуміти фінтех-ринок своєї країни та загалом цей фінансовий сектор.

Зростання використання цифрових технологій приносить з собою загрози кібербезпеці. Це викликатиме у споживачів сумніви. Фінтех-компанії повинні вдосконалювати свої системи безпеки та захисту даних, щоб уникнути кібератак та втрати конфіденційної інформації. Це також допоможе вирішити питання довіри споживачів до цифрових фінансових послуг. Забезпечення конфіденційності даних, прозорості та ефективності послуг є ключовими факторами для побудови довіри споживачів.

Ринок фінтех-індустрії стає все більш конкурентним і ситим. Для молодих фінтех-стартапів може бути важко залучити капітал та знайти своє місце на ринку. Ці перешкоди можуть призвести до консолідації галузі та посилення роль та позицій вже встановлених компаній.

Вказані недоліки можуть мати вплив на розвиток фінтех-індустрії, і успіх будь-якої компанії в цьому секторі залежатиме від її здатності адаптуватися до змін, ефективно вирішувати виклики та використовувати можливості, які пропонує майбутнє.

Розвиток фінтех-індустрії, яка поєднує фінанси та технології, має значний вплив на сучасне суспільство та економіку. Одна з найголовніших переваг розвитку фінтех-індустрії – це зручність та доступність фінансових послуг. Мобільні додатки та онлайн-платформи дозволяють проводити операції, такі як платежі, перекази коштів, заявки на кредити, безпосередньо зі смартфона або комп'ютера. Це значно спрощує фінансові операції та робить їх більш зручними для користувачів. Розвиток фінтех-індустрії також сприяє покращенню доступності фінансових послуг. Традиційні банківські послуги можуть бути обмеженими для певних категорій людей, таких як малі підприємці, молоді люди без кредитної історії або мешканці віддалених районів. Фінтех-компанії впроваджують інноваційні підходи до оцінки кредитоспроможності та надання фінансових послуг, що дозволяє залучати більше людей до фінансової системи. Крім того, фінтех-інновації сприяють зниженню витрат на фінансові послуги. Багато фінтех-компаній пропонують послуги з меншими комісіями та нижчими відсотковими ставками порівняно з традиційними банками. Варто зауважити, що інноваційні стартапи впроваджують нові технології та рішення, що стимулює конкуренцію на ринку

фінансових послуг. Це спонукає традиційні банки до впровадження нових технологій та поліпшення своїх послуг, що сприяє загальному покращенню фінансової сфери. Узагальнюючи, розвиток фінтех-індустрії приносить багато користі, такі як зручність та доступність фінансових послуг, покращення доступності для різних категорій споживачів, зниження витрат та стимулювання інновацій. Це створює більш конкурентну та динамічну фінансову сферу, що приносить користь як індивідуальним споживачам, так і економіці загалом.

КЛЮЧОВІ АСПЕКТИ ТА ВИКЛИКИ ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ

KEY ASPECTS AND CHALLENGES OF DIGITAL TRANSFORMATION IN THE ECONOMY

***Сергій Дрозд**, аспірант*
Сумський державний університет, Україна

Цифрові трансформації в економіці охоплюють широкий спектр змін, які відбуваються внаслідок використання та впровадження новітніх цифрових технологій та розвитку цифрової інфраструктури. Ці трансформації роблять значний вплив на різні аспекти економіки, включаючи виробництво, розподіл, маркетинг, продажі, фінанси і управління.

Розглянемо ключові аспекти цифрових трансформацій в економіці:

Одним за найважливіших аспектів є ефективність виробництва тому впровадження цифрових технологій, таких як автоматизація, роботизація, Штучний (ШІ) та Інтернет речей (IoT), дозволяє підвищити ефективність виробництва. Це може включати в себе використання автоматизованих систем виробництва, аналітику даних для оптимізації процесів та підвищення якості продукції.

Використання методів цифрового маркетингу та електронна комерції є технологією без якої не можливо уявити сучасні продажі. Цифрові технології дозволяють компаніям досягти ширшої аудиторії через інтернет. Маркетингові кампанії можуть бути спрямовані на конкретних споживачів за допомогою персоналізації, а електронна комерція надає можливість здійснювати продажі онлайн без фізичних магазинів. Також впровадження глобальних моделей бізнесу котрі можуть забезпечувати доступ до світових ринків. Електронна комунікація, електронна торгівля та онлайн-сервіси створюють нові можливості для міжнародного співробітництва і торгівлі, зменшуючи географічні обмеження.

В свою чергу розвиток фінансових технологій дав можливості для покупців товарі та послуг робити це зручно та швидко. Онлайн-платежі, мобільні додатки для управління фінансами, електронні гроші та блокчейн-технології є лише кількома прикладами новітніх методів оплати. Саме ці способи оплати змінюють спосіб, яким фінансові установи працюють, і як клієнти здійснюють фінансові операції.

Цифрові трансформації в економіці сприяють збору великої кількості інформації, аналізу та використанню цих обсягів даних. Аналітика Big Data дозволяє підприємствам отримувати цінні інсайди щодо споживачів, ринків та власної діяльності для прийняття кращих рішень. В той же момент штучний

інтелект використовується для автоматизації процесів, прогнозування тенденцій, вирішення складних задач та поліпшення ефективності бізнесу (Revenko et al., 2017).

В наш час можливо використовували концепції "Індустрії 4.0" на практиці: інтегровані цифрові технології в традиційні виробничі процеси, призводять до створення "розумних" фабрик із застосуванням автоматизованих систем, ШІ, IoT та інших інноваційних рішень. Це включає в себе використання роботів, автономних транспортних засобів, систем моніторингу та контролю, що забезпечують більшу ефективність, гнучкість та масштабованість виробництва.

Стартапи просувають використання цифрових інновацій на своєму прикладі. Збільшення перспективних цифрових технологій стимулюють зростання інноваційних стартапів у різних сферах економіки. Цифрові трансформації сприяють зниженню бар'єрів до входу на ринок і створюють сприятливе середовище для розвитку технологічних стартапів. Стартапи використовують нові технології для розробки інноваційних продуктів і послуг, які можуть змінити традиційні галузі і створити нові ринки.

Започаткування нових моделей бізнесу та споживання можливе лише за допомогою всебічної цифрової трансформації яка перетворює традиційні моделі бізнесу і споживання. Наприклад, підприємства можуть пропонувати послуги на основі підписки (subscription-based services), моделі "власність як послуга" (ownership-as-a-service) або використовувати мультиплатформені підходи для залучення споживачів (Pogodina et al., 2019).

Цифрові трансформації в економіці мають значний вплив на бізнес-середовище, ринкові умови та спосіб життя людей. Вони відкривають нові можливості та виклики для підприємств і суспільства в цілому. Деякі з цих викликів включають:

Потреба в цифрових навичках: тобто вимагають наявності кваліфікованих працівників з цифровими навичками. Люди повинні набувати нові знання та навички, щоб використовувати цифрові технології ефективно і адаптуватися до змін.

Забезпечення належного рівня доступності інтернету: Цифрові трансформації передбачають широкий доступ до надійного інтернету. Однак, у деяких регіонах світу існує нерівномірність у доступі до інтернету, що створює цифровий розрив між різними суспільствами та економіками.

Існують проблеми безпеки та конфіденційності: Розширення цифрових технологій також породжує проблеми безпеки та конфіденційності. Збільшення обсягів даних, їх зберігання в хмарних сервісах та збільшення кількості кібератак вимагають підвищення рівня кібербезпеки і захисту особистих даних.

І все це світворює проблеми приватності та етики в результаті збільшених обсягів збирання та обробки особистих даних котрі вимагають суворих заходів забезпечення приватності та етики. Потрібні правові, регуляторні та етичні рамки для захисту конфіденційності і запобігання зловживанням даними.

Цифрові трансформації можуть призвести до автоматизації рутинних робіт і зміни потреб на ринку праці. Виникнення нових технологій може призвести до зникнення деяких робочих місць, тоді як виникнення нових ринків може створити нові можливості зайнятості.

Зі збільшенням використання цифрових технологій зростає ймовірність кібератак та кіберзлочинності. Захист від кіберзагроз і кібербезпека стають надзвичайно важливими для суспільства.

Можлива поява цифрового розриву між різними секторами, галузями та країнами. Організації і країни, які не встигають адаптуватися до швидкого розвитку цифрових технологій, ризикують відстати і втратити конкурентоспроможність.

Екологічні виклики: Цифрові трансформації також мають вплив на екологію. Збільшення використання цифрових технологій призводить до зростання енергоспоживання та викидів парникових газів. Важливо розробляти та використовувати екологічно сталі технології, щоб зменшити негативний вплив на довкілля.

Розвиток цифрових технологій викликає нестандартні правові завдання для регуляторних органів та створення нових форм правового контролю. Потрібно розробляти відповідні закони та політики, щоб забезпечити ефективний захист споживачів, конкуренцію, інтелектуальну власність та інші аспекти цифрової економіки (Nosova et al., 2021).

Цифрові трансформації в економіці мають великий потенціал для створення нових можливостей у економіці, привернувши увагу світових лідерів до покращення ефективності, інновацій та конкурентоспроможності. Однак цифрові трансформації, також вимагають уваги до соціальних, етичних, безпекових та регуляторних викликів, щоб забезпечити стале та економічно раціональне впровадження цифрових технологій.

Загалом цифрові перетворення можуть порушити традиційні бізнес-моделі, створили нові можливості та змінили економіку. Застосування цифрових технологій має вирішальне значення для бізнесу, щоб залишатися конкурентоспроможним, адаптуватися до мінливої ринкової динаміки та використовувати переваги цифрової економіки.

Таким чином, цифрова трансформація в економіці охоплює різні ключові аспекти та виклики, такі як впровадження технологій, прийняття рішень на основі даних, клієнтоорієнтованість, інновації бізнес-моделі, організаційна культура, кібербезпека, застарілі системи, дотримання

нормативних вимог, управління змінами та вирішення проблем цифровий розрив. Організації та країни повинні вирішувати ці виклики стратегічно та цілісно, щоб успішно орієнтуватися та залишатися конкурентоно здатними.

Список літератури

1. Revenko, L., & Revenko, N. (2017). Global trends and national specifics of the development of a digital economy record of the united state, india, china and the EU. Mezhdunarodnye Protsessy, 15(4), 20-39. doi:10.17994/IT.2017.15.4.51.2

2. Pogodina, T., Udaltsova, N., & Filushina, A. (2019). Paradigm shift in technological development of socio-economic system in the context of digital transformation. Journal of Advanced Research in Law and Economics, 10(2), 653-662. doi:10.14505/jarle.v10.2(40).27

3. Nosova, S., Norkina, A., Makar, S., Fadeicheva, G., (2021). Digital transformation as a new paradigm of economic policy. Procedia Computer Science, 190, 657-665. https://doi.org/10.1016/j.procs.2021.06.077

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ З МЕТОЮ ВИЯВЛЕННЯ ТА УНИКНЕННЯ КОРУПЦІЇ

USE OF ARTIFICIAL INTELLIGENCE FOR MONITORING PUBLIC PROCUREMENTS WITH THE PURPOSE OF DETECTING AND AVOIDING CORRUPTION

Сергій Миненко, доктор філософії
Сумський державний університет, Україна
Валерія Кочнєва, студентка
Сумський державний університет, Україна

Публічні закупівлі – важлива частина якісного функціонування держави. Саме процес ведення публічних закупівель забезпечує державу необхідними товарами, роботами та послугами. Та водночас, цей напрям діяльності держави вважається одним з найбільш вразливих до корупції, тому перед учасниками публічних закупівель, контрольними органами та громадянами, що цікавляться темою законності публічних закупівель, постає питання моніторингу закупівель та виявлення можливих проявів корупції на етапах проведення закупівель. Одним з можливих інструментів моніторингу та виявлення порушень можуть бути спеціалізовані системи (платформи) підкріплені технологіями штучного інтелекту. Метою нашої роботи є аналіз можливостей та досвіду використання технологій штучного інтелекту для моніторингу публічних закупівель з метою виявлення та уникнення корупції.

Публічні закупівлі займають значну частину ВВП. Обсяг державних закупівель в Україні щороку складає близько 13% ВВП (Реформа державних закупівель, б. д.), а для прикладу в ЄС 14% ВВП (близько 2 трильйонів євро) щороку (European Added Value Unit, 2023, с. 6). Представник глобальної антикорупційної організації – Transparency International Ukraine визначає публічні закупівлі, як придбання товарів, робіт та послуг, які здійснюють за кошти платників податків та дозволяють органам влади та їхнім структурним підрозділам забезпечувати функціонування держави.

На разі, в Україні усі публічні закупівлі проводяться на спеціалізованому майданчику Prozorro, основою якого є прозорість публічних закупівель. За 2022 рік в системі Prozorro відбулося 160 тисяч конкурентних закупівель майже на 200 млрд грн (*Річний звіт Prozorro за результатами 2022 року*, б. д.). Хоча створення й впровадження такої системи значно зменшило прояви корупції та порушень в публічних закупівлях, це не дозволило позбутися їх взагалі. Учасники закупівель, яким це вигідно, пристосувалися до системи та знаходять способи здійснення вигідних махінацій. Національне

агентство з питань запобігання корупції виділило такі найпоширеніші корупційні ризики пов'язані з публічними закупівлями (НАЗК, б. д.):

– завищення очікуваної вартості та обсягів закупівлі;
– штучне розділення предмета закупівлі для уникнення конкретних процедур;
– дискримінаційні умови у тендерній документації та штучне обмеження конкуренції;
– необгрунтоване застосування переговорної процедури закупівлі;
– необ'єктивність, необгрунтованість та упередженість під час розгляду тендерної пропозиції;
– вимога паперової документації у складі тендерної пропозиції та зразків товару (продукції);
– необгрунтоване внесення змін до договору про закупівлю через укладення додаткових угод;
– недопостачання товарів (робіт/послуг), або приймання продукції, яка не відповідає умовам договору.

Паралельно з впровадженням платформи для електронних закупівель був розроблений моніторинговий портал Dozorro. Через деякий час моніторинговий портал був посилений технологіями штучного інтелекту. Таким чином, була створена програма, яка навчається фіксувати закупівлі з корупційними ризиками. Навчання штучного інтелекту розпочалося з того, що розробники надіслали на опрацювання 20 експертам близько 3500 різних закупівель, при цьому, для об'єктивності, були приховані суми закупівель та імена замовників. Результати цього експертного опитування були використані для навчання штучного інтелекту. Система самостійно намагалася визначити закупівлі з корупційними ризиками та надсилала результати громадським організаціям Dozorro-спільноти. Якщо порушення підтвердилися програма запам'ятовувала свій вибір, таким чином відбувалося постійне навчання штучного інтелекту. З часом система Dozorro стала більш гнучкою й здатною виявляти нові порушення в системі. Як зазначав розробник Володимир Фльонц «Як тільки експерти та громадські активісти побачать, що з'явилися нові «алгоритми зради», система автоматично перебудовується».

Такого роду моніторингова система це дійсно важливий крок на шляху до подолання корупції в публічних закупівлях, але виявлення порушень у веденні закупівель не означає боротьбу з корупцією. Важливо не тільки виявляти такі випадки, а й застосовувати певні заходи до порушників. Так, наприклад, якщо виявляється порушення і учасник вважає, що замовник порушив його права, він може звернутися до Колегії АМКУ, яка займається розглядом скарг. Якщо скарга була прийнята і підтверджений факт порушення Колегія АМКУ може вжити конкретних заходів, наприклад змінити тендерну документацію, скасувати процедуру, скасувати рішення відхилення учасника

чи призначення переможця та інше. Встановленням факту антиконкурентних дій учасників чи змови між учасником та замовником займається сам Антимонопольний комітет, або його відділи.

Додатково платформа Dozorro пропонує низку таких аналітичних інструментів, як Публічний модуль аналітики, Професійний модуль аналітики та Медичний модуль аналітики. Ці аналітичні інструмент дають змогу більш детально досліджувати та аналізувати публічні закупівлі, використовуючи вбудовані графіки та таблиці.

Ще одним прикладом використання штучного інтелекту в публічній сфері є сервіс для громадського контролю публічних витрат бразильських парламентарів Serenata.ai, який забезпечений моделлю штучного інтелекту Rosie, що аналізує витрати та виявляє серед них підозрілі (*Як штучний інтелект використовується у сфері відкритих даних*, б. д.). Загалом впродовж часу існування системи було надіслано понад 600 скарг щодо майже 630 підозрілих витрат на суму понад 65,5 тис. дол. Хоча цей приклад не стосується безпосередньо публічних закупівель, але схожі системи можуть бути застосовані для виявлення корупційних ризиків в публічних закупівлях.

Отже, підсумовуючи можемо стверджувати про важливість використання додаткових інструментів моніторингу публічних закупівель та виявлення випадків корупції чи порушень. Хоча електронний формат ведення закупівель й зробив цей процес більш прозорим та зменшив ризики корупції, все ж таки випадки порушень у веденні закупівель часто зустрічаються і тому, застосування такого інструменту як штучний інтелект може значно збільшити ефективність процесу моніторингу й виявлення випадків корупції.

Список літератури

1. *Реформа Державних Закупівель*. (б. д.). Міністерство економіки України. https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=38c083f3-2571-466a-9583-3b43c2804ad9&title=ReformaDerzhavnikhZakupivel

2. European Added Value Unit. (2023). *Stepping up the EU's efforts to tackle corruption* (Cost of NonEurope Report).

3. *Річний звіт Prozorro за результатами 2022 року*. (б. д.). Інформаційний ресурс – Інфобокс Прозорро. https://infobox.prozorro.org/articles/richniy-zvit-prozorro-za-rezultatami-2022-roku

4. *НАЗК визначило 25 типових корупційних ризиків у публічних закупівлях.* (б. д.). НАЗК. https://nazk.gov.ua/uk/novyny/nazk-vyznachylo-25-typovyh-koruptsijnyh-ryzykiv-u-publichnyh-zakupivlyah/

5. *Як штучний інтелект використовується у сфері відкритих даних*. (б. д.). Дія.Відкриті дані. https://diia.data.gov.ua/info-center/aiod

ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО І ЛЮДЕЙ

PROSPECTS FOR THE DEVELOPMENT OF THE DIGITAL ECONOMY AND ITS IMPACT ON SOCIETY AND PEOPLE

Владислава Лук'янова, *студентка*
Сумський державний університет, Україна
Валерій Яценко, *к. т. н, доцент*
Сумський державний університет, Україна

Сучасні реалії такі, що динамічний розвиток інформаційних технологій, повсюдне ускладнення бізнес-процесів, а також накопичення значних обсягів даних об'єктивно призвели до виникнення цифрової економіки. Цифровий тип економіки впливає на всі галузі без винятку, починаючи від роздрібної торгівлі й закінчуючи освітою, енергетикою тощо. Наступ нової цифрової економіки на позиції старої промислової є закономірним об'єктивно неминучим процесом.

Цифрова економіка є головним показником соціально-економічної сучасності, що впливає на всі сфери соціального життя. Місце країни у світовій спільноті визначає рівень впливу цифровізації як тенденції розвитку на національне, економічне та соціальне середовище.

Метою дослідження є аналіз перспективи розвитку цифрової економіки та її вплив на суспільство і людей.

Цифровізація – впровадження цифрових технологій, задля перетворення усіх державних послуг на зручні онлайн сервіси, веб-портали та платформи. Основна мета цифровізації полягає у трансформації існуючих та створенні нових галузей економіки, а також сфер життєдіяльності у нові більш ефективні та сучасні (What is digital economy?).

Унаслідок цифрового характеру розвитку економіки і суспільства ефективність розвитку інфокомунікацій виходить за рамки та має позагалузевий сумісний характер, що виявляється в інших сферах економіки, системі державного управління та соціальному житті населення. Інфокомунікаційний характер формування нового технологічного укладу і цифрової економіки зумовлює необхідність розробки новітньої цифрової реальності, науково-методичного супроводу системи управління в сполучених галузях діяльності та національній цифровій економіці загалом.

Цифрові технології дозволяють підприємствам здійснювати комерційну діяльність більш ефективно та рентабельно, відкриваючи безліч нових перспектив. Цифрова трансформація бізнесу та мережева організація платформної інфраструктури цифрової економіки зумовлюють зближення

галузей, стирання кордонів бізнесу, зростання масштабів і синергетичної ефективності цифрових компаній. Цифрові сервіси дозволяють сформувати великі системи, що підпорядковуються не теорії внутрішніх фірмових витрат, а законам ефективності мереж та інформаційних технологій.

Крім того цифрова економіка створює нові проблеми й виклики перед суспільством та державою у сферах безпеки, соціальної трансформації, сталого суспільного розвитку.

Кібератаки на державні та комерційні органи, крадіжка інформації, особистих даних є одними з основних проблем при переході до інформаційного суспільства. Аналіз світового досвіду із забезпечення кібербезпеки критичної інфраструктури свідчить, що будь-яка держава, при переході до цифровізації, має зосередити свої зусилля на убезпеченні своїх інформаційних активів. Особливо це актуально для України, адже інформаційні небезпеки у сфері економічної діяльності наразі є аспектами проблеми державної цілісності. Україні потрібно на державному рівні вирішувати питання щодо зміни надлишкових застарілих потоків інформації на новітні , які можуть забезпечити сталий економічний розвиток.

Міжнародна організація OECD (Organisation for Economic Co-operation and Development) виділяє три основні компоненти цифрової економіки:

– підтримуюча інфраструктура або (апаратне та програмне забезпечення, телекомунікації, мережі та ін.);

– електронний бізнес або e-business бізнес (ведення господарської діяльності та бізнесу через комп'ютерні мережі);

– електронна комерція або e-commerce (логістика товарів через Інтернет) (Digital Economy – Ukraine).

В Україні найбільший попит в цифрових технологіях припадає на агропромисловий сектор, завдяки яким передові компанії збільшують свій рівень прибутковості до 90%. Для медицини цифрова економіка означає послідовний перехід до онлайн-медицини. Приміром, на заміну медичного огляду передбачається використання сенсорів і датчиків онлайн-спостереження та використання системи, що забезпечує автоматизацію ведення обліку медичних послуг в електронному вигляді. Для освіти цифрова економіка – це запровадження цифрової освіти, коли учень має в школі доступ до Wi-Fi, електронні підручники, планшет, мультимедійний контент і т.д.

Впровадження новітніх технологій, якість інтернет-інфраструктури та інноваційний клімат – це ті напрями, які мають спонукати розвиток цифрової економіки в Україні. Першочерговою стратегією розвитку цифрової економіки в Україні має стати «цифровізація» країни, формування внутрішнього ринку інформаційно-комунікаційних технологій та мотивацій і потреб споживачів у «цифрових технологіях». Цивілізована цифрова інфраструктура – база розвитку цифрової економіки. Однак, за даними рейтингу Всесвітнього

економічного форуму щодо технологічного розвитку, який включає технологічну адаптацію та використання ІКТ, Україна посіла лише 85 місце серед інших країн. Для визначенні рейтингу використовують чотири показники: кількість інтернет-користувачів, підключення до широкосмугового Інтернет, пропускна спроможність Інтернету та мобільні підключення до широкосмугового зв'язку.

В перспективі Україні потрібні значні обсяги інвестицій, зокрема в розвиток Big Data, CRM-технологій, HR-процесів, Інтернету речей, штучного інтелекту, хмарних технологій тощо. Для державної влади актуальними є розширення сектору послуг цифрового уряду, електронної митниці, проведення цифрового перепису населення, використання технологій «смарт-сіті», створення робочих місць, розвиток освіти, охорони здоров'я, громадської безпеки, транспорту та охорони навколишнього середовища тощо.

Україна визначила цифрову трансформацію як пріоритет політики, що відзначено успіхами у впровадженні систем ProZorro та eHealth, покриттям мобільного зв'язку 4G та запровадженням електронних послуг у державному та приватному секторах. Цифровізація України відбувається спільними зусиллями експертів та бізнес-спільноти.

У пріоритетах цифрових перспектив України залишаються законодавство про цифрову економіку та телекомунікації, цифрову інфраструктуру, включаючи стратегію широкосмугового зв'язку, програму безготівкової економіки в сферах електронної торгівлі, електронної довіри та кібербезпеки, а також ініціативу «Розумні міста – розумні регіони», спрямовану на децентралізацію та впровадження електронних навичок, електронної охорони здоров'я та eTrade по регіонах України (Ukraine – EU4Digital).

Отже, цифрова економіка – потужний домінуючий компонент соціально-економічного розвитку, джерело надходження активів та гарантія політичної стабільності в державі. Незважаючи на те, що процес трансформації в нашій державі тільки починається, економіка України не стоїть осторонь від світових тенденцій, прагнучі активної інтеграції у світове суспільство.

Список літератури

1. What is digital economy? | Deloitte Malta | Technology. (б. д.). Deloitte Malta. URL: https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html.

2. Digital Economy – Ukraine | Statista Market Forecast. (б. д.). Statista. URL: https://www.statista.com/outlook/co/digital-economy/ukraine#internet-penetration.

3. Ukraine – EU4Digital. (б. д.). EU4Digital. URL: https://eufordigital.eu/countries/ukraine.

РОЗВИТОК ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

DEVELOPMENT OF ELECTRONIC COMMERCE IN THE DIGITAL ECONOMY

Дмитро Діденко, *студент,*
Сумський державний університет
Світлана Коломієць*, к.ф-м.н., доцент*
Сумський державний університет

Прискорений розвиток інформаційних технологій, використання інформаційних технологій для виготовлення та реалізації товарів і послуг, надання державних послуг, освіти громадян, розвиток електронної комерції – основні риси сучасного стану цифрової економіки.

Серед основних компонентів цифрової економіки - підтримуюча інфраструктура (апаратне та програмне забезпечення, телекомунікації, мережі тощо); електронний бізнес (реалізація господарської діяльності та бізнес-процесів через комп'ютерні мережі); електронна комерція (Digital enablers of the global economy).

Електронна комерція (e-commerce) є однією з ключових складових цифрової економіки і відіграє важливу роль у сучасному бізнесі. Вона охоплює процес купівлі, продажу та обміну товарів і послуг через мережу Інтернет.

Цифрова економіка розширює можливості для підприємств здійснювати торгівлю на міжнародному рівні без фізичних обмежень. Електронна комерція дозволяє компаніям розповсюдити товари на глобальні ринки і залучати клієнтів з усього світу.

Електронна комерція забезпечує зручність та доступність споживачів до здійснення онлайн-послуг та робить процес покупки швидшим і зручнішим.

Електронна комерція відкриває можливості для компаній представляти широкий асортимент товарів і послуг на своїх веб-сайтах або платформах електронної комерції. Це дозволяє споживачам мати доступ до різноманітних пропозицій і здійснювати вибір з більшого числа варіантів.

Застосування технологій штучного інтелекту і аналізу даних у електронній комерції дозволяє створювати персоналізовані рекомендації та пропозиції для споживачів. Базуючись на попередніх покупках, вподобаннях та поведінці клієнта, компанії можуть надавати індивідуальні рекомендації, що збільшує шанси на здійснення покупки.

За останні роки спостерігається зростання використання мобільних пристроїв для здійснення покупок. Користувачі все частіше використовують смартфони і планшети для перегляду товарів, замовлень та оплати. Тому

розробка мобільних додатків та оптимізація веб-сайтів для мобільних пристроїв стає все більш важливою для бізнесу.

Характерна риса сучасного стану розвитку електронної комерції - зростання екосистем онлайн-торгівлі. Онлайн-платформи розширюють свої екосистеми, надаючи користувачам широкий спектр послуг. Онлайн-платформи пропонують не лише товари, а й широкий спектр послуг, зокрема доставку, фінансові та маркетингові рішення. Це створює зручність для покупців та забезпечує додаткові можливості для бізнесів.

Забезпечення безпеки та довіри є важливим аспектом сучасної електронної комерції. Компанії приділяють значну увагу захисту персональних даних клієнтів, забезпеченню безпечних платежів та захисту від шахрайства. Розвиток технологій шифрування та інших заходів безпеки є ключовими для підтримки довіри споживачів.

Загалом, електронна комерція в умовах цифрової економіки надає більше можливостей для бізнесу та споживачів. Вона дозволяє підприємствам розширити свою аудиторію, забезпечує споживачам зручність та доступність при покупках, індивідуальність пропозицій та безпеку транзакцій.

На сьогоднішній день одним з найбільш ефективних рішень у сфері електронної комерції є використання веборієнтованих інформаційних систем. Такі системи дозволяють зібрати весь асортимент товарів на одному сайті, що забезпечує клієнтам легкий доступ до всієї інформації про товар, можливість замовлення безпосередньо на сайті магазину. Важливою перевагою веборієнтованих систем є також те, що всі дані про товар зберігаються в одній базі даних, що забезпечує їх зручну обробку та аналіз.

Веборієнтована система сприяє автоматизації багатьох рутинних завдань, зокрема обліку товарів, замовлень, платежів тощо. Така система забезпечує можливість збільшення обсягів продажів шляхом залучення нових клієнтів та покращення взаємодії з наявними клієнтами через персоналізовані пропозиції, акції та знижки.

Розуміння актуальних тенденцій у галузі веб-розробки, використання сучасних інструментів та технологій дозволяє досягти успішних результатів у створенні веб-систем, що відповідають вимогам сучасного ринку та забезпечують конкурентні переваги.

Список літератури

1. Digital enablers of the global economy. OECD iLibrary. https://www.oecd-ilibrary.org/science-and-technology/digital-enablers-of-the-global-economy_f0a7baaf-en

2. Дейтон Т. & Котлер Ф. (2021). Маркетингові дослідження: Стратегічне планування, збір та аналіз даних, інтерпретація результатів. Київ: Видавничий дім "Ін Юре".

3. Росс, Д., & Вебер, Р. (2021). Управління базами даних: Завдання, методи і засоби. Київ: Видавничий дім "Ін Юре".

ВПЛИВ ЦИФРОВОЇ ЕКОНОМІКИ НА СТАН ГРОМАДСЬКОГО ЗДОРОВ'Я НАСЕЛЕННЯ

IMPACT OF THE DIGITAL ECONOMY ON THE PUBLIC HEALTH

Ілля Лубенець, *студент,*
Сумський державний університет
Світлана Коломієць*, к.ф-м.н., доцент*
Сумський державний університет

Надшвидкий розвиток цифрових технологій впливає на всі сфери економіки. Вплив цифрової економіки на стан громадського здоров'я є актуальною та складною проблемою, яка вимагає детального дослідження та аналізу.

За визначенням Всесвітньої організації охорони здоров'я (ВООЗ), громадське здоров'я – це мистецтво та наука профілактики захворювань, продовження тривалості життя та промоції здоров'я через організовані зусилля суспільства.

Громадське здоров'я – це сукупність загальної політики в галузі охорони здоров'я та розподілу ресурсів; політики управління в системі охорони здоров'я; заходів, спрямованих на захист здоров'я населення, запобігання захворюванням, травматизму, інвалідності, смерті; промоції здорового способу життя; збереження здорового середовища й умов життя для теперішнього та майбутніх поколінь тощо (World Health Organization).

Місія громадського здоров'я – максимально поліпшити здоров'я та добробут людей та громад на національному та глобальному рівнях. У центрі уваги охорони громадського здоров'я знаходиться весь спектр здоров'я і благополуччя, а не викорінення лише окремих хвороб.

Система громадського здоров'я розглядається як основа профілактичної медицини, що передбачає основні заходи у сфері охорони здоров'я спрямовані на збереження здоров'я населення та зменшення витрат на медичне обслуговування (Півень, 2020).

Громадське здоров'я обумовлене комплексною дією соціальних, поведінкових, біологічних та інших детермінантів. ВООЗ розглядає детермінанти здоров'я як комплекс індивідуальних, соціальних, економічних, екологічних факторів, які впливають як на стан здоров'я окремих людей, так і груп населення.

Детермінанти громадського здоров'я включають широкий спектр фізичних, соціальних, економічних, культурних чинників, що взаємодіють між собою та впливають на рівень здоров'я населення.

Соціально-економічні детермінанти громадського здоров'я визначаються соціальними та економічними умовами, в яких живе людина. Ці детермінанти включають широкий спектр факторів, які впливають на здоров'я та хвороби на рівні спільноти і національного рівня.

Соціальні детермінанти громадського здоров'я включають такі фактори, як освіта, рівень доходу, умови праці, житлові умови, доступ до послуг охорони здоров'я та соціальної підтримки тощо. Зокрема, низький рівень освіти може призвести до обмеженого доступу до інформації щодо здоров'я, незнання профілактичних заходів та непродуктивних здорових звичок. Нерівність у розподілі доходів може впливати на доступ до якісної медичної допомоги та засобів для здорового способу життя тощо.

Економічні детермінанти громадського здоров'я охоплюють різні чинники, зокрема рівень економічного розвитку, зайнятість населення, інфраструктура, інвестиції в охорону здоров'я, соціальний захист тощо. Соціально-економічні детермінанти громадського здоров'я взаємодіють між собою та мають кумулятивний вплив на здоров'я населення.

Як підкреслюється в документах ВООЗ, метою дій урядів країн світу, спрямованих на зміцнення потенціалу та послуг охорони громадського здоров'я, є забезпечення умов, за яких люди можуть залишатися здоровими, зміцнювати своє здоров'я і благополуччя або попереджати погіршення здоров'я.

Цифровізація економіки відкриває нові можливості для системи громадського здоров'я, зокрема

– дозволяє поліпшити доступність та ефективність медичних послуг для населення через використання онлайн-платформ та електронної медичної документації;

– дозволяє забезпечити медичне обслуговування віддаленим регіонам, зменшуючи географічні та доступові обмеження;

– сприяє покращенню обміну медичною інформацією та співпраці між медичними закладами та фахівцями, що дозволяє раціональніше використовувати ресурси системи охорони здоров'я;

– надає можливість швидкого доступу до різноманітної медичної інформації, онлайн-консультацій та мобільних додатків для здоров'я;

– сприяє досягненню більш високого рівня обізнаності населення щодо здорового способу життя через використання інтернет ресурсів, мобільних додатків, соціальних мереж тощо;

– аналіз великих обсягів медичних даних за допомогою алгоритмів штучного інтелекту та машинного навчання надає можливість виявляти паттерни, тенденції та ризикові групи для розвитку захворювань.

Цифрова економіка надає можливість значно покращити рівень громадського здоров'я в Україні, проте важливо враховувати певні виклики, а

також етичні, правові та соціальні аспекти, забезпечити рівний доступ та захист прав громади в цифровому просторі.

Серед основних викликів цифровізації сектору охорони здоров'я

– захист конфеденційної інформації під час збору, обробки та збереження великого масиву медичних даних;
– ризики витоку персональних даних, зловживання медичною інформацією;
– можливість кібератак;
– нерівний доступ до інформаційних технологій, низька цифрова грамотність різних вікових груп населення, що може створювати нерівності в доступі до системи охорони здоров'я;
– можливість поширення через мережу інтернет недостовірної, некоректної інформації щодо здоров'я населення;
– підвищення цифрової грамотності працівників сфери охорони здоров'я;
– необхідність вирішення питань щодо нормативно-правового регулювання та стандартизації в галузі цифрового здоров'я тощо.

Цифровізація сфери громадського здоров'я вносить виклики, які потребують належного вирішення, що сприятиме успішній трансформації системи громадського здоров'я в епоху цифрової економіки.

Вплив цифрової економіки на рівень громадського здоров'я в Україні дуже тісно пов'язаний з розвитком цифрової інфраструктури, доступом до інформаційних технологій, розвитком системи електронного здоров'я, підвищенням рівня електронної грамотності та забезпеченням цифрової безпеки в сфері охорони здоров'я, що вимагає проведення подальших наукових досліджень та впровадження результатів дослідження в практичну діяльність.

Список літератури

1. Public health services. World Health Organization. URL: https://www.euro.who.int/en/health-topics/Healthsystems/public-health-services (date of access: 2.05.2023).
2. Півень Н. В. (2020). Операційний посібник «Розробка та фінансування регіональних і місцевих програм громадського здоров'я».
3. Koibichuk, V., Kolomiiets, S., Drozd, S. (2022). Public health system effectiveness: determinants and impacts. Szczecin: Centre of Sociological Research, p. 135. DOI: 10.14254/978-83-966582-7-2/2022.

СЕКЦІЯ 2 КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

АНАЛІЗ ВПЛИВУ ВЕЛИКИХ КІБЕРІНЦИДЕНТІВ НА АКЦІЇ КОМПАНІЇ

ANALYSIS OF THE IMPACT OF MAJOR CYBER INCIDENTS ON THE COMPANY'S STOCKS

Vadym Dun, *student*
Sumy State University, Ukraine
Serhii Mynenko, *PhD*
Sumy State University, Ukraine

In the modern world where information reigns supreme, cyber threats pose a significant risk to the financial stability and security of organizations. Data privacy and cybersecurity issues have emerged as major drivers of business risk in recent years. Major cyber incidents such as hacking, data breaches, and malware have the potential to cause significant financial losses and impact a company's stock price. Understanding the financial impact of such cyber incidents is crucial as it enables investors, financial analysts, and regulators to develop effective risk management strategies and make informed investment decisions. This analysis also contributes to the development of cybersecurity policies and practices at a global level by identifying vulnerabilities and deficiencies in data protection systems. Measures can be developed to prevent and respond to cyber threats while improving risk management practices in this area. This paper provides a basic overview of the aftermath of the 2017 Equifax cyberattack.

There are many definitions in this field, but let us focus on the following - major cyber incidents can be defined as serious breaches of information system security that lead to unauthorized access to sensitive data, information leakage, disruption of computer networks and serious consequences for organizations and individuals (NCSC, 2023). Such incidents can include hacking attacks, viruses, phishing attacks, data breaches, attacks on critical infrastructure, and other forms of cyber threats. They can occur either within a single organization or on a national or international scale.

In terms of company shares, first of all, they are a tool, and I play an essential role in the financial sector. They represent shares in companies that investors can buy. Stocks allow you to invest money and benefit from growth and dividends. They also reflect the capitalization of companies, which indicates their importance and attractiveness to investors. Changes in stock prices can be an indicator of economic health and market confidence. Companies may also issue new shares to raise additional capital. Stocks provide liquidity to the market,

allowing investors to buy and sell them. In general, stocks provide an investment opportunity, access to capital and serve as an indicator of the health of the economy.

But we are going to focus on a relatively recent incident that happened to Equifax. This situation is one of the most popular - this large-scale cyberattack compromised the personal information of approximately 147 million people. In the wake of the attack, Equifax's stock plummeted and the company faced significant financial and reputational losses, but let's go in order.

Equifax is a widely recognized multinational consumer credit reporting agency based in Atlanta, Georgia. It is one of the top three largest credit reporting agencies in the world, alongside Experian and TransUnion. With millions of consumers and businesses globally, Equifax collects and analyzes credit and demographic information. It offers credit monitoring, fraud prevention services, and data insights to both individuals and businesses. Notably, Equifax is a member of the S&P 500® Index, and its common stock is traded on the New York Stock Exchange under the symbol EFX. (Investopedia, 2023)

To avoid describing the details of the attack process itself, for easier understanding we can use the illustration by Government Accountability Office, based on information provided by Equifax (GAO, 2018):

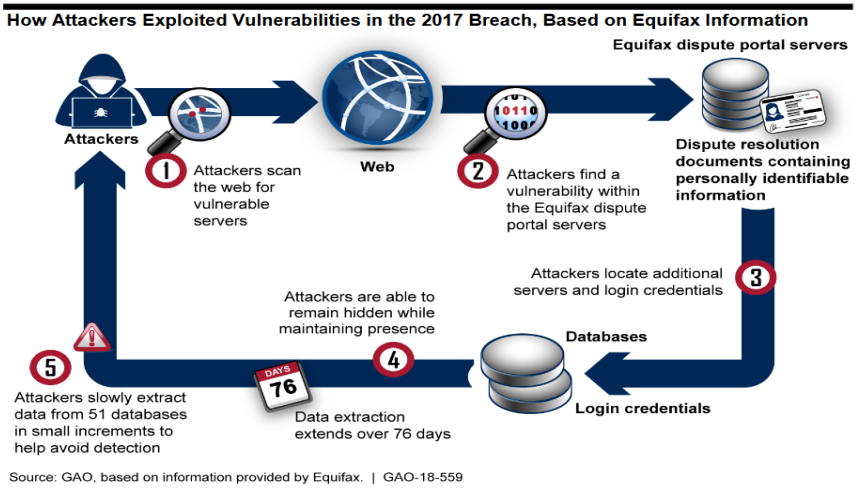

Figure 1. Scheme How Attackers Exploited Vulnerabilities

The announcement of the cyberattack triggered a negative reaction from investors and the market, resulting in a sharp drop in the stock price in the first two days after the announcement. The decline in the share price was more than 30%, a

significant drop. This indicates the seriousness and magnitude of the incident and caused a loss of investor confidence. The stock price continued to decline in the following weeks, with a total loss in value of approximately 35%. This share price decline reflects the serious negative impact of the cyberattack on the company's financial position and reputation in the market, and reputation is more important than anything else in our time, and investors simply do not want to take those risks and try to get out of the market as quickly as possible (Carsten Giebe, 2020). Below we can see the graphic (Investing.com, 2023):

Figure 2. Price History - NYSE:EFX

Following the decline in Equifax's stock price, the company faced a period of market volatility. Restoring investor and market confidence was paramount to the company's ability to halt this steep decline. According to the company's financial reports, Equifax reported a 2.7 percent decline in annual revenue compared to the previous year. The stock's drop wiped out about $6 billion of its market value This shows that the incident had a negative impact on the company's overall financial performance. (MarketWatch, 2017) The attack did not put the company out of business, but it did result in serious legal repercussions and a significant amount of compensation and fines - It is clear that ultimately good risk must result in increased profitability or company value. Most times this will be reflected in business and financial metrics such as profitability and company valuation. (E. Ted Prince, 2016) And until all these nuances are settled, we can't see any stability in the stock price, and it wasn't until 2019 that the company agreed to pay a $700 million fine to the U.S. Federal Trade Commission and other regulators. In addition, a $380.5 million restitution agreement was reached that

included cash payments to affected customers and expenses related to fraud protection and credit identity monitoring (Investopedia, 2023).

Summarizing all of the above, we can formulate a kind of prediction of the consequences of cyberattacks. The impact of these actions on stocks can be seen with the naked eye - in Equifax's experience, we can see that the company can lose up to 35% of shareholder value in an instant. Although the stock has recovered somewhat over time and with the implementation of security enhancements, the impact of the cyberattack has left a lasting impact on the company's reputation and financial performance. All of this suggests that cyber-attacks can have serious financial consequences for companies, including significant losses in stock value and the emergence of a period of market volatility. It is important to note that the change in Equifax's stock price as a result of the cyberattack is only part of the complex financial impact. The company also faced high investigation and remediation costs, fines and legal fees, and a loss of customer and market confidence. This case is an example of how cyber incidents can seriously impact a company's financial position and reputation, particularly in the context of our company's specific circumstances.

References

1. National Cyber Security Centre (2023). About NCSC: Incident Management. https://www.ncsc.gov.uk/section/about-ncsc/incident-management
2. Investopedia (2023). Top Three Credit Bureaus. https://www.investopedia.com/personal-finance/top-three-credit-bureaus/
3. Government Accountability Office. (2018). Equifax Data Breach: Actions Needed to Strengthen Response and Recovery Efforts. https://www.gao.gov/assets/gao-18-559.pdf
4. Carsten Giebe (Armg Publishing) (2020). Big Data & Analytics as a sustainable Customer Loyalty Instrument in Banking and Finance. https://armgpublishing.com/wp-content/uploads/2020/01/7-2.pdf
5. Investing.com (2023) Equifax, Inc. Stock Chart. https://ru.investing.com/pro/NYSE:EFX/charts
6. MarketWatch. (2017). Equifax's stock has fallen 31% since the breach disclosure. https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14
7. E. Ted Prince (Armg Publishing) (2016). Risk Management and Behavioral Finance. https://armgpublishing.com/wp-content/uploads/2016/12/files/fmir/volume-2-issue-2/1.pdf

РИЗИКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ У ТРАНСКОРДОННІЙ ЕЛЕКТРОННІЙ КОМЕРЦІЇ

THE RISKS OF ELECTRONIC PAYMENTS IN CROSS-BORDER E-COMMERCE

Kuan Zhang, *PhD student*
Sumy State University, Ukraine

Cross-border e-commerce has revolutionized the way businesses and consumers engage in international trade. Electronic payments play a pivotal role in facilitating these transactions, offering convenience, speed, and accessibility. However, along with the numerous benefits come inherent risks that must be addressed to ensure the security and trustworthiness of cross-border electronic payments [1]. This abstract explores the risks associated with electronic payments in cross-border e-commerce and discusses potential solutions to mitigate these risks.

1. Security Risks:

Electronic payments in cross-border e-commerce are susceptible to various security risks [2]. Payment information leakage, phishing attacks, and data breaches pose significant threats to the integrity and confidentiality of sensitive financial data. Cybercriminals employ sophisticated techniques to gain unauthorized access to payment details and exploit them for fraudulent activities. These risks undermine consumer trust and can lead to financial losses for both businesses and consumers.

To address security risks, robust measures should be implemented, such as using secure encryption protocols, adopting multi-factor authentication, and regularly updating payment platforms and systems with security patches. Additionally, educating users about best practices in maintaining strong passwords, identifying phishing attempts, and reporting suspicious activities can enhance overall security.

2. Fraud Risks:

Cross-border e-commerce opens avenues for fraud, including unauthorized transactions, chargebacks, and identity theft. Fraudulent activities can arise from stolen payment credentials, counterfeit products, or dishonest sellers misrepresenting their goods and services [3]. Such risks erode trust between buyers and sellers, tarnish reputations, and deter consumers from engaging in cross-border transactions.

To combat fraud risks, businesses must implement stringent verification processes, adopt risk assessment and monitoring systems, and establish clear refund and dispute resolution mechanisms. Utilizing advanced fraud detection technologies and collaborating with trusted payment service providers can help identify and prevent fraudulent activities promptly.

3. Compliance Risks:

Operating in cross-border e-commerce requires adherence to different international regulations and compliance standards. Payment service providers must comply with anti-money laundering (AML) and Know Your Customer (KYC) requirements. Failure to comply with these regulations can lead to legal repercussions, financial penalties, and reputational damage.

To mitigate compliance risks, businesses should conduct thorough due diligence on payment service providers, ensuring they have the necessary certifications, licenses, and regulatory compliance. Establishing internal controls, performing regular audits, and maintaining transparent transaction records can contribute to a compliant cross-border payment environment.

4. Payment Reconciliation Risks:

The complexity of cross-border e-commerce transactions can lead to challenges in payment reconciliation [4]. Differences in payment processing times, multiple intermediaries involved, and varying settlement cycles across countries can result in reconciliation discrepancies and potential cash flow disruptions.

To minimize payment reconciliation risks, businesses should implement robust payment tracking and reconciliation systems. Automation, integration with financial management platforms, and timely communication with payment service providers can streamline the reconciliation process and reduce potential errors and delays.

While electronic payments have revolutionized cross-border e-commerce, they also introduce inherent risks that must be proactively addressed [5]. Security risks, fraud risks, compliance risks, and payment reconciliation risks are among the key challenges that businesses and payment service providers face in this context. By implementing robust security measures, adopting fraud detection technologies, ensuring compliance with regulations, managing currency risks.

References

1. Liu, A., Osewe, M., Shi, Y., Zhen, X., & Wu, Y. (2021). Cross-border e-commerce development and challenges in China: A systematic literature review. *Journal of theoretical and applied electronic commerce research*, *17*(1), 69-88.

2. Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security*, *24*(1), 10-15.

3. Kovacs, L., & David, S. (2016). Fraud risk in electronic payment transactions. *Journal of Money Laundering Control*, *19*(2), 148-157.

4. Trautman, L. J. (2015). E-Commerce, cyber, and electronic payment system risks: lessons from PayPal. *UC Davis Bus. LJ*, *16*, 261.

5. Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018, December). A review of e-payment system in e-commerce. In *Journal of Physics: Conference Series* (Vol. 1140, No. 1, p. 012033). IOP Publishing.

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ

INTERNATIONAL COOPERATION IN THE FIELD OF CYBER SECURITY: CHALLENGES AND OPPORTUNITIES

Анна Голопьорова, *студентка*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н, доцент*
Сумський державний університет, Україна

Швидкий розвиток сучасних технологій породжує й нові загрози для інформаційної безпеки сфер діяльності держави. Наразі кіберпростір є необмеженим та вимагає значної співпраці з боку різних країн для усунення кіберризиків, що також не залишаються на місці. Складність кібератак зростає з розвитком технологій. В умовах глобалізації і взаємозалежності країн, жодна держава не може впоратися з цими проблемами самостійно та гарантувати безпеку свого кіберпростору. Співпраця між країнами, міжнародними організаціями та приватним сектором є ключовим фактором успіху в боротьбі з кіберзагрозами. Ефективне міжнародне співробітництво є важливим елементом для розробки протидії кіберзагрозам та покращення безпеки країн та подальшого безпечного розвитку різних сфер людської діяльності.

Метою дослідження є обґрунтування необхідності подолання загроз у кіберпросторі з якими стикаються країни шляхом міжнародної співпраці та можливості, шляхи, виклики міжнародної співпраці у боротьбі з кіберзагрозами.

Впровадження інформаційно-телекомунікаційних технологій в різноманітні сфери людської діяльності країнами по всьому світу впливають на необхідність протидії кіберінцедентів та кіберзлочинів, що зростають у кількості та урізноманітнюються. Такий прискорений розвиток та підвищення загрози спонукають країни до співпраці.

Міжнародна співпраця в сфері кібербезпеки є пріоритетним для багатьох країн, в тому числі й в Україні, яка бореться ще й з проблемами внаслідок гібридної війни з РФ та масовими кібератаками. Така політика подана в статті 14 Закону України «Про основні засади забезпечення кібербезпеки України». За законом «Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю» [1].

На сьогоднішній день існує ряд міжнародних угод та конвенцій, спрямованих на боротьбу з кіберзлочинністю та захист кіберінфраструктури.

Однак, виникають проблеми в їхньої реалізації та виконанні, оскільки кожна країна має свою національну законодавчу базу та політику в цій сфері. Співробітництво між країнами та гармонізація правових норм можуть забезпечити ефективнішу протидію кіберзагрозам. Розробка міжнародних норм та стандартів є однією з ключових можливостей міжнародного співробітництва в галузі кібербезпеки. Узгоджені міжнародні норми та стандарти сприяють спільним підходам до кібербезпеки, поліпшенню взаємодії між країнами та створенню загального розуміння щодо викликів у кіберпросторі.

До інших викликів у сфері міжнародного співробітництва у кібербезпеці належить складність атрибуції та ідентифікації кіберзлочинців. Часто кібератаки вчиняються через хостингові платформи в інших країнах або з використанням анонімних мереж, що ускладнює процес виявлення та притягнення винних до відповідальності. Співробітництво у сфері кібербезпеки має включати обмін технічною інформацією та розвиток механізмів для спільного розслідування та притягнення злочинців до відповідальності.

Важливу роль у забезпеченні міжнародного співробітництва в сфері кібербезпеки займають міжнародні організації. Тут значну увагу варто приділити ООН. Безпека кіберпростору відіграє важливу роль у досягненні Цілей сталого розвитку ООН. ООН сприяє використанню інформаційних технологій для соціального та економічного розвитку, але одночасно акцентує увагу на необхідності забезпечення кібербезпеки для запобігання кіберзлочинності та захисту прав людини в кіберпросторі.

Наразі також триває процес обговорення необхідності створення єдиного кіберпростору – «Cyber United Nations». Така ініціатива була запропонована Україною та має за мету підвищення протидії кібератак для всіх країн шляхом об'єднання зусиль. Дана пропозиція свідчить про продовження та посилення співпраці країн та важливої ролі й нашої країни в процесах посилення безпеки.

Позитивні наслідки міжнародної співпраці прослідковуються також в рамках ЄС (яскравий приклад співпраці в межах країн, що належать до союзу та активно співпрацюють для покращення та посилання міжнародного співробітництва в межах своїх країн), НАТО (розглядає кіберпростір як важливий елемент військової сфери та вважає необхідним його регулювання в рамках міжнародного співробітництва задля безпеки), ОБСЄ (виступає платформою для обміну інформації, розвиває стратегії та взаємодіє з іншими організаціями.

Співпраця в межах наведених країн показує ефективність сумісної боротьби проти загроз кіберпростору та необхідність обміну інформацією про нові загрози та практичні методи для їх протидії. Співробітництво між НАТО, ОБСЄ та ЄС не обмежується власними межами, але також включає партнерські

взаємини з іншими країнами та організаціями. Це сприяє зміцненню глобальної співпраці в сфері кібербезпеки та забезпеченню безпеки в кіберпросторі.

При цьому можливою є співпраця не лише організацій, а й країн окремо. Через війну в Україні та необхідність посилення безпеки кіберпростору країни, розпочато співробітництво з США. Така практика показує переваги співробітництва інших поза рамками організації та дієвість і такого методу сумісного захисту.

Одним з можливих напрямків співробітництва є створення міжнародних центрів реагування на кіберзагрози. Ці центри можуть об'єднувати фахівців та ресурси з різних країн для оперативного реагування на кібератаки та координації заходів з кібербезпеки. Вони можуть стати платформою для спільного розроблення та обміну інформацією про нові загрози, а також для проведення тренувань та навчання фахівців.

Взаємодія з приватним сектором є також важливим аспектом міжнародного співробітництва в галузі кібербезпеки. Компанії, що спеціалізуються в інформаційно-комунікаційних технологіях, мають значний вплив на кібербезпеку та можуть сприяти досягненню спільних цілей. Заохочення співпраці з приватним сектором може включати створення платформ для обміну інформацією та розробки спільних стратегій. Важливо залучати приватні компанії до діалогу з урядами та міжнародними організаціями з метою обговорення проблем кібербезпеки та спільного розроблення рішень. Таким чином можна отримати повне бачення ситуації пов’язаної з кіберпростором та покращити безпеку шляхом повної співпраці.

У підсумку, міжнародне співробітництво у сфері кібербезпеки виступає необхідною умовою для забезпечення безпеки в цифровому просторі. Наразі країни вже практикують співпрацю в межах міжнародних організацій та поза ними, однак можливості та необхідність в повній співпраці ще не вичерпані. Виклики, пов'язані з кіберзагрозами, вимагають спільних зусиль та координації для злагодженої роботи. Обмін інформацією, розробка спільних регулюючих документів з урахуванням сучасних стандартів протидії кіберзагроз, розширення технологічного співробітництва – основні можливості міжнародної співпраці. Тільки шляхом спільних зусиль можна забезпечити стійку та безпечну кіберінфраструктуру для майбутнього розвитку всіх сфер людської діяльності.

Список літератури

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 45 : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 29.05.2023).

КІБЕРБЕЗПЕКА У МЕРЕЖАХ 5G: ПРАКТИЧНІ ВИКЛИКИ ТА РИЗИКИ

CYBERSECURITY IN 5G NETWORKS: PRACTICAL CHALLENGES AND RISKS

Олександр Воробйов, *студент*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н, доцент*
Сумський державний університет, Україна

Поява бездротової технології п'ятого покоління, має значно пришвидшити передачу даних на телефони та з них, більш ширше покриття та стабільний зв'язок, а саме досконаліше використання радіо діапазону та можливості одночасного доступу до мобільного інтернету більшої кількості пристроїв.

Технологія 5G як нова і проривна технологія, що широко розповсюджується, домінуватиме у сфері цивільних телекомунікацій у майбутньому і стане основою суспільства (Fulton, 2021).

Мережі 5G значно швидші, ніж їх попереднє покоління 4G, це дає можливість користувачам отримувати більшу кількість даних за менший час. Це дуже корисно в широкому спектрі діяльності, від потокового медіа до гри в онлайн-ігри. Але це також створює дуже великий ризик для безпеки. Адже швидше передається більша кількість даних, зловмисники мають більше можливостей для перехоплення та використання конфіденційної інформації.

Мережі 5G більш вразливі, ніж їх попередники. Вони призначені для обробки великої кількості даних. Розгортання 5G мереж, поряд з безпрецедентними можливостями, потенціює зростанню існуючого рівня кіберзагроз і створює нові виклики, що робить їх привабливими цілями для зловмисників

Метою дослідження є аналіз практичних викликів та ризиків кібербезпеки у мережах 5G.

Одна з найголовніших переваг рішень для забезпечення безпеки 5G є надання кращого захисту даних. Оскільки мережі 5G обробляють більшу кількість даних, компаніям потрібно забезпечити більш безпечну передачу даних між різними пристроями. Рішення безпеки 5G забезпечують розширені можливості шифрування, автентифікації та виявлення вторгнень для захисту даних. Це дає гарантії, що до особистих даних не зможуть отримати доступ неавторизовані особи.

Іншою важливою перевагою рішень безпеки 5G є підвищена конфіденційність. Мережі 5G мають можливість передавати величезну

кількість даних, і компаніям потрібно вживати заходів, щоб надати надійнішу безпеку цих даних. Для безпеки 5G мають такі функції, а саме наскрізне шифрування, автентифікація користувачів і брандмауери для захисту даних від несанкціонованого доступу.

При передачі великої кількості даних, зростає кількість ризиків.

Потенційним ризиком для безпеки мереж 5G є висока ймовірність витоку даних. Адже мережі 5G, забезпечують більш високі швидкості, зловмисники можуть легко та швидко отримати доступ до конфіденційних даних, які зберігаються в мережах. Це може зробити підприємства чи особу вразливими до крадіжки даних, маніпуляцій та інших моментів.

Іншим потенційним ризиком для безпеки мереж 5G є підвищений ризик розподілених атак на відмову в обслуговуванні (DDoS). DDoS-атаки – це різновид кібератак, під час яких зловмисник намагається перевантажити систему запитами, щоб порушити її служби. Завдяки мережам 5G, які забезпечують більш високі швидкості та надійніші з'єднання, DDoS-атаки можуть бути потужнішими та важчими для захисту.

Також, мережі 5G також представляють потенційну можливість для зловмисників використовувати збільшені швидкості та надійність для здійснення більш потужних і складних кібератак. Ці атаки можуть використовуватися для націлювання на критичну інфраструктуру, викрадення конфіденційних даних або порушення роботи служб. Мережі 5G використовують кілька діапазонів радіочастот, які може бути важко відстежити. Це означає, що зловмисники можуть діяти з різних місць, що ускладнює виявлення та стримування їхньої діяльності (Lin et al., 2021).

Отже, мережі 5G пропонують переваги, такі як більш висока швидкість і надійніше з'єднання, але також пов'язані з підвищеними ризиками. Мережі 5G також дають можливість зловмисникам використовувати збільшені швидкості та надійність для проведення більш складного та цілеспрямованого спостереження. Це може включати відстеження місцезнаходження окремих осіб або моніторинг їх активності в Інтернеті. Крім того, оскільки технологія 5G є відносно новою, існує недостатнє розуміння та усвідомлення пов'язаних з нею ризиків безпеки.

Щоб позбутися потенційних ризиків в безпеці, потрібно вжити заходів безпеки для захисту мереж 5G. Таких як, впровадження надійніших протоколів шифрування, моніторинг мереж на наявність підозрілої активності та регулярне оновлення заходів безпеки. Це забезпечить безпеку мереж 5G і забезпечить користувачам очікувану швидкість і надійність. В країнах ЄС повинні обмінюватися даними щодо ризиків кібербезпеки мереж 5G, а також розробити заходи для їх подолання.

Технологія 5G має великий потенціал для революції у варіантах передачі та зберігання даних, також в майбутньому використовувати для

посилення стратегій кібербезпеки, такі як розробка нових правил , що до конфіденційності та захисту даних наприклад Загальний регламент захисту даних Європейського Союзу (GDPR). Але повний потенціал 5G для підвищення безпеки буде реалізований лише в тому випадку, якщо постачальники послуг та інші зацікавлені сторони запровадять ефективні протоколи безпеки.

Список літератури

1. Fulton, S. (2021). What is 5G? Your guide to the current generation of wireless communications. ZDNET. URL: https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/

2. Lin, Z., Perine, C., Vosseler, R., Lin, W. (2021). Attacks from 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Networks – IIoT World. (б. д.). IIoT World. URL: https://www.iiot-world.com/ics-security/cybersecurity/attacks-from-4g-5g-core-networks-risks-of-the-industrial-iot-in-compromised-campus-networks/

КІБЕРБЕЗПЕКА БІЗНЕСУ МАЛИХ ТА СЕРЕДНІХ ПІДРПРИЄМСТВ: ДОСВІД ЄС

CYBERSECURITY OF SMALL AND MEDIUM-SIZED ENTERPRISES: EU EXPERIENCE

***Віталія Койбічук**, к.е.н, доцентка*
Сумський державний університет, Україна

З розвитком процесів діджиталізації розвиваються й кіберзагрози й кіберзлочинні схеми, особливо у фінансових системах та індрустрії фінансових послуг, включаючи, але не обмежуючись, послуги інтернет-банкінгу, необанкінгу та грошові перекази, роздрібні платіжні системи, мобільні банківські та платіжні системи, цифрові валюти та інші фінансові послуги. Ці загрози включають крадіжку інформації та коштів клієнтів, відмивання грошей, несанкціоновані перекази та інші зловмисні дії, відмову в обслуговуванні, впровадження шкідливих програм, програм-вимагачів, фішинг, соціальну інженерію та витоки даних. Атаки на фінансові установи можуть мати серйозні ризики для безпеки клієнтів, операцій і фінансів (Kuzmenko et. al, 2021). Тому, надзвичайно важливим для компаній, банків, фінансових установ, підприємств, (всіх соціально-економічних об'єктів) стежити за станом своєї кібербезпеки та мати надійний захист від потенційних атак, а також повинні застосовувати безпечні методи автентифікації клієнтів і шифрування даних, щоб захистити конфіденційні дані клієнтів. Зокрема, Агентство Європейського Союзу з кібербезпеки (ENISA) рекомендує дотримуватися 12 кроків для якісної кібербезпеки ведення бізнесу малими та середніми підприємствами (Cybersecurity guide for SMEs, 2021).

1. Розвивати гарну культуру кібербезпеки: призначити відповідальну особу за організацію кібербезпеки; проводити аудити кібербезпеки; пам'ятати про захист даних.Надійна кібербезпека – запурока сталого розвитку та успіху будь-якого бізнесу. Тому необхідно призначити відповідальну особу, яка повинна забезпечити відповідні ресурси, такі як час від персоналу, придбання програмного забезпечення, послуги і обладнання для кібербезпеки, навчання персоналу та розвиток ефективної політики щодо кібербезпеки. Крім того необхідно мати відкриту підтримку керівництва щодо ініціатив у сфері кібербезпеки, проведення відповідних тренінгів для співробітників та надання чітких, конкретних правил, викладених у політиках кібербезпеки, що регулярно переглядаються та оновлюються. У політиках мають бути прописані наслідки, з якими може зіткнутися працівник, якщо не буде дотримуватимуться політики кібербезпеки. Регулярні аудити повинні проводитися особами, які мають відповідні знання, навички та досвід та не

залежать від щоденних ІТ-операцій. Згідно із Загальним регламентом ЄС щодо захисту даних, будь-які підприємства, фінансові установи, які обробляють або зберігають персональні дані резидентів Європейської економічної зони, повинні забезпечити відповідні засоби контролю безпеки для захисту цих даних. Це гарантує захист інтересів третіх сторін, які працюють від імені відвідного підприємства, та надає їм заходи безпеки.

2. Забезпечити відповідне навчання. Проводити регулярні тренінги з кібербезпеки для всіх співробітників, щоб вони могли розпізнавати різні загрози кібербезпеці та боротися з ними. Ці тренінги мають бути адаптовані для малих підприємств та зосереджені на реальних ситуаціях.

3. Забезпечити ефективне управління третьою стороною. Переконатися, що всі постачальники, особливо ті, хто мають доступ до конфіденційних даних та/або систем, активно керуються та відповідають узгодженим рівням безпеки. В контрактних угодах повинно бути прописано, як постачальники відповідають вимогам безпеки.

4. Розробити план реагування на інциденти. Офіційний план реагування на інциденти має містити чіткі вказівки, ролі та обов'язки, задокументовані для забезпечення своєчасного, професійного та належного реагування на всі інциденти безпеки. Для того, щоб швидко реагувати на загрози безпеці, необхідно досліджувати та аналізувати інструменти, що можуть відстежувати та створювати сповіщення, за умов підозрілих дій або порушення безпеки.

5. Безпечний доступ до систем. Використовувати фразу-пароль, що є набором принаймні трьох випадкових поширених слів, об'єднаних у фразу, яка забезпечує дуже хороше поєднання запам'ятовуваності та безпеки: не використовувати повторно в іншому місці; не діліться з колегами; увімкнути багатофакторну автентифікацію; використовувати спеціальний менеджер паролів. За умов використання типового паролю, рекомендовано робити його довгим, із символами верхнього та нижнього регістру та спеціальними символами. Уникати використання «123», «пароль», особистої інформації, що є відкритому доступі в Інтернеті.

6. Безпека пристроїв. Ключовим кроком у програмі кібербезпеки є забезпечення безпеки пристроїв, якими користуються співробітники (настільні ПК, ноутбуки, планшети чи смартфони), тому необхідно зберігати програмне забезпечення виправленим та оновленим (в ідеалі використовувати централізовану платформу для керування виправленнями). Централізоване кероване антивірусне ПЗ має бути впроваджено на всіх типах пристроїв та підтримуватися в актуальному стані, щоб забезпечити його постійну ефективність. Використовувати ПЗ для блокування електронних листів зі спамом, електронних листів із посиланнями на шкідливі веб-сайти, електронних листів із шкідливими вкладеннями, вірусами, фішингових

електронних листів. Захист даних через шифрування. Малі та середні підприємства повинні гарантувати, що дані, що зберігаються на мобільних пристроях, таких як ноутбуки, смартфони зашифровані. Для даних, що передаються через загальнодоступні мережі, такі як мережі Wi-Fi готелів чи аеропортів, переконайтеся, що дані зашифровані, використовуючи віртуальну приватну мережу (VPN) або доступ до веб-сайтів через безпечне з'єднання за допомогою протоколу SSL/TLS. Переконайтеся, що на їхніх власних веб-сайтах використовується відповідна технологія шифрування для захисту даних клієнтів під час їх передачі через Інтернет.

7. Безпека мережі. Спрощуючи роботу персоналу віддалено, багато МСП дозволяють персоналу використовувати власні ноутбуки, планшети та/або смартфони. Це викликає кілька проблем із безпекою конфіденційних бізнес-даних, що зберігаються на цих пристроях. Одним із способів управління цим ризиком є керування мобільними пристроями. Це дозволить: здійснювати контроль над пристроями, яким дозволено користуватись послугами й системами МСП; на таким пристроях має бути встановлене актуальне сучасне антивірусне ПЗ; доступ до таких пристроїв – через надійні паролі або PIN-код; дистанційно стерти будь-які дані МСП з пристрою, якщо власник пристрою повідомить про втрату чи викрадення пристрою, або якщо робота власника пристрою закінчиться з МСП. Наступна рекомендація – використовувати брандмауери та регулярно перевіряти роботу та налаштування пристроїв, що залучені у віддаленому доступі до ресурсів МСП.

8. Удосконалення фізичної безпеки. Усюди, де міститься важлива інформація, слід застосовувати відповідні засоби фізичного контролю. Наприклад, службовий ноутбук або смартфон не можна залишати без нагляду на задньому сидінні автомобіля. Кожен раз, коли користувач відходить від свого комп'ютера, він повинен заблокувати його. В іншому випадку потрібно увімкнути функцію автоматичного блокування на будь-якому пристрої, який використовується для комерційних цілей. Конфіденційні друковані документи також не слід залишати без нагляду, а якщо вони не використовуються, надійно зберігати.

9. Захист резервних копій. Резервне копіювання має бути регулярним та автоматизованим, бажано шифрувати резервні копії. Проводити тестування щодо здатності відновлення. В ідеалі слід проводити регулярне тестування повного відновлення від початку до кінця.

10. Синхронізувати з хмарними технологіями. Пропонуючи багато переваг, хмарні рішення все ж представляють деякі унікальні ризики, які МСП слід враховувати перед тим, як співпрацювати з постачальником хмарних технологій. ENISA опублікувала «Посібник з хмарної безпеки для малих і середніх підприємств» (ENISA, 2021), до якого малим і середнім підприємствам слід звернутися під час переходу на хмару.

Вибираючи хмарного постачальника, МСП має переконатися, що він не порушує жодних законів чи правил, зберігаючи дані, особливо персональні, за межами ЄС/ЄЕЗ. Наприклад, Загальний регламент захисту даних (GDPR) ЄС вимагає, щоб персональні дані жителів ЄС/ЄЕЗ не зберігалися та не передавалися за межі ЄС/ЄЕЗ, за винятком дуже особливих умов.

11. Захист онлайн-сайтів Вкрай важливо, щоб МСП гарантували, що їхні онлайн-сайти налаштовані та обслуговуються безпечним способом

і що будь-які персональні дані або фінансові деталі, такі як дані кредитної картки, належним чином захищені. Це передбачає проведення регулярних тестів безпеки веб-сайтів для виявлення будь-яких потенційних слабких місць у безпеці та проведення регулярних перевірок для забезпечення належного обслуговування та оновлення сайту.

12. Шукати та ділитись інформацією. Ефективним інструментом боротьби з кіберзлочинністю є обмін інформацією. Обмін інформацією щодо кіберзлочинності є ключовим для того, щоб МСП краще розуміли ризики, з якими вони стикаються. Компанії, які дізнаються про виклики кібербезпеки та про те, як ці проблеми вдалося подолати, з більшою ймовірністю вживуть заходів для захисту своїх систем, ніж якби вони почули подібні подробиці з галузевих звітів або опитувань щодо кібербезпеки.

Захист фінансових систем необхідний для того, щоб запобігти негативним наслідкам для економіки та громадян. Це дозволяє банкам, інвесторам та підприємствам діяти з певною довірою і впевненістю, що їх фінансові активи захищені. Якісний та високий рівень кібербезпеки допомагає захистити фінансову інформацію організації від несанкціонованого доступу, маніпуляцій або крадіжки, допомагає переконатися, що всі фінансові операції є законними та відповідають чинним законам і нормам. Крім того, фінансова кібербезпека допомагає захистити клієнтів і зацікавлених сторін від потенційних фінансових втрат та протидіяти кібератакам, кібершахрайствам.

Список літератури

1. Kuzmenko O.V., Kubalek J., Bozhenko V.V., KushneryovS., Vida I. (2021) An Approach to Managing Innovation to Protect Financial Sector against Cybercrime. Polish Journal of Management Studies. Vol. 24 (2). P. 276-291. https://doi.org/10.17512/pjms.2021.24.2.17

2. Cybersecurity guide for SMEs - 12 steps to securing your business. URL: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

3. ENISA (2021). Cloud Security Guide for SMEs. Retrieved from: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

ПОЗИТИВНІ Й НЕГАТИВНІ СТИМУЛИ ДО ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ

POSITIVE AND NEGATIVE INCENTIVES FOR THE USE OF CRYPTOCURRENCIES IN ECONOMIC CRIME

Сергій Миненко, доктор філософії
Сумський державний університет, Україна
Ксенія Могильна, студентка
Сумський державний університет, Україна

Криптовалюти набули значного поширення протягом останніх років, проте, завдяки анонімності й децентралізації вони також стали зручним інструментом у сфері економічної злочинності. Розуміння позитивних і негативних стимулів до використання криптовалют у економічній злочинності має вирішальне значення для розробки ефективної політики та стратегій боротьби з їх незаконним використанням, тому ця тема є актуальною для наукової спільноти. Метою цієї роботи є вивчення технічних та концептуальних характеристик криптовалют, що є позитивними та негативними стимулами їх залучення до економічної злочинності.

Для усвідомлення ролі криптовалют у економічній злочинній діяльності важливо розуміти сутність поняття «криптовалюта». За визначенням (Yaga та et al., 2018) криптовалюти є цифровими активами в системі, які криптографічно надсилаються від одного користувача мережі блокчейн до іншого за допомогою цифрових підписів із парами асиметричних ключів. Основними відмінностями криптовалют від електронних національних валют є те, що їх емісують децентралізовано без участі державних установ, також криптовалюти існують виключно у цифровій формі. Ще однією відмінною рисою криптовалют є типи транзакцій, зокрема можливість переказів «від особи до особи» (або P2P) й обмінів на криптовалютних біржах. Транзакції «від особи до особи» є прямими переказами між користувачами, тобто здійснюються без залучення посередників у вигляді криптовалютних бірж або інших фінансових установ, таким чином, їх важко відслідкувати й контролювати. Обміни на криптовалютних біржах, тобто платформах, які дозволяють купувати та продавати криптовалюти, є більш публічними та захищеними за рахунок нагляду самих бірж та держави.

Очевидно, що справжній обсяг криптовалюти задіяної в економічній злочинності точно оцінити неможливо через відсутність вичерпної бази даних, яка б відстежувала всі транзакції, та анонімність багатьох переказів, що ускладнює ідентифікацію зловмисників. Однак наявні оцінки обсягів

криптовалюти пов'язаних з незаконними акаунтами здатні надати загальне уявлення про тенденції цього ринку (рис. 1). За даними дослідження Chainalysis Inc, загальна вартість криптовалюти, отримання якої було пов'язано з злочинністю, у 2022 році досягла рекордного значення 20,6 мільярдів доларів США (Grauer et al., 2023), не зважаючи на загальний спад ринку протягом року. Крім того, з рис. 1, очевидно, що протягом 2017-2022 років цей показник мав загальну тенденцію до зростання, що також свідчить про збільшення обсягів залучення крипитовалют до злочинної діяльності.

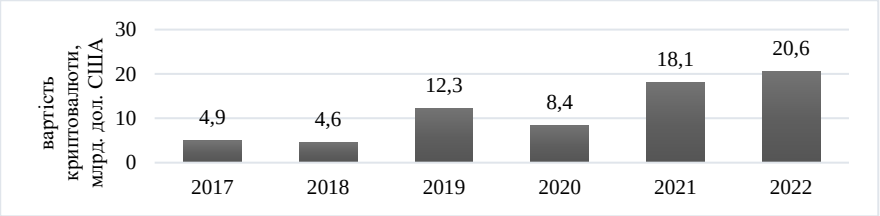

Рисунок 1. Вартість криптовалюти, отриманої незаконними акаунтами 2017-2022 років (ілюстрація створена автором на основі даних (Grauer et al., 2023)

З огляду на поширення використання криптовалют, як інструменту відмивання доходів від незаконної діяльності, шахрайства, ухилення від сплати податків, фінансування тероризму та інших економічинх злочинів, очевидно, що криптовалюти мають певні технічні й концептуальні особливості, що створюють позитивні стимули для їх використанню у злочинній діяльності. Пропонуємо охарактеризувати основні з них.

1. Низький рівень державного регулювання: у більшості країн державні інституції не мають уповноважень для контролю майнінгу й обігу криптовалют, створення й ідентифікації облікових записів пов'язаних з ними, вилучення цифрових активів отриманих незаконним шляхом тощо, що створює позитивні економічні стимули для використання криптовалют для економічної злочинності.

2. Труднощі ідентифікації учасників транзакцій: хоча блокчейн містить публічний запис кожної транзакції, обробленої мережею, ідентифікувати залучених сторін без додаткової інформації (яку можуть надати біржі або інтернет магазини) часто є неможливим (Brenig et al., 2015), також ідентифікація осіб задіяних у транзакції ускладнюється можливістю створення кількох облікових записів однією особою, усе це збільшує анонімність використання криптовалют і зменшує ризики отримання відповідальності за їх використання у злочинній діяльності.

3. Простота конвертації: здатність легко конвертувати криптовалюти у фіатні валюти й навпаки полегшує злочинцям відмивання незаконно здобутих

доходів, уникаючи їх виявлення правоохоронними органами і видаючи за законно здобуті кошти.

4. Доступність: доступність і простота використання криптовалют можуть створити стимул для використання їх як інструменту економічних злочинів, оскільки вони забезпечують ефективний спосіб передачі цінностей через кордони країн без потреби в посередниках або державного нагляду, виключно за наявності пристрою з доступом до Інтернету.

5. Швидкість і низька вартість транзакцій: транзакції фіатних валют зазвичай передбачають високі комісії та значні витрати часу, що робить переміщення великих сум грошей більш складним і дорогим, в той час, як криптовалюти пропонують майже миттєвий час обробки транзакцій, комісії за які є відносно низькими або відсутніми, що робить їх більш привабливим варіантом для економічних злочинців.

6. Безвідкличність: після підтвердження криптовалютної транзакції протокол не пропонує жодних функціональних можливостей для її скасування і повернення стягнених коштів, ця схожість крипитовалютних операцій з готівковими робить їх зручним інструментом для шахрайства.

7. Можливість здійснення платежів без посередника: здійснення транзакціїї з використанням криптовалюти не має необхідності у взаємодії з третіми сторонами для обробки транзакцій (Gowda & Chakravorty, 2021), що робить криптовалютні транзакції значно менш прозорими та контрольованими фінансовими інституціями, державою й громадськістю, а також ускладнює для правоохоронних органів виявлення та відстеження злочинної діяльності.

Не зважаючи на значну кількість позитивних стимулів, що сприяють використанню криптовалют в незаконній діяльності, деякі їх характеристики навпаки роблять криптовалюти менш привабливим інструментом для використання в економічній злочинності. Такими характеристиками можуть бути:

1. Низька ліквідність: хоча все більше продавців пропонують криптовалюти як спосіб оплати за реальні і цифрові товари та послуги, проте криптовалюти все ще є значно менш ліквідними за національні валюти, що обмежує шляхи використання коштів здобутих незаконним шляхом і створює необхідність обміну криптовалют на фіатні валюти.

2. Висока волатильність: криптовалюти відомі своєю мінливістю цін (Baur & Dimpfl, 2021), така нестабільність може ускладнити злочинцям збереження вартості коштів здобутих незаконним шляхом та підвищити ризик фінансових втрат, таким чином, висока волатильність, характерна для криптовалют, є несприятливим фактором для їх використання в економічних злочинах.

3. Запис транзакцій у публічній книзі блокчейну: криптовалюти використовують публічні книги, які реєструють усі транзакції та є видимими

для всіх користувачів, що робить можливим відстеження потенційно злочинних транзакцій, а також дій ідентифікованих злочинних акаунтів правоохоронними органами (Morishima & Matsutani, 2019), що полегшує відстеження злочинної діяльності.

4. Необхідність наявності технічних знань: самостійне використання криптовалют вимагає від злочинців наявності певного рівня технічних знань і навичок, що може стати перешкодою для використання криптовалют, як інструменту економічних злочинів окремими особами.

Підсумовуючи, незважаючи на труднощі з виявленням і ідентифікацією злочинців, наявні оцінки свідчать про загальну тенденцію до зростання участі криптовалют у економічній злочинній діяльності протягом 2017-2022 років. У дослідженні було сформульовано та охарактеризовано основні технічні та концептуальні позитивні стимули до використання криптовалют у економічній злочинності. Також виявлено і розглянуто фактори, що є негативними стимулами до використання криптовалют у економічній злочинності. Результати роботи дозволяють розуміти сприятливі та несприятливі для залучення до економічної злочинності характеристики криптовалют, що може бути використаним для подальшого вивчення та розробки системи державного регулювання цифрових активів, яка покликана запобігати злочинній діяльності та створювати безпечне інвестиційне середовище шляхом, що мінімально заважатиме розвитку інновацій та зростанню галузі цифрових активів.

Список літератури

1. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). NISTIR 8202. *Blockchain Technology Overview*. National Institute of Standards and Technology.

2. Grauer, K., Jardine, E., Leosz, E., & Updegrave, H. (2023). *The 2023 crypto crime report*. Chainalysis.

3. Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. ECIS 2015 *Completed Research Papers*, Paper 20.

4. Gowda, N., & Chakravorty, C. (2021). Comparative study on cryptocurrency transaction and banking transaction. *Global Transitions Proceedings*, 2(2), 530–534.

5. Baur, D. G., & Dimpfl, T. (2021). The volatility of Bitcoin and its role as a medium of exchange and a store of value. *Empirical Economics*, 61, 2663–2683.

6. Morishima, S., & Matsutani, H. (2019). Acceleration of anomaly detection in blockchain using in-gpu cache. *2018 IEEE intl conf on parallel & distributed processing with applications, ubiquitous computing & communications, big data & cloud computing, social computing & networking, sustainable computing & communications*. IEEE.

ПЕРСОНАЛ КОМПАНІЇ ЯК «БРАМА» ДЛЯ КІБЕР АТАК

COMPANY PERSONNEL AS A «GATEWAY» FOR CYBER ATTACKS

Назар Фененко, студент
Сумський державний університет, Україна

Сучасний цифровий світ ставить безпрецедентні виклики з точки зору кібербезпеки. Все більше компаній використовують сучасні технології в своїх бізнес-процесах для поліпшення продуктивності та збільшення прибутку. Насправді цей процес є незворотнім і приносить компаніям позитивні результати, проте перехід в цифровий світ несе за собою нові загрози.

Все частіше ми чуємо з новин інформацію про витік даних, або втрату інформації в технологічних гігантів, часто це стосується соціальних мереж, де більшість людей зберігають про себе багато індивідуальної інформації.

Якщо навіть лідери ринку схильні до витоку інформації, що ж вже говорити про невеликі компанії, які не мають серйозних систем захисту інформації. Таких компаній незлічена кількість і практично всі мають потенційні ризики, як з боку недобросовісних конкурентів, так з боку хакерських організацій, мета яких заволодіти інформацією з метою її подальшого використання в корисливих цілях.

Можна довго говорити про причини атак на інформаційні ресурси компанії, але їх результат завжди один, це фінансові та репутаційні втрати для організації. Інколи ці проблеми можуть бути дуже легко вирішені, проте інколи компаніям доводиться виплачувати суттєві штрафи, як це було з компанією GT Advanced, котра втратила 50 мільйонів доларів[1], за витік інформації про майбутні характеристики продукції Apple.

Проте інколи витік інформації приводить до непередбачуваних наслідків, як це було з банком Credit Suisse [2], коли висвітлена інформація привела до корупційного скандалу, що завдала достатньо суттєвого репутаційного удару по структурі банку.

Беручи до уваги реальні ризики втрати інформації компанії все частіше використовують різні методи захисту інформації, як на апаратному рівні, так і на програмному. Організація різнорівневих систем доступу, використання біометрії, двохрівнева аутентифікація, фізичні системи захисту, все це має дуже велике значення для забезпечення безпеки даних.

Проте треба розуміти, що ми у своїй основі працюємо з людьми, цей фактор має непередбачувані наслідки, оскільки поведінка людини не має чіткого алгоритму. Тому робота з персоналом на тему кібербезпеки має без перебільшення основоположне значення.

Аналізуючи інформаційний простір можна побачити, що навіть державні організації дуже серйозно відносяться до підготовки своїх спеціалістів, як це було з держслужбовцями [3]. Дана акція має серйозне підґрунтя, оскільки велика частина працівників не оцінюють загрози серйозно.

Таким чином, що навіть базове навчання з кібербезпеки має велике значення для інформаційної обізнаності персоналу, що може гарантувати відносну захищеність від базових атак. Персонал має чітко розуміти, що є інструкції поведінки з інформаційними ресурсами і недбале відношення може привести до реальних негативних результатів.

До базового навчання можна віднести правила використання устаткування та режимів доступу, передача інформації між співробітниками, використання тільки своїх автентифікаційних даних, та неможливість їх передачі іншим співробітникам, навіть якщо це знайома людина, оскільки навіть давно знайомий співробітник може виявитись зловмисником, якого підкупила конкуруюча організація.

Також співробітники мають бути обізнані про зовнішні загрози, які в основі своїй мають більш вагомі загрози. По перше це вміння користування поштовими сервісами. Корпоративні поштові аккаунти як правило мають захист, проте його може бути недостатньо. Тема фішинга дуже актуальна навіть в сучасний час, зловмисники використовують дуже багато підходів, як зменшити пильність співробітників.

Персонал може навіть не зрозуміти, що на компанію була зроблена фішингова атака, оскільки листи можуть виглядати максимально правдоподібно, вони можуть навіть імітувати вимоги від керівництва передати дані негайно, що збільшує стрес для робітника, та зменшує його пильність.

Правильна комунікація до персоналу про обережність прийняття рішень в ситуаціях, коли пропозиція занадто гарна, щоб бути правдою. Наприклад коли псевдо керівник просить передати дані швидко, оскільки він зараз вирішує питання контракта, а за швидке реагування обіцяє підвищення або збільшення заробітної плати. Така пропозиція може зменшити пильність співробітника, як результат привести до необдуманих дій.

Також важливий момент вигорання персоналу[4], оскільки робота в стресовій ситуації призводить до зменшення пильності, тому керівники мають серйозно відноситись до емоційного стану робітників, щоб забезпечити їх продуктивну роботу.

Звісно треба розуміти, що обізнаність персоналу залежить від їхніх початкових знань. Очевидно що компанії які працюють в IT індустрії мають більш серйозну обізнаність в кіберзагрозах, тому для такого персоналу можна проводити навчання більш високого рівня, в той час для підприємств державного сектора, або підприємств які тільки проходять процес цифровізації

необхідно в першу чергу провести базове навчання і тільки потім переходити до більш серйозних практик.

Таким чином можна сказати, що правильний підхід в організації обізнаності співробітників має дуже велике значення в забезпеченні інформаційної безпеки компанії. Навіть базова обізнаність може врятувати організацію як мінімум від репутаційних втрат, а також може навіть врятувати від банкрутства.

Добре обізнаний персонал, в тому числі в правовому полі, гарантовано суттєво зменшить ризики для компанії, а як результат приведе до збільшення прибутку за рахунок нівелювання незапланованих витрат.

Список літератури

1. Стала відома сума штрафу для постачальників Apple за витік даних про iPhone і iPad URL: https://www.unian.ua/science/995983-stala-vidoma-suma-shtrafu-dlya-postachalnikiv-apple-za-vitik-danih-pro-iphone-i-ipad.html
2. Як Credit Suisse потрапив у скандал і до чого тут Україна URL: https://news.uaportal.com/ukr/section-articles/news-kak-credit-suisse-popal-v-skandal-i-pri-chem-tut-ukraina-21-02-2022.html
3. Для державних службовців організували тренінг з кібергігієни URL: https://osvita.loda.gov.ua/?page=blog&id=641
4. Емоційне вигорання URL: https://healthcenter.od.ua/psyhichne-zdorovya/emoczijne-vygorannya/

ПЕРСПЕКТИВИ РОЗВИТКУ ХАКТИВІЗМУ ТА ХАКЕРСЬКИХ АТАК В СФЕРІ ФІНАНСОВИХ ПОСЛУГ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ

PROSPECTS FOR THE DEVELOPMENT OF HACKTIVISM AND HACKER ATTACKS IN THE FINANCIAL SERVICES SECTOR: CHALLENGES AND WAYS TO COUNTERACT

Єлизавета Литюга, *студентка*
Сумський державний університет
Валерій Яценко*, к.т.н., доцент*
Сумський державний університет

Тема хакерства та її наслідків для цифрової економіки є вельми значущою, оскільки кількість кіберзлочинів ("взломи" банківських рахунків і кібервандалізм) постійно зростає. Тема хактивізма протягом багатьох років цікавила вчених з усього світу, наприклад, Андерсен Рон у своїх дослідженнях розглядає феномен хактивізму і звертає увагу на його вплив на політичну арену та громадську активність, Макгрегор Річар аналізує роль хакерів і хакерських атак в кібербезпеці, визначає основні типи атак і розглядає стратегії протидії, Менделсон Майкл в своїх дослідженнях зосереджується на етичних аспектах хактивізму та хакерства, досліджує моральні проблеми, пов'язані з цими явищами, Шанмугам Нірмала вивчає вплив хактивізму на фінансовий сектор та аналізує ризики та виклики, які це створює для фінансових установ, Дітон Пітер досліджує політичний хактивізм із застосуванням технологій, зокрема розглядає вплив соціальних мереж на організацію політичних рухів. На жаль, незважаючи на істотне державне фінансування програм кібербезпеки, хакери продовжують завдавати великої шкоди економічній та соціально-політичній діяльності громадян та країни в цілому. Мета даного дослідження – проаналізувати роль хактивізму в контексті фінансових послуг та з'ясувати, які соціальні, політичні та економічні фактори сприяють його розвитку, вивчити типи хакерських атак, які загрожують фінансовому сектору України та визначити їх особливості та наслідки, розглянути перспективи розвитку кібератак та шляхи вирішення цієї проблеми у планетарному масштабі.

Хактивізм – це поєднання понять "хакерство" та "активізм", що означає використання технічних навичок і комп'ютерної експертизи для досягнення політичних, соціальних або етичних цілей. Цей термін походить від словосполучення "хакерський активізм" і відображає зв'язок між хакерськими здібностями та соціальним ангажуванням.

Ще на самому початку функціонування інтернету з'явилися так звані "хакери", які з виробничих, романтичних або ж корисливих міркувань взламували приватні бази даних. Для злому з метою несанкціонованого

проникнення в приватний або корпоративний кіберпростір, хакери використовували широкий діапазон різноманітних комплексних методів програмування та репрограмування. Ці перші хакери, "герої комп'ютерної революції", як їх іменує Стівен Леві, – так звані "білі хакери". Такі "етичні хакери" – це, насамперед, професійні програмісти, які здійснювали взлом даної комп'ютерної системи з метою корекції програм, запобігання кіберзлочинам. Ці ексцентричні ентузіасти кіберпростору використовували термін hack ("зламати"), щоб описати оригінальний спосіб для істотного поліпшення продуктивності комп'ютерних систем. Вони змогли знайти неортодоксальні рішення для найскладніших проблем комп'ютерної техніки. З деякими нюансами до цієї першої хвилі руху хакерів можна віднести Білла Гейтса, Стіва Возняка, Річарда Столлмана і Марка Цукерберга.

Хакерів, по суті своїй кіберзлочинців, які зламують комп'ютерні мережі заради грошей і викрадення конфіденційних даних, ставлячи під загрозу безпеку персональних і корпоративних комп'ютерів, підключених до мережі інтернет, називають "чорними хакерами". Найбільш відома в історії кіберзлочинності група Кевіна Митника (Kevin David Mitnick). Він і його друзі виграли майже мільйон доларів у Лас-Вегасі за допомогою перепрограмування ігрових автоматів. Кевін Митник, незважаючи на віртуозні хакерські техніки злому неймовірно захищених баз даних, був виявлений агентами ФБР, засуджений і покараний. Після звільнення з федеральної в'язниці, в 1998 році, Кевін Митник, "Робін Гуд" інформаційного суспільства, який незаконно проник у комп'ютерні системи багатьох відомих компаній, у мас-медійному хайпі, перетворився з хакера на одного з найзатребуваніших експертів із кібербезпеки у світі.

І, нарешті, існують "сірі хакери", які працюють у морально-етичному інтервалі між "білими" і "чорними" в "сірій зоні" кіберпростору.

Хактивізм, як невидимий кримінальний фронтир, у різних своїх проявах істотно зачіпає моральні (публікація конфіденційної інформації користувачів в інтернеті) і матеріальні (онлайн-шахрайства з номерами кредитних карток і фальшивими чеками, зламані банківські рахунки) інтереси мільйонів громадян. Шляхом численних зломів комп'ютерних мереж, фішинг-атак, "троянських коней" тощо. Кіберзлочинці перетворюють вкрадені ними дані на мільйони доларів. За деякими оцінками, на частку незаконної торгівлі припадає одна п'ята частина світового ВВП. Темі незаконної торгівлі більше уваги приділяє у свої дослідженнях Родрігес М. (Rodriguez et al, 2021).

Проте іноді неможливо зрозуміти мотиви хактивізму. Їхні кібератаки нагадують банальний вандалізм і злісне хуліганство в планетарному масштабі. У листопаді 2008 року комп'ютерний черв'як Conficker (шкідлива програма була написана на Microsoft Visual C++) заразив перший комп'ютер, а вже через місяць Conficker проник у 1,5 мільйона комп'ютерів у 195 країнах. У січні 2009 року хробак влаштувався у восьми мільйонах комп'ютерів. Серед заражених

виявилися комп'ютери банків, телекомунікаційних компаній і деякі урядові комп'ютерні мережі (включно з британським парламентом, французькими та німецькими військовими мережами). Кібератака стала серйозною світовою загрозою. Економічні збитки, завдані Conficker мережевому співтовариству, оцінюється в 9,1 млрд. доларів. В інформаційному суспільстві з'явився новий вид високотехнологічної злочинної діяльності – кіберзлочинність. Сформувався новий антропологічний тип злочинця – кваліфікований програміст, хакер. Формування безпечної цифрової економіки, криптоекономіки супроводжується зростанням кіберзлочинності.

Очевидно, що кіберзлочинність завдає не тільки прямих збитків бізнесу, підприємствам і окремим громадянам. Вона так само безпосередньо впливає на економіку окремих держав. Розглянемо якого роду кіберзагрози можуть становити небезпеку для фінансової сфери України:

Найактуальнішою проблемою звичайно ж є хакерські атаки, спонсоровані державою противником. Цілі кіберзагрози – це порушення стабільного функціонування найбільших фінансових інститутів держави та (або) отримання можливості контролю і маніпулювання її діяльністю для завдання економічної шкоди країні в цілому. Об'єктами кіберзагрози можуть бути центральні банки, фондові біржі, фінансові Data-центри, майнінгові ферми. Особливостями фінансової кіберзагрози є інфраструктурна підтримка атак за допомогою військової інфраструктури ініціатора атаки, масштабність і системність характеру атаки. Прикладами хакерських команд можуть бути Equation Group, Lazarus.

Фінансові диверсії на фінансовому ринку, ініційовані найбільшими фінансовими корпораціями. Цілі кіберзагрози – формування на фондових біржах панічних настроїв, зниження вартості або виключення з котирувального листа окремих бізнесів шляхом інформаційних вкидань (фейк-новин, інформації, яка ганьбить ділову репутацію компанії та її топ-менеджерів), організація витоку інсайдерської інформації, хакерських атак на активи компанії (організація штучних збоїв або аварій). Об'єктами кіберзагрози можуть бути акції найбільших бізнесів, а також втручання в процеси участі окремих бізнесів у міжнародних інвестиційних програмах і проєктах (переважно – сфера військово-промислового комплексу та енергетики). Хакери штучно погіршують рейтингові позиції найбільших бізнесів держави, знижують їхню інвестиційну привабливість, відсторонюють державу від міжнародних інвестиційних проєктів і програм. Прикладами хакерських команд є Cobalt, BlackEnergy, Idustroyer, HAVEX.

Конструювання і запуск соціоінженерних троянів. Доступ до критичної банківської інфраструктури хакери отримують через менш захищені приватні та публічні акаунти, які перебувають поза контуром основної банківської інфраструктури, а отже, мають вищу вразливість. Головною метою

є отримання через акаунти приватних і публічних осіб - клієнтів банків доступу до всієї банківської інфраструктури та здійснення операцій з її виведення з ладу, а також викрадення персональних даних клієнтів та їхніх грошових коштів. Об'єктами кіберзагрози є програмні модулі соціальних мереж, акаунти в інтернет-банкінгу, файлові менеджери власників банківських карток тощо. Приклади хакерських команд: APT10, WINNITI, Regin, REXAN.

Інфраструктурні атаки на IoT-мережі (інтернет речей). Через злам облікового запису або елементів фінансової інфраструктури хакери отримують можливість впливати на фізичну інфраструктуру, що знаходиться за контурами банку, а також конструювати соціальний хаос або техногенні події. Цілі кіберзагрози – отримання контролю над бізнес-процесами фінансово-промислових екосистем, а також заподіяння їм прямої та непрямої шкоди внаслідок порушення стабільності їхньої роботи, а також розкрадання або маніпулювання приватними даними користувачів таких екосистем. Об'єкти кіберзагрози: системи дистанційної оплати платних автошляхів, сервіси дистанційної медицини, системи "розумного будинку" і "безлюдного офісу", інтегровані в банківську бізнес-модель. Приклади хакерських команд: Fancy Bears, Lizard Squad, Anonymous.

Як випливає з наведеного аналізу, Україна наразі перебуває під впливом серйозних ризиків, зумовлених кіберзагрозами, орієнтованими на ослаблення її економіки та посилення соціально-економічних заворушень і напруженості. З метою ефективної боротьби з кіберзлочинністю важлива подальша консолідація зусиль і органів влади, і бізнес-спільноти, і просунутих в IT-технологіях користувачів. І не окремо взятої країни, а всіх держав, і особливо передових у сфері інформаційних комунікаційних технологій. Для боротьби із загрозою кіберзлочинності, яка, безумовно, зростатиме з подальшим розширенням сфери використання інформаційних технологій, надаючи все більші можливості для протиправної діяльності як індивідуумам, так і злочинним групам, необхідна постійна міжнародна співпраця. Контролювати кіберзлочинність і боротися з нею на рівні окремої держави практично неможливо. Наразі у формуванні міжнародної стратегії боротьби з кіберзлочинністю задіяні понад сорок країн світу, і процес цей обіцяє бути довгим. Ухвалення міжнародних норм і стандартів має супроводжуватися внесенням змін до національного законодавства держав. Координація зусиль держав необхідна для забезпечення швидкого реагування на розвиток комп'ютерних технологій і затвердження відповідних норм.

Список літератури

1. Rodriguez, M. (2021). The Role of Hacktivism in Shaping Financial Services Policies. International Journal of Information Security, 20(5), 587-604. doi:10.1007/s10207-021-00503-2

ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНИХ ТРЕНДІВ КІБЕРЗЛОЧИНІВ

FORECASTING CYBERCRIME INFORMATION TRENDS

Катерина Солярова, *студентка*
Сумський державний університет, Україна
Ганна Яровенко, *д.е.н., доцент*
Сумський державний університет, Україна

Прогнозування інформаційних трендів кіберзлочинів свідчить про те, які методи та напрямки можуть використовуватися злочинцями у цифровому простору. За останні п'ять років найчастішими видами кібератак були такі:

- Social Engeneering
- DoS Attacks
- Password Attack

Наукові дослідження щодо кіберзлочинів стверджують, що йде постійне зростання кількості кібератак, а також і їхня складність.

Для проведення дослідження використовувалася мова програмування Python.

Спершу треба провести первинний статистичний аналіз. Він показує загальну кількість кібератак, середнє значення, стандарте відхилення, максимальне та мінімальне значення для кожного з видів кібератак. Таку статистику основних метрик числових змінних отримали, використовуючи метод describe() бібліотеки Pandas.

Для того, аби оцінити наскільки відповідають нормальному закону розподілу дані в ряді, було використано графічний аналіз, який був представлений у вигляді гістограм та графіків. Для побудови гістограм використовувався метод hist() бібліотеки Pandas. Для побудови графіків треба визначити його розмір, його можна визначити за допомогою методу figsize(), самі графіки були побудовані за допомогою методу plot().

Для оцінки відповідності розподілу даних нормальному закону, можна скористатися критерієм Харке-Бера.

Формула для цього критерію має такий вигляд:

$$JB = n * \left(\frac{S^2}{6} + \frac{(K-3)^2}{24}\right), \quad (1)$$

Де JB – статистика критерію Харке-Бера,
n – кількість спостережень (даних),
S – оцінка стандартного відхилення даних,
K – оцінка ексцесу даних. [1]

Одним з найбільш використовуваним тестом перевірки часового ряду на стаціонарність є розширений тест Дікі-Фулера. Він дозволяє виявити наявність авторегресії в ряді, тобто зв'язок між значеннями у різні моменти часу. [2]

Тест Дікі-Фулера має такий вигляд:

$$Y_t = \alpha + \varphi Y_{t-1} + \varepsilon, \quad (2)$$

де Y_t – значення часового ряду в момент часу t,

α – константа,

φ – коефіцієнт авторегресії,

ε – випадкова складова, яка представляє помилку або шум в часовому ряді. [3]

Для виявлення та аналізу циклічних коливань показника треба провести перевірку сезонної компоненти. Для цього ряд можна розглянути, як мультиплікативну комбінацію або адитивну, а також аналізувати залишки.

Останнім кроком було побудова SARIMA моделі та прогнозу для кожного ряду.

SARIMA модель являється потужним інструментом для аналізу та прогнозування часових рядів із сезонними впливами. Ця модель показує більш точні прогнози та складну динаміку даних, які містять сезонні та несезонні коливання.

Для побудови SARIMA моделі в Python треба використати бібліотеку Statsmodels.

Для оцінки SARIMA моделі використаємо такі критерії, як AIC (Akaike's Information Criterion) та BIC (Bayesian Information Criterion). Ці критерії потрібні нам для порівняння наших моделей та вибору кращої, яка має найменшу втрату інформації. Це означає, що вона має більшу ймовірність наблизити реальні дані та мати меншу складність.

Формула критерію AIC виглядає таким чином:

$$AIC = -2 * \log(L) + 2 * k, \quad (3)$$

де log(L) – логарифм максимальної правдоподібності моделі;

k – кількість параметрів в моделі. [4]

Формула критерію BIC виглядає наступним чином:

$$BIC = -2 * \log(L) + k * \log(n), \quad (4)$$

де log(L) – логарифм максимальної правдоподібності моделі;

k – кількість параметрів в моделі;

n – розмір вибірки.

Модель з найменшим значенням AIC або BIC вважатиметься кращою, оскільки вона має більшу ймовірність наблизити дійсні дані та меншу складність.

Для проведення прогнозу використаємо функцію predict() бібліотеки Scikit Learn. Ця функція показує передбачені значення або мітки для нових даних.

Для оцінки точності та надійності прогнозів було розраховано значення Люнга-Бокса та залишкового розподілу. Значення Люнга-Бокса показує, чи існує значуща автокореляція в залишках після врахування моделі. Залишковий розподіл перевіряє, наскільки добре залишки моделі відповідають передумовам моделювання, зокрема, нормальному розподілу.

Список літератури

1. R. S. Tsay, Analysis of Financial Time Series (third edition). Hoboken: John Wiley & Sons, Inc. 2010.
2. Лук'яненко І. Г., В. М. Жук. АНАЛІЗ ЧАСОВИХ РЯДІВ Побудова ARIMA, ARCH/GARCH моделей з використанням пакета E.Views 6.0. – Київ: НаУКМА, 2013. – 188 с.
3. Тест Дікі-Фуллера. [Електронний ресурс]. URL: https://dickey-fuller-test.
4. Hirotsugu Akaike. A New Look at the Statistical Model Identification / Akaike Hirotsugu, 1974. – (IEEE). — С. 716 – 723.

ОСОБЛИВОСТІ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

FEATURES OF THE STATE REGULATION OF THE CYBER SECURITY OF FINANCIAL INSTITUTIONS IN EUROPEAN UNION

Вікторія Боженко, *к.е.н., доцент*
Сумський державний університет, Україна
Олександр Роєнко, *аспірант*
Сумський державний університет, Україна

Зростаючі загрози у віртуальному просторі, дистанційний режим праці, стрімка діджиталізація, геополітичні конфлікти та постійно зростаючі вимоги дотримання нормативних вимог створили суттєве навантаження на індустрію фінансових послуг в останні роки (Stavrova, 2021; Melnyk et al., 2022). Хоча фінансові установи, як правило, випереджають інші галузі щодо рівня зрілості кіберзахисту через їх суворо регульований характер, кіберзлочинці та зловмисники з національних держав продовжують вважати їх цілями високої цінності. У звіті Boston Consulting Group (2019) зазначено, що компанії фінансового сектора в 300 разів частіше, ніж інші компанії, виступають цілями кібератак. Відповідно зростають операційні витрати банків та інших фінансових установ на підвищення рівня їх інформаційної безпеки. Цей факт підтверджується оцінкою Fortunly про те, що витрати на кібератаки в банківській галузі досягли 18,3 мільйона доларів на рік на компанію, що включають не лише фінансові втрати, але й репутаційні втрати.

Фінансові установи особливо страждають від проблем безпеки через розгалужену інфраструктуру, активи високої вартості, поширеність пристроїв Інтернету речей, які можна використовувати, і людський фактор, який продовжує залишатися найслабшою ланкою в захисті безпеки (Fernando Alonso Ojeda Castro , 2021; Koibichuk & Dotsenko, 2023). Кіберзлочинці постійно удосконалюють інструменти та техніки здійснення кібератак, використовуючи штучний інтелект і автоматизацію, і тому фінансові установи повинні постійно вдосконалювати систему захисту інформаційної інфраструктури, підвищувати рівень обізнаності працівників й клієнтів у сфері інформаційної безпеки.

Згідно з опитуванням, проведеним Конференцією наглядових органів державних банків (Conference of State Bank Supervisors, 2022) понад 85% респондентів зі сфери банківських послуг оцінили ризик кібербезпеки як «надзвичайно важливий» як головний внутрішній ризик, що більш ніж удвічі перевищує будь-яку іншу категорію операційного ризику.

Статистичні показники злочинів, здійснюваних у кіберпросторі, які постійно зростають, демонструють важливість удосконалення правового

регулювання систем інформаційної безпеки на державному та наднаціональному рівнях, а також посилення кооперації в рамках різних міжнародних організацій для протидії кіберзагрозам (Zadorozhnyi et al., 2021).

Поточна ситуація в секторі фінансових послуг ЄС щодо законодавства про кібербезпеку є багаторівневою та складною. У багатьох державах-членах фінансовий сектор визначається як критична інфраструктура відповідно до інших секторів, таких як енергетика та охорона здоров'я. Оскільки фінансові установи підпадають під дію різних сфер регулювання та нагляду, існує не один основний європейський режим кібербезпеки для сектору фінансових послуг.

Основними нормативно-правовими актами, які регулюють сферу інформаційної безпеки фінансових установ є:

Директива щодо безпеки мережевих та інформаційних систем (Directive on Security of Network and Information System), що визначає формування національного регулятора у сфері інформаційної безпеки у межах кожної країни Європейського Союзу, обов'язковість повідомлення про будь-які значні кіберінциденти у межах країни, які можуть поставити під загрозу безперервність надання основних послуг тощо (Carnegie Endowment for International Peace, 2021).

1) Директива щодо загального регламенту про захист даних (General Data Protection Regulation) визначає конкретні вимоги щодо конфіденційності, безпеки персональних даних та управління порушенням у цій сфері (Calliess & Baumgarten, 2020).

2) Закон про цифрову операційну стійкість (Digital Operational Resilience Act) посилює систему управління ризиками у сфері інформаційно-комунікаційних технологій, покращує тестування фінансових систем і вдосконалює нагляд за сторонніми постачальниками інформаційно-комунікаційних технологій. Виробники повинні забезпечити відповідність цифрових продуктів основним вимогам кібербезпеки та процедурам оцінки відповідності перед розміщенням їх на ринку, а також системно проводити оцінювали ризиків кібербезпеки цифрових продуктів протягом всього терміну служби даного продукту.

Важливим елементом державного регулювання сфери інформаційної безпеки є об'єднання представників державного та приватного секторів, які функціонують над побудовою довіри, розвитком співробітництва та діалогу, враховуючи інтереси усіх учасників процесу. Однією з форм співпраці є розбудова механізму економічних кластерів, які можна широко визначити як групу економічних суб'єктів та інституцій, які територіально розташовані неподалік і мають достатні масштаби для розвитку спеціалізованої експертизи, послуг, ресурсів, умінь та навичок. Прикладами успішних кластерних утворень у країнах Європейського союзу є: земля Північний Рейн-Вестфалія у Німеччині та країна Басків в Іспанії. Крім цього, провідними європейськими учасниками зі сфери кібербезпеки була заснована Європейська робоча група

лідерів кібербезпеки. Вона працювала над низкою конкретних рекомендацій для європейських громадян, бізнесу та промислової політики щодо питань кібербезпеки. До складу робочої групи входили Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, Infi neon та Thales.

Таким чином, за останні десять років у сфері регулювання інформаційно-комунікаційних технологій зафіксовано суттєвий прогрес у частині розробки та імплементації нормативно-правових актів з кібербезпеки в Європі. Проте більшість європейських стандартів не застосовуються безпосередньо в усіх державах-членах, а мають бути перенесені в національне законодавство, створюючи подальшу фрагментацію та відмінності.

Список літератури

1. Boston Consulting Group (2019). Global Wealth 2019: Reigniting Radical Growth. URL: https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth

2. Calliess, C., Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal* 21, 1149–1179. https://doi.org/10.1017/glj.2020.67

3. Carnegie Endowment for International Peace (2021). The European Union, Cybersecurity, and the Financial Sector: A Primer / Krüger P. S., Brauchle J.-P. URL: https://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf

4. Conference of State Bank Supervisors (2022). CSBS National Survey of Community Banks 2022. URL: https://www.csbs.org/system/files?file=2022-09/CB22pub_2022_survey_Final_n092122.pdf

5. Ed. Fernando Alonso Ojeda Castro (2021). Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century. *SocioEconomic Challenges, 5*(4), 98-113. https://doi.org/10.21272/sec.5(4).98-113.2021

6. Koibichuk, V.& Dotsenko, T. (2023). Content and Meaning of Financial Cyber Security: a Bibliometric Analysis. *Financial Markets, Institutions and Risks, 7*(1), 145-153. https://doi.org/10.21272/fmir.7(1).145-153.2023

7. Melnyk, M., Kuchkin, M., Blyznyukov, A. (2022). Conceptualization and Measuring the Digital Economy. *Business Ethics and Leadership, 6*(2), 127-135. https://doi.org/10.21272/bel.6(2).127-135.2022

8. Stavrova, E. (2021). Banks' Digital Challenges. *Business Ethics and Leadership, 5*(3), 87-96. https://doi.org/10.21272/bel.5(3).87-96.2021

9. Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. Marketing and Management of Innovations, 4, 36-46. https://doi.org/10.21272/mmi.2021.4-03

МАСШТАБИ НЕЗАКОННОГО МАЙНІНГУ КРИПТОВАЛЮТ

THE SCALE OF ILLEGAL CRYPTOCURRENCY MINING

Вікторія Боженко, *к.е.н., доцент*
Сумський державний університет, Україна
Іван Гончарук, *аспірант*
Сумський державний університет, Україна

Поєднання безпрецедентно м'якої грошово-кредитної політики провідних центральних банків в умовах пандемії, активного пошуку прибутковості інвесторами, а також потреб громадян і бізнесу в швидких платежах дало сильний поштовх розвитку ринку криптовалют (Kibaroğlu, 2020; Lopez et al., 2021). Незважаючи на заборони з боку низки регуляторів, криптовалюти, що є цифровими грошовими сурогатами, набувають все більшого поширення, що формує нові виклики для суспільства та регуляторів, а також потенційні загрози для економіки та фінансової системи. Найбільше зростання ринку криптовалют спостерігалося в 2021 р., протягом січня-листопада 2021 року обсяги ринку збільшилися майже в 4 рази. Проте вже наступного року відбулася рецесія, і капіталізація ринку тримається на рівні близько 1 трлн дол США.

Криптовалюти популярні серед інвесторів оскільки вони є альтернативою традиційним централізованим банківським системам. Це означає, що замість того, щоб проходити до банку, транзакції відбуваються за допомогою децентралізованої системи, яка підтримується мережею користувачів. Проте ця децентралізація та відсутність регулювання також робить криптовалюти неймовірно привабливими для злочинців. Вони люблять використовувати криптовалюти як інструмент купівлі-продажу товарів на чорному ринку без державного нагляду або вимагання фінансової винагороди від цілей атак програм-вимагачів (Koibichuk et al.,2021; Yarovenko, et al.,2022).

Interpol (2020) щорічно випускає звіти із оцінкою небезпеки організованої злочинності в інтернеті, необхідної для розробки стратегій боротьби із нею (фішинг, соціальна інженерія, вірус-вимагач, розподілена відмова в обслуговуванні (DDoS), спуфінг). Одним із ключових загроз у сучасному світі, які визначені у цьому звіті, є прихований майнінг (криптоджекінг),а саме несанкціоноване використання обчислювальних потужностей інших осіб для видобутку криптовалюти.

На практиці існує три механізми здійснення незаконного майнінгу криптовалют: 1) через бінарні файлів – видобування криптовалюти за допомогою шкідливих програм, завантажених на пристрій користувача; 2) через браузер – видобування криптовалюти через веб-браузер за допомогою

шкідливого JavaScript, вбудованого у веб-сторінку або деякі її частини/об'єкти; 3) через хмарні технології – пошук слабких місць у захисті файлів та коді ключі API для доступу до хмарних служб (Hernandez-Suarez et al., 2022).

За даними компанії SonicWall (2023) обсяг прихованого майнінгу криптовалют в 2022 році досягнув свого рекордного рівня – кількість виявлених атак зросла до 139,261 млн, що на 45.48% більше, ніж у 2021 року, та на +155,29% порівняно з 2018 роком. Щодо географічного розподілу, то 75% світового обсягу криптоджекінг припадає на країни північної Америки (105,9 млн дол США). Протягом останніх двох років відбулося суттєве нарощення незаконних операцій з прихованого майнінгу криптовалют у країнах Європи (з 3,4 млн дол США у 2021 р. до 22 4 млн дол США у 2022 р.).

За даними компанії SonicWall, кількість атак на урядовий сектор, охорону здоров'я та освіту знизилася на 78%, 87% та 96% відповідно. Проте випадки прихованого майнінгу у фінансовій галузі зросли на 269%, а у роздрібній торгівлі – на 63%.

Для визначення сезонних коливань незаконного видобутку криптовалют протягом 2019-2022 років розраховано індекс сезонності. Індекси сезонності показують, у скільки разів фактичний рівень ряду в момент або інтервал часу і більший за середній рівень Індекс сезонності (I_S) за методом простої середньої визначають за формулою:

$$I_S = {\bar{y}_i}/{\bar{y}_t} \times 100 \quad (1)$$

де $\bar{y}_i$– середні місячні дані прихований майнінгу криптовалют;

$\bar{y}_t$ – загальні місячні майнінгу криптовалют.

Сезонна хвиля незаконного майнінгу криптовалют у світі подана на рисунку 1.

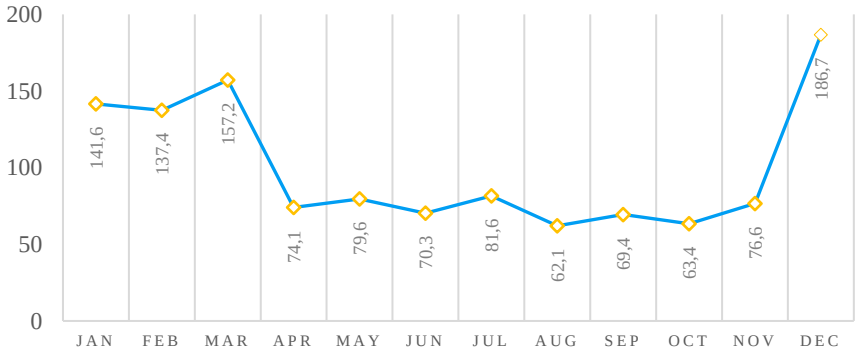

Рисунок 1. Сезонна хвиля незаконного майнінгу криптовалют у світі, %

Отримані результати дозволяють стверджувати, що протягом грудня – березня у середньому зростають обсяги незаконного майнінгу криптовалют у світі. З кожним місяцем кількість атак з метою видобування криптовалюти зростає, що свідчить про наступні загрози: зниження продуктивності обчислювальних пристроїв, збільшення споживання енергії, підозрілий мережевий трафік, швидке розряджання акумулятора та інші фізичні пошкодження пристроїв.

Для захисту від криптоджекінгу доцільно дотримуватися базових приниципів мережевої гігієни, а саме регулярне оновлення антивірусних програм, не завантажувати підозрілі програми з невідомих ресурсів, встановлювати надійні паролі, використовувати багаторівневі рішення з безпеки, підвищувати обізнаність співробітників у сфері кібербезпеки, а також здійснювати моніторинг систем компанії щодо надмірного споживання енергії.

Список літератури

1. Lopez, B.S., García, D. I., Alcaide, A.V. (2019). Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges, 3*(4), 13-24. http://doi.org/10.21272/sec.3(4).13-24.2019.

2. Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L.K., Olivares, Mercado, J., Portillo-Portilo, J., Avalos, J.-G., García Villalba, L.J. (2022). Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks. Applied Science. 12, 3234. https://doi.org/ 10.3390/app12073234

3. Interpol (2020). Cryptojacking. URL: https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

4. Kibaroğlu, O. (2020). Self Sovereign Digital Identity on the Blockchain: A Discourse Analysis. *Financial Markets, Institutions and Risks, 4*(2), 65-79. https://doi.org/10.21272/fmir.4(2).65-79.2020.

5. Koibichuk, V., Ostrovska, N., Kashiyeva, F., & Kwilinski, A. (2021). Innovation technology and cyber frauds risks of neobanks: gravity model analysis. Marketing and Management of Innovations, 1, 253-265. https://doi.org/10.21272/mmi.2021.1-19

6. SonicWall (2023). Sonic wall Cyber Threat Report. Charting Cybercrime's Shifting Frontlines. URL: https://www.sonicwall.com/2023-cyber-threat-report/

7. Yarovenko, H., Rogkova, M. (2022). Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system. *Financial Markets, Institutions and Risks, 6*(3), 93-104. https://doi.org/10.21272/fmir.6(3).93-104.2022

КІБЕРФРОНТ У ВІЙНІ РОСІЇ ПРОТИ УКРАЇНИ

THE CYBER FRONT IN RUSSIA'S WAR AGAINST UKRAINE

Архипов Станіслав, *студент*
Сумський державний університет, Україна

Війна на українському кіберфронті почалася у 2014 році, коли росія запустила масштабну DDoS-атаку на Дарницьку ТЕЦ. Згодом таких атак стало більше. Через три дні після лютневого вторгнення росії кібератаки на державно-військовий сектор України зросли на 196% порівняно з довоєнним періодом. Рекордом стали 275 DDoS-атак на день. Найпотужніші перевищували 100 Gbps.

Україна теж розгорнула активні дії. За чотири місяці великої війни наша IT-армія атакувала понад 4 200 російських онлайн-ресурсів. Кількість фішингових листів східнослов'янськими мовами зросла в сім разів. Третина шкідливих листів була надіслана російським одержувачам з українських адрес електронної пошти.

На початку війни зарубіжні кіберспеціалісти відзначали координованість дій військових та хакерів. Наприклад, 1 березня росія обстріляла ракетами київську телевежу, що призвело до зупинки телевізійного мовлення. Водночас росіяни здійснили кібератаку по Концерну радіомовлення, радіозв'язку і телебачення.

Щойно почалася велика війна, найпопулярніші російські APT-групи – угруповання висококваліфікованих хакерів – приєдналися до атак на Україну.

У травні APT28 атакувала місцеві органи влади, імовірно, з метою шпигунства та викрадення тактичних та стратегічних даних. Крім хакерів російськомовного угруповання Conti, групи кіберзлочинців, такі як CoomingProject, оголосили, що допомагатимуть російському уряду і захищатимуть російські цілі від атак.

Ключове проросійське хактивістське угруповання Killnet – група, що просуває політичні ідеї через незаконне використання мереж, – постійно атакує об’єкти критичної інфраструктури країн НАТО за допомогою складних DDoS-атак.

У середині березня 2022 року українська урядова команда реагування на комп'ютерні надзвичайні події CERT повідомила, що кілька груп APT атакували об’єкти критичної інфраструктури. За тиждень війни було 65 таких атак.

Кіберстратегія українських сил стала великою несподіванкою для світу. До цього часу росія мала перевагу, оскільки на її боці були найвідоміші групи APT. Проте Україна сформувала потужну кіберармію за лічені дні.

У перші дні війни IT-армія налічувала 175 тис добровольців з усього світу: від білих хакерів та хактивістів до представників таких технологічних компаній як SpaceX Ілона Маска. Навіть всесвітньовідомі Anonymous Collective виступили на боці України, пообіцявши діяти проти росії в кіберпросторі.

У цей же час українці на підпільних форумах закликали допомогти захистити український кіберпростір. Канал досі активний і налічує близько 262 тис учасників. Зараз там публікуються успішні атаки, здійснені проти росії.

Зарубіжні експерти відзначають процес створення фінансованої державою кіберармії безпрецедентним. Ніколи раніше жодному уряду не вдавалося завербувати незалежних кандидатів до глобальної волонтерської організації.

Anonymous за час війни запустила DDoS-атаки на корпоративні, новинні та державні сайти, скомпрометувала понад 90 баз даних телекомунікаційних, роздрібних та урядових організацій росії. Ось найпотужніші атаки 2022 року.

Україна зробила значні інвестиції для покращення кіберзахисту після двох масштабних кібератак у 2015 році та 2017 роках.

Крім того, підтримка країн та глобальних волонтерських організацій дає значні переваги, що має привести до перемоги України на обох фронтах.

Список літератури

1. BBC NEWS: https://www.bbc.com/ukrainian/features-65284915;
2. DW: https://www.dw.com/uk/viina-rf-proty-ukrainy-shcho-vidbuvaietsia-na-kiberfronti/a-61839765;
3. Кібербез:https://cybersec.net.ua/statti/497-kiberviina-rosii-proty-ukrainy-zhyttievo-vazhlyvi-uroky-dlia-zakhodu.html;
4. Кібер фронт у гібридній війні росії проти України: https://elartu.tntu.edu.ua/bitstream/lib/41085/2/MCTD_2023_Kryskov_A-Cyber_front_in_the_hybrid_72-74.pdf.

КЛЮЧОВІ АСПЕКТИ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ

KEY ASPECTS OF RESPONSIBLE BEHAVIOR OF FINANCIAL SERVICES CONSUMERS IN CYBER SPACE

Ганна Яровенко, *д.е.н., доцент*
Сумський державний університет, Україна

Реалії сьогодення свідчать про те, що половина населення світу знаходиться онлайн і залишає за собою цифровий слід, який постійно зростає. Це пов'язано із переведенням більшості послуг онлайн та формуванням єдиної кіберплощини для представників бізнесу та урядових організацій. Статистика свідчить про те, що близько 89% американців і 70% європейців користуються Інтернетом щодня, і глобальний рівень проникнення Інтернету продовжує швидко зростати. Якщо треба уявити обсяги інформації, яка проходить через Інтернет-сервери, то треба представити, що на будь-якій людині сьогодні два-три десятки датчиків, автомобіль має 500 пристроїв, 600 датчиків є у сучасному будинку, 6000 – у сучасному літаку (World Economic Forum, 2019). Звісно, що кожен прилад генерує інформацію, яка акумулюється у базах даних та на серверах приватних компаній, уряду, персональних пристроях. У таких умовах важко уявити, що персональна інформація може стати бажаним об'єктом для кіберзлочинців, які намагатимуться використовувати її у злочинних цілях, що може викликати негативні наслідки не тільки для окремих користувачів, але призвести до дестабілізації економічних, політичних та соціальних процесів в країні.

Контролювати все це дуже складно, особливо в масштабах цілої країни, але забезпечити відповідне підґрунтя для ефективного реагування на кіберзлочинність, особливо для учасників фінансового кіберпростору, це нагальна потреба як для споживачів фінансових послуг, так й для тих, хто їх надає. Одним із головних завдань є створення відповідних умов для всіх учасників даного процесу, пов'язаних із забезпеченням відповідальної поведінки. Що це означає у даному контексті? Відповідальна поведінка – це поведінка певного суб'єкта за певних обставин, яка відповідає законам, звичаям і нормам, які зазвичай очікуються від цього суб'єкта за цих обставин. Тобто, це ті дії, які здійснюють фізичні та юридичні особи, учасники процесу надання та отримання фінансових послуг, які не призводять до створення ситуацій, якими можуть скористатися сторонні особи – кіберзлочинці. Тому слід розрізняти три аспекти відповідальної поведінки.

Перший напрямок пов'язаний із забезпеченням умов відповідальної поведінки з боку міжнародних організацій та уряду. Для вирішення даного питання міжнародне право формує загальну правову основу для використання

різними країнами інформаційно-комунікаційних технологій у кіберпросторі. Вони повинні робити все можливе, щоб спробувати припинити міжнародно-протиправні дії у вигляді кібератак, кібертероризму, кібершпигунства, тощо, які походять з їх території. Також країни повинні виконувати свої зобов'язання згідно з міжнародним гуманітарним правом, тобто дотримуватися принципів обережності, відмінності, пропорційності, необхідності та гуманності у своїх кібероперація. Дотримання прав повинно відбуватися не тільки на макрорівні, але й для кожної окремої людини – користувача кіберпростору.

Жоден уряд не має достатніх фінансових, технічних, програмних, організаційних ресурсів, необхідних для реагування на кіберзлочинність. Саме тому фізичні та юридичні особи повинні самостійно забезпечувати власну безпеку в процесі здійснення ними різних операцій у кіберпросторі. Тому другим аспектом відповідальної поведінки є та, яку повинні самостійно забезпечувати представники бізнесу, в тому числі фінансового сектора. У більшості випадків їм бракує стимулів та ресурсів зосередитися на кіберзахисті споживачів. Але з іншого боку, якщо вони відчувають себе незахищеними в процесі здійснення фінансових операцій через програмні та мобільні додатки та Інтернет, то клієнти можуть відмовлятися від таких послуг або змінити їх надавача. Тому представники фінансового сектору зацікавлені у збереженні та розширені бази клієнтів, що вимагає від них впровадження більш ефективних заходів кіберзахисту.

Щодо третього аспекту відповідальної поведінки, то споживачі фінансових сервісів та послуг вважають, що особисто вони повинні нести відповідальність за власну безпеку в Інтернеті, але більшість із них не мають знань чи мотивації для цього. Так, за даними Economist Intelligence Unit (2018), 93% користувачів називають конфіденційність і безпеку однією із своїх головних проблем. За опитуванням громадської думки, яку проводила Європейська комісія (World Economic Forum, 2019), було виявлено, що 86% людей вважають, що вони мають підвищений ризик стати жертвами кіберзлочинців, особливо у фінансовій сфері. За даними PwC (World Economic Forum, 2019), 92% споживачів кажуть, що компанії повинні бути активними щодо захисту даних, 82% погоджуються, що уряд повинен регулювати процес, як компанії використовують особисті дані, і 72% вважають, що бізнес, а не уряд, найкраще підготовлений для їх захисту. Відповідно до звіту Gigya (2017), тим часом 63% людей вважають, що люди самі несуть відповідальність за свої дані, тоді як 19% вважають, що відповідальність лежить на брендах, а 18% вважають, що уряди повинні взяти на себе ініціативу в захисті користувачів. Дослідження GDMA (2018) показує різні результати: 38% респондентів кажуть, що споживачі несуть відповідальність за свої дані, а 15% очікують, що уряди активізуються. 5% вважають, що підприємства та організації повинні бути підзвітними. За звітом GDMA (2018) 35% людей вважають, що це питання

потребує об'єднаних зусиль споживачів, урядів і брендів. Звіт The Economist Intelligence Unit (2018) показує, що 31% опитаних людей очікують, що виробники пристроїв і постачальники послуг співпрацюватимуть з урядами та дотримуватимуться стандартів конфіденційності.

Тобто, відповідальність за власну безпеку та транзакцій у кіберпросторі в більшості випадків повинна забезпечуватися за рахунок власної відповідальної поведінки споживача фінансових послуг та сервісів. Які заходи доцільно вживати для того, щоб знизити ризики стати кібержертвою? Головними з них є використання системи складних паролів, особливо для мобільних платіжних додатків. Також доцільним є застосування двохфакторної ідентифікації, особливо для онлайн-банкінгу. Обмеження використання спеціальних додатків у публічних мережах може допомогти знизити ризики здійснення кіберзлочинів. Встановлення лімітів на онлайн-операції, використання окремих телефонних номерів для фінансових установ, не розголошення персональної інформації стороннім особам, не зберігання паролів в окремих файлах – це елементарні заходи, які допоможуть знизити кіберризики.

Таким чином, зростання обсягів інформації та переведення багатьох транзакцій онлайн сприяють збільшенню кіберзлочинів. Цей процес є незворотним, але є багато засобів для його контролю. Тому для забезпечення ефективної взаємодії між представниками фінансового сектору та споживачами його сервісів та послуг у кіберпросторі потрібно дотримуватися трьох ключових аспектів, пов'язаних з їх відповідальною поведінкою. Активна участь міжнародних організацій, цілеспрямовані заходи безпеки фінансових установ та персональні заходи безпеки – це той важливий базис, який буде створювати комфортні та безпечні умови для розвитку фінансового сектору у кіберплощині.

Список літератури

1. GDMA (2018). Global data privacy: What the consumer really thinks. Retrieved from https://dma.org.uk/uploads/misc/5b0522b113a23-global-data-privacy-report---final-2_5b0522b11396e.pdf (28.05.2023).

2. Gigya (2017). Privacy_Survey_Report. Retrieved from http://info.gigya.com/rs/672-YBF-078/images/201704-Gigya-DS-Privacy_Survey_Report-web.pdf (28.05.2023).

3. The Economist Intelligence Unit (2018). What the Internet of Things means for consumer privacy. Retrieved from https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf (28.05.2023).

World Economic Forum (2019). Who should be responsible for protecting our personal data? Retrieved from https://www.weforum.org/agenda/2019/01/who-should-take-charge-of-our-cybersecurity/ (28.05.2023).

ВИКЛИКИ КІБЕРБЕЗПЕКИ, ЩО СТОЯТЬ ПЕРЕД ГАЛУЗЗЮ ФІНАНСОВИХ ПОСЛУГ

CYBERSECURITY CHALLENGES FACING THE FINANCIAL SERVICES INDUSTRY

***Xinxin Wang**, president*
Jiamusi University, China

Explore the talent cultivation model of "Digital technology+", and strengthen the impact of talent cultivation models and curriculum systems in universities on talent cultivation in the digital era. The development of the digital economy involves a wide range of industries, and the construction of disciplines and majors in universities must adhere to characteristic development, determine main goals, strengthen the "digital elements", strengthen the "professional foundation", further improve and revise high-level talent training plans for disciplines and majors related to characteristic advantageous industries, and vigorously promote the interdisciplinary and integrated training mode of big data talents. At present, the talent team in the field of digital economy in university platform economy is relatively scattered, with diverse disciplinary backgrounds, especially lacking top-notch leading talents and teams. We need to further optimize the structure of the talent team, integrate existing talents in the field of digital economy, and guide teachers from relevant disciplines to gather in the field of platform economy and digital economy. System is one of the important means to regulate employee behavior. In the actual work of enterprises, it is necessary to develop management systems and measures that are in line with the actual situation of the company to ensure the normal and safe operation of the network. Artificial intelligence can respond to vulnerabilities faster and plays a crucial role in advancing network security solutions. Artificial intelligence has demonstrated high efficiency in protecting cloud services, local infrastructure, and detecting atypical user behavior. The government believes that the stability of society, the protection of civil rights and freedoms, the rule of law and order, and the maintenance of national wealth and even national integrity largely depend on effective solutions to ensure information security and protection at this stage.

Digital transformation of the economy

The Digital transformation of colleges and universities is an important part of the Digital transformation of the economy. With the support of digital campuses, we aim to provide more flexible resources for innovation and entrepreneurship education. Based on the digital environment, we aim to build an educational model of "creativity, innovation, and entrepreneurship", collaborate with Chaoxing Erya

and others, introduce a Panya teaching management platform, and offer elective courses on innovation and creativity, as well as practical training courses on V-synthesis and V-creation, as well as Chaoxing Erya entrepreneurship courses.

With the rapid development of information technology, innovation and entrepreneurship education is also changing day by day. Based on the support of digital environment, utilizing digital teaching and training platforms, utilizing flipped classrooms and blended learning models, we fully leverage students' dominant position in innovation and entrepreneurship activities. We introduce training platforms to build a "pre class, in class, and post class" full process innovation and entrepreneurship practice platform, and use online platforms to push communication and resources for students, Send knowledge points and notifications to facilitate students' online self-directed learning. Regularly conducting special surveys on students' innovation and entrepreneurship learning activities, investigating the supportive attitude, communication effectiveness, and teaching efficiency of students introduced by digital platforms, can mobilize resources from all parties.

Cyberthreats in the financial sector

The leakage of digital campus information data in universities is one of the major network threats in the financial field, which is closely related to people's work and life. In digital campuses, information data leakage is very common, and data security is also a key concern. In the platform, a large amount of information related to student innovation and entrepreneurship is stored. Once data leakage occurs, the harm caused cannot be ignored. In this process, regular security meetings should be held to help students understand the importance of data security, operate strictly according to requirements, provide a central computer room for students' innovation and entrepreneurship activities, regularly backup data, improve data security warning mechanisms, build financial guarantees related to information and data security, include operators, and provide financial and technical support from operators. The school is responsible for providing venue and policy support, and a specialized financial institution is established by the school to handle fund business and solve financial and technical security issues for students. Starting from practical teaching, we will help students successfully complete the design and planning process, and build a comprehensive risk project, Develop a project management manual to provide guidance for practical learning activities.

Corporate solutions for cybersecurity

System is one of the important means to regulate employee behavior, and through the constraints of the system, errors or accidents caused by human factors can be avoided. In the actual work of enterprises, it is necessary to develop

management systems and measures that are in line with the actual situation of the company to ensure the normal operation and safe operation of the network.

To effectively manage the entire network, it is necessary to have a dedicated person responsible for maintaining and managing this large computer network group, and this person must be familiar with computer knowledge and have rich practical experience to be competent in this job. Therefore, it is necessary to equip professional technical personnel as full-time personnel to carry out daily management and maintenance work.

In order to better ensure the normal and secure operation of the network, it is necessary to have corresponding hardware equipment to support it, such as switches, routers, and antivirus software, which are essential hardware facilities.

Innovative technologies in countering cyber threats

Artificial intelligence can respond to vulnerabilities faster and plays a crucial role in advancing network security solutions. Artificial intelligence provides a more proactive approach to network security. Artificial intelligence has demonstrated high efficiency in protecting cloud services, local infrastructure, and detecting atypical user behavior. As we further explore and discover the future of automation, enterprises must prioritize learning artificial intelligence, supporting their security measures, and promoting methods for sustained growth.

Industrial control systems are designed to operate and support critical infrastructure, widely used in industries such as energy and utilities, oil and gas, pharmaceutical and chemical production, food and beverage, and manufacturing. Due to the increasing geographical location of connected devices, threats are increasing. Although attacks on such systems may cause significant damage, they remain a soft target for opponents due to their external interaction through IoT platforms and clouds.

The existing cloud environment is not suitable for handling complex computationally intensive technologies, which are increasingly paving the way for mainstream and commercial applications. With more and more cloud computing and on prem deployed in almost every industry, such as space exploration, drug discovery, financial modeling, automobile design, system engineering and use, security will become a concern at a faster speed.

State regulation of cybersecurity

The Russian government believes that the stability of society, the protection of civil rights and freedoms, the rule of law and order, as well as the maintenance of national wealth and even national integrity, largely depend on effective solutions to issues such as ensuring information security and protection at this stage. Therefore, since the late 1980s, the highest state authority of the Russian Federation has made a series of decisions that attach great importance to protecting information security.

The Russian State Technical Committee, established in January 1992, is mainly responsible for implementing unified technical policies and coordinating work in the field of information protection. This committee leads the national information security and is responsible for maintaining the anti technology reconnaissance system, ensuring that information security is not subject to foreign technology reconnaissance, while also ensuring that information within the Russian Federation is not lost through technological channels.

Russia has established a comprehensive national system for information protection, ensuring unified national policies in the field of information protection by implementing the regulations of the National Technical Commission directly managed by the President of the Russian Federation, while balancing the interests of the state, society, and individuals. The Russian Federation government, starting from several aspects such as information security, economic security, national defense security, ecological security, and social security, divides information security strategies into two categories: discretionary security policies and selective security policies. It proposes the concept of subject object hierarchical access to control access, that is, only when the current security capability of the subject is not lower than the critical mark of the object, can information be transmitted "upwards".

In addition, the Russian Federation government has done a lot of work in ensuring information security in the fields of fiscal credit and banking. The central bank system has studied the issue of protecting information processing technology equipment and actively promoted the use of secure information technology and network technology. In the field of encryption, the School of Cryptography is engaged in research on encryption technology, focusing on strengthening research in optical fiber communication encryption and quantum encryption.

References

1. Khitskov, E. A., Veretekhina, S. V., Medvedeva, A. V., Mnatsakanyan, O. L., Shmakova, E. G., & Kotenev, A. (2017). Digital transformation of society: problems entering in the digital economy. *Eurasian Journal of Analytical Chemistry*, *12*(5), 855-873.

2. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, *105*, 102239.

3. Kravets, A. G., Bui, N. D., & Al-Ashval, M. (2014). Mobile security solution for enterprise network. In *Knowledge-Based Software Engineering: 11th Joint Conference, JCKBSE 2014, Volgograd, Russia, September 17-20, 2014. Proceedings 11* (pp. 371-382). Springer International Publishing.

4. Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. *Wireless Personal*

Communications, *95*, 169-185.

5. Shackelford, S. J., & Craig, A. N. (2014). Beyond the new digital divide: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. *Stan. J. Int'l L.*, *50*, 119.

6. Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309.

СОЦІО-ДЕМОГРАФІЧНІ ДЕТЕРМІНАНТИ ВРАЗЛИВОСТІ КОРИСТУВАЧІВ ФІНАНСОВИХ ПОСЛУГ ДО КІБЕРРИЗИКІВ

SOCIO-DEMOGRAPHIC DETERMINANTS OF THE VULNERABILITY OF FINANCIAL SERVICES USERS TO CYBER RISKS

Олена Пахненко, *к.е.н., доцент*
Сумський державний університет, Україна

Разом із розвитком цифрового банкінгу та збільшенням частки фінансових послуг, які надаються через мобільні додатки, зростають і ризики кібершахрайства та завдання фінансової шкоди споживачам фінансових послуг у кіберпросторі – при здійсненні онлайн шопінгу, проведенні цифрових платежів, в операціях з віртуальними активами тощо. Вирішення питань кібербезпеки у сфері фінансових послуг, безумовно, є результатом комплексних синергетичних дій органів державного регулювання, фінансових установ та технологічних компаній. Але разом із тим, самі споживачі фінансових послуг також несуть відповідальність за дотримання правил безпеки у кіберпросторі та збереження особистих фінансових даних.

У наукових дослідженнях з кібербезпеки розглядається вплив таких параметрів, як вік, стать, рівень освіти, національність та інших соціо-демографічних детермінант, що характеризують споживачів фінансових послуг, на особливості їх поведінки у кіберпросторі та вразливість до кіберзагроз (Anwar et al., 2017; Branley et al., 2022; Daengsi et al., 2022; Dam & Deshpande, 2020).

Особливості реакції особи на кіберризики, здатність виявляти ознаки шахрайської поведінки, правильно реагувати та захищати свої фінансові дані залежать загалом від рівня обізнаності про кібербезпеку, фінансової та цифрової грамотності, наявності попереднього досвіду взаємодії із кіберзлочинцями. Не можна ігнорувати і такі індивідуальні характеристики особистості, як ступінь довірливості, відкритості та схильність до ризику.

Сама по собі приналежність особи до певної соціально-демографічної групи за віком, статтю чи іншою ознакою, не може бути детермінантою її вразливості до кіберзагроз. Однак ці критерії дуже часто корелюють із іншими більш об'єктивними характеристиками – рівнем цифрових знань і навичок, фінансової грамотності та обізнаності з кібербезпеки. До прикладу, використаємо для аналізу показник рівня цифрових навичок. Відповідно до даних Євростату, в країнах-членах ЄС у 2021 році частка населення віком від 16 до 74 років, що мала базовий або вище базового рівень цифрових навичок, складала трохи більше половини – 54%. Згідно із методологією Євростату, загальний рівень цифрових навичок визначається кількістю типів

здійснюваних операцій, що вимагають наявності цифрових навичок, на відповідному рівні (базовому, вище базового тощо).

У розрізі вікових та гендерних груп в країнах ЄС прослідковуються значні відмінності у рівні цифрових навичок між віковими групами, тоді як відмінності у цифрових навичках залежно від статі є незначними (рис. 1).

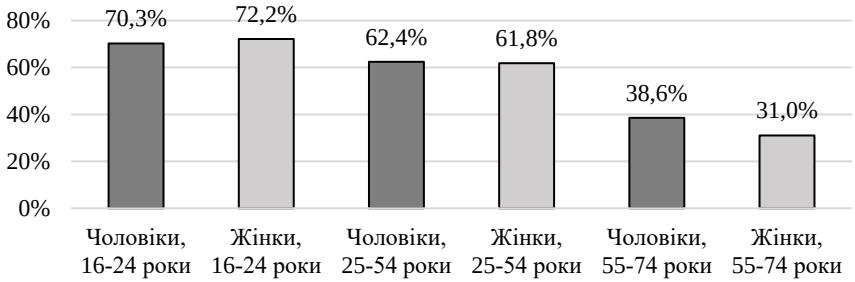

Рисунок 1. Частка осіб з рівнем цифрових навичок на базовому чи вище базового рівня у країнах ЄС у розрізі вікових та гендерних груп (сформовано автором на основі даних Eurostat, 2023)

В цілому спостерігається зниження рівня цифрових навичок із зростанням віку особи, що пов'язано зокрема із інноваційністю цифрових технологій та їх порівняно нещодавньою появою. У віковій групі від 16 до 24 років вищий рівень цифрових навичок демонструють жінки, в групі 25-54 роки показники чоловіків і жінок практично вирівнюються, а серед осіб старших 55 років значно вищою є частка чоловіків із базовим чи вище базового рівнем цифрових навичок. Наведені дані стосуються країн-членів ЄС, в яких питанням гендерної рівності приділяється багато уваги. В цілому ж у світі прослідковується значно нижчий рівень цифрової і фінансової грамотності серед жінок.

Аналізуючи ситуацію у розрізі країн-членів ЄС, можна виявити однакові закономірності зміни рівня цифрової грамотності за віковими категоріями. Водночас, загальний рівень цифрових навичок населення суттєво відрізняється між країнами. Наприклад, у Болгарії, Румунії, Албанії частка населення, що має цифрові навички не нижче базового рівня, не перевищує 30%. Натомість, у Ісландії, Нідерландах, Фінляндії, Норвегії та Швейцарії цей показник досягає майже 80%.

Зважаючи на високу динаміку розвитку цифрових технологій, задачі підвищення фінансової та цифрової обізнаності населення, інформування про кібербезпеку споживачів фінансових послуг є надзвичайно актуальними і повинні вирішуватися із залученням усіх стейкхолдерів – державних

регуляторів, надавачів фінансових послуг (фінансових установ, ФінТех компаній), громадських організацій, закладів освіти. Просвітницька діяльність у даному напрямку є одним із базових завдань формування достатнього рівня обізнаності у сфері кібербезпеки, що має суттєво зменшити вразливість споживачів фінансових послуг до кіберризиків, принаймні в тій частині, що залежить від їх особистих рішень, умінь і необхідних навичок при здійсненні онлайн покупок, виборі платіжної системи, перевірці підозрілих сайтів, виявленні ознак шахрайської поведінки тощо.

На даний момент в багатьох країнах світу наявні ініціативи, спрямовані на промоцію платіжної безпеки та цифрової фінансової грамотності. В Україні такі програми реалізуються Національним банком України. Основні правила платіжної безпеки публікують на своїх сайтах комерційні банки. Втім, враховуючи поки що недостатній рівень обізнаності населення з цих питань, особливо серед старших поколінь, а також активний розвиток цифрових технологій та можливості появи у зв'язку із цим нових шахрайських схем, актуальність питань захисту споживачів фінансових послуг від кіберзагроз в наступні роки бути лише підвищуватися.

Список літератури

1. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69,* 437–443. https://doi.org/10.1016/j.chb.2016.12.040

2. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*, *2022*, Article 2693080. https://doi.org/10.1155/2022/2693080

3. Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies, 27,* 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

4. Dam, L., & Deshpande, K. (2020). Relationship Between Demographic Variables and Awareness on Cybersecurity Threats: An Empirical Analysis. *The Orissa Journal of Commerce, 41*(2), 112-122. Available at SSRN: https://ssrn.com/abstract=3789806

5. Eurostat, 2023, Database – Eurostat. Available online: https://ec.europa.eu/eurostat/web/main/data/database

СЕКЦІЯ 3 ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ

КОНВЕРГЕНЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ФІНАНСОВИМ ЗЛОЧИНАМ

CONVERGENCE OF THE CYBER SECURITY SYSTEM AND COMBATING FINANCIAL CRIMES

***Альона Рапута**, студентка*
Сумський державний університет, Україна

На сьогоднішній день існує серйозна загроза людству у сфері фінансової безпеки з боку кібертероризму. Аналіз актуальності проблеми конвергенції системи кібербезпеки та протидії фінансовим злочинам спрямований на виявлення необхідності використання інновацій, змін, які можливі в ході виявлення взаємозв'язків між цими системами.

Фінансові злочини та зростаюча складність кібератак стали поширеною проблемою для фінансових установ по всьому світу. Впровадження засобів інформаційної безпеки в банківську інфраструктуру дозволяє захистити дані, ресурси та створити міцну основу для дотримання нормативних вимог. Стратегія безпеки даних має бути комплексною, охоплювати людей, процеси та технології, які, завдяки постійному розвитку науки, набувають нових форм та методів для боротьби з незаконними діями шахраїв у сфері фінансів.

Розробка надійної системи кібербезпеки дозволяє не тільки чітко бачити загрози, але й допомагає забезпечити дотримання нормативних вимог [1]. Щоб відповідати нормативним вимогам і протидіяти зростаючій кількості кіберзагроз і шахрайств, фінансова індустрія потребує інструментів, оснащених штучним інтелектом, а також багаторівневою системою захисту від кіберзагроз, яка підтримує швидке та масштабоване виявлення та вирішення проблем. Впровадження цих інструментів значно підвищить надійність захисту даних у сфері фінансів та допоможе протистояти кіберзагрозам, які на сьогоднішній день є актуальною проблемою у всіх сферах, а особливо у сфері фінансів.

Сфера фінансів - сфера обігу грошових і валютних цінностей, а також цінних паперів - найважливіший елемент економіки, який активно розвивається [2]. Дана сфера стала однією з найбільш привабливих для злочинної діяльності.

Злочинна діяльність у фінансовій сфері характеризується вчиненням комплексу протиправних дій, спрямованих на перешкоджання руху переважно грошових коштів або їх замінників [2].

Корисливим злочинам часто сприяє ситуація слабкого контролю за порядком роботи систем, слабкий захист систем від несанкціонованого доступу. Наприклад, недостатній захист від шахрайських дій банківських платіжних документів, недостатня якість їх виготовлення та захищеність [2].

Саме за таких умов ефективним рішенням буде конвергенція системи кібербезпеки та протидії фінансовим злочинам.

Адже в умовах, коли фінансова система держави є вразливою у сфері фінансової безпеки та має нерозвинену систему кіберзахисту – спокій і надійність не гарантовані.

В процесі вивчення теми кібербезпеки та протидії фінансовим злочинам були виявлені фактори, які варто враховувати при аналізі даної теми:

– Конфіденційність даних означає, що дані доступні лише уповноваженим особам.

– Цілісність даних означає впевненість у тому, що дані не будуть фальсифіковані або погіршені під час або після подання. Це переконання, що дані не були змінені навмисно чи ненавмисно.

– Доступність даних означає, що інформація доступна авторизованим користувачам у разі потреби. Щоб система продемонструвала доступність, вона повинна мати добре функціонуючі обчислювальні системи, засоби контролю безпеки та канали зв'язку.

– Глобальний індекс кібербезпеки (GCI), надійний орієнтир, який вимірює прихильність країн кібербезпеці в усьому світі.

– Індекс готовності мережі - має на меті виміряти ступінь готовності країн використовувати можливості інформаційних та комунікаційних технологій.

– Національний індекс кібербезпеки (NCSI) вимірює рівень готовності країни запобігати кіберзагрозам, а також готовність керувати кібер-інцидентами, злочинністю та масштабними кризами.

– Рівень цифрової трансформації (DDL) – це процес повної заміни ручних, традиційних і застарілих способів ведення бізнесу новітніми цифровими альтернативами.

– Індекс злочинності є потужним, але простим для розуміння рейтингом злочинності.

В процесі аналізу теми «Конвергенція системи кібербезпеки та протидії фінансовим злочинам» був проведений канонічний аналіз для виявлення залежності між вищезазначеними факторами.

Канонічний аналіз – це багатовимірний метод аналізу, який передбачає визначення зв'язків між групами змінних у наборі даних. Основною метою

канонічного аналізу є знаходження максимальних кореляцій між групами змінних [3].

Канонічний аналіз даних був проведений за допомогою програми STATISTICA.

	Canonical Analysis Summary (Convergensy.sta) Canonical R: .95472 Chi²(7)=170.94 p=0.0000	
N=76	Left Set	Right Set
No. of variables	1	7
Variance extracted	100.000%	43.6225%
Total redundancy	91.1491%	39.7615%
Variables: 1	DDL	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок 1. Результати канонічного аналізу

На рисунку 1 наведено результати аналізу впливу фактору «Рівень цифрової трансформації» на фактори протидії фінансовій злочинності в країнах.

Як видно, отримане значення канонічного R = 0,95472 є високим, що свідчить про наявність сильного взаємозв'язку між факторами, які характеризують рівень цифрової трансформації та боротьбу з фінансовою злочинністю.

Критерій Пірсона, який складає 170,94, і рівень значущості якого не перевищує 0,05 (p = 0,0000), підтверджує статистичну значущість коефіцієнта кореляції. Значення надлишковості для лівого набору, який являє собою фактор - «Рівень цифрової трансформації», становить 91,1491%. Це свідчить про те, що фактори правої вибірки, які описують боротьбу з фінансовими злочинами, на 91,149% пояснюють мінливість індексу рівня цифрової трансформації, що свідчить про високе значення впливу. Процес боротьби з фінансовим шахрайством в країні залежить від кіберзахисту фінансових систем, оскільки індекс цифрової трансформації на рівні 39,761% описує мінливість факторів, що характеризують боротьбу з фінансовими шахрайствами у країнах.

Отримане значення є високим, і це вказує на те, що система кібербезпеки (індекс рівня цифрової трансформації) має сильний вплив на боротьбу з фінансовим шахрайством.

Таким чином, у процесі аналізу впливу факторів кібербезпеки було виділено один показник, який має сильний вплив на фактори, що

характеризують боротьбу з фінансовою злочинністю, це «рівень цифрової трансформації».

Отже, важливість кібербезпеки зростає. Насправді, наше суспільство є більш технологічно залежним, ніж будь-коли, і немає жодних ознак того, що ця тенденція сповільниться.

Однією з переваг конвергенції кібербезпеки та запобігання фінансовим злочинам є захист мереж і даних від несанкціонованого доступу. Фінансові дані потребують надійного захисту від злочинного використання, яке є серйозною загрозою для функціонування та існування фінансових систем. Тому важливо захистити дані від несанкціонованого доступу, і саме один із показників, який був виявлений у ході дослідження, а саме – «Рівень цифрової трансформації», може допомогти покращити ситуацію, яка складається на сьогоднішній день у сфері фінансів. Для покращення рівня безпеки фінансових установ, попередження протизаконних дій у сфері фінансів потрібно провести процес трансформації та заміни застарілих, ручних способів захисту та збереження інформації на більш новітні цифрові альтернативи.

Список літератури

1. Проект Закону України від 19.06.2015 № 2126а. Про основні засади забезпечення кібербезпеки України. URL: https://ips.ligazakon.net/document/JH1N268A?an=13

2. Задубінний А. В. 2021. Стратегія кібербезпеки України: цілі та пріоритети. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/

3. Пасько Н. О. 2023. Кібербезпека як ключовий фінтех-тренд року: що варто знати про загрози та захист. URL: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/

КІБЕРБЕЗПЕКА В МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВАХ: РОЗРОБКА ТА ВПРОВАДЖЕННЯ СТРАТЕГІЙ ЗАХИСТУ

CYBERSECURITY IN SMALL AND MEDIUM-SIZED ENTERPRISES: DEVELOPMENT AND IMPLEMENTATION OF PROTECTION STRATEGIES

Анастасія Савенко, студентка
Сумський державний університет, Україна
Валерій Яценко, к.т.н, доцент
Сумський державний університет, Україна

В сучасному світі, де все більше підприємств залежать від комп'ютерних систем та електронних пристроїв, кібербезпека стає все більш актуальною та важливою проблемою для малих та середніх підприємств (МСП). У зв'язку з зростаючими загрозами кібербезпеки, захист даних та комп'ютерних систем МСП є великою та складною задачею. Однак, не забезпечення адекватного рівня кібербезпеки може призвести до надмірних витрат на відновлення даних та втрати довіри споживачів. Приділення уваги проблемі кібербезпеки в МСП є ключовим для забезпечення їх сталого розвитку та позиції на ринку.

Метою даної роботи є дослідження питання кібербезпеки в малих та середніх підприємствах, а також розробки та впровадження стратегій захисту.

В сучасному світі інноваційних технологій людська діяльність переходить до кіберпростору, що полегшує та покращує її. Таким чином, держава, приватні підприємства, соціально-адміністративний сектор тримають за ціль повну цифровізацію систем та баз даних. При цьому проблема забезпечення безпеки у кіберпросторі залишається не до кінця пропрацьовоною та потребує значних ресурсів з боку держави, однак через недофінансування та неможливість охопити безпеку кожної фізичної та юридичної особи окремо, безперебійне функціонування інформаційних та комунікаційних систем знаходиться під загрозою. На базі такого переміщення, виник та розпочав свій розвиток приватний сектор із забезпечення надійності безпеки у кіберпросторі, висвітлення основних функцій та необхідності якого є актуальним як для підприємців, що хочуть скористатися послугами IT компаній, так і робочих кадрів та підприємців у сфері кібербезпеки, що тільки розпочинають чи планують розпочати свою діяльність.

З прогресом технологій та підвищенням рівня підключення до мережі Інтернет, МСП стають все більш вразливими до кібератак та кіберзлочинності. У малих та середніх підприємств часто недостатньо ресурсів та експертизи в

області кібербезпеки, що створюєся зону вразливості для хакерів та кіберзлочинців. До загроз для МСП можна віднести наступні:

– фішингові атаки та віруси, оскільки часто призводять до викривлення або втрати важливої інформації;

– кібератаки, які можуть призвести до відключення важливих систем та збоїв у роботі підприємства;

– несанкціонований доступ до конфіденційної інформації та даних клієнтів;

– втрати даних та відмови забезпечення правильного функціонування систем.

Забезпечення кібербезпеки є надзвичайно важливим для малих та середніх підприємств (МСП) з наступних причин:

1. Обмежені ресурси: МСП, зазвичай, мають обмежені фінансові, технічні та людські ресурси для вирішення кібербезпекових проблем. Вони можуть не мати великого бюджету на кібербезпеку або доступу до широкого кола експертів. Це робить їх вразливими перед кіберзлочинцями, які можуть спрямувати свої атаки на слабкі місця;

2. Цінність даних: МСП зберігають і обробляють значну кількість цінних даних, таких як фінансова інформація клієнтів, інтелектуальна власність, персональні дані тощо. Компрометація цих даних може призвести до серйозних фінансових втрат, порушення довіри клієнтів та збитків у репутації підприємства;

3. Законодавчі вимоги: Багато країн встановлюють обов'язкові законодавчі вимоги щодо кібербезпеки, особливо щодо захисту персональних даних. Невиконання цих вимог може призвести до значних адміністративних санкцій та штрафів для МСП;

4. Постійні загрози: Кіберзлочинці постійно розвиваються та удосконалюють свої методи атак. Малі та середні підприємства, які не приділяють належної уваги кібербезпеці, можуть стати привабливою мішенню для кіберзлочинців.

Якщо розглядати попит на українському ринку, то можна навести дані з проведеного опитування з кібербезпеки бізнесу в Україні. Опитування проводили протягом майже двох місяців узимку, у ньому взяли участь 150 українських підприємств. Найбільше було компаній зі сфер ритейлу (23%), IT (14%), державного сектора (14%). Також в опитуванні взяли участь середній бізнес, фінансові, страхові компанії та інші. 91% організацій вважають, що мають повний або достатньо повний набір технологій. 52% зазначили, що можуть бачити стан речей в IT-інфраструктурі. Рівень повноцінного використання таких технологій, як багатофакторна автентифікація (MFA), захисний DNS, контроль взаємодії пристроїв у мережі (NDR), управління подіями кібербезпеки (SIEM), та іншого зрідка перевищує 40%. Від 50% до

60% респондентів розповіли, що взагалі не використовують такі технології, як програмування систем безпеки, кіберрозвідка, захист із використанням методів обману тощо. Також лише 41% компаній зазначили, що мають виокремленого CISO (керівник відділу IT-безпеки, директор з IT-безпеки).

Оскільки кібербезпека є критично важливим елементом успішної діяльності МСП, розробка та впровадження ефективних стратегій та заходів захисту є необхідними. Ці заходи можуть включати наступні елементи:

– створення стратегії та політики кібербезпеки, яка включає плани на випадок кібератак та інші ризики;

– встановлення міцних паролів та керування доступом до важливої інформації та систем;

– застосування системи бекапу даних та створення копій безпеки;

– забезпечення оновлення програмного забезпечення та антивірусних програм для дотримання стандартів безпеки;

– запровадження мережевої безпеки та систем поширення даних.

Забезпечення високого рівня кібербезпеки в МСП є критично важливим для успішної діяльності та майбутнього розвитку. Розробка та впровадження ефективних стратегій та заходів захисту надасть підприємству можливість протидіяти загрозам і захистити комп'ютерні системи та інформацію, збережений у них. Навчання працівників та відповідність вимогам щодо кібербезпеки повинні бути складовими частинами успішної політики цього питання. МСП повинні зробити все можливе, щоб захистити свою інформацію та зберегти довіру клієнтів та інвесторів.

У сучасному світі, де цифрові технології займають все більш важливу роль в бізнес-середовищі, кібербезпека стає вирішальною складовою для успіху малих та середніх підприємств (МСП). Малим та середнім підприємствам дедалі більше загрожують кібератаки, оскільки вони можуть бути менш захищеними та мати обмежені ресурси для кібербезпекових заходів.

Список літератури

1. Лише 41% компаній мають директора з IT-безпеки, третина не перевіряє аварійне відновлення – дослідження з кібербезпеки - ITC.ua. ITC.ua. URL: https://itc.ua/ua/articles/lyshe-41-kompanij-mayut-dyrektora-z-it-bezpeky-tretyna-ne-pereviryaye-avarijne-vidnovlennya-doslidzhennya-z-kiberbezpeky/ (дата звернення: 28.03.2023).

2. Microsoft Digital Defense Report 2022. Microsoft. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (date of access: 28.03.2023).

3. Про основні засади забезпечення кібербезпеки України : закон від 05.10.2017 р. № № 2163-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Tet

4. Захист персональних даних за правилами GDPR – ECPL.com.ua. URL: https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/

5. Трофіменко О. Г., Трофименко Е. Г. Кібербезпека України: аналіз сучасного стану. URL: http://dspace.onua.edu.ua/bitstream/ handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence (дата звернення: 28.03.2023).

ІНВЕСТИЦІЇ В КІБЕРБЕЗПЕКУ ЯК ДРАЙВЕР РОЗВИТКУ КОМПАНІЇ

INVESTMENTS IN CYBER SECURITY AS A DRIVER OF THE COMPANY'S DEVELOPMENT

***Анна Поліщук**, студентка*
Сумський державний університет, Україна

Кількість і витонченість кібератак зростає протягом багатьох років, спричинені розвитком великих даних, хмарних обчислень і віддаленої роботи. З більшою кількістю доступу до даних, ніж будь-коли раніше, складність захисту цифрових систем зросла експоненціально. Результат: високий і зростаючий попит на послуги безпеки, які можуть збільшити акції, пов'язані з кібербезпекою, на роки вперед. Ці тенденції можуть запропонувати одні з найбільш привабливих довгострокових інвестиційних можливостей у технології сьогодні. Сюди входить як зростаюча кількість постачальників кібербезпеки, так і все частіше оборонні компанії, які прагнуть зміцнити свої кіберпотенціали на тлі зростаючих загроз з-за кордону.

Інвестиції в кібербезпеку можуть виступати суттєвим драйвером розвитку компанії, особливо в сучасній цифровій епоці, коли кіберзагрози стають все більш поширеними і складними. Ось деякі способи, які підтверджують роль інвестицій в кібербезпеку як каталізатора розвитку компанії:

1. Захист корпоративних активів: Інвестиції в кібербезпеку дозволяють компаніям захистити свої корпоративні активи, такі як конфіденційна інформація, інтелектуальна власність, клієнтські дані тощо. Збитки від кібератак можуть бути великими, включаючи втрату довіри клієнтів, шкоду репутації і фінансові втрати. Інвестиції в кібербезпеку допомагають запобігти таким проблемам і зберегти цінні активи.

2. Забезпечення дотримання нормативних вимог: Багато галузей мають строгі нормативні вимоги щодо захисту інформації та персональних даних. Інвестиції в кібербезпеку дозволяють компаніям виконувати ці вимоги і уникнути штрафів та санкцій, пов'язаних з порушенням правил. Це особливо важливо в таких сферах, як фінанси, охорона здоров'я та електронна комерція.

3. Збільшення конкурентоспроможності: Компанії, які вкладають в кібербезпеку, можуть стати більш конкурентоспроможними на ринку. Клієнти все більше враховують рівень захисту інформації, коли вибирають постачальників послуг або партнерів. Інвестиції в кібербезпеку демонструють зобов'язання компанії до захисту даних клієнтів і підвищують її довіру.

4. Зменшення ризику: Інвестиції в кібербезпеку допомагають зменшити ризик від кібератак і інших загроз. Це включає в себе використання

передових технологій захисту, впровадження моніторингу безпеки та реагування на інциденти, навчання персоналу та розробку стратегій відновлення після кібератаки. Зменшення ризику сприяє стабільності бізнесу та збереженню репутації компанії.

5. Розширення можливостей: Інвестиції в кібербезпеку можуть створювати нові можливості для компанії. Наприклад, вони можуть дозволити впровадження нових цифрових рішень, які розширюють діяльність компанії або покращують взаємодію з клієнтами. Захищена інфраструктура може також сприяти швидкому розвитку інноваційних проектів.

6. Узагаління: Інвестиції в кібербезпеку є важливим драйвером розвитку компанії, оскільки вони допомагають захистити активи, виконати нормативні вимоги, підвищити конкурентоспроможність, зменшити ризик і розширити можливості. Правильно спрямовані інвестиції в кібербезпеку можуть стати основою стійкого і успішного розвитку компанії у цифровому світі [1].

Інвестиції в кібербезпеку можуть стати суттєвим драйвером розвитку компанії. Зростаюча загроза кібератак та кіберзлочинності ставить компанії перед необхідністю забезпечити захист своїх цифрових активів та конфіденційності даних. Інвестування в кібербезпеку може мати кілька переваг для компанії:

Захист від кіберзагроз: Інвестиції в кібербезпеку дозволяють компанії побудувати потужні захисні системи, які зменшують ризик кібератак і злочинних дій. Це допомагає зберегти репутацію компанії та уникнути фінансових втрат, пов'язаних зі зламом безпеки.

Дотримання регулятивних вимог: Багато галузей мають обов'язкові вимоги щодо кібербезпеки, які компанії повинні виконувати. Інвестиції в кібербезпеку допоможуть компанії відповідати цим вимогам та уникнути штрафів та інших правових наслідків.

Залучення клієнтів та партнерів: Забезпечення високого рівня кібербезпеки може бути конкурентною перевагою, що привертає нових клієнтів та партнерів. Компанії, які показують, що вони серйозно ставляться до захисту даних та конфіденційності, зазвичай мають більшу довіру своїх стейкхолдерів.

Інноваційний потенціал: Інвестиції в кібербезпеку можуть стимулювати розробку нових технологій та інноваційних рішень, які відповідають викликам сучасного цифрового середовища. Це може допомогти компанії зайняти лідируючі позиції на ринку та стати інноваційним лідером.

Керування ризиками: Інвестиції в кібербезпеку сприяють виявленню потенційних ризиків та їх врегулюванню. Це дозволяє компанії активно керувати кібербезпековими загрозами та знижувати можливі втрати в разі інцидентів [2].

Інвестування в кібербезпеку вимагає стратегічного підходу та аналізу ризиків, але може стати важливим фактором, який сприяє розвитку та стійкому функціонуванню компанії в сучасному цифровому світі .

Загалом, інвестиції у кібербезпеку є однією із найбільш ефективних стратегій запобігання фінансових збитків, спричинених кібератаками. Компанія, яка не є заплямованою численними випадками втрати даних чи коштів клієнтів, вважатиметься надійним партнером на ринку і, як наслідок, зможе збільшити свій потенційний дохід. Саме тому, найбільш дієвим методом пристосування введення бізнесу є інвестиції компаній у кібербезпеку.

Список літератури

1. Бурячок, В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спец. техніка. 2011.№ 3. С. 104–114. URL: http://nbuv.gov.ua/UJRN/sstt_2011_3_16

2. Бондаренко Р. В. Інформаційна безпека держави / Р. В. Бондаренко, В. М. Михальчук // Інвестиції: практика та досвід. 2021. № 5. С. 95–101. URL: http://nbuv.gov.ua/UJRN/ipd_2021_5_17

ВАЖЛИВІСТЬ ІНВЕСТИЦІЙ У КІБЕРБЕЗПЕКУ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КОМПАНІЙ

THE IMPORTANCE OF INVESTING IN CYBERSECURITY TO INCREASE THE COMPETITIVENESS OF COMPANIES

Діана Харченко, *студент*
Сумський державний університет, Україна

У світі, де практично кожна компанія має віртуальний простір, кібербезпека стає все більш актуальною та важливою. Кібератаки стають дедалі складнішими, атакуючи не лише корпоративні системи, а й персональні дані клієнтів, що може серйозно вплинути на бізнес.

Дослідження показують, що зловмисники, атакуючи комп'ютерні системи, використовують все більш складні й сучасні методи швидкого й ефективного отримання конфіденційної інформації. Кібератаки можуть призвести до значних фінансових втрат, порушень бізнес-процесів і завдати шкоди репутації компанії. Щороку хакерські атаки коштують компаніям мільярди доларів.

Відомим прикладом корпоративних кібератак є атака Equifax 2017 року, під час якої злочинці вкрали особисту інформацію понад 145 мільйонів користувачів, включаючи номери соціального страхування та іншу конфіденційну інформацію (Tara Siegel Bernard, 2017). Атака призвела до значної втрати довіри клієнтів і призвела до збитків для компанії.

Однією з найбільших проблем, з якою стикаються компанії, є забезпечення кібербезпеки під час зберігання, обробки та передачі конфіденційної інформації. Захист від кібератак ставатиме дедалі складнішим, а витрати на підтримку онлайн безпеки можуть значно зрости. Тому інвестиції в кібербезпеку стають ключовим фактором успішної роботи та конкурентоспроможності компанії.

Провідні компанії та експерти вже давно визнали важливість інвестування в Інтернет-безпеку для отримання конкурентної переваги, особливо сьогодні, коли більшість компаній працюють в Інтернеті.

За останні роки, багато експертів в області кібербезпеки досліджували важливість інвестицій у дану сферу для підвищення конкурентоспроможності компаній.

У статті "Why Cybersecurity is Important for Business?" автори наголошують, що кібербезпека стала ключовою складовою успіху сучасного бізнесу. Вони зазначають, що якщо компанія постраждає від кібератаки, це може коштувати їй не лише грошей, але й довіри та репутації споживачів, що призведе до величезних збитків. Автори стверджують, що інвестиції в онлайн

безпеку можуть допомогти підприємствам знизити ризики та стати більш конкурентоспроможними (Ron Lieber, 2019).

У статті "The Importance of Investing in Cybersecurity" автори зазначають, що кібербезпека повинна бути важливим пунктом у стратегії будь-якої компанії. Вони стверджують, що інвестиції в кібербезпеку допомагають компаніям захистити свої активи та дані, а також захистити свою репутацію та довіру споживачів. Автори підкреслюють, що організації повинні розглядати кібербезпеку як постійний процес, а не просто одноразову інвестицію (К. МакГінніс, 2018).

У статті "The Business Case for Cybersecurity" автори пишуть, що інвестування в кібербезпеку може мати позитивний вплив на фінансові результати компанії. Вони стверджують, що компанії, які забезпечують високий рівень кібербезпеки, можуть залучати нових клієнтів, зберігати існуючих та отримувати більші прибутки (К. МакГінніс, 2018).

Згідно з дослідженням компанії IBM Security та Ponemon Institute, середній витрати на Інтернет-безпеку для компаній у 2020 році становлять 3.86 мільйонів доларів. У той же час вартість даних, які підприємства повинні захищати, може досягати мільярдів доларів. Недоліки кібербезпеки можуть призвести до крадіжки особистих даних, втрати клієнтів, шкоди репутації, штрафів для порушників і навіть закриття бізнесу (Ponemon Institute, 2022).

Дослідження Accenture показують, що компанії, які інвестують у кібербезпеку, можуть отримати значні прибутки. Зокрема, компанії в енергетичному, фінансовому та технологічному секторах можуть збільшити свої річні прибутки на 5,2%, 4,8% і 3,8% відповідно, інвестуючи в кібербезпеку.

Експерти компанії Deloitte підкреслюють, що витрати на кібербезпеку можуть стати інвестицією в репутацію компанії, оскільки підвищення рівня кібербезпеки може допомогти зберегти довіру клієнтів та партнерів.

У свою чергу, компанія McAfee зазначає, що кібербезпека може стати фактором, який підвищує конкурентоспроможність компанії. Відповідно до дослідження "Winning the Game", проведеного компанією McAfee в партнерстві з Інститутом Економіки та Миру, компанії, які інвестували в кібербезпеку, мають більші шанси підтримувати своє ділове ім'я і репутації.

Багато компаній розуміють важливість кібербезпеки і вже активно інвестують у цей напрямок. Наприклад, компанія Microsoft відвели 1 мільярд доларів на інвестиції в кібербезпеку у 2020 році, а компанія IBM - 1,4 мільярда доларів. За даними дослідження PwC, 55% компаній планують збільшити свої витрати на кібербезпеку у найближчі 12 місяців. Таким чином, можна зробити висновок, що кібербезпека стає все більш і більш важливою для компаній будь-якого розміру, і інвестиції в цю галузь дозволять підвищити конкурентоспроможність і зберегти репутацію компанії (PWC, 2021)..

Окрім великих компаній, експерти також наголошують на важливості кібербезпеки для малого та середнього бізнесу. Наприклад, згідно з дослідженням

компанії Verizon, 43% кібератак спрямовані саме на малі та середні компанії, тому інвестиції в кібербезпеку є важливим фактором для захисту бізнесу від кіберзагроз.

Недостатня кібербезпека може стати причиною банкрутства малого бізнесу через втрату даних та репутації. Однак, на жаль, багато малих та середніх компаній не вважають кібербезпеку пріоритетним питанням через обмежені бюджети та незнання технологій. Тому важливо, щоб держава та інші зацікавлені сторони забезпечували належну підтримку цього сектору та надавали можливості для підвищення свідомості та розуміння проблеми.

Отже, дослідження показують, що компанії, які інвестують у кібербезпеку, мають менші ризики втратити дані, що може призвести до серйозних фінансових втрат та втрати довіри клієнтів. Вони можуть отримати конкурентну перевагу, приваблюючи клієнтів, які ставлять на перший план питання безпеки та конфіденційності.

На основі огляду літератури та аналізу досвіду провідних компаній у галузі кібербезпеки можна зробити висновок про важливість інвестицій у цю галузь для підвищення конкурентоспроможності компаній. Інтернет-безпека стала необхідною складовою успішного бізнесу в епоху цифрової трансформації, де практично кожна компанія має віртуальний простір.

Незважаючи на те, що кібербезпека є складною галуззю, яка потребує великих витрат, інвестиції у цю сферу можуть принести значну вигоду компаніям. За даними досліджень, підвищення рівня кібербезпеки може зменшити ризик кібератак на 60-70%, що може допомогти компаніям отримати конкурентну перевагу на ринку, збільшити довіру клієнтів, збільшити продуктивність працівників та зменшити ризик втрати даних.

Список літератури

1. Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber (2017). Equifax Says Cyberattack May Have Affected 143 Million in the U.S., 1. Вилучено із: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

2. Ron Lieber (2019). Why Cybersecurity is Important for Business?, 1. Вилучено із: https://onlinedegrees.und.edu/blog/why-cyber-security-is-important-for-business/

3. К. МакГінніс (2018), "The Business Case for Cybersecurity", Harvard Business Review. Вилучено із: https://hbr.org/2018/03/the-business-case-for-cybersecurity

4. Ponemon Institute (2022), "Cost of a Data Breach Report 2022", IBM Security. Вилучено із: https://www.ibm.com/reports/data-breach

5. PWC (2021). Cybersecurity, Risk & Regulatory Вилучено із: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory.html

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ЦИФРОВІЙ ЕКОНОМІЦІ: ТЕХНОЛОГІЧНІ ТА ЕТИЧНІ АСПЕКТИ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE DIGITAL ECONOMY: TECHNOLOGICAL AND ETHICAL ASPECTS

***Поліна Терляківська**, студентка,*
Сумський державний університет, Україна
***Валерій Яценко**, к.т.н., доцент*
Сумський державний університет, Україна

Штучний інтелект (ШІ) і цифрова економіка взаємодіють у тісному зв'язку, відкриваючи нові можливості для розвитку бізнесу та підвищення продуктивності. ШІ допомагає вирішувати складні завдання, аналізувати великі обсяги даних та впроваджувати інновації в цифрову економіку. Цифрова економіка надає ШІ доступ до великої кількості даних, які необхідні для навчання та покращення алгоритмів ШІ. Результатом їх взаємодії є підвищена ефективність бізнес-процесів, розширення ринків та поява нових інноваційних продуктів та послуг.

Мета дослідження полягає у розкритті ролі штучного інтелекту в цифровій економіці з урахуванням технологічних та етичних аспектів.

ШІ і цифрова економіка взаємодіють у різних аспектах, що відкриває широкі можливості для розвитку бізнесу та трансформації економічного ландшафту. Можна виділити кілька ключових аспектів їх взаємодії:

1. *Аналітика та прийняття рішень*. ШІ має потужні аналітичні можливості, що дозволяють швидко та точно аналізувати великі обсяги даних, виявляти складні залежності та робити прогнози. Це надає компаніям цінні інсайти, розкриває ринкові тенденції, передбачає попит на товари та послуги, що допомагає приймати об'єктивні та кращі рішення.

2. *Покращення ефективності операцій*. ШІ дозволяє автоматизувати рутинні та повторювані завдання, що сприяє підвищенню продуктивності та зниженню витрат. Наприклад, автоматизовані процеси виробництва, логістики, обслуговування клієнтів та управління запасами дозволяють ефективніше використовувати ресурси та скорочувати час, необхідний для виконання завдань.

3. *Покращення користувацького досвіду*. ШІ допомагає створювати персоналізовані рішення та послуги для клієнтів. Воно аналізує дані про користувачів, їх поведінку та вподобання, щоб надавати індивідуальні рекомендації, персоналізовану рекламу та підтримку. Це поліпшує користувацький досвід та сприяє збільшенню лояльності клієнтів.

4. *Розвиток нових продуктів та послуг*. ШІ активно сприяє інноваціям в цифровій економіці, допомагаючи компаніям розробляти нові продукти та

послуги. Він може використовуватись для створення розумних пристроїв, вбудованих систем, віртуальної та доповненої реальності, автономних систем, голосових асистентів та багатьох інших інноваційних рішень. ШІ дозволяє підприємствам впроваджувати новаторські розробки та займати провідні позиції на ринку.

5. *Розробка інтелектуальних систем*. ШІ допомагає створювати інтелектуальні системи, які здатні адаптуватися та навчатися з досвіду. Використання нейромереж, глибокого навчання та машинного навчання дозволяє системам удосконалюватись, а також адаптуватись до змінних умов. Це робить їх більш гнучкими та ефективними в розв'язанні складних задач.

6. *Розширення ринків та глобалізація*. ШІ сприяє розширенню ринків та глобалізації підприємств. Завдяки автоматизації та покращеному аналізу даних, компанії можуть працювати більш ефективно на міжнародному рівні, розуміти споживацькі преференції та місцеві контексти, а також адаптувати свої продукти та послуги до різних ринків. Це дозволяє підприємствам здійснювати глобальні операції та займати лідируючі позиції на світовій арені.

7. *Покращення кібербезпеки*. ШІ може бути використаний для виявлення та запобігання кібератакам та несанкціонованому доступу. Він допомагає аналізувати великі обсяги даних, виявляти аномалії та вразливості у системах, а також реагувати на кіберзагрози у режимі реального часу. Це сприяє забезпеченню безпеки в цифровому просторі та захисту конфіденційної інформації.

8. *Створення нових робочих місць*. Хоча використання ШІ може призвести до автоматизації певних робочих місць, воно також відкриває нові можливості для створення робочих місць, пов'язаних з розробкою, впровадженням та підтримкою ШІ. Запит на фахівців у галузі машинного навчання, аналізу даних, розробки алгоритмів та інших сфер, пов'язаних з ШІ, постійно зростає. Це сприяє стимулюванню інновацій та підтримці зростання робочих місць у цифровій економіці.

9. *Підтримка розробки економічних моделей*. ШІ може бути використаний для моделювання та прогнозування економічних процесів. Він надає можливість створювати складні економічні моделі, аналізувати взаємодію різних факторів та здійснювати прогнозування економічного розвитку. ШІ використовується для обробки великого обсягу даних та виявлення складних залежностей між економічними змінними, що допомагає економістам та дослідникам зрозуміти та передбачити майбутні тенденції у галузі економіки. Це сприяє поліпшенню точності та надійності економічних прогнозів і допомагає приймати обґрунтовані рішення в економічних сферах.

ШІ грає важливу роль в цифровій економіці, впливаючи на технологічні, економічні та етичні аспекти суспільства. Розглянемо більш детально технологічні та етичні аспекти.

Технологічні аспекти:

1. *Автоматизація та ефективність*: ШІ може автоматизувати рутинні завдання, зменшуючи залежність від людської праці. В результаті цього підприємства можуть підвищити ефективність виробництва та оптимізувати свої операції.

2. *Аналіз даних*: ШІ здатний обробляти та аналізувати великі обсяги даних швидше, ніж люди. Це дозволяє отримувати цінні інсайти, прогнозувати тенденції та приймати кращі рішення на основі фактів.

3. *Розвиток нових технологій*: ШІ сприяє розвитку інших передових технологій, таких як розпізнавання образів, голосові інтерфейси, робототехніка тощо.

Етичні аспекти:

1. *Робочі місця та безробіття*. Впровадження ШІ може призвести до змін в ринку праці. Деякі види робіт можуть бути замінені ШІ, що призводить до втрати робочих місць для людей. Це ставить питання соціального захисту та перекваліфікації працівників.

2. *Прозорість та відповідальність*. Розробка ШІ повинна враховувати етичні принципи, щоб забезпечити прозорість, відповідальність та справедливість. Це означає, що алгоритми машинного навчання повинні бути справедливими, уникати дискримінації тощо.

3. *Конфіденційність*. Збір і обробка великих обсягів даних ШІ може порушувати приватність та конфіденційність особистої інформації. Захист особистих даних та встановлення ясних правил щодо їх використання є важливим етичним аспектом в розвитку ШІ.

4. *Вплив на суспільство*. ШІ може мати глибокий вплив на суспільство, включаючи зміну робочих місць, економічну нерівність та зміну способу життя людей. Це вимагає постійного вивчення та розуміння соціальних наслідків впровадження ШІ та прийняття відповідних заходів для мінімізації негативних впливів.

Отже, ШІ відіграє важливу роль в цифровій економіці, впливаючи на різні аспекти бізнесу та суспільства. Він забезпечує точний аналіз великих обсягів даних, покращує ефективність операцій підприємств, розробляє персоналізовані рішення для клієнтів, сприяє розвитку нових продуктів та послуг, а також підтримує розробку економічних моделей. Все це допомагає підприємствам досягати конкурентної переваги, підвищувати продуктивність та покращувати користувацький досвід Але, використання ШІ в цифровій економіці потребує збалансованого підходу, де технологічні можливості супроводжуються етичними принципами. Запровадження правильних політик та регуляторних рамок може допомогти забезпечити, що ШІ сприяє сталим соціально-економічним перевагам без негативних наслідків для суспільства.

ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

BLOCKCHAIN TECHNOLOGY FOR COUNTERING CYBER THREATS IN THE FINANCIAL SERVICES SECTOR

Артем Штефан, студент
Сумський державний університет, Україна

Величина успіху релізу децентралізованої електронної платіжної системи біткоін (Bitcoin) у 2009 році, що започаткувала період динамічних змін у поглядах на грошові ресурси, не була би можливою без інтегрованої технології розподіленої бази даних блокчейн (Blockchain), оскільки вона показала принципово новий підхід до безпекової архітектури зберігання даних, а також проведення транзакцій.

Зі зростанням попиту на електронні гроші у вигляді криптовалют, у нерозривному зв'язку, збільшувався і обсяг їх блокчейну. Так, протягом січня 2019 – червня 2022рр. розмір зазначеної розподіленої бази даних збільшився з 197.53 до 404.43 гігабайт (204.74%) і продовжує зростати до сьогодні. Для наочної демонстрації динаміки величини блокчейну Bitcoin пропонується звернутися до рисунка, наведеного нижче (рис. 1).

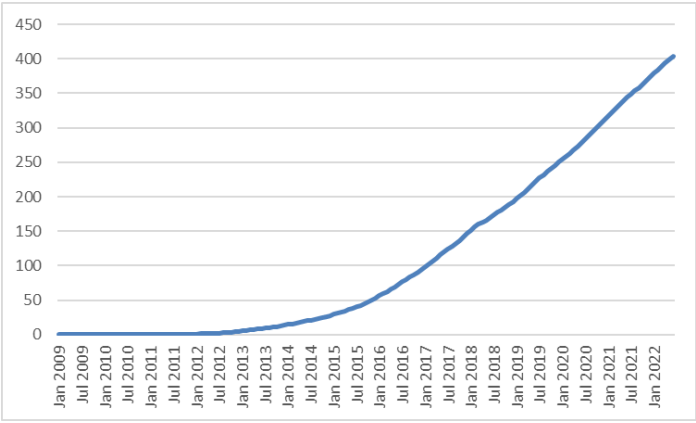

Рисунок 1. Розмір блокчейну Bitcoin, гігабайт (січень 2009 – червень 2022)

Побудовано на основі даних з джерела [1]

Наведений вище графік підтверджує швидкий темп зростання блокчейн біткоін.

Технологія блокчейн стала відомою завдяки високому ступеню захищеності від зламів, тому доречним буде окреслення її архітектури, принципу роботи. Як уже зазначалося, розглядувана технологія базується на фрагментованій базі даних. Це означає, що кожен екземпляр запису у ній розподіляється на різних електронно-обчислювальних машинах. Децентралізація робить такі сукупності даних значно захищенішими, порівняно з базами даних у класичному їх розумінні.

Структура блокчейн включає три складові:

– користувацькі додатки;
– децентралізований реєстр;
– однорангова мережа.

Додатки дозволяють здійснювати контроль над інформацією, що зберігається в блокчейн, відстежувати транзакції тощо, за допомогою зрозумілого користувачеві графічного інтерфейсу.

Наступна складова, децентралізований реєстр, підтверджує узгодженість і захищеність глобального реєстру. На цьому рівні транзакції можуть бути згруповані в блоки, які криптографічно пов'язані один з одним. Транзакції можна визначити як обмін токенами між двома учасниками. Кожна транзакція проходить процес валідації, перш ніж вона буде вважатися легітимною [2].

Під одноранговою мережею варто розуміти сукупність вузлів – комп'ютерів, які зберігають однаковий набір даних і пов'язані між собою. Крім того, вони можуть проводити обмін інформацією з однаковим обсягом прав. Дуже показовим прикладом можна назвати обмін криптовалютою між її тримачами без послуг посередників у вигляді банків [3].

Варто зазначити, що кожен зі своєрідних блоків, на які розбивається інформація, захищається хешем, який змінюється в усього ланцюга блоків щоразу при роботі з ним.

Етапи роботи описаної системи в узагальненому вигляді наведено на схемі нижче (рис. 2).

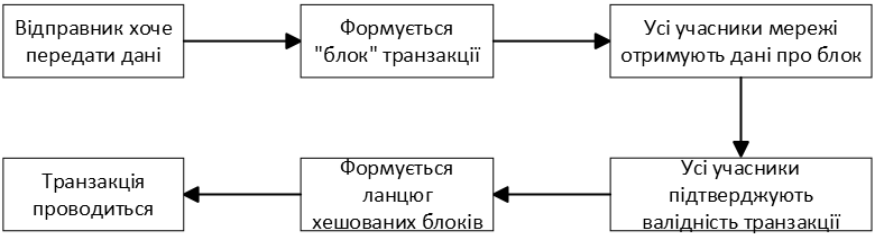

Рисунок 2. Порядок роботи блокчейн

Побудовано на основі даних з джерела [2]

Два основні типи блокчейнів – публічний і приватний, пропонують різні підходи до забезпечення цілісності і безпеки даних. Так, публічні блокчейни використовують комп'ютери, підключені до загальнодоступного Інтернету для перевірки транзакцій і об'єднання їх для додавання до реєстру. З іншого боку, приватні блокчейни, як правило, дозволяють приєднуватися лише юридичним особам. Будь-яка організація може приєднатися до публічних блокчейнів, але вони можуть не підходити для підприємств, які турбуються про конфіденційність інформації будь-якого характеру, що передається мережею [4].

На сьогоднішній день досліджувана технологія використовується, переважно, в якості утворення цифрового аналогу цінних паперів, невзаємозамінних токенів (NFT); для проведення грошових розрахунків між тримачами відповідних крипторесурсів.

Попри те, що не в усіх країнах світу вона регламентована у правовому аспекті, перспективи її використання у традиційній фінансовій сфері, завдяки безпековій компоненті, є очевидними. Крім того, практично всі існуючі фінансові послуги можливо надавати таким чином. Однак необхідно врахувати той факт, що відсутність посередників у порядку розрахунків може призвести до збільшення частки тіньової економіки, що суперечить державним інтересам.

Таким чином, вищезазначене вказує на необхідність проведення подальших досліджень з метою пошуку компромісу між ефективною протидією кіберзагрозам та прозорістю у сфері фінансових послуг.

Список літератури

1. *Bitcoin blockchain size 2009-2022 | Statista*. (б. д.). Statista. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

2. Shekhar Sarmah, S. (2018). Understanding Blockchain Technology. *Computer Science and Engineering*, *8*(2), 23–29. http://article.sapub.org/10.5923.j.computer.20180802.02.html

3. *Що таке однорангові мережі (P2P) в блокчейні? | EXBASE.IO*. (б. д.). EXBASE.IO - create crypto wallet online | Cryptocurrency Wallet. https://exbase.io/uk/wiki/odnorangovi-merezhi

4. *What Is Blockchain and How Does It Work? | Synopsys*. (б. д.). Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. https://www.synopsys.com/glossary/what-is-blockchain.html

ЦИФРОВІ ІННОВАЦІЇ У ФІНАНСОВИХ ПОСЛУГАХ: НОВІ МОЖЛИВОСТІ ТА ВИКЛИКИ БЕЗПЕКИ

DIGITAL INNOVATION IN FINANCIAL SERVICES: NEW OPPORTUNITIES AND SECURITY CHALLENGES

Катерина Славгородська, *студентка*
Сумський державний університет, Україна
Валерій Яценко, *к.т.н., доцент*
Сумський державний університет, Україна

У сфері фінансових послуг спостерігається цифрова трансформація, яка охоплює розвинуті країни з ринковою економікою і надає перспективну цифрову альтернативу традиційним банкам. Сучасні компанії, що надають фінансові послуги, стикаються з численними викликами, багато з яких пов'язані з швидкими змінами в технологіях. Хоча більшість з них прийняла технологічну революцію, все ще існують значні проблеми, з якими їм доводиться зіткнутися. Однак цифрові інновації також відкрили багато можливостей, таких як миттєві цифрові платежі, блокчейн, штучний інтелект і т. д.

Мета дослідження – аналіз цифрових інновацій у фінансових послугах, нових можливостей та викликів безпеки.

Перший виклик безпеки, на який я хотіла б звернути увагу – кіберзлочинність. Це дуже розповсюджена проблема зараз, бо попит формує пропозицію, тому оскільки зростають можливості переводити фінансову систему в режим онлайн, то зростає і бажання злочинців нажитись на цьому. Зростає кількість витоків даних, до яких залучені фінансові компанії. Фірми, що надають фінансові послуги, являються головними мішенями для кіберзлочинців. Через те, що вони зберігають конфіденційні дані, то з більшою ймовірністю можуть стати об'єктом атаки. Керівники фінансових установ вже добре знайомі з впливом кіберзагроз на їхню галузь. На жаль, навряд чи ситуація зміниться на краще найближчими роками через наступні чинники:

– використання сторонніх постачальників;

– стрімкий розвиток, складність технологій;

– транскордонний обмін даними;

– збільшення використання мобільних технологій клієнтами, включаючи швидке зростання Інтернету.

Кібербезпека вже є важливою, і вона стане ще більш значущою для установ та їхніх регуляторів у майбутньому. Виклик буде полягати в тому, щоб збалансувати безпеку зі зручністю для клієнтів. Маючи відповідні інструменти, фінансові установи повинні покращити свою здатність управляти

кібер-ризиками. Наприклад, фінансові установи повинні впроваджувати інструменти інтелектуального аналізу даних

та інші технології для виявлення аномалій в системах безпеки і шахрайства.

Зважаючи на ефективність конкуренції, яка базується лише на цифрових технологіях, банкам і кредитним спілкам потрібно буде розглянути можливість відмови від непрофільних операцій та використання інтелектуальної автоматизації. Крім того, організаціям потрібно буде переосмислити процеси бек-офісу і замінити застарілу інфраструктуру. Сектор фінансових послуг повільно впроваджує цифрову трансформацію. Проблеми із застарілими системами в поєднанні з великими обсягами даних і небажанням здійснювати потенційно ризиковані процеси змін, призвели до того, що багато компаній відстають коли справа доходить до впровадження нових технологій.

Щоб залишатися конкурентоспроможними з точки зору витрат і мати гнучкість, якої вимагають інновації, фінансовим установам потрібно буде оновити свою інфраструктуру, щоб зробити її більш гнучкою. Їм знадобиться архітектура, яка зможе адаптуватися до змін вимог і взаємодіяти з даними і системами, які можуть бути де завгодно. І в більшості випадків фінансовим установам знадобиться значна переорієнтація.

Технології змінили очікування споживачів та бізнесу в сфері платежів. Доступність миттєвих платежів пропонує банкам привабливу можливість досягти швидкості транзакцій, яку споживачі очікують від банківського обслуговування, та підвищити рівень задоволеності клієнтів. Завдяки миттєвим платежам більше транзакцій буде здійснюватися в цифровому вигляді, а не готівкою, а це означає, що платежі стануть більш дешевшими і зручнішими для користувачів. Нарешті, розширюючи та поєднуючи можливості миттєвих платежів з рішеннями для електронної та мобільної комерції, банки та кредитні спілки зможуть розробити інноваційний портфель нових послуг.

Фірми, що надають фінансові послуги, впроваджують технологію блокчейн для підвищення ефективності, рентабельності та безпеки в усьому спектрі фінансових послуг. Деякі фінансові установи вже почали тестувати використання блокчейну для міжбанківських переказів. Багато хто бачить величезні переваги в оптимізації та автоматизації процесів за допомогою смарт-контрактів. Технологія блокчейн використовується в біткоїнах, платіжних транзакціях, банківській сфері та інших галузях. Криптовалюта - це засіб обміну, наприклад, долар США. Блокчейн надає різні переваги у фінансових послугах, такі як підвищена прозорість, точне відстеження і зниження витрат. Системи блокчейн можуть бути набагато дешевшими, ніж існуючі платформи, оскільки вони усувають цілий рівень накладних витрат,

пов'язаних з підтвердженням автентичності. Блокчейн призводить до швидших і дешевших розрахунків і може заощадити мільярди доларів від транзакційних витрат, одночасно підвищуючи прозорість.

У сфері бізнесу по наданню фінансових послуг, власники постійно стикаються з новими конкурентами, мінливою демографічною ситуацією та зростаючими очікуваннями клієнтів. Технології пропонують рішення, що дозволяють фінансовим установам скоротити витрати і стати більш ефективними в тому, що вони роблять.

Але більшість технологій не є запатентованими, тому це схоже на перегони: якщо фінансові установи не встигнуть моргнути оком, вони можуть виявити, що їх конкурент вже створив переваги, з якими їм тепер важче зрівнятися. Компанії, що надають фінансові послуги мають різноманітні можливості та виклики, з якими вони стикаються сьогодні через стрімкий розвиток цифрових інновацій.

Цифрові інновації мають значний вплив на сектор фінансових послуг, пропонуючи нові можливості, які змінюють спосіб, яким ми взаємодіємо з грошовою системою. За останні роки фінансові компанії активно впроваджують технології, такі як миттєві цифрові платежі, блокчейн, штучний інтелект та інші, що дозволяють прискорити процеси, поліпшити доступність послуг та забезпечити зручність для клієнтів.

Однак, разом з новими можливостями постають і виклики безпеки. Цифрові фінансові послуги стикаються з ризиками, пов'язаними з кіберзлочинністю та крадіжками особистої інформації. Забезпечення кібербезпеки стає невід'ємною частиною успішної цифрової трансформації у фінансових послугах. Компанії повинні інвестувати в розробку та впровадження ефективних заходів безпеки, таких як шифрування даних, мультифакторна аутентифікація та системи виявлення загроз. Розуміння ризиків та постійне моніторингове оновлення системи безпеки є необхідними для запобігання кібератакам та захисту даних клієнтів.

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЙНІ ПРОЦЕСИ У РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

DIGITAL TECHNOLOGIES AND INNOVATION PROCESSES IN THE DEVELOPMENT OF THE DIGITAL ECONOMY

Христина Чуб, студентка
Сумський державний університет, Україна
Валерій Яценко, к.т.н., доцент
Сумський державний університет, Україна

Цифрові технології та інноваційні рішення, впродовж останніх десятиліть, щодня змінюють спосіб життя людей, функціонування підприємств і навіть цілих держав, впливаючи на усі сфери життя суспільства. Вони дозволяють обробляти величезні обсяги даних, що в свою чергу створює нові можливості. Більше того, вони стають ключовими факторами, що визначають економічний розвиток країн.

Метою дослідження є аналіз сучасного стану цифрової економіки, ознайомлення з наявними цифровими технологіями та інноваційними процесами, що підтримують розвиток цифрової економіки, виявлення переваг впровадження цифрових технологій, викликів, що стоять на шляху переходу до цифрової економіки та способів їх подолання.

По своїй сутті цифрова економіка є економікою, у якій основним каталізатором розвитку виступають цифрові технологій. Характеризується вона зростанням важливості цифрових платформ, цифрових послуг та товарів. Швидкість та динамічність змін, глобалізація є її особливостями. В свою чергу цифрові технології стимулюють інноваційні процеси, виникнення нових продуктів, послуг та ідей, що можуть бути пов’язані зі змінами у підходах до управління, в організаційних процесах, а також способах співпраці. Разом цифрові технології на інновації мають значний вплив на різні сектори економіки. Серед найбільш перспективних цифрових технологій, що мають неабиякий вплив на цифрову економіку, можна виділити 8 основних напрямів (рис. 1).

Інституційно-правове оформлення розвитку цифрової економіки в Україні розпочалося у 2013 році. У січні 2018 року Уряд схвалив Концепцію розвитку цифрової економіки та суспільства України на 2018– 2020 роки та затвердив план заходів щодо її реалізації.

До основних напрямів розвитку цифрової економіки в Україні можна віднести подолання цифрового розриву в суспільстві та цифровізацію реального сектора економіки. Існують два сценарії розвитку цифрової економіки України: інерційний (еволюційний) та цільовий (форсований). Форсований сценарій передбачає перехід української економіки до цифрової

за 3–5 років та перетворення України (до 2030 р.) на європейського лідера у галузі інновацій та нових технологій з часткою цифрової економіки розміром 65% у загальному ВВП. Проте з повномасштабним вторгненням російської федерації на територію України цей процес може значно сповільнитися.

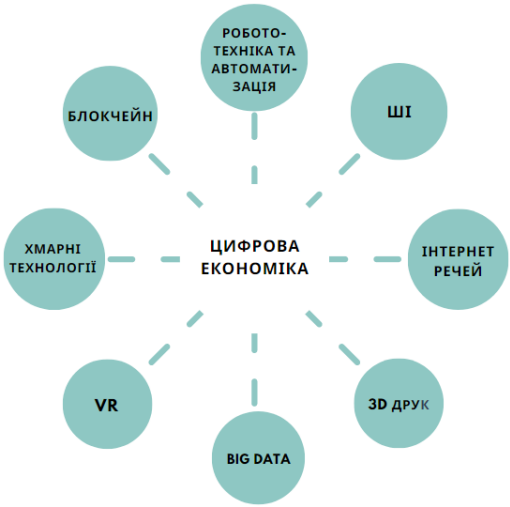

Рисунок 1. Найбільш перспективні напрямки розвитку цифрових технологій, що мають вплив на цифрову економіку

Блокчейн. Технологія, що дозволяє безпечно та надійно зберігати дані у вигляді ланцюжка блоків. Завдяки цьому можна створювати нові продукти (сервіси), що будуть забезпечувати безпеку та прозорість у найрізноманітніших галузях. Для прикладу, у фінансовій галузі блокчейн може бути використаний для проведення безпечних транзакцій, а також зменшення ризиків шахрайства.

Технології автоматизації та робототехніки. Їхнє впровадження дозволяє збільшити продуктивність праці, зменшити витрати на експлуатацію та оплату праці, покращити якість продукту. Відбувається одночасно втрата робочих місць та створення нових, що потребують перекваліфікації та навчання персоналу. За даними Міжнародної федерації робототехніки (2018), продажі промислових роботів у світі подвоїлися між 2011 та 2017 роками. Ця тенденція зберігається і надалі. Країнами з найвищою щільністю роботів на сьогоднішній день є Республіка Корея (710 роботів на 10 000 працівників) та Сінгапур (658 роботів).

Хмарні технології. За допомогою них, можна зберігати та обробляти великі обсяги даних на віддалених серверах (більше не потрібно

використовувати локальні пристрої збереження, а за необхідності можна колективно працювати над файлами легко редагуючи та обмінюючись даними на відстані), створювати резервні копії важливих даних (більше немає загрози випадкового пошкодження чи втрати даних), можна використовувати потужні обчислювальні ресурси без необхідності фізичного володіння ними, а також доступ до своїх даних з будь-якого пристрою, у якого є доступ до Інтернету. Це все значно спрощує роботу бізнесу.

Інтернет речей. Технологія під'єднує об'єкти (які на перший погляд не мають ніякого зв'язку з Інтернетом) обладнані спеціальними датчиками до мережі Інтернет та надає їм здатність взаємодіяти між собою. Яскравими прикладами може бути створення розумних пристроїв (таких як розумні годинники, а в медицині це розумні пристрої для відстеження стану пацієнта тощо), розумні будинки (якими можна керувати на відстані регулюючи температуру, освітлення, безпеку приміщення і т.д.) і навіть створення цілих розумних міст.

Штучний інтелект (ШІ). Його поле застосування дуже широке. Серед основних його способів використання можна виділити: розпізнавання та обробка зображень (аналіз медичних зображень, виявлення обєктів та осіб, відеоспостереження тощо), обробка природної мови (автоматичний переклад, голосові помічники, розпізнавання та синтез мови, аналіз тексту), робототехніка та автономні системи, прогнозування та аналітика даних (фінансові прогнози, медична діагностика, маркетинговий аналіз і т.п.), надання персоналізованих послуг (створення персоналізованих рекомендацій, реклами, музики, фільмів і т.д.). І це лише частина можливих способів його застосування.

Технології Big Data (великі дані) аналізують великі обсяги даних, виявляють зв'язки, тренди та закономірності; допомагають знайти проблемні зони в ділових процесах; збирають та аналізують дані про користувачів для створення персоналізованої реклами та пропозицій. Підприємства застосовують їх для покращення стратегічних рішень, оптимізації ресурсів, підвищення продуктивності, зниження витрат, створення нових бізнес-моделей та потрібних ринку товарів (послуг) тощо.

Технології віртуальної реальності (VR) використовуються в ігровій індустрії, кіно, туризмі (люди можуть відвідувати визначні місця у віртуальному форматі); медицині, авіації, військовій сферах задля створення в безпечних віртуальних середовищах реальних ситуацій для навчання та тренувань; для моделювання та візуалізації архітектурних проектів та дизайнів задля того, щоб на ранніх етапах реалізації отримати уявлення про фінальний вигляд продукту; у маркетингу VR використовують для покращення маркетингових кампаній та продажів (дозволяючи клієнтам перед покупкою

переглянути віртуальні магазини з віртуальними товарами та випробувати їх у віртуальному форматі).

Тривимірний (3D) друк може кардинально змінити виробничий процес. З допомогою 3D-друку можна швидко створювати прототипи, виготовляти вироби на замовлення. Так підприємства підвищують ефективність виробничих процесів, скорочуючи час та витрати на розробку та виготовлення товарів, що задовільнять індивідуальні потреби клієнтів. У деяких країнах вже можна знайти низку підприємств, що займаються 3D-друком.

Незважаючи на усі переваги та потенціал цифрових технологій, їх впровадження також має свої проблеми. Найбільшою серед них є кібербезпека: загроза конфіденційності та безпеки інформації. Тому зараз надзвичайно важливим завданням є розробка ефективного кіберзахисту. Ринок праці також потерпає від динамічних змін під впливом запровадження автоматизованих систем та штучного інтелекту. Небезпека цифрового розриву — розрив між тими, хто має доступ до цифрових технологій, і тими у кого немає можливості їх використовувати та отримувати знання з їх допомогою. Є необхідність розробити етнічні норми щодо етичного використання цифрових технологій. Всі ці проблеми вимагають уваги та вирішення.

Вирішити їх можна шляхом вдосконалення систем кібербезпеки, систем виявлення та запобігання кібератак, розробкою політики конфіденційності, контролю доступу до даних, забезпечення доступу до цифрових технологій для усіх груп населення та підвищення кіберграмотності. Звичайно ж це потребує не малих інвестицій. Необхідно створити сприятливі умови. Держава, бізнес, міжнародні організації повинні об’єднатися заради досягнення поставленої мети. Їхня співпраця забезпечить обмін знань найкращих у своїй справі, розробки спільних стратегій та стартапів для розвитку цифрової економіки.

Отже, нині цифрові технологій та інновації мають вплив фактично на всі сфери економіки та суспільства. Вони підвищують продуктивність, створюють нові можливості для підприємництва, змінюють бізнес-моделі, способи виробництва та споживання. В цілому вони покращують якість життя людей. Розвиток цифрової економіки вимагає забезпечення доступу до цифрових технологій та ефективного регулювання. Це забезпечить зростання ВВП та конкурентоспроможність країн. Проте, існують, існували та будуть існувати, проблеми та виклики, які винникають в процесі впровадження цифрових технологій. Насамперед це кібербезпека та робочі місця. Розробка та запровадження відповідних законодавчих норм та стандартів, розвиток кіберзахисту, забезпечення доступу до цифрових технологій для всіх верств населення, освітні заходи по кіберграмотності є надзвичайно важливими кроками у забезпечені успішного переходу до цифрової економіки.

ТЕНДЕНЦІЇ МОДЕЛЮВАННЯ DUE DILIGENCE ДЛЯ ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ

TRENDS IN DUE DILIGENCE MODELING TO COUNTER FINANCIAL CYBER FRAUD

Тетяна Доценко, *доктор філософії*
Технічний університет Берліну, Німеччина
Дарина Бережна, *студентка*
Сумський державний університет, Україна

Суттєвим ризиком для фінансово-економічної безпеки та стабільності сучасних суб'єктів господарювання є фінансові шахрайства, що можуть статися через відсутність чіткої ясності функціонування організації, неналежну діяльність установи, недоліки інформаційного та технічного забезпечення, фінансові питання. Для запобігання шахрайствам, виходячи із специфіки функціонування підприємств, потрібно проводити їх перевірки, такі як аудит, оцінка, податкові перевірки. А в сучасних цифровізованих умовах функціонування суб'єктів господарювання, особливої актуальності набуває удосконалення системи фінансового захисту, в тому числі через застосування такої процедури перевірки як Due diligence, що є особливо ефективною в аспекті протидії фінансовим кібершахрайствам.

Поняття due diligence є відносно новою категорією, що набуває активного використання серед сучасних науковців світу: Елбел Дж., Бозе О'Рейлі С., Грзіч Р., Дева С., Ліеса К.Р.Ф., Седано Т. Г., Літвін Д., Гуаніпа Х. Дж., Чіма Дж. Т., Камолетто С., Корацца Л., Піцці С., Сантіні Е., та ін. Однією з головних причин проведення перевірок виступають ризики та загрози фінансових злочинів та, згідно останніх тенденцій, кібершахрайств, що досліджуються науковцями: Ніколлс Дж., Куппа А., Ле-Хак Н., Хіран К. К., Рао С.С., Шарма Р., Міна Р., Ліонов С., Главічка Р., Бойко А., Миненко С., Гарай- Фодор М., Кузьор А., Брожек П., Кузьменко О., Яровенко Х., Васильєва Т., Белло М., Гріффітс М., та ін. При чому, у напрямку протидії фінансовим шахрайствам, в тому числі й кібершахрайствам, практики починають використовувати елементи методики due diligence підприємств: Калина І., Хурдей В., Шевчук В., Власюк Т., Леонідов І., Читіміра Х., Мунедзі С.

Особливу роль у дослідженні економічних процесів відводять моделюванню. Досліджуючи поняття due diligence, не можливо не відмітити важливість моделювання його процесів та етапів, що висвітлюють наступні фахівці: Каранланте М., Д'Амато В., Ферсіні П., Форте С., Мелісі Г., Рой В., Дежарден Д., Фертел К., Уелле-Пламондон К., Аман А., Реджі Д. Дж., Лі З. , Лю В., Сунь Ю., Юксель С., Дінсер Х., Лю Ю., Фен Ю., Чжоу Б. (Carannante et al., 2023;

Aman et al., 2022; Li et al., 2022). Додатково слід зупинитися на моделюванні в аспекті протидії фінансовим кібершахрайствам, як визначальної складової досліджуваного питання, що представлені у роботах: Лінь К., Гао Ю., Васильєва Т.А., Кузьменко О.В., Стоянець Н.В., Артюхов А.Є., Боженко,В.В.; Кузьор А., Васильєва Т., Кузьменко О., Койбічук В., Брожек П., Кузьменко О.В., Кубалек Й., Боженко В.В., Кушнерьов О.С., Віда І., Вахід С.Д. М., Буя А.Г., Хасрол Йоно М.Н.Х., Азіз А.А. , Буджа А.Г., Вахід С.Д.М., Рахман Т.Ф.А., Дераман Н.А., Джоно М.Н.Х.Х., Азіз А.А. (Vasilyeva et al., 2022; Kuzior et al., 2022; Kuzmenko et al., 2021).

Проаналізувавши літературні надбання з досліджуваного питання, було сформульовано поняття Due Diligence – як наукової категорії, що передбачає проведення сукупності дій: різновекторне дослідження та оцінка роботи суб'єкта, з глибоким вивченням фінансового стану, оцінкою ризиків (в тому числі фінансових, інвестиційних), аналіз місця об'єкта на ринку, з особливим акцентом на питання, пов'язані з безпекою, правами людини та навколишнього середовища - для формування комплексного висновку щодо фінансового, юридичного, інвестиційного стану суб'єкта дослідження, наявних ризиків. Due Diligence включає наступні етапи: проведення консультаційної діяльності із зацікавленими сторонами; процеси збору та використання експертиз; проводиться пошук та збір даних (в тому числі щодо політики кібербезпеки); здійснюється вивчення, консолідація та аналіз даних, аналіз потенційних ризиків, перевірка відповідності загальним і специфічним галузевим стандартам; формування висновку щодо стану підприємства з досліджуваного питання, прийняття відповідного рішення.

Важливою складовою оцінки функціонування підприємств є моделювання таких вищеописаних процесів due diligence: модель due diligence на основі машинного навчання передбачає оцінку прибутковості операцій з проблемними кредитами на вторинному ринку, моделювання складних взаємозв'язків між показниками; вдосконалення процесу належної перевірки шляхом розробки алгоритму штучного інтелекту; модель due diligence на основі оцінки ризиків передбачає комплексну методологію виконання належної перевірки ризиків багатонаціональної інженерно-будівельної організації третіми сторонами; модель due diligence на основі глибокого активного навчання НЛП передбачає формування моделі належної перевірки та прогнозування навколишнього середовища; адаптацію та розширення існуючих моделей обробки інформації природною мовою НЛП шляхом додавання даних екологічної сфери (EDD); моделі NAP, mHRDD, BHR оптимальності оцінки впровадження керівних принципів ООН щодо бізнесу та прав людини. National Action Plans Model – модель національних планів дій щодо бізнесу та прав людини, національна політична стратегія з урахуванням практик держав, що передбачає запропоновану урядом систему «м'яких» політичних інструментів, що описують пріоритети уряду, за яких майбутні дії орієнтовані на сприяння виконанню юридичних або реалізації політичних зобов'язань щодо перевірки прав людини, усунення

негативних наслідків прав людини внаслідок господарської діяльності; модель консенсусної багатовимірної перевірки інвестиційних проектів на основі фінансових технологій передбачає груповий підхід до оцінки фінансових альтернатив для інвестиційних проектів; комп'ютерна модель due diligence через AHP та big data передбачає кількісну оцінку поточної технічної належної перевірки.

Розглядаючи питання моделювання процесів due diligence, зупинимося на актуальних тенденціях цієї процедури перевірки в аспекті моделювання протидії фінансовим кібершахрайствам. Так, вартими детального розгляду є наступні моделі: модель зображення жертви кіберзлочину передбачаэ створення фазового зображення жертви кіберзлочину на основі методів систематизації, порівняння, групування, логічного узагальнення, бібліометричного аналізу, регресійного аналізу (метод сигма-обмеженої параметризації), алгоритм асоціативних правил; економетрична модель впливу цифровізації на економічні трансформації на основі розроблених квантильних регресій (з урахуванням національного показника кібербезпеки) - передбачає обґрунтування існування процесів конвергенції у напрямку цифровізації країн, враховуючи певні індикатори - рівень національної кібербезпеки, легкість отримання електроенергії, легкість ведення бізнесу, індекс протидії відмиванню грошей, рівень цифрового розвитку країни; модель машинного пов'язаного навчання (SVM) для захисту фінансового сектору від кіберзлочинності - передбачає забезпечення управління кібербезпекою за допомогою аналізу великих обсягів даних, що дозволяє на ранніх стадіях виявити та оцінити потенційні чинники кіберзагроз; моделі оцінки оцінки впливових факторів поінформованості про кібербезпеку передбачає кількісне дослідження факторів організаційного, соціального та індивідуального вплив на обізнаність про кібербезпеку; модель обізнаності про кібербезпеку для людей похилого віку передбачає розробку організаційної, соціальної та індивідуальної моделі поінформованості про кібербезпеку (Osicsam) для людей похилого віку.

Аналіз результатів світових і вітчизняних досліджень дозволяє виявити та оцінити пріоритети та тренди на сучасному фінансовому ринку, зміщення вектору досліджень у напрямку вивчення проблем кіберзлочинності. Так, модернізація процесів забезпечення фінансової, а особливо кібербезпеки підприємств, стає пріоритетним напрямком для керівництва сучасних суб'єктів господарювання. При чому, дієвим інструментом для протидії фінансовим кібершахрайствам є застосування процесів due diligence підприємств, як новітньої системи перевірки стану діяльності суб'єкта, моделювання таких процесів. Використання на підприємствах методик і моделей due diligence, дозволить сформувати керівні принципи та політику фінансової безпеки підприємств, що в свою чергу допоможе знизити рівень негативних наслідків в тому числі і фінансових кіберзагроз, фінансових кіберризиків, що можуть бути присутні у бізнес процесах;

максимізувати можливі позитивні ефекти від прийняття сформованих з урахуванням ряду факторів, управлінських рішень.

Роботу виконано в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України», № держреєстрації: 0121U100467; «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів», № держреєстрації: 53.16.01-22/24.3П-01; «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку» № держреєстрації: 0121U109559. The article was written during a research stay at the Technical University of Berlin, Department of Health Care Management.

Список літератури

1. Aman, A., & Reji, D. J. (2022). Environmental due diligence data: A novel corpus for training environmental domain NLP models. Data in Brief, 45 doi:10.1016/j.dib.2022.108579
2. Carannante, M., D'Amato, V., Fersini, P., Forte, S., & Melisi, G. (2023). Machine learning due diligence evaluation to increase NPLs profitability transactions on secondary market. Review of Managerial Science, doi:10.1007/s11846-023-00635-y
3. Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. Journal of Open Innovation: Technology, Market, and Complexity, 8(4) doi:10.3390/joitmc8040195
4. Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. [Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością] Polish Journal of Management Studies, 24(2), 276-291. doi:10.17512/pjms.2021.24.2.17
5. Li, Z. (2022). Operationalising the UN guiding principles on business and human rights through human rights due diligence: A critical assessment of current states practices. Academic Journal of Interdisciplinary Studies, 11(4), 8-21. doi:10.36941/ajis-2022-0094
6. Vasilyeva, T. A., Kuzmenko, O. V., Stoyanets, N. V., Artyukhov, A. E., & Bozhenko, V. V. (2022). THE DEPICTION OF CYBERCRIME VICTIMS USING DATA MINING TECHNIQUES. [Побудова портрету кібержертви з використанням технологій data-mining] Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (5), 174-178. doi:10.33271/nvngu/2022-5/174