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

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 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

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

СЕКЦІЯ 1 ЦИФРОВІ ТРАНСФОРМАЦІЇ В ЕКОНОМІЦІ

ДОСЛІДЖЕННЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ В ЕКОНОМІЦІ

STUDY OF DIGITAL TRANSFORMATIONS IN THE ECONOMY

Іван Нестеренко, студент
Сумський державний університет, Україна

Науковий керівник:
Ганна Яровенко, д.е.н., доц.,
Сумський державний університет, Україна

В сучасному світі існує тенденція проникнення цифрових технологій та інноваційних моделей бізнесу у різні сфери та галузі господарського та суспільного життя, що призводить до структурних змін економіки. Таким чином, у результаті такої еволюції формується цифрова економіка, яка відрізняється від традиційної економіки більш активним застосуванням цифрових технологій. Розвиток цифрової економіки впливає на конкурентоспроможність країни, саме тому держава і бізнес повинні приділяти особливу увагу на розвиток даної сфери (Селезньова та Чумак, 2022).

Впровадження цифрових технологій позитивно впливає на економічне зростання та розвиток країни в цілому. Саме тому більший доступ до цифрових технологій створює можливості для працевлаштування, підвищує продуктивність, дозволяє здобути нові професійні навички, покращує умови праці (Tan et al., 2021).

Цифровізація має вплив на зростання продуктивності праці, підвищення конкурентоспроможності підприємств, зменшення витрат на виробництво, підвищення ступеня задоволеності людських потреб, залучення інвестицій. Проте окрім позитивного впливу, цифровізація може сприяти розвитку загроз в області кібербезпеки (несанкціонований доступ до конфіденційної інформації та інші загрози кібербезпеки), розвитку безробіття, цифрову нерівність (розриви в рівні освіти та умовах доступу до цифрових послуг та продуктів між громадянами та бізнесами всередині країн, а також між державами).

Всесвітній економічний форум визначив сектор ІКТ як один із основних секторів, що сприяє зростанню виробництва. Крім того, очікується, що це вплине на зростання ВВП від 1,4% на ринках, що розвиваються. Також, було досліджено, що на рівні загальної економіки збільшення індексу розвитку цифрової екосистеми на 1% потенційно може збільшити ВВП на душу

населення на 0,13%. Проте, позитивні наслідки для покращення економіки не будуть миттєвими, оскільки досягнення технологічних інновацій потребує часу (Tan et al., 2021). Країни з найрозвинутішою цифровізацією можуть збільшити економічні вигоди приблизно на 20% більше, аніж країни, цифровізація яких знаходиться на початковому етапі. Крім цього, цифровізація покращує якість життя та поліпшує доступ громадян до державних послуг. Покращення умов доступу громадян до державних послуг стимулює уряд працювати з більшою прозорістю та ефективністю, що також позитивно впливає на економічний розвиток країни [6].

Для того, щоб забезпечити позитивний вплив цифровізації і зменшити негативні наслідки, країнам потрібно визначити особливості до впровадження цифрових технологій в усіх сферах, при цьому врахувавши особливості процесів, що відбуваються та поточний стан і особливості розвитку економічних, соціальних, політичних, національних, культурних та інших економічно-соціальних сфер (Хаустова, 2023).

Для здійснення ефективного процесу цифровізації (не кажучи вже про трансформацію, яка за своєю суттю є глибшою і потребує більше уваги, зусиль, ресурсів) в першу чергу необхідно сформувати її мету, чітко поставити і зрозуміти задачі, а отже – здійснити аналіз поточної ситуації. Це суттєву звузить коло областей, за якими варто здійснювати зміни і дасть змогу визначитися з технологіями. Після цього стає можливим постановка цілей (адже трансформація не здійснюється заради трансформації), будується стратегія, дорожня карта та обираються інформаційні технології. Важливою є оцінка та встановлення обмежень власного бюджету, оскільки впровадження нових технологій тягне не лише затрати на технології, але і на навчання персоналу (або найм нового), їх обслуговування.

Цифрова трансформація має здійснюватися на основі чіткого керівництва, контролю та співставленні контрольних та необхідних показників. Роль керівника полягає також у формуванні відповідної корпоративної культури та у співпраці з персоналом. Суттєві зміни часто викликають опір працівників, а впровадження технологій, які можуть замінювати ручну працю, перебудовувати бізнес-процеси, ущільнюючи їх, звужуючи функції та зливаючи окремі бізнес-процеси в один, викликати перебудову бізнес-моделі в цілому – тим більше. Важливою є мотивація, переконання працівників у позитивній ролі трансформації, її необхідності для покращення показників діяльності та результативності. Окремо стоїть питання навчання співробітників, оскільки нові технології потребують зовсім іншого рівня знань, умінь, навичок роботи з ними. Водночас важливо виводити з роботи старі технології, оскільки це тягне зусилля по підтримці їх у робочому стані і по суті дублюванні затрат – фінансових, трудових, інтелектуальних (Дергачова та Колешня, 2020).

Для дослідження цифрових трансформацій в економіці, доцільно дослідити 5 основних груп показників: розвиток рівня цифровізації населення, зміни у поведінці громадян і споживчих звичках при розвитку цифровізації, вплив у бізнес-середовищі, розвиток інфраструктурних аспектів, зміни у таких сферах, як здоров'я та екологія, пов'язані з розвитком Інтернет сфери. Для дослідження процесу цифровізації були обрані такі країни: Бельгія, Болгарія, Чехія, Данія, Німеччина, Естонія, Ірландія, Греція, Іспанія, Франція, Хорватія, Італія, Кіпр, Латвія, Литва, Люксембург, Угорщина, Мальта, Нідерланди, Австрія, Польща, Португалія, Румунія, Словенія, Словаччина, Фінляндія, Швеція. Для вивчення процесу впливу розвитку цифровізації на економіку країн, був обраний період з 2014 по 2023 роки.

Для реалізації даного дослідження було обрано кластерний аналіз. За його результатами серед найрозвинутіших країн в області цифровізації можна виділити наступні: Данія, Люксембург, Нідерланди, Фінляндія, Швеція. Всі ці країни знаходяться у центрі цифрової революції та активно інтегрують сучасні технології в усі сфери життєдіяльності. Проаналізовані країни мають високий рівень інвестицій з боку держави, що сприяє швидким темпам розвитку цифрових технологій, цифрових державних послуг, мобільного широкосмугового зв'язку, цифрових навичок населення, залученню іноземних бізнесів.

Середніми за розвитком цифровізації можна вважати наступні країни: Бельгію, Чехію, Німеччину, Естонію, Ірландію, Іспанію, Францію, Кіпр, Латвію, Литву, Угорщину, Мальту, Австрію, Словенію, Словаччину. Всі ці країни мають достатньо розвинену цифрову інфраструктуру та цифрові навички. В цих країнах є перспективи для розвитку цифровізації, тому уряди розробляють різні програми, які забезпечують прогрес в електронній комерції, кібербезпеці, сприяють залученню інновації та розробленню стартапів, розвитку технологій та досліджень.

Найменш розвиненими країнами в області цифровізації є Болгарія, Греція, Хорватія, Італія, Польща, Португалія, Румунія. Всі ці країни активно працюють над розвитком цифровізації, розробляючи програми і плани, які сприяють розвитку цифрової інфраструктури та оцифруванню. Проте слабкі показники цифрових навичок та недостатній рівень інвестицій в діджиталізацію є основними каталізаторами розвитку цієї галузі в проаналізованих країнах.

Отже, цифровізація має надважливий вплив на економіку країни. Впровадження цифрових технологій сприяє підвищенню продуктивності праці, оптимізації бізнес-процесів, створенню нових можливостей для ведення бізнесу, а також покращенню якості життя населення в цілому. При цьому впровадження діджиталізації потребує вирішенню декількох проблем, а саме забезпечення кібербезпеки та захисту даних, подолання цифрового розриву

між різними верствами населення та адаптації робочої сили до нових умов. В цілому сучасні цифрові технології забезпечують створення нових перспектив для підвищення ефективності, інновацій та конкурентоспроможності, що дозволяє економіці країни адаптуватися до швидких змін та викликів в сучасному світі.

Роботу виконано в рамках НДР № 0124U000544 «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором»

Список використаних джерел

1. Tan, N.N., Ngan, H.T.T., Hai, N.S., & Anh, L.H. (2021). The Impact of Digital Transformation on the Economic Growth of the Countries. In *Prediction and Causality in Econometrics and Related Topics*. Cham, 670–680. https://doi.org/10.1007/978-3-030-77094-5_49

2. Хаустова, М.Г. (2023). Вигоди, ризики та проблеми цифровізації суспільства: загальнотеоретичний аспект. *Аналітичне та порівняльне правознавство, 5,* 753–759. https://doi.org/10.24144/2788-6018.2023.05.135.

3. Дергачова, Г.М., Колешня, Я.О. (2020). Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут»*, 280-290. URL: https://ev.fmm.kpi.ua/article/view/216367/216461.

4. Селезньова, Г. О., Чумак, Г. М. (2022). Вплив розвитку цифрової економіки на конкурентне середовище вітчизняних підприємств. *Підприємництво та інновації, 25*, 69–74. https://doi.org/10.32782/2415-3583/25.11.

ЦИФРОВІЗАЦІЯ ЯК ФАКТОР ПОСИЛЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ КРАЇНИ

DIGITAL ECONOMY AS A FACTOR IN STRENGTHENING THE COUNTRY'S COMPETITIVENESS

Катерина Дідоренко, студентка
Сумський державний університет, Україна

Сьогодні цифровізація є одним із ключових факторів, що визначають економічне зростання та конкурентоспроможність країн на світовому ринку. Цифрові технології, такі як штучний інтелект, великі дані, інтернет речей та блокчейн, кардинально змінюють способи виробництва, управління та споживання. Вони дозволяють підвищити ефективність бізнес-процесів, знижують витрати та відкривають нові можливості для створення інноваційних продуктів та послуг.

Крім цього, у сучасних умовах глобалізації та зростаючої конкуренції між країнами, здатність інтегрувати цифрові рішення стає вирішальним чинником для забезпечення економічної стабільності та зростання. Країни, які активно впроваджують цифрові технології, демонструють вищі темпи економічного розвитку, що дозволяє їм успішніше конкурувати на міжнародній арені.

Цифровізація сприяє підвищенню прозорості та відкритості економічних процесів, що знижує рівень корупції та покращує бізнес-клімат. Вона також надає нові можливості для розвитку малого та середнього бізнесу, забезпечуючи доступ до глобальних ринків та фінансових ресурсів.

Дослідження впливу цифровізації на конкурентоспроможність економіки є надзвичайно актуальним. Воно дозволяє виявити ключові напрями розвитку цифрових технологій, оцінити їх вплив на економічні показники та розробити рекомендації для політиків та бізнесу щодо ефективного використання цифрових інновацій. Це, у свою чергу, сприятиме підвищенню конкурентоспроможності національних економік та забезпеченню стійкого економічного зростання у довгостроковій перспективі.

Для оцінювання ступеня зв’язку між цифровізацією та конкурентоспроможністю країни використано кореляційний аналіз Спірмена. За його розрахунками встановлено, що коефіцієнт дорівнює 0,53, що вказує на помірний позитивний монотонний зв'язок між глобальним індексом конкурентоспроможності країн та індексом цифрової економіки і суспільства. Найбільше значення коефіцієнта кореляції між Глобальним індексом конкурентоспроможності країн та Індекс електронного уряду

дорівнює 0.6430, тоді як коефіцієнт кореляції між Глобальним індексом конкурентоспроможності країн та Глобальним індексом інновацій дорівнює 0.5185. Всі ці значення коефіцієнта кореляції свідчать про помірний позитивний зв'язок між Глобальним індексом конкурентоспроможності та індексами. Оскільки рівень значущості був менше 0,05, це означає, що результати кореляційного аналізу Спірмена є статистично значущими.

На основі проведеного дослідження та отриманих результатів можна сформулювати кілька рекомендацій, спрямованих на підвищення рівня конкурентоспроможності країн Європи через активізацію процесів цифровізації.

1. Розвиток цифрової інфраструктури

Інвестувати в цифрову інфраструктуру: Забезпечення високошвидкісного інтернету у всіх регіонах країни, включаючи віддалені та сільські місцевості. Це створить основу для розвитку цифрової економіки та підвищить доступність цифрових послуг для бізнесу і населення.

Підтримка розвитку 5G: Активне впровадження технології 5G, що забезпечить швидкий та надійний зв'язок, сприятиме розвитку Інтернету речей та розширить можливості для інноваційних проектів.

2. Підтримка електронного уряду

Забезпечення доступності електронних послуг: Розширення спектру державних послуг, доступних в онлайн-режимі, що спростить взаємодію громадян і бізнесу з державою, зменшить бюрократичні перешкоди та підвищить прозорість державного управління.

Інтеграція електронних рішень: Інтеграція електронних рішень в усі рівні державного управління, що дозволить оптимізувати процеси, знизити витрати та підвищити ефективність роботи державних органів.

3. Стимулювання інновацій та досліджень

Збільшення інвестицій в наукові дослідження та розробки (R&D): Підтримка науково-дослідних установ та інноваційних підприємств через податкові пільги, гранти та інші фінансові стимули для збільшення обсягів інвестицій в R&D.

Формування інноваційних екосистем: Створення сприятливих умов для співпраці між університетами, науково-дослідними інститутами та приватним сектором, що дозволить прискорити комерціалізацію наукових досягнень та технологічних інновацій.

4. Підготовка кадрів для цифрової економіки

Підвищення рівня цифрової грамотності: Впровадження програм з навчання та підвищення кваліфікації в області цифрових технологій для всіх вікових груп, що сприятиме формуванню компетентної робочої сили, здатної адаптуватися до вимог цифрової економіки.

Розвиток STEM-освіти: Підтримка освітніх програм в галузях науки, технологій, інженерії та математики (STEM), що сприятиме підготовці фахівців, здатних генерувати інноваційні рішення та підтримувати розвиток високотехнологічних галузей.

5. Сприяння підприємництву та стартапам

Підтримка стартапів та підприємницьких ініціатив: Надання фінансової та консультаційної підтримки стартапам, створення бізнес-інкубаторів та акселераторів для стимулювання підприємницької активності та впровадження нових технологій.

Залучення іноземних інвестицій: Створення сприятливого інвестиційного клімату через стабільну правову базу, прозорі правила гри та стимулюючі податкові умови для залучення іноземних інвесторів у високотехнологічні та інноваційні сектори економіки.

Реалізація зазначених рекомендацій сприятиме підвищенню рівня цифровізації економіки, що, у свою чергу, позитивно вплине на конкурентоспроможність країн. Цифрова трансформація, підтримка інновацій та розвиток електронного уряду створюють необхідні умови для сталого економічного зростання та підвищення добробуту громадян.

МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВПЛИВУ РІВНЯ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНИЙ РОЗВИТОК

MODELLING AND FORECASTING THE IMPACT OF THE LEVEL OF THE COUNTRY'S DIGITIZATION ON ITS ECONOMIC DEVELOPMENT

Володимир Науменко, студент
Сумський державний університет, Україна

Науковий керівник:
Ганна Яровенко, д.-рка екон. наук, доцентка
Сумський державний університет, Україна

Цифрова трансформація – це процес впровадження інформаційно-комунікаційних технологій (ІКТ) для проектування нових продуктів, послуг та операцій через цифровізацію бізнес-процесів. Основна мета цмфровізації – підвищення цінності через інновації, покращення якості обслуговування та підвищення ефективності діяльності компаній. Використання нових технологій у виробництві сприяє зниженню собівартості продукції та підвищенню ефективності різних галузей, таких як електронна комерція, цифровий банкінг, промисловість та інші.

Дослідження Світового банку показали що, зростання доступу до Інтернету на 10% позитивно впливає на економічний розвиток країн з середнім рівнем розвитку, сприяючи інноваціям та підвищенню продуктивності.

Дослідники, такі як Антонюк Л., Ільницький Д., Лігоненко Л., Біла С., Дєєва Н., Лазебник Л., Піжук О., Побоченко Л., (Antoniuk et al.., 2021); (Bila S.,20210); (Dieieva N. Et al. 2018); (Lazebnyk L.,2020); (Pizhuk O., 2020); (Pobochenko L., 2020) вивчають різні аспекти впливу ІКТ на економіку та формування компетенцій. Закордонні науковці, такі як Brynjolfsson E., McAfee A., Chui M., Manyika J., Davenport T.H., Kane G. (Brynjolfsson E., 2014); (McAfee A.,2015); (Chui M., Manyika, J., Miremadi M, 2018); (Davenport T.H. et al. 2018); (Kane G. 2t al., 2019) досліджують вплив цифрових технологій на продуктивність праці, інновації, економічний розвиток та співпрацю між людьми і машинами.

Для дослідження статистичними показниками були індекси та фактичні значення, такі як ВВП на душу населення, експорт та імпорт ІКТ послуг, індекс розвитку електронного уряду, глобальний індекс інновацій, індекс свободи Інтернету та інші для оцінки рівня розвитку цифрової економіки.

Для аналізу використовуються мова програмування Python та редактор Visual Studio Code. Оцінювались параметри MSE, що вимірює середньоквадратичну відстань між фактичними і прогнозованими значеннями, MAD – середню абсолютну відстань, а RMSE – корінь з MSE, що показує середньоквадратичне відхилення в одиницях вихідних даних.

На етапі первинного аналізу було визначено, що потрібна нормалізація даних. Нормалізація є критичним етапом передобробки для забезпечення коректної роботи моделей машинного навчання. Використання метода Box-Cox дозволяє зменшити вплив масштабів різних показників на результати моделювання та підвищити точність моделей.

У дослідженні використано наступні моделі машинного навчання:

1.Лінійна регресія (LinearRegression).

2.Випадковий ліс (RandomForestRegressor).

3.Модель ближчих сусідів (KNeighborsRegressor).

4.Модель опорних векторів (SVR).

Всі ці моделі є потужними інструментами в машинному навчанні.

Найкращими виявилися Random Forest Regressor та Linear Regression (рис. 1-2).

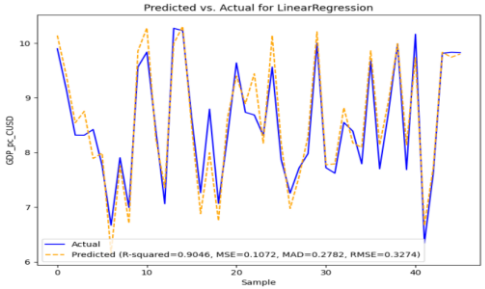

Рисунок 1. Графік результатів моделі Linear Regression
Джерело: розроблено автором

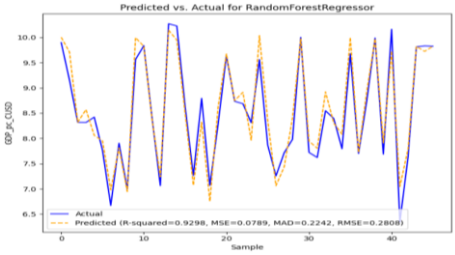

Рисунок 2. Графік результатів моделі Random Forest Regressor
Джерело: розроблено автором

Для лінійної регресії отримали рівняння:

GDP_pc_CUSD = 4,558 + 0,113 * ITC_SE + 5,874 * EGDI + 0,928 * GII + 0,001 * FN -0.033 * CC_EXPORT -0,0001 * CC_IMPORT -0,124 * ITC_EXPORT + -1,139 * EPI

Важливість показників для методу випадкового лісу представлені на рисунку 3.

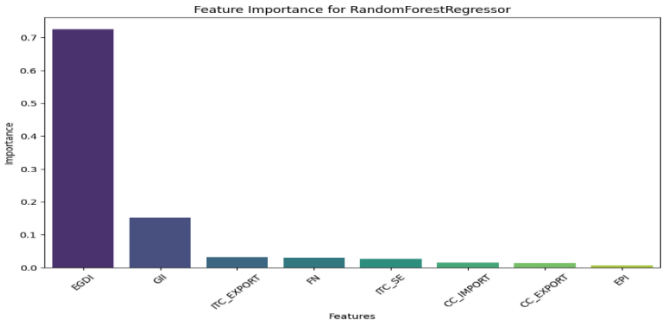

Рисунок 3. Виведення важливості показників для методу RandomForestRegressor

Джерело: розроблено автором

Лінійною регресією також визначено, що E-Participation Index має вклад в значення ВВП на душу населення. Параметри Freedom on the Net,. має незначний вплив.

Найбільший вплив при лінійному прогнозуванні та для моделі випадкового лісу має E-Government Development Index, що свідчить про важливість розвитку електронного державного управління. Розвинута телекомунікаційна інфраструктура надає можливість владі швидко реагувати та приймати рішення в умовах екстрених ситуацій

У моделі випадкового лісу параметр Freedom on the Net вказаний як важливий для прогнозування. Свобода та доступність Інтернету в країні в умовах воєнного стану дозволяє громадянам отримувати інформацію через різноманітні електронні джерела та засоби комунікації.

Також у моделі лінійної регресії є змінні з від’ємними коефіцієнтами, а саме відсоток послуг зв'язку, комп'ютерів тощо у загальному обсязі експорту та імпорту послуг, доля експорту послуг із ІКТ у загальному обсязі експорту послуг й індекс електронної участі. Такі тенденції можна пояснити тим, що значні витрати на цифровізацію та кіберзахист призводять до зменшення залученості ресурсів до розвитку інших секторів економіки, що спричиняє зниження валового внутрішнього продукту за нестабільних періодів.

Отже, отримані результати моделювання свідчать про те, що моделі є адекватними та здатні виконувати об'єктивні прогнозування то моделювання впливу рівня цифровізації країни на її економічний розвиток.

Роботу виконано в рамках НДР № 0124U000544 «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором»

Список використаних джерел

1. Антонюк, Л. Л., Ільницький, Д. О., Лігоненко, Л. О., Денісова, О. О. (2021). Цифрова економіка: Вплив інформаційно-комунікаційних технологій на людський капітал та формування компетентностей майбутнього: монографія. Київ: КНЕУ.

2. Біла, С. О. (2021). Цифрові технології в бізнесі та управлінні: світовий досвід. In Т. І. Татомир & Л. Г. Квасній (Eds.), Теоретичні та практичні аспекти розвитку Інтернет-економіки: міждисциплінарний навчальний посібник (pp. 156-180). Дрогобич: ПОСВІТ.

3. Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. New York, NY: W.W. Norton & Company.

4. Chui, M., Manyika, J., & Miremadi, M. (2018). The new artificial intelligence frontier: How companies can use AI to innovate. McKinsey & Company.

5. Davenport, T. H., & Kirby, J. (2018). Human + machine: Reimagining work in the age of AI. Harvard Business Review Press.

6. Дєєва, Н. Е., & Делейчук, В. В. (2018). Механізми залучення інвестицій емітентами в умовах розвитку цифрової економіки. Київ: Молодий вчений.

7. Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2019). The technology fallacy: How people are the real key to digital transformation. MIT Press.

8. Лазебник, Л. Л. (2020). Сутність, особливості та параметри цифрової економіки. Економічний вісник, (1), 22-29.

9. McKinsey Global Institute. (2015). Digital America: A tale of the haves and have-mores. McKinsey & Company.

10. Піжук, О. І. (2020). Цифрова трансформація економіки України: обмеження та можливості: монографія. Ірпінь: Університет державної фіскальної служби України.

11. Побоченко, Л. М., & Ковбич, Т. К. (2020). Діджиталізація економіки в процесі становлення інформаційного суспільства. In Тези доповідей на міжнародній науково-практичній конференції "Сучасні міжнародні відносини: актуальні проблеми теорії і практики", 17 квітня 2020 року (pp. 123-127). Київ.

РОЛЬ ЦИФРОВІЗАЦІЇ В ПРОТИДІЇ КОРУПЦІЇ

THE ROLE OF DIGITIZATION IN COMBATING CORRUPTION

Дмитро Харченко, студент
Сумський державний університет, Україна

Корупція є однією з найсерйозніших проблем, яка гальмує розвиток суспільства, підриває економічний розвиток і знижує довіру громадян до державних інститутів. У сучасних умовах цифровізація відкриває нові можливості для протидії корупції через запровадження прозорих та ефективних механізмів управління. Однією з найбільш значущих проблем, спричинених корупцією, є втрата довіри громадян до влади. Коли люди бачать, що уряд та державні установи втягнуті в корупційні схеми, вони втрачають віру в справедливість і законність. Це, у свою чергу, підриває легітимність державних структур і може призвести до соціальних протестів і політичної нестабільності. Економічні втрати від корупції також надзвичайно значні. Корупційні дії знижують ефективність державних витрат, оскільки кошти, спрямовані на розвиток інфраструктури, охорони здоров'я, освіти та інших важливих сфер, використовуються не за призначенням. Це призводить до погіршення якості державних послуг та перешкоджає економічному зростанню.

Цифровізація дає змогу створювати електронні урядові платформи та відкриті бази даних, які сприяють підвищенню прозорості державних процесів. Наприклад, такі платформи дозволяють громадянам і незалежним організаціям контролювати діяльність державних службовців і витрати державного бюджету. Оцифрування державних архівів та документів значно підвищує прозорість та доступність інформації. Це також ускладнює можливості для підробки документів та маніпулювання офіційними даними. Оцифровані документи легше зберігати, передавати та перевіряти, що допомагає боротися з корупційними схемами.

Одним із головних аспектів електронного уряду є надання громадянам і бізнесу можливості отримувати державні послуги онлайн. Це означає, що замість традиційного візиту до державних установ чи великої кількості паперової документації громадяни та підприємства можуть оформляти послуги онлайн. Наприклад: подача заяв, сплата податків, отримання документів і багато іншого, що спрощує і прискорює процес взаємодії з владою. Крім того, електронний уряд передбачає використання цифрових технологій для оптимізації внутрішніх процесів державних установ. Це може включати впровадження систем електронного документообігу, систем

електронного обліку, аналізу даних та інших інструментів, які дозволяють державним органам виконувати свої функції більш ефективно. Однією з ключових переваг електронного урядування є підвищення прозорості та відкритості діяльності уряду. Через відкриті електронні майданчики громадяни мають можливість отримати доступ до інформації про діяльність органів влади, видатки бюджету, результати перевірок та іншу важливу інформацію. Це допомагає підвищити підзвітність уряду громадянам і зменшити можливості для корупції (На, L. T., 2023).

Запровадження електронних майданчиків для державних закупівель, таких як ProZorro в Україні, забезпечує відкритий доступ до інформації про тендери, зменшує можливість для змови та корупційних схем. Електронні майданчики забезпечують відкритий доступ до всієї інформації про тендери, включаючи вимоги до учасників, умови тендерів, пропозиції учасників та результати відбору. Це забезпечує прозорість процесу державних закупівель, роблячи його доступним для всіх зацікавлених сторін, включаючи громадськість, ЗМІ та антикорупційні організації. Прозорість знижує ризик змови та корупційних схем, оскільки всі етапи процесу закупівель підлягають громадському контролю. Це також допомагає залучити більше учасників і збільшити конкуренцію. Дослідження показали, що цифровізація може значно підвищити відкритість, публічність і прозорість державного управління, виявити корупційні зв'язки, схеми та взаємовідносини, оптимізувати антикорупційну діяльність правоохоронних органів та обмежити можливості корупціонерів (Кубатко, О., 2023).

Технології блокчейн забезпечують високий ступінь безпеки та прозорості даних. Незмінність записів у блокчейні унеможливлює фальсифікацію даних, що важливо для запобігання корупції (Guo, H., 2022). Ці технології можна використовувати у багатьох сферах. Нижче наведено деякі з них: електронне голосування; управління документами та реєстрами; цифрова ідентифікація; управління фінансовими потоками та держзакупівлі; системи охорони здоров'я;

Електронні системи контролю фінансових операцій дозволяють виявляти підозрілі операції та запобігати відмиванню грошей. Це сприяє більш ефективному розподілу державних ресурсів. Аналітичні інструменти та технології обробки великих даних (Big Data) дозволяють проводити поглиблений аналіз державних витрат, виявляючи аномалії та потенційні корупційні схеми. Використання таких технологій допомагає передбачити та запобігти можливим корупційним діям. Такі системи дозволяють автоматично контролювати транзакції та виявляти аномалії, які можуть свідчити про незаконну діяльність. Використовуючи машинне навчання та алгоритми штучного інтелекту, ці системи можуть аналізувати величезні

обсяги даних у режимі реального часу, виявляючи транзакції, які відрізняються від нормальних моделей поведінки (Elvrida N., 2022).

Таким чином, для протидії корупції необхідно створити умови для прозорого, ефективного і підзвітного державного управління, зменшуючи можливості для корупційних дій, а саме за рахунок автоматизації державних послуг та процесів,, впровадження прозорих електронних тендерів, впровадження систем електронного декларування майна та доходів державних службовців, використання блокчейн для моніторингу ланцюгів поставок та витрат державних кошті, публікація державних даних у відкритих форматах, доступних для аналізу та моніторингу з боку громадськості.

Роботу виконано в рамках НДР № 0122U000783 «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів»

Список використаних джерел

1. Кубатко, О., Харченко, Д., Півень, В., & Литвиненко, Д. (2023). Роль економічних і цифрових чинників у боротьбі з корупцією. Економіка та суспільство, (48). https://doi.org/10.32782/2524-0072/2023-48-19

2. Bota-Avram, C. (2023). Exploring the impact of digitalisation and technology on corruption: Evidence from cross-country panel data within a cultural-economic framework. Kybernetes. https://doi.org/10.1108/k-03-2023-0522

3. Elvrida N. Sinaga, A. W. (2022). Digitalization and big data in preventing corruption in education sector: Towards inclusive and equitable education. Scientium Law Review (SLR), 1(1), 13–24. https://doi.org/10.56282/slr.v1i1.53

4. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 100067. https://doi.org/10.1016/j.bcra.2022.100067

5. Ha, L. T., To, T. T., Thi Thanh Huyen, N., Hoa, H. Q., & Ngoc, T. A. (2023). The roles of e-government in combating corruption: Evidence from European countries. Journal of Science and Technology Policy Management. https://doi.org/10.1108/jstpm-04-2022-0065

ЦИФРОВІ НАВИЧКИ: ВИКЛИКИ ТА МОЖЛИВОСТІ

DIGITAL SKILLS: CHALLENGES AND OPPORTUNITIES

Захарченко Андрій, студент
Сумський державний університет, Україна

У сучасному світі цифрові навички стають все більш важливими для успішної інтеграції в суспільство та економіку. Вони охоплюють широкий спектр вмінь, від базових операцій з комп'ютерами до складних технічних завдань, таких як програмування та аналіз великих даних. Розвиток цифрових технологій відкриває нові можливості, але також створює низку викликів.

Один з основних викликів – це цифрова нерівність. Значна частина населення не має доступу до інтернету та сучасних технологій, що створює розрив у рівнях цифрових навичок між різними соціально-економічними групами. Це поглиблює соціальну нерівність і обмежує можливості для розвитку та самореалізації багатьох людей. Відповідно до досліджень Європейської Комісії, цифрова нерівність є серйозною перешкодою на шляху до створення інклюзивного цифрового суспільства. Відсутність доступу до інтернету і сучасних технологій обмежує можливості навчання, працевлаштування та соціальної взаємодії, що є особливо важливим у контексті глобалізації та економічного розвитку. Наприклад, у країнах з низьким рівнем доходу доступ до інтернету часто є обмеженим, що значно ускладнює можливість отримання освіти та пошуку роботи в умовах цифрової економіки.

Освітні системи також стикаються з проблемами, оскільки не завжди встигають адаптуватися до швидких змін у технологічному середовищі. Навчальні програми часто залишаються застарілими, а методи викладання не враховують нові потреби учнів. Ніл Селвін (2016) зазначає, що традиційна освіта не завжди встигає за цифровою трансформацією, що створює додаткові бар'єри для учнів. Викладачі часто не мають необхідних знань та вмінь для ефективного використання цифрових інструментів, що знижує якість освіти та обмежує можливості учнів. Крім того, відсутність сучасних технічних засобів у школах і університетах ще більше ускладнює процес навчання.

Крім того, використання цифрових технологій викликає етичні та правові питання. Це стосується конфіденційності даних, безпеки та етики використання інформаційних технологій. Потреба у регуляції цих аспектів є нагальною, щоб забезпечити безпечне та етичне використання цифрових

технологій. Лючіано Флоріді (2013) наголошує на важливості етичного підходу до управління інформаційними технологіями. Без відповідного регулювання і освіти у сфері етики цифрових технологій існує ризик зловживань, що може мати серйозні наслідки для суспільства. Наприклад, витік конфіденційних даних може призвести до значних втрат для компаній та приватних осіб, а також спричинити серйозні порушення прав людини.

Відсутність мотивації та ресурсів для навчання новим цифровим навичкам також є значною проблемою. Багато дорослих людей не мають можливостей для отримання додаткової освіти, що обмежує їхні можливості на ринку праці. Дослідження OECD показують, що без постійного навчання та підвищення кваліфікації робоча сила не зможе ефективно адаптуватися до нових вимог цифрової економіки. Це особливо важливо в умовах швидких змін на ринку праці, коли нові технології та інновації постійно змінюють вимоги до працівників. Наприклад, у багатьох галузях економіки, таких як виробництво, фінанси та послуги, впровадження нових технологій значно змінює вимоги до кваліфікації працівників, і ті, хто не має відповідних навичок, ризикують залишитися без роботи.

Проте розвиток цифрових навичок відкриває значні можливості. Розширення доступу до інтернету та цифрових ресурсів сприяє зменшенню цифрового розриву і забезпечує інклюзивність. Інноваційні освітні технології, такі як онлайн-курси та віртуальні класи, роблять навчання більш доступним і гнучким. Підвищення цифрових навичок дозволяє людям підвищити свою конкурентоспроможність на ринку праці та відкрити нові можливості для кар'єрного зростання. Наприклад, багато компаній пропонують онлайн-курси та програми підвищення кваліфікації для своїх працівників, що дозволяє їм отримувати нові знання та навички без відриву від роботи.

Крім того, цифрові технології підтримують і розвиток творчості, надаючи інструменти для реалізації інноваційних проектів. Вони сприяють культурному та соціальному розвитку, дозволяючи створювати нові форми мистецтва та взаємодії. Це особливо важливо в умовах глобалізації, коли цифрові навички стають ключовим фактором конкурентоспроможності на міжнародному рівні. Наприклад, розвиток цифрових технологій дозволяє художникам і музикантам створювати нові форми мистецтва, використовуючи віртуальну та доповнену реальність, що відкриває нові горизонти для творчості.

Для успішного розвитку цифрових навичок необхідна інтеграція цих компетенцій в освітні програми на всіх рівнях. Регулярне підвищення кваліфікації вчителів та викладачів також є критично важливим, щоб забезпечити актуальність навчання. Державна підтримка та інвестиції у

розвиток цифрової інфраструктури, особливо в малозабезпечених та віддалених районах, можуть значно покращити ситуацію. Заохочення приватного сектору до впровадження програм навчання цифровим навичкам для працівників також є важливим кроком у цьому напрямку. Наприклад, компанії можуть співпрацювати з університетами та іншими навчальними закладами для розробки спеціальних програм навчання, що відповідають потребам ринку праці.

Одним з ефективних способів розширення доступу до цифрових навичок є створення публічних цифрових центрів, де люди можуть безкоштовно або за символічну плату отримувати необхідні знання та практичні навички. Такі центри можуть бути особливо корисними у віддалених районах, де доступ до інтернету та комп'ютерів є обмеженим. Вони можуть забезпечити навчання з основ цифрової грамотності, програмування, веб-дизайну та інших важливих навичок, що допоможе підвищити рівень цифрових компетенцій у суспільстві.

Важливим аспектом є також співпраця між урядами, освітніми установами та приватним сектором у розробці та впровадженні програм з розвитку цифрових навичок. Це може включати фінансування навчальних програм, створення грантів та стипендій для студентів, а також підтримку стартапів, що працюють у сфері освіти та технологій. Наприклад, уряди можуть надавати фінансову підтримку школам та університетам для впровадження сучасних технологій у навчальний процес, а також стимулювати розвиток інноваційних освітніх проектів.

Інноваційні підходи до навчання, такі як гейміфікація та використання віртуальної та доповненої реальності, можуть зробити процес навчання більш цікавим та ефективним. Це може сприяти залученню більшої кількості людей до навчання та підвищенню їхньої мотивації. Наприклад, використання ігрових елементів у навчальних програмах може допомогти учням краще засвоювати матеріал та підвищувати інтерес до навчання. Віртуальна та доповнена реальність можуть забезпечити більш реалістичні та інтерактивні навчальні досвіди, що сприятиме кращому розумінню складних концепцій та розвиткові практичних навичок.

Список використаних джерел

1. European Commission. (2020). Digital Education Action Plan. Retrieved from https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
2. Selwyn, N. (2016). Digital technology and the contemporary university: Degrees of digitization. Routledge.
3. Floridi, L. (2013). The ethics of information. Oxford University Press.

4. Organisation for Economic Co-operation and Development (OECD). (2019). Getting Skills Right: Future-Ready Adult Learning Systems. OECD Publishing.

5. Florida, R. (2002). The Rise of the Creative Class: And How It's Transforming Work, Leisure, Community, and Everyday Life. Basic Books.

ТЕОРЕТИЧНІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКІВ КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ОХОРОНИ ЗДОРОВ'Я

THEORETICAL ASPECTS OF INTERCONNECTIONS OF CYBER SECURITY AND HEALTH CARE SECURITY

Даніїл Савченко, студент
Сумський державний університет, Україна

Тетяна Доценко, доктор філософії
Сумський державний університет, Україна,
Технічний університет Берліну, Німеччина

В сучасному цифровому світі, де віртуальна реальність переплітається з реальним життям, питання кібербезпеки та безпеки міцного здоров'я стають дедалі більш актуальними та важливими. Зростання залежності від інформаційних технологій вносить свої виклики і загрози, які впливають на економічний, соціальний та медичний аспекти суспільства. В цьому контексті виникає потреба в розробці комплексних економіко-математичних моделей, спрямованих на аналіз та прогнозування взаємозв'язків між кібербезпекою та безпекою міцного здоров'я країн світу.

Поняття кібербезпеки і безпеки охорони здоров'я є відносно новими категоріями, що набувають активного використання серед сучасних науковців світу: Алкудхайбі А. (Alqudhaibi et al., 2024), Феррейра Д. (Ferreyra et al., 2024), Фатокун Ф. (Fatokun et al., 2024), Хоссейн М. (Hossain et al., 2024), Ху К. (Hu et al., 2024).

Кібербезпека (cyber security) – це заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях. Кібербезпека це те, що забезпечує конфіденційність, цілісність і доступність даних протягом їх всього життєвого циклу. Виклики сучасної кібербезпеки наступні: у цифрову еру кібербезпека є критичною проблемою для людей, корпорацій та урядів; зі збільшенням використання технологій і цифрових пристроїв як ніколи необхідно захищати електронні пристрої, мережі та дані від небажаного доступу, крадіжки та пошкодження; з розвитком технологій дія кібербезпеки щодо захисту організації, співробітників і критично важливих активів від кіберзагроз стикається з кількома проблемами. Для кращого захисту від кіберзагроз необхідно знати типи кібербезпеки: безпека мережі, безпека програми, інформаційна безпека, хмарна безпека, безпека інтернету речей, управління ідентифікацією та доступом.

Безпеки охорони здоров’я включає зобов’язання щодо безпеки працівників, надання та адекватний доступ до засобів безпеки та засобів індивідуального захисту, а також широкі зусилля з навчання, які використовують протоколи, що вимагають певних заходів безпеки. Виділяють категорії небезпек, пов’язаних з роботою системи охорони здоров’я: біологічні небезпеки, хімічні небезпеки, механічні небезпеки навколишнього середовища, фізичні небезпеки, психосоціальні небезпеки.

Зв'язок між кібербезпекою та безпекою охорони здоров'я можна представити наступною схемою (рисунок 1).

Рисунок 1. Взаємозв’язок між кібербезпекою та безпекою охорони здоров'я

Джерело: сформовано автором

Ця схема демонструє взаємозв'язок між кібербезпекою та безпекою охорони здоров'я, акцентуючи на загрозах, які виникають внаслідок вразливостей у медичних системах, таких як кібератаки на медичні системи. Це призводять до вразливостей у медичних інформаційних системах, що в свою чергу може призвести до зловмисних дій, таких як витік даних, шифрування даних або блокування доступу. При чому зв'язок між кібербезпекою та безпекою охорони здоров'я також полягає в тому, що кібербезпека дозволяє забезпечувати захист інформаційних систем, даних медичних установ, персональної інформації пацієнтів, що є критичним для безперебійного функціонування закладів охорони здоров’я, надійного захисту пацієнтів. А вразливості в системі кібербезпеки можуть призвести до витоків важливої конфіденційної інформації, порушень у функціонуванні

медичних систем, загроз для здоров'я пацієнтів. В свою чергу, ефективна кібербезпека є невід'ємною складовою загальної безпеки охорони здоров'я.

Особливе місце у дослідженні напрямків кібербезпеки та безпеки охорони здоров’я відводиться саме моделюванню таких систем. Це дможе суттєво допомогти у прийнятті обґрунтованих управлінських рішень, підвищенні рівня безпеки медичного персоналу, пацієнтів, оптимізації роботи медичних закладів в умовах обмеженості ресурсів, а також надзвичайних ситуацій.

Моделювання кіберзагроз – це процес аналізу різноманітних ділових і технічних вимог до системи, визначення потенційних загроз і документування того, наскільки ці загрози роблять систему вразливою. Загроза стосується будь-якого випадку, коли неавторизована сторона отримує доступ до конфіденційної інформації, програм або мережі організації. Процес моделювання кіберзагроз включає наступні ключові кроки: постановка цілі; візуалізація; визначення загрози; пом’якшення; перевірка. Наступним виділено три методологій моделювання кіберзагроз: STRIDE (методологія, розроблена корпорацією Майкрософт для моделювання загроз, пропонує мнемоніку для визначення загроз безпеці в шести категоріях: підробка, втручання, відмова, розголошення інформації, відмова в обслуговуванні, підвищення привілеїв); DREAD (спосіб класифікувати й оцінювати ризики безпеки за п’ятьма категоріями: потенційна шкода, відтворюваність, можливість використання, постраждалі користувачі, виявленість); P.A.S.T.A («Процес симуляції атак і аналізу загроз» – семиетапна методологія, орієнтована на ризик; пропонує динамічну ідентифікацію загроз, процес підрахунку та оцінювання; після того, як експерти проведуть детальний аналіз виявлених загроз, розробники можуть розробити стратегію пом’якшення, орієнтовану на ресурси, проаналізувавши програму через погляд, орієнтований на зловмисників).

Моделювання безпеки охорони здоров'я - це процес побудови та застосування моделей для аналізу, оцінки та прогнозування безпеки в системах охорони здоров'я, що включає наступні напрямки: аналіз ризиків; прогнозування подій; оцінка ефективності заходів; планування ресурсів; симуляції. Можна виділити основні моделі охорони здоров’я: модель Беверіджа (уряд діє як єдиний платник, усуваючи будь-яку конкуренцію на ринку, щоб зберегти низькі витрати та стандартизувати виплати; будучи єдиним платником, національна служба охорони здоров’я контролює, що можуть робити «внутрішні мережеві» провайдери та які вони можуть стягувати; фінансується за рахунок податків); модель Бісмарка (більш децентралізована форма охорони здоров’я; роботодавці та працівники несуть відповідальність за фінансування своєї системи медичного

страхування через «лікарняні фонди», створені шляхом відрахувань із заробітної плати; постачальники та лікарні, як правило, є приватними, хоча страхові компанії є державними); національна модель медичного страхування (держава діє як єдиний платник за медичні процедури; провайдери є приватними; моделлю керують приватні постачальники, але виплати надходять від державної програми страхування, у яку платить кожен громадянин; є універсальним страхуванням, яке не приносить прибутку та не відмовляє у виплаті претензій); кишенькова модель (пацієнти повинні платити за свої процедури зі своєї кишені; заможні отримують професійну медичну допомогу, а бідні – ні, якщо тільки вони якимось чином не знайдуть достатньо грошей).

Отже, взаємозв'язки між кібербезпекою та безпекою охорони здоров'я є критично важливими і необхідними для забезпечення безпечного, надійного, ефективного функціонування медичних систем, захисту здоров'я пацієнтів у цифрову епоху. Результати досліджень, проведених у цій роботі, мають потенціал відіграти важливу роль у формуванні політики в галузі кібербезпеки, а також слугувати основою для подальших наукових досліджень у цій області.

Список використаних джерел

1. Alqudhaibi, A., Krishna, A., Jagtap, S. et al. (2024). Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discov Food*, 4, 2. https://doi.org/10.1007/s44187-023-00071-7.

2. Diaz Ferreyra, N.E., Vidoni, M., Heisel, M. (2024). Cybersecurity discussions in Stack Overflow: a developer-centred analysis of engagement and self-disclosure behaviour. *Soc. Netw. Anal. Min*., 14, 16. https://doi.org/10.1007/s13278-023-01171-z.

3. Faith Fatokun, Zalizah Awang, Suraya Hamid, Johnson O. Fatokun and Azah Norman. (2024). Cybersecurity Knowledge Deterioration and the role of Gamification Intervention. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 43, 1, pp.66–94. https://doi.org/10.37934/araset.43.1.6694.

4. Hossain, M.A., Islam, M.S. (2024). Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. *Cybersecurity*, 7, 16. https://doi.org/10.1186/s42400-024-00205-z.

5. Hu, C., Wu, T., Liu, C. et al. (2024). Joint contrastive learning and belief rule base for named entity recognition in cybersecurity. *Cybersecurity*, 7, 19. https://doi.org/10.1186/s42400-024-00206-y.

СЕКЦІЯ 2 КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

ІДЕНТИФІКАЦІЯ ТА УПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ В ЕЛЕКТРОННОМУ БАНКІНГУ: ДОСВІД ЄС

IDENTIFICATION AND PREVENTION OF CYBER FRAUD IN ELECTRONIC BANKING: EU EXPERIENCE

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

Сучасний світ став гіперз'єднаним, й кіберзлочинці становлять значну загрозу внутрішній безпеці кожній країні, особливо країнам, які мають високий рівень розвитку економіки та цифрової грамотності. За даними Міжнародного союзу електрозв'язку (ITU), станом на 2023 рік у 175 країнах світу існують національні центри кібербезпеки (НЦКБ), задачею яких є підвищення обізнаності про кібербезпеку, реагування на кіберінциденти моніторинг кіберзагроз, співпраця з іншими країнами.

В глобальному просторі Міжнародні агеніції та дослідницькі компанії публікують у відкритому доступі інформацію щодо типів, видів кіберзагроз та надслідками, що пов'язані у разі їхнього настання, та відповідно необхідністю упередження кібервзломів. Таку статистичну звітність можна спостерігати у базах даних Євростат, Статистика, Світовий банк, статистика ОЕСД. Приватні аналітичні компанії, діяльність яких безпосередньо стосується питань кібербезпеки (наприклад e-Governance Academy, Surfshark VPN service, The Fletcher School, Kaggle та ряд інших), науково-дослідницькі інститути в межах реалізації своїх наукових грантів публікують у відкритому доступі інформацію (проте її не так вже й багато, що обумовлюється об'єктивними причинами), що пов'язана з проблемами кібербезпеки, методологічиними підходоми до її визначення та оцінювання.

Зокрема, в країнах Європи з 2004 року Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (The European Union Agency for Cybersecurity, ENISA) опікується питаннями щодо високого загального рівня кібербезпеки. Агентство ENISA сприяє кіберполітиці ЄС, підвищує надійність продуктів, послуг і процесів інформаційно-комунікаційних технологій за допомогою схем сертифікації кібербезпеки. Законадавча база ЄС дуже потужна та спрямована на формування безпечного інформаційного простору для суб'єктів економіко-політичної діяльності та охоплює різні сфери діяльності держав (освітньо-наукову, соціальну, медичну, страхову). Зокрема дослідження "Cybersecurity Assessments", що було проведено за 2018-2022 роки ENISA (ENISA, January 2024), описує різні способи оцінки кібербезпеки

ІКТ-рішень, таких як стандарти, національні та приватні схеми та методології сертифікації.

Проте не зважаючи на потужну нормативну базу ЄС щодо протидії кіберзлочинам, стан ландшафту загроз кібербезпеці, уразливостей та інцидентів кібербезпеки залишається надзвичайно широким. Прямими загразоми були й залишаються: програми-вимагачі; шкідливе програмне забезпечення; соціальна інженерія; загрози для даних; загрози доступності: відмова в обслуговуванні; загроза доступності: Інтернет-загрози; маніпулювання інформацією та втручання; атаки на ланцюги поставок (ENISA Threat Landscape 2023).

Відліковою точкою для виявлення шахрайств в електронному банкінку є перевірка дотриманню стандартного набору правил Європейського банківського управління (European Banking Authority, EBA) для регулювання та нагляду за банківською діяльністю у всіх країнах ЄС, адже саме банківська система є найбільш вразливою для використання великої кількості різноманітних витонтчених шахрайських схем із залученням всіх учасників фінансових операцій: клієнтів банку (фізичних чи юридичних осіб), співробітників банків, економічних агентів (підприємства, фірми), держава.

Європейська система центральних банків (ЄСЦБ) містить:

- Європейський центральний банк;
- Національні центробанки з усіх 27 держав-членів Євросоюзу.

Окремо виділяють Євросистему, що об'єднує основні банківські структури 20 країн-членів ЄС, які перейшли на валюту євро. Євросистема та ЄСЦБ співіснуватимуть доти, доки є країни-члени Євросоюзу за межами єврозони.

Європейський центральний банк (ЄЦБ) є ядром ЄСЦБ і Євросистеми. Він був створений 1 червня 1998 року. ЄЦБ є незалежним у здійсненні своїх повноважень і є юридичною особою відповідно до міжнародного публічного права. Штаб-квартира знаходиться у Франкфурті-на-Майні, Німеччина.

ЄЦБ Європейський центральний банк має три органи, які приймають рішення, а також керують ЄСЦБ та Євросистемою:

1. Рада керівників ЄЦБ – головний орган, який приймає рішення. Він формулює грошово-кредитну політику зони євро та приймає керівні принципи, необхідні для виконання завдань.

2. Виконавча рада – оперативний орган ЄЦБ та Євросистеми, який реалізує грошово-кредитну політику зони євро відповідно до рішень Ради керуючих та керує поточною діяльністю Європейського центробанку. До його складу входять президент, віце-президент та ще чотири члени.

3. Генеральна рада створена як третій директивний орган ЄЦБ. Це перехідний орган, який існуватиме доти, доки всі держави-члени ЄС не перейдуть на євро, після чого його розпустять.

Є також наглядова рада, створена після того, як на ЄЦБ було покладено конкретні завдання щодо пруденційного нагляду за кредитними організаціями в рамках Єдиного наглядового механізму (ЄЕС) з метою сприяння надійності та стабільності банківської системи.

16 січня 2023 року набула чинності Директива (ЄС) 2022/2555 (NIS2, 2023), яка замінила Директиву (ЄС) 2016/1148. Агентство Європейського Союзу з кібербезпеки (The European Union Agency for Cybersecurity, ENISA) вважає, що NIS2 покращує існуючий стан кібербезпеки в ЄС за допомогою:

– створення необхідної структури управління кіберкризою (CyCLONe) (Європейська мережа організації зв'язку з кіберкризами – це мережа співпраці національних органів держав-членів, які відповідають за управління кіберкризами (мережа була запущена в 2020 році та офіційно оформлена 16 січня 2023 року з набранням чинності NIS2, стаття 16);

– підвищення рівня гармонізації щодо вимог безпеки та зобов'язань щодо звітності, а також генерація нових ідей за допомогою експертних оцінок для покращення співпраці та обміну знаннями між державами-членами;

– заохочення держав-членів до впровадження нових сфер інтересів, таких як ланцюг постачання, управління вразливістю, основний Інтернет та кібергігієна в їхні національні стратегії кібербезпеки.

– охоплення більшої частки економіки та суспільства шляхом включення більшої кількості секторів, що означає, що більше суб'єктів зобов'язані вживати заходів для підвищення рівня кібербезпеки.

Таким чином, алгоритм виявлення шахрайств в електронному банкінгу країн ЄС містить десять базових кроків.

Крок 1. Збір та моніторинг даних: збір та моніторинг транзакцій та активностей клієнтів в реальному часі.

Крок 2. Використання системи аналітики для відстеження звичайних та незвичайних фінансових операцій.

Крок 3. Використання алгоритмів машинного навчання та штучного інтелекту для аналізу та класифікації транзакцій та активностей клієнтів.

Крок 4. Виявлення незвичайних патернів або аномалій, що можуть вказувати на шахрайську діяльність.

Крок 5. Введення правил та обмежень: встановлення правил і обмежень для фінансових транзакцій, які можуть бути підозрілими (наприклад, великі перекази на незвичайні рахунки).

Крок 6. Використання системи оцінки ризику для класифікації та відстеження транзакцій за їхнім рівнем підозрілості.

Крок 7. Міжнародне співробітництво: обмін інформацією з іншими фінансовими установами та правоохоронними органами в ЄС та інших країнах для виявлення міжнародних шахраїв.

Крок 8. Повідомлення та дії: створення системи повідомлень та сповіщень для виявлення та реагування на підозрілу активність.

Крок 9. Заборона або блокування підозрілих транзакцій та рахунків.

Крок 10. Постійне вдосконалення алгоритмів та стратегій виявлення шахрайства на основі набутого досвіду та нових загроз.

Слід також зазначити, що кожний банк чи фінансова установа в ЄС може мати власну стратегію та технологічні рішення для боротьби з шахрайством, які відповідають їхнім потребам та ресурсам.

Окремо для ідентифікації та оцінювання ризиків, запобігання кібершахрайств в електронному банкінгу ENISA рекомендує застосовувати комплексну систему методів. Зокрема, в звіті ENISA Cyber Insurance – Models and methods and the use of AI, (2024) розглядуються класичні актурні підходи, моделі зараження, теоретико-ігрові аспекти, статистичні методи, стохастичне моделювання ризиків, методи навчання під наглядом, неконтрольоване навчання, навчання з підкріпленням, машинне навчання та штучний інтелект, моделювання частоти та серйозності втрат за допомогою нейронних мереж, регресійних лісів, узагальнених лінійних змішаних моделей. При цьому в звіті підкреслюється важливість проблеми збору відповідних даних достатньої якості та деталізації, також необхідність розробки та вдосконалення існуючих підходів до моделювання протидії кіберзлочинам, розробки моделей динамічної стратегічної взаємодії, що включають реалістичні моделі мережі.

Список використаних джерел

1. Cybersecurity Assessments: European Union Agency for Cybersecurity, January 2024. URL : https://www.enisa.europa.eu/publications/cybersecurity-market-assessments

2. ENISA serves as the CyCLONe Secretariat boosting cooperation among national Cyber Crises Liaison Organisations. URL : https://www.enisa.europa.eu/topics/incident-response/cyclone

3. ENISA Threat Landscape 2023. URL : https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. European Banking Authority. URL : https://www.eba.europa.eu/homepage

5. Cyber Insurance – Models and methods and the use of AI: European Union Agency for Cybersecurity, February 2024. Retrieved from https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai

КОНВЕРГЕНЦІЙНІ ПРОЦЕСИ МІЖ КІБЕРЗЛОЧИННІСТЮ ТА ТІНЬОВОЮ ЕКОНОМІКОЮ

INTERCONNECTION BETWEEN CYBERCRIME AND TRADITIONAL SHADOW ECONOMY

Роєнко Олександр, аспірант
Сумський державний університет, Україна

Цифрова ера змінила ландшафт злочинності, об'єднавши сфери кіберзлочинності та традиційної тіньової економіки в складну, переплетену мережу. Кіберзлочинність, яка характеризується такими злочинами, як хакерство, викрадення особистих даних і онлайн-шахрайство, використовує анонімність і охоплення Інтернету для сприяння незаконній діяльності. Водночас традиційна тіньова економіка, що охоплює нерегульовану економічну діяльність, як-от відмивання грошей, торгівля наркотиками та транзакції на чорному ринку, знайшла нові шляхи та інструменти в кіберпросторі. Таке зближення не тільки збільшує масштаби злочинних операцій, але й ускладнює боротьбу з ними. Розуміння взаємозв'язку між цими двома сферами має вирішальне значення для розробки комплексних стратегій протидії загрозам, що розвиваються, створеними сучасними злочинними підприємствами.

Одним із найбільш форм протиправної діяльності у мережі Інтернет є використання криптовалют для відмивання грошей. Кіберзлочинці використовують цифрові валюти для відмивання грошей, отриманих через незаконну діяльність в Інтернеті (атаки програм-вимагачів, шахрайство або продаж викрадених даних). Криптовалюти пропонують анонімність і децентралізацію, що робить їх привабливим варіантом для передачі та конвертації незаконних доходів у законні активи (Caporale et al., 2021). Ця практика часто поширюється на традиційну тіньову економіку, де відмиті кошти інвестуються в підприємства, нерухомість або інші підприємства, що працюють поза межами регуляторного нагляду.

На сьогодні відбувається стрімкий розвиток даркнет-порталів, які сприяють продажу незаконних товарів і послуг, таких як наркотики, зброя, підроблена валюта, і навіть торгівлі людьми (Chertoff & Simon, 2015). Продавці на цих платформах часто використовують методи кіберзлочинців для забезпечення анонімності, такі як шифрування та використання псевдонімів, тоді як покупці та продавці беруть участь у транзакціях, які віддзеркалюють транзакції традиційних чорних ринків, але з додатковим рівнем цифрового захисту.

Крадіжка особистих даних і фінансове шахрайство є сферами, де кіберзлочинність підтримує традиційну тіньову економіку. Викрадені особисті дані продаються в темній мережі та використовуються для створення підроблених документів, відкриття шахрайських банківських рахунків або забезпечення позик, що сприяє різноманітній незаконній діяльності. Викрадені кошти часто спрямовуються в різнозноманітні канали тіньової економіки, фінансуючи такі операції, як організовані злочинні синдикати, наркокартелі та мережі торгівлі людьми.

Однією із форм конвергенції кіберзлочинності та нелегальної економічної діяльності є атаки програм-вимагачів, коли кіберзлочинці шифрують дані жертви та вимагають плату за їх розповсюдження. Викуп, який зазвичай сплачується в криптовалюті, часто підтримує іншу незаконну діяльність у тіньовій економіці. Крім того, навички та ресурси, необхідні для здійснення таких атак, можуть бути передані або розвинені групами, що діють у традиційному злочинному світі, що ще більше стирає межі між цими сферами.

Виробництво та розповсюдження підроблених товарів, які є поширеною формою тіньової економіки, яка значно посилилися завдяки кіберзлочинності. Хакери викрадають інтелектуальну власність, комерційні таємниці та проекти, які потім використовуються для виробництва підробленої продукції. Ці товари часто продаються в Інтернеті через незаконні канали з використанням кібертехніки, щоб уникнути виявлення та правоохоронних органів. Прибутки від цих продажів повертаються в тіньову економіку, фінансуючи інші незаконні операції.

Для оцінювання взаємозв'язку між рівнем кіберзлочинності та обсягом тіньової економіки використано кореляційний аналіз. Для характеристики обсягу протиправної діяльності в інтернет просторі використано інтегральний індикатор Cyber-Safety Score (SEON, 2023), який відображає середнє значення трьох основних індексів у сфері кібербезпеки – National Cyber Security Index, Global Cybersecurity Index, Cybersecurity Exposure Index. Обсяг тіньової економіки враховувався на основі Quarterly Informal Economy Survey (World Economics, 2024). Коефіцієнт кореляції Пірсона становить -0,739, що наявність тісного оберненого лінійного зв'язку між даними процесами. Графічне представлення між рівнем кіберзлочинності та обсягом тіньової економіки подано на рисунку 1.

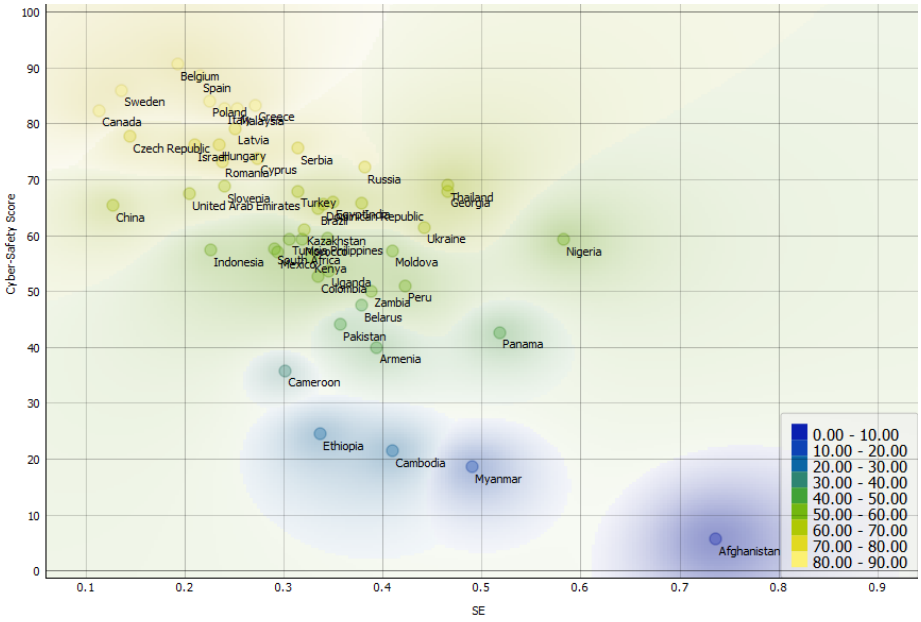

Рисунок 1. Взаємозв'язок між рівнем кіберзлочинності та обсягом тіньової економіки

Загалом, взаємозв'язок між кіберзлочинністю та традиційною тіньовою економікою багатогранний, цей симбіоз не тільки ускладнює боротьбу з цими злочинами, але й підкреслює необхідність скоординованих зусиль між кіберекспертами, правоохоронними органами та міжнародними органами для ефективного вирішення проблем, пов'язаних із цим мінливим кримінальним середовищем.

Список використаних джерел

1. Caporale, G. M., Kang, W. Y., Spagnolo, F., & Spagnolo, N. (2021). Cyber-attacks, spillovers and contagion in the cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money*, *74*. https://doi.org/10.1016/j.intfin.2021.101298

2. Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. *Global Commission on Internet Govrnance*, (6), 6–8. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

3. SEON (2023). Global Cybercrime Report: Which Countries Are Most at Risk in 2023?. URL: https://seon.io/resources/global-cybercrime-report/

4. World Economics (2024). Quarterly Informal Economy Survey (QIES). URL: https://www.worldeconomics.com/Informal-Economy/

АНАЛІЗ ОСНОВНИХ ТРЕНДІВ НА СВІТОВОМУ РИНКУ КІБЕРСТРАХУВАННЯ

ANALYSIS OF THE MAIN TRENDS IN THE GLOBAL CYBER INSURANCE MARKET

Ксенія Могильна, *студентка*
Сумський державний університет, Україна

Науковий керівник:
Сергій Миненко, доктор філософії
Сумський державний університет, Україна

У сучасному світі новітні технологічні досягнення переплітаються з повсякденним життям, а шкода від кібератак і кіберінцидентів стає надзвичайно вагомою. На тлі повномасштабного вторгнення Росії в Україну імператив захисту від кіберзагроз вийшов на новий рівень, про що свідчить хвиля кібератак, спрямованих на українські організації протягом 2022-2023 років. У цьому контексті розуміння й аналіз ринку кіберстрахування набуває першорядного значення, адже розвиток кіберстрахування дозволяє організаціям зменшити ризики пов'язані з кіберзагрозами. З огляду на актуальність цієї теми метою цього дослідження є вивчення останніх тенденцій ринку кіберстрахування у глобальному світовому ландшафті, контекстуалізуючи дискурс у горнилі ринкових тенденцій, сучасних геополітичних подій і розвитку технологій штучного інтелекту.

Нюансоване вивчення тенденцій ринку кіберстрахування вимагає розуміння основних теоретичних засад цієї сфери, з цією метою необхідно розтлумачити головну дефініцію. За визначенням Л. Албон та ін. «Кіберстрахування – це широкий термін для позначення страхових полісів, які стосуються збитків першої та третьої сторони в результаті комп'ютерної атаки або збою в роботі систем інформаційних технологій організації» (S. Romanosky et al., 2019). Таке визначення є достатньо повним, однак його можна дещо доповнити узагальнивши небезпеки «комп'ютерної атаки або збою в роботі систем інформаційних технологій фірми» (S. Romanosky et al., 2019) за допомогою терміну «кіберризик», оскільки саме він є основним об'єктом кіберстрахування.

За тлумаченням Р. Пікус і Ю. Бабенко «Кіберризик – це ймовірність настання подій, які вражають роботу IT-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій, що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації (Пікус & Бабенко, 2022). Таке

визначення наголошує на широкому спектрі інцидентів, які підпадають під сферу дії кіберстрахування.

Розглянутий теоретичний підхід підкреслює важливість кіберстрахування для зменшення ризиків у цифровому середовищі. Однак, через молодий статус цієї сфери воно може бути недостатньо впровадженим у стратегії управління ризиками компаній. Результати аналізу статистичних даних звіту Hiscox про кібернетичну готовність 2023 року вказують на зростання використання кіберстрахування серед великих компаній з 72% у 2021 році до 75% у 2022-2023 роках (Lamb, 2023). Це свідчить про збільшення усвідомлення необхідності захисту від кіберризиків серед цих компаній. Однак серед малих підприємств з меншою кількістю працівників використання кіберстрахування менш поширене. Частка малих компаній, які користуються кіберстрахуванням, зросла з 50% у 2021 році до 57% у 2022 році, але незначно знизилася до 56% у 2023 році (Lamb, 2023), можемо приспустити, що причиною нижчого рівня використання кіберстрахування серед малого бізнесу можуть бути такі фактори, як висока вартість, недостатня обізнаність про ризики, складність полісів та недооцінка кіберзагроз.

Іншим важливим показником для аналізу ринку кіберстрахування є річні світові витрати на кіберстрахування. За статистичними даними можна стверджувати, що світові витрати на кіберстрахування показують стабільний ріст, з 2,5 мільярдів доларів у 2015 році до 16,4 мільярдів доларів у 2023 році (Cybersecurity Insurance Market: Forecast 2024 – 2032, 2023). Цей ріст є наслідком зростаючого усвідомлення кіберризиків і збільшення попиту на страховий захист. За результатами аналізу статистичних даних (Cybersecurity Insurance Market: Forecast 2024 – 2032, 2023), можемо побачити, що темпи зростання підсилилися під час початку пандемії COVID-19 у 2020 році (зростання на 60,0%) та під впливом повномасштабного вторгнення Росії в Україну в 2022 році (зростання на 51,1%). Такі події підвищили кіберризики, спонукаючи компанії збільшувати свої витрати на кібербезпеку, включаючи кіберстрахування.

У рамках дослідження було виявлено, що збільшення кіберризиків через пандемію COVID-19 та російсько-український конфлікт призвело не лише до зростання попиту на кіберстрахування, але й до перегляду умов полісів. Наприклад, премії кіберстрахування на ринку США зросли з 10 млрд. доларів США у 2021 році до близько 12 млрд. доларів США у 2022 році й очікувано продовжуватимуть зростати з середнім приростом у 20% на рік до 2025 року (Farley, 2023). Іншою поширеною зміною змісту страхових полісів пов’язаною з війною в Україні є виключення або значне зниження рівня покриття для кіберінцидентів, які можуть бути пов’язані кібервійнами.

Прикладом таких винятків для таких інцидентів є чотири виключення щодо кібервійни та кібероперацій Lloyd's Market Association (Farley, 2023).

Ще однією важливою характеристикою ринку кіберстрахування є асиметричність у поширеності кіберстрахування в різних галузях. Деякі, такі як освіта, готельний бізнес та ігрова індустрія, показують високий рівень використання кіберстрахування, перевищуючи 65% (Pendleton et al., 2021). З цього зрозуміло, що у цих галузях фахівці визнають ризики цифрових операцій, обробки конфіденційної інформації та потребу їх надійного страхового захисту. Однак у виробництві, професійних послугах та фінансових установах використання кіберстрахування нижче 45% (Pendleton et al., 2021). Ця різниця може бути зумовлена різним сприйняттям ризиків, обмеженістю ресурсів або регуляторними міркуваннями у кожному секторі. Втім, варто відмітити, зростання частки компаній, які використовують кіберстрахування у всіх галузях протягом 2016-2020 років (Pendleton et al., 2021), на основі якого можна стверджувати, що перегляд стратегій кібербезпеки ставав все важливішим для компаній різних галузей протягом досліджуваного періоду.

Після виконаного аналізу ринку кіберстрахування стає очевидним, що ця галузь активно розвивається в умовах цифровізації, а декілька домінуючих тенденцій, виявлених у попередньому аналізі, змінюють ландшафт страхового покриття та стратегії управління ризиками у всьому світі. На основі проведеного аналізу можна виокремити основні тенденції притаманні ринку кіберстрахування, перелік яких наведено нижче.

1. Зростання обсягу ринку. Останні світові події, такі як пандемія COVID-19 та російсько-українська війна, підвищили кількість, масштаби та вартість кіберризиків, підкресливши потребу у надійному страховому захисті для зменшення фінансових втрат від кіберінцидентів.

2. Збільшення глобальних премій. Зростання потенційної вартості збитків від кіберінцидентів призвело до збільшення глобальних страхових премій, відображаючи зростаюче визнання фінансового впливу кібератак на підприємства та організації в усьому світі.

3. Зменшення покриття кіберризиків, пов'язаних з кібервійнами та кіберопераціями. Спостерігається тенденція до скорочення покриття ризиків, пов'язаних з кібервійнами та кіберопераціями, через зростання світової геополітичної напруженості. Шляхом оновлення умов покриття цих ризиків у страхових полісах, страховики намагаються впоратися зі складнощами та невизначеністю, притаманними цим новим загрозам.

4. Асиметрія у різних галузях. Рівень поширення кіберстрахування значно варіюється між галузями, з освітою, послугами та охороною здоров'я, які виявляють вищі темпи впровадження порівняно з виробництвом, професійними послугами та фінансовими установами.

5. Складність андеррайтингу. Відсутність стандартизованого покриття, обмежений досвід менших страхових організацій, труднощі у доступі до статистичної інформації значно ускладнюють процес андеррайтингу – виявлення, аналіз та оцінка ризиків.

6. Використання інструментів аналізу даних. Застосування сучасних інструментів аналізу даних, таких як штучний інтелект та машинне навчання, може полегшити проблеми з андеррайтингом. Ці інструменти дозволяють страховикам розробляти складніші моделі оцінки та прогнозування кіберризиків, що допомагає їм адаптувати страхові рішення до змінних потреб клієнтів у цифровому середовищі.

Підсумовуючи, у дослідженні було проаналізовано загальні тенденції сучасного світового ринку кіберстрахуваня, включаючи вплив соціальних та геополітичних процесів, зміну умов страхових полісів, ускладнення процесів андеррайтингу та інтеграцію передових інструментів аналізу даних, які сприяють глибшому розумінню управління ризиками у кіберстрахуванні. Отримані результати можуть будуть використані для подальших досліджень ринку кіберстрахування в Україні, включаючи розробку стандартизованого покриття та політик, спрямованих на спрощення процесу андеррайтингу та підвищення прозорості ринку.

Роботу виконано в рамках НДР № 0122U000783 «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів»

Список використаних джерел

1. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1). https://doi.org/10.1093/cybsec/tyz002

2. Пікус, Р. В., & Бабенко, Ю. Л. (2022). Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава*, (2), 134–140. https://doi.org/10.32702/2306-6806.2022.2.134

3. Lamb, E. (2023). *Hiscox cyber readiness report* 2023. Hiscox. https://www.hiscox.co.uk/sites/default/files/documents/2023-10/Cyber-Readiness-Report-2023-UK.pdf

4. *Cybersecurity Insurance Market: Forecast 2024 – 2032* (Report GMI6407). (2023). Global Market Insights. https://www.gminsights.com/industry-analysis/cybersecurity-insurance-market

5. Farley, J. (2023). 2023 U.S. cyber market conditions outlook report. Gallagher. https://www.ajg.com/us/-/media/files/gallagher/us/2023-us-cyber-market-conditions-outlook-report.pdf

6. Parashchak, O. (2023). *Cyber insurance 2023 global insurance ranking of cyber insurers by premiums*. Beinsure Digital Media. https://beinsure.com/global-ranking-cyber-insurers/#top-5-insurer-by-gross-direct-premiums-written-for-cyber-insurance

ТЕНДЕНЦІЇ РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ У СВІТІ

TRENDS IN THE DEVELOPMENT OF THE CYBER INSURANCE MARKET IN THE WORLD

Ольга Горбачова, студентка
Сумський державний університет, Україна

В епоху стрімкого цифрового розвитку та пандемії COVID-19 кіберстрахування стає все більш критичним, адже кібератаки сягають небачених масштабів у всьому світі. Особливо гостро це питання стоїть в освітній сфері, де спостерігається значне зростання кіберзагроз, зокрема в Північній Америці, Європі та Африці. З огляду на це, стає очевидною нагальна потреба у постійному вдосконаленні стратегій кібербезпеки та активному усуненні вразливих місць. Це дозволить гарантувати безпеку та надійність цифрових активів компаній.

Згідно зі звітом SonicWall Cyber Threat Report (2023) кількість інцидентів зі зловмисним програмним забезпеченням зросла у 2022 році вперше з 2018 року, досягнувши 5,5 мільярдів атак. Хоча у 2023 році кількість атак програм-вимагачів зменшилася на 21%, але залишається значною, що створює серйозні загрози для бізнесу, а також помітно зросла кількість DDoS-атак, що може призвести до відключення веб-сайтів, завдаючи фінансових втрат.

Один із механізмів перерозподілу кібернетичного ризику є страхування, яке стає все більш популярним, дозволяючи компаніям продовжувати далі функціонувати за умови настання кіберінциденту. .

Кіберстрахування – це страховий продукт, який використовується для захисту компаній та окремих користувачів від ризиків, пов’язаних з Інтернетом, і загалом від ризиків, пов’язаних з інфраструктурою та діяльністю інформаційних технологій (Kesan & Yurcik, 2013).

Зростання кібератак і посилення правил захисту даних та вимог відповідності зробили кіберстрахування все більш популярним. Шахраї постійно розробляють нові методи вторгнень та крадіжок даних, що ставить організації перед загрозою. А за новими правилами організаціям доводиться приймати заходи для захисту персональних даних, оскільки порушення цих правил може призвести до значних штрафів. Крім того, зростання цифровізації бізнесу робить організації більш залежними від технологій. Це збільшує потенційну поверхню атаки для кіберзлочинців. Крім того, зростання цифровізації бізнесу робить організації більш залежними від технологій. Це збільшує потенційну поверхню атаки для кіберзлочинців.

Однак ринок кіберстрахування все ще перебуває на стадії розвитку. Загалом, кіберстрахування стикається з низкою викликів, таких як відсутність історичних даних, брак кіберданих та складність визначення кібератак. Додатковою проблемою є низьке усвідомлення ризиків. Щоб подолати ці проблеми, потрібно розвивати нові методи андеррайтингу, проводити більш глибокий аналіз ризиків та співпрацювати з організаціями для вдосконалення процесу кіберстрахування (Nishanka, 2018).

Регіонально, ринок кіберстрахування демонструє різний рівень активності. Північна Америка та Європа залишаються лідерами, хоча Азіатсько-Тихоокеанський регіон показує найбільший потенціал для динамічного розвитку. Серед головних гравців ринку, Chubb Ltd та American International Group, Inc. відзначаються значною присутністю та впливом.

Страхування кібервідповідальності стає все більш популярним серед підприємств, оскільки воно надає комплексний захист від фінансових та юридичних наслідків кіберінцидентів. Іншими популярними продуктами є страхування кібербезпеки та страхування від технологічних помилок і упущень.

Проте ринок кіберстрахування зазнає викликів, таких як складний процес андеррайтингу та дисбаланс між попитом і пропозицією, що призводить до зростання цін на страхові премії. Гармонізація мови та процесів андеррайтингу, використання аналітики великих даних та поліпшення управління претензіями є ключовими тенденціями розвитку ринку. Загалом, ринок кіберстрахування продовжує розвиватися, стаючи важливим елементом для захисту від кіберзагроз у сучасному світі.

Список використаних джерел

1. Sonicwall. 2023 SONICWALL CYBER THREAT REPORT: Report. 2023 p. URL: https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf (date of access: 23.03.2024);

2. Kesan, J., & Yurcik, W. (2013). The economic case for cyberinsurance. *Dissent*, *Aut / Win*(41), 18–21. Retrieved from http://search.informit.com.au.wwwproxy0.library.unsw.edu.au/documentSummary;dn=291645822148222;res=IELAPA

3. Nishanka, A. K. (2018). Evaluating Cyber Infrastructure for Cyber-Insurance in the Corporate World: An Analytical Focus. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2864383

РОЛЬ КІБЕРСТРАХУВАННЯ У ПІДВИЩЕННІ РІВНЯ КІБЕРСТІЙКОСТІ КОМПАНІЙ

THE ROLE OF CYBER INSURANCE IN INCREASING THE LEVEL OF CYBER RESILIENCE OF COMPANIES

Валерія Кочнєва, студентка
Сумський державний університет, Україна

Науковий керівник:
Вікторія Боженко, к.е.н., доцентка
Сумський державний університет, Україна

У епоху стрімкого розвитку цифрових технологій, питання кібербезпеки особливо актуальне для компаній, що впроваджують у своїй діяльності інформаційні технології. Більшість компаній використовують у своїй діяльність мережеві та цифрові технології, зважаючи на переваги цих технологій: можливість автоматизувати бізнес-процеси, підтримувати та підвищувати рівень конкурентоспроможності.

Проте, стрімкий технологічний розвиток, окрім переваг створює й нові ризики для компаній пов'язані з можливими кібератаками. Технологічна сторона кіберзлочинів модернізується на рівні з іншими технологіями, що, в свою чергу, підвищує вразливість компаній.

Попри постійні заходи попередження здійснення кіберзлочинів, їх кількість зростає з кожним роком, як і витрати компаній від здійснення кіберзлочинів. Окрім того, відповідно до звіту Cost of a Data Breach Report 2023 від IBM Corporation, у 2023 році загальна середня вартість від витоку даних внаслідок здійснення кібератаки, досягла історичного максимуму в 4,45 млн дол. США, що на 2,3% більше за попередній рік (IBM Corporation, 2023).

Станом на 2023 рік найбільші витрати внаслідок витоку даних спостерігаються у таких галузях, як охорона здоров'я (10,93 млн дол.), фінансова (5,9 млн дол.), фармацевтична (4,82 млн дол.), енергетична (4,78 млн дол.) та промисловість (4,73 млн дол.) *(IBM Corporation, 2023).*

Зважаючи на постійне зростання витрат від кіберзлочинів та зростання їх кількості, існують різні методи захисту компаній від кіберзлочинності. Проте виконання усіх необхідних вимог для підтримання кібербезпеки, не захищає компанію цілком від настання кіберінциденту. Навіть найбільш технологічно озброєні та захищені компанії піддаються кібератакам: масова атака на сервери Microsoft Exchange у січні 2021 року, масштабний витік даних клієнтів Facebook у 2021 році, отримання кіберзлочинцями доступу

до персональної інформації користувачів Samsung, у 2023 році (*Biggest Data Breaches in US History (Updated 2024) | UpGuard*; *High-Profile Company Data Breaches*). Відповідно до Travelers Risk Index 57% власників компаній вважають кібератаки неминучими (*What is Cyber Insurance? | IBM*). Тому, наступним важливим пунктом для компаній у прийнятті рішень, щодо забезпечення кібербезпеки, має постати кіберстрахування.

Існують різні визначення поняття кіберстрахування. Зокрема онлайн-журнал Forinsurer визначає кіберстрахування, як страховий продукт для захисту бізнесу та фізичних осіб від ризиків, пов'язаних із використанням інтернету, зберіганням та обробкою даних в електронному вигляді, роботою з IT-інфраструктурою. Компанія IBM визначає кіберстрахування як інструмент для покриття фінансових витрат, що виникають у результаті атак програм-вимагачів, витоку даних та інших кіберінцидентів (What is Cyber Insurance? | IBM). Компанія CFC визначає кіберстрахування, як продукт, що допомагає компаніям реагувати та відновлювати фінансові витрати, пов’язані з настанням кіберінциденту, що включає збитки від збоїв у роботі, витрати на усунення та відновлення, судові збори, шкоду репутації, регуляторні штрафи тощо (Is cyber insurance worth it? | CFC). У будь-якому випадку, кіберстрахування є методом усунення фінансових збитків, яких зазнала компанія після настання кіберінциденту чи кіберзлочину.

Кіберстрахування поділяють на 2 види: страхування першої особи та страхування третіх осіб. Страхування першої особи покриває фінансові збитки, яких зазнають самі страхувальники у результаті кіберподії. Зазвичай страхування першої особи включає експертну підтримку для вирішення кіберінциденту та відновлення систем і даних у стані, в якому вони були до інциденту, а також відшкодовування втрат коштів. Страхування третіх осіб покриває позови щодо відповідальності, подані у зв’язку з порушенням безпеки мережі або конфіденційності, як-от нездатність запобігти крадіжці особистих даних. Страхування третіх осіб зазвичай включає відшкодування збитків, які страхувальник юридично зобов’язаний сплатити третім особам, судові збори, понесені для захисту страхувальника від позову про відповідальність, а також штрафи призначені регуляторами та іншими органами.

Серед компаній, що зіткнулись з витоком даних внаслідок кібератак у 2023 році, 51% компаній підвищили інвестиції спрямовані на підвищення рівня кіберзахисту компанії (Cost of a Data Breach Report 2023). При чому 18% компаній збільшили свої інвестиції на забезпечення кіберстрахування. За оцінкою IBM, за 2023 збитки від витоку даних внаслідок кібератак компаній, що мали кіберстрахування, у середньому на 196 452 дол. менше ніж збитки компаній, що не мали такого страхування. Кіберстрахування суттєво знижує обсяг витрат пов’язаних з настанням кіберінциденту.

Більшість страхових рішень у страхуванні кіберризиків здатні покривати такі витрати пов'язані з настанням кіберзлочину (*What is Cyber Insurance? | IBM*,):

– частина або усі витрати пов'язані з втратою доходу через кібератаку;

– витрати пов'язані з ремонтом системи, судовими дослідженнями, реагуванням на інциденти;

– витрати пов'язані з судовим процесом, пов'язаним з наслідками кібератаки: витоком даних клієнтів, судових позовів та інше;

– деякі страхові компанії можуть надавати допомогу по моніторингу використання персональної інформації клієнтів та сповіщення клієнтів про виникнення кіберінциденту;

– деякі страхові компанії надають можливість покриття витрат за викуп програм-вимагачів, проте це залежить від розміру викупу;

– витрати на розслідування, штрафи та перевірки.

Обсяг послуг, які покриває кіберстрахування не є вичерпним і залежить від обраного виду страхування та компанії, що надає страхування. Водночас компаніям, що обирають кіберстрахування варто усвідомлювати, що кіберстрахування не покриває усі наявні збитки від настання кіберінциденту, наприклад, якщо настання кіберінциденту спричинене недосконалістю безпеки систему, яка була відома компанії чи недбалістю співробітників компанії.

Кіберстрахування є одним з важливих факторів розвитку кіберстійкості компанії. На перший погляд, говорячи про поняття кіберстійкості на думку може спадати саме здатність компанії та системи вистояти проти кіберзлочину, проте під терміном «кіберстійкість» також розуміють і здатність компанії відновлюватись після настання кібератак. Кіберстрахування і є тим інструментом який допоможе компаніям відновити свою діяльність, нівелювати отримані фінансові збитки, та полегшити період після настання кіберзлочину.

Кіберстрахування, на відміну від заходів попередження кіберзлочинів, створює для компаній так звану «подушку безпеки». Як зазначалося раніше, навіть найбільш модернізовані та технологічно озброєні компанії не захищені цілком від можливих кібератак, тому кіберстрахування може допомогти компаніям легше оговтатись від настання кіберінциденту у фінансовому, операційному та юридичному полі.

Варто також зазначити, що кіберстрахування не є панацеєю від кіберінцидентів і не кожен інцидент може бути застрахованим та відшкодованим компанії. Проте, разом із методами попередження кіберзлочинів будь-який варіант кіберстрахування підвищує кіберстійкість компанії, а саме її можливість відновитись на ринку без вагомих втрат навіть за настання кіберінциденту.

Список використаних джерел

1. IBM Corporation. (2023). *Cost of a Data Breach Report 2023*.
2. Business *(2024).* How to Protect Your Business From Cybercrime. https://www.business.com/articles/cyber-crime-to-reach-2-trillion-what-can-we-do/
3. *Forinsurer* Страхування кібер-ризиків. Cyber insurance. *:* https://forinsurer.com/theme/48.
4. *IBM. What is Cyber Insurance? URL:* https://www.ibm.com/topics/cyber-insurance
5. *CFC (2024). Is cyber insurance worth it? URL:* https://www.cfc.com/en-gb/resources/articles/2024/01/is-cyber-insurance-worth-it/
6. *UpGuard* (2024). *Biggest Data Breaches in US History (Updated 2024). URL:* https://www.upguard.com/blog/biggest-data-breaches-us
7. Electric. *High-Profile Company Data Breaches*. URL: https://www.electric.ai/blog/recent-big-company-data-breaches

КОРУПЦІЯ ЯК ІНСТРУМЕНТ ПРОНИКНЕННЯ ТА ВИКРАДАННЯ ІНСАЙДЕРСЬКИХ ДАНИХ

CORRUPTION AS A TOOL FOR PENETRATING AND STEALING INSIDER DATA THREFT

Іван Гончарук, аспірант
Сумський державний університет, Україна

У сучасному взаємопов'язаному та оцифрованому світі організації стикаються з цілою низкою викликів безпеці, які загрожують їхній цілісності та діяльності. Серед цих викликів внутрішні загрози – зловмисна діяльність, ініційована окремими особами в організації - є особливо згубною через їхній потенціал обходити традиційні заходи безпеки. Хоча внутрішні загрози можуть виникати з різних мотивів, корупція в організації може значно посилити ці ризики. Корупція, що проявляється у зловживанні владою для отримання особистої вигоди, створює середовище, в якому неетична поведінка стає нормою, а протоколи безпеки послаблюються. У цій статті досліджується, як корупція не лише формує культуру, сприятливу для внутрішніх загроз, але й посилює шкоду, завдану такими діями. Вивчаючи взаємозв'язок між корупцією та внутрішніми загрозами, звертається увага на важливість дотримання етичних стандартів і надійних практик безпеки для захисту активів і репутації організації.

У дослідженні встановлено, що в середньому між працевлаштуванням працівника та здійсненням ним шахрайських операцій проходить 5 років, тоді як між початком шахрайства та його виявленням – 42 місяці (Miller, 2021).

Моделі змови між корумпованими інсайдерами та зовнішніми кіберзлочинцями часто дотримуються різних стратегій і тактик, які використовують як внутрішній доступ, так і зовнішні шкідливі можливості, а саме:

– фінансові стимули та підкуп. Зовнішні кіберзлочинці можуть пропонувати фінансові стимули або хабарі корумпованим інсайдерам в обмін на доступ до конфіденційної інформації, облікових даних для входу або систем (Benk et al., 2018).

– крадіжка та продаж даних: корумповані інсайдери можуть викрасти цінні дані, такі як інтелектуальна власність, інформація про клієнтів або власні технології, і продати їх кіберзлочинцям. Ці дані можуть бути використані для подальших злочинних дій, таких як викрадення особистих даних, шантаж або конкурентна розвідка (Moore et al., 2015).

– спільний доступ до облікових даних: Інсайдери можуть надати кіберзлочинцям законні облікові дані для входу або створити бекдори в системі, що дозволить зовнішнім зловмисникам обійти заходи безпеки та отримати несанкціонований доступ до мережі організації.

– розміщення зловмисного програмного забезпечення: кіберзлочинці можуть співпрацювати з інсайдерами, щоб розмістити зловмисне програмне забезпечення, як-от програми-вимагачі або шпигунські програми, у системах організації. Інсайдери можуть допомогти, вимкнувши програмне забезпечення безпеки, відкривши інфіковані вкладення або безпосередньо встановивши шкідливі програми.

– полегшення фішингових атак. Інсайдери можуть допомогти кіберзлочинцям створювати більш переконливі фішингові атаки, надаючи інформацію про стилі спілкування організації, внутрішній жаргон і конкретні цілі. Ці інсайдерські знання підвищують вірогідність успіху фішингових електронних листів (Kratcoski, 2018).

– використання вразливостей системи: Інсайдери, які знають IT-інфраструктуру організації та протоколи безпеки, можуть інформувати кіберзлочинців про конкретні вразливості. Потім кіберзлочинці можуть використовувати ці недоліки для проникнення в мережу (English et al., 2019).

– прикриття слідів: корумповані інсайдери можуть допомогти кіберзлочинцям, підробляючи журнали, відключаючи системи моніторингу або вводячи в оману внутрішні розслідування, щоб приховати злом і участь інсайдерів. Це ускладнює для організації виявлення загрози та реагування на неї.

– інсайдерська торгівля: у деяких випадках корумповані інсайдери можуть передавати зовнішнім особам конфіденційну інформацію про діяльність компанії, фінансовий стан або стратегічні плани. Цю інформацію можна використовувати для інсайдерської торгівлі або для інформування про кібератаки, які можуть вплинути на ціни акцій.

– соціальна інженерія: кіберзлочинці можуть покладатися на інсайдерів, щоб надати особисту інформацію про ключових співробітників або організаційні процедури, які можуть бути використані для проведення атак соціальної інженерії. Це може включати видавання себе за керівників чи IT-спеціалістів, щоб отримати подальший доступ або маніпулювати іншими працівниками.

– примус і шантаж: у певних ситуаціях кіберзлочинці можуть примусити або шантажувати інсайдерів, щоб вони співпрацювали з ними. Це може включати погрози розкрити власну незаконну діяльність або особисті секрети інсайдера, якщо вони не сприяють досягненню цілей кіберзлочинців.

Таким чином, для посилення кібербезпеки суб'єкта господарювання доцільно посилювати контроль за дотриманням етичних стандартів та надійних практик безпеки для захисту активів та репутації компанії.

Список використаних джерел:

1.Benk, S., McGee, R. W., & Budak, T. (2018). A public perception study on bribery as a crime in Turkey. *Journal of Financial Crime*, *25*(2), 337–353. https://doi.org/10.1108/JFC-07-2017-0061

2.English, K. V., Obaidat, I., & Sridhar, M. (2019). Exploiting Memory Corruption Vulnerabilities in Connman for IoT Devices. In *Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019* (pp. 247–255). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DSN.2019.00036

3.Kratcoski, P. C. (2018). *Fraud and Corruption: Major Types, Prevention, and Control*. *Corporate Communications* (p. 301).

4.Miller S. Spotlight on Insider Fraud in the Financial Services Industry. URL: https://apps.dtic.mil/sti/pdfs/AD1123958.pdf

5.Moore, C., & Gino, F. (2015). Approach, Ability, Aftermath: A Psychological Process Framework of Unethical Behavior at Work. *Academy of Management Annals*, *9*(1), 235–289. https://doi.org/10.1080/19416520.2015.1011522

СЕКЦІЯ 3 ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS

Avhusta Hrytsenko, student,
Sumy State University, Ukraine

Scientific adviser:
Olena Pahnenko, PhD, Associate Professor
Sumy State University, Ukraine

In the digital age, the proliferation of interconnected devices and reliance on technology has transformed the way we live, work, and interact. However, alongside the benefits of connectivity and innovation come unprecedented cybersecurity challenges. The increasing frequency and sophistication of cyber threats, ranging from malware and phishing attacks to data breaches and ransomware incidents, pose significant risks to individuals, organizations, and societies at large. In response to these evolving threats, there has been a growing recognition of the need for advanced cybersecurity measures capable of effectively detecting, mitigating, and preventing cyber-attacks in real time. In this context, the role of artificial intelligence (AI) has emerged as a game-changer in the field of cyber security.

Cybersecurity is a specific practice of protecting systems, networks, and programs from digital attacks. This term is often used interchangeably with “information security” and means a set of security measures and policies aiming to prevent data from disruptions or unauthorized access, use, disclosure, or modification (Ghelani, 2022). Cyber threats have a profound impact on various areas from individuals and organizations to governments and critical infrastructures. Thus, there is a huge need for proactive measures to enhance resilience, safeguard critical infrastructure, and protect individuals' rights and freedoms in cyberspace. Additionally, this problem is complicated by the spreading use of AI. Cyberattackers are developing AI-enabled malware that is adaptive, has the ability to understand the target environment, evade detection, continue to learn, and make advanced decisions. In this regard, malware is getting smarter and cyberthreats are evolving and becoming more sophisticated and complex. Hence, human intervention and capacity are not enough to sufficiently deal with advanced threats, the speed of processes, the amount of data, and the vulnerability of intrusion.

Thus, the countering of advanced adversaries requires an active approach to security that will place an emphasis on proactive measures, real-time detection, active monitoring, and mitigation of key threats. Therefore, innovative approaches such as the application of AI tools that have a learning capacity, are adaptable, analysis-driven, and able to detect user behavior and make intelligent and real-time decisions become a new powerful weapon in fighting cyber threats (Kadel et al., 2023).

Artificial Intelligence is the development of complex computer systems with the aid of human mentality which is able to perform its function like a human being. AI is a comprehensive scientific system with varying branches in math, computer science, and philosophy whose purpose is to develop another system that shows intelligence properties.

The integration of AI offers a promising avenue for countering the ever-evolving landscape of cyber threats. AI systems possess the capability to process vast amounts of data at incredible speeds, enabling them to detect patterns, anomalies, and potential threats more effectively than traditional methods (Agrawal et al., 2023). Moreover, AI-driven algorithms can adapt and learn from new data, continuously improving their ability to identify and mitigate risks. By automating threat detection, response, and remediation processes, AI not only enhances the efficiency of cyber security operations but also minimizes human error and response times (Tao et al., 2021). Additionally, AI facilitates predictive analytics (Kadet et al., 2023), allowing organizations to anticipate and proactively address emerging threats before they materialize. However, while AI holds immense potential in bolstering cyber defenses, it is not without challenges. Ethical considerations, biases in AI algorithms, and the potential for adversaries to exploit AI systems are among the concerns that must be carefully navigated (Dash et al., 2022). Nonetheless, with vigilant oversight, collaborative efforts, and ongoing innovation, the strategic deployment of AI can serve as a powerful tool in the fight against cyber threats, contributing to a more secure digital landscape for individuals, businesses, and governments alike.

The use of AI in cybersecurity has been instrumental in enhancing protection across various critical areas, including the following (Li & Liu, 2021).

AI is widely employed in protecting corporate networks by continuously monitoring network traffic for anomalies and potential threats. AI-driven intrusion detection systems (IDS) and intrusion prevention systems (IPS) analyze network behavior in real time, enabling rapid identification and mitigation of suspicious activities. AI-powered endpoint security solutions utilize machine learning algorithms to detect and respond to malware, ransomware, and other cyber threats targeting corporate devices.

Financial institutions face significant cybersecurity threats due to the sensitive nature of the data they handle. AI plays a crucial role in safeguarding

financial systems by detecting fraudulent transactions, identity theft, and unauthorized access. Furthermore, AI-driven risk assessment models help financial institutions evaluate and mitigate potential risks associated with lending, investments, and other financial activities.

Governments and state institutions rely on robust cybersecurity measures to protect sensitive information and critical infrastructure from cyber threats. AI is utilized in state information systems to bolster defenses against cyber-attacks, espionage, and other malicious activities. AI-driven threat intelligence platforms collect, analyze, and disseminate information about emerging cyber threats, enabling governments to proactively respond to potential risks. Additionally, AI-powered security analytics tools assist in identifying and mitigating vulnerabilities within state IT infrastructure, enhancing overall resilience against cyber threats.

AI technologies are employed to safeguard user data from unauthorized access, data breaches, and privacy violations. AI-driven identity and access management (IAM) systems utilize biometric authentication, behavioral analysis, and anomaly detection to verify user identities and prevent unauthorized access to sensitive data. Furthermore, AI-powered data loss prevention (DLP) solutions monitor and control the movement of confidential information across networks, ensuring compliance with data protection regulations such as GDPR and CCPA.

However, the application of AI in cybersecurity also presents several challenges that must be carefully addressed. Among these challenges are the following ethical issues and potential for abuse, dependence on accuracy and timeliness of data, and presence and possibility of development of countermeasures by attackers(Bhatnagar et al., 2018). Additionally, the growing use of AI in this field undoubtedly leads to the growth and changes in cyber-attacks. For instance, expansion of existing threats due to the lowered costs of attacks or change to the typical character of threats due to the AI features itself. The possible changes in the cyber threats because of the use of AI can be illustrated through three main security domains, such as digital, physical, and political (Bhatnagar et al., 2018).

1. Digital security. The current trade-off between attack effectiveness and scalability will be reduced by using AI to automate cyberattack-related chores. This could increase the risk of labor-intensive cyberattacks (like spear phishing). It is also reasonable to anticipate new attacks that take advantage of software flaws (automated hacking), human weaknesses (speech synthesis used for impersonation), or AI system vulnerabilities (data poisoning and adversarial examples).

2. Physical security. The hazards connected to drone attacks could increase if artificial intelligence (AI) is used to automate processes related to carrying out attacks using drones and other physical systems (e.g., through the deployment of autonomous weapons systems). It is also reasonable to anticipate fresh attacks that utilize physical systems that would be impossible to control remotely, such as a

swarm of thousands of micro-drones, or manipulate cyber-physical systems, like crashing autonomous cars.

3. Political security. The possibilities of privacy invasion and social manipulation may increase if AI is used to automate operations related to surveillance (e.g., analyzing mass-collected data), persuasion (e.g., developing targeted propaganda), and deception (e.g., editing films). Furthermore, it is reasonable to anticipate new attacks that capitalize on the enhanced ability to examine human emotions, behaviors, and beliefs using the data at hand. While these issues are particularly important in the setting of authoritarian nations, they may also make it more difficult for democracies to continue having honest public discussions.

Concluding, the role of AI in countering cyber threats is pivotal in addressing the ever-evolving landscape of digital risks and vulnerabilities. AI-powered technologies offer unprecedented capabilities in detecting, mitigating, and responding to cyber-attacks with speed and accuracy. From automated threat detection to adaptive defense mechanisms, AI strengthens cybersecurity across various domains, including corporate networks, financial institutions, state information systems, and the personal privacy of users. However, the widespread adoption of AI in cybersecurity also presents challenges and threats, such as ethical considerations, dependence on data accuracy, and the possibility of adversarial exploitation.

References

1. Agrawal, J., Kalra, S. S., & Gidwani, H. (2023). AI in cyber security. *International Journal of Communication and Information Technology*, *4*(1). https://doi.org/10.33545/2707661x.2023.v4.i1a.59

2. Bhatnagar, S., Cotton, T., Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Carrick, J. S., Seán, F., Héigeartaigh, Ó., Beard, S., … Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction. *ArXiv Preprint ArXiv:1802.07228*, *February 2018*.

3. Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. *International Journal of Software Engineering & Applications*, *13*(5). https://doi.org/10.5121/ijsea.2022.13502

4. Kadel et al., (2023). Emergence of AI in cyber security. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets32643

5. Ghelani, D. (2022). X(X): XX-XX Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal*

of Science, Engineering and Technology, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX

6. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*. https://doi.org/10.1016/j.egyr.2021.08.126

7. Tao, F., Akhtar, M., & Jiayuan, Z. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28). https://doi.org/10.4108/eai.7-7-2021.170285

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN COUNTERING CYBER THREATS

Вікторія Біловодська, студентка,
Сумський державний університет, Україна

Перші інструменти штучного інтелекту почали використовуватися в кінці вісімдесятих років минулого століття. Це були системи оповіщення про кіберзагрози на основі заздалегідь визначених правил та параметрів. З роками роль штучного інтелекту почала зростати завдяки прогресу в області машинного навчання, а прорив для штучного інтелекту забезпечив розвиток нейромереж за останній час. Наразі, інструменти штучного інтелекту активно використовуються у протидії кіберзагрозам.

Згідно зі звітом ENISA Threat Landscape 2022 визначено низку груп таких загроз: програми-здирники, шкідливе програмне забезпечення, соціальна інженерія, загрози для даних, загрози доступності (відмова в обслуговуванні), загрози доступності (Інтернет-загрози), дезінформація, атаки на ланцюги постачання.

За інформацією ENISA у 2022 році кількість атак загалом зменшилася в порівнянні з 2021 роком. Частково це пов'язано з тим, що обробка та аналіз інцидентів тривають і звіти не є остаточними, а також відкритим характером збору інформації в ETL, що може ненавмисно вносити упередженість у результати. Кіберзагрози зазвичай націлені на різні сектори діяльності, в багатьох випадках проявляються через використання вразливостей в базових ІКТ-системах різних напрямів.

Звіт ENISA за 2022 рік надає статистику, яка демонструє, що протягом аналізованого періоду спостерігалася велика кількість інцидентів, що були спрямовані на державні органи влади та постачальників цифрових послуг. Значна їх кількість була спрямована на кінцевих споживачів в різних секторах. Варто відзначити, що фінансова та сфера охорони здоров'я піддалися значній кількості атак. (European union agency for cybersecurity (ENISA): Threat landscape 2022 report is released - identity theft observatory system, б. д.)

Безумовно, наявність кіберзагроз потребує активних дій щодо їх уникнення та ліквідації наслідків. У цьому вже незамінними стали інструменти штучного інтелекту і вони мають ряд переваг.

Першим плюсом є швидкість реагування. Засоби штучного інтелекту здатні аналізувати мережевий трафік та величезні обсяги даних безперервно та в режимі реального часу, а також реагувати на будь-які аномалії та загрози

миттєво. Завдяки цьому він перевершує можливості людського реагування в тисячі разів.

Розвиток інструментів та алгоритмів штучного інтелекту знижує дефіцит кадрів, надають організаціям змогу використовувати наявні ресурси кібербезпеки набагато ефективніше (Cain et al., 2018).

Ще однією перевагою використання штучного інтелекту є підвищення за допомогою цих інструментів ефективності функціонального тестування цифрових продуктів для завчасного виявлення вразливостей в коді. Крім того, алгоритми машинного навчання та нейромережі мають властивість вчитися, тож можуть постійно вдаватися до нових методів перевірки. Фактично ШІ здатний ефективно імітувати дії злочинців, аби визначити ключові ризики та напрямки атаки системи.

Можливості штучного інтелекту у акумулюванні та аналізі великих обсягів даних щодо вразливостей систем, природи кібератак та поведінки користувачів дозволяє ефективно визначати потенційні ризики та проблеми у кібербезпеці компанії. Нейромережі та алгоритми машинного навчання можуть використовувати ці дані для прогнозування майбутніх кібератак та їх наслідків, визначення векторів загроз, ризиків тощо.

З іншого боку, хакери також можуть використовувати штучний інтелект для автоматизації процесу пошуку та експлуатації вразливостей у мережах та додатках. ШІ легко може збільшити ефективність атак, перебираючи паролі і ключі швидше, ніж будь-яка звичайна програма. До того ж, хакери можуть застосовувати штучний інтелект для розробки більш складних та невиявлених шкідливих програм, які легко обходять системи виявлення та антивірусні програми.

Все вищеперераховане підкреслює важливість розвитку засобів і методів захисту від кіберзагроз за допомогою ШІ, а також навчання співробітників компаній і користувачів ПК правилам безпеки. Адже з появою ШІ як інструменту для хакерів, кібербезпека стала ще складнішим завданням.

Інструменти штучного інтелекту можуть використовуватися для ідентифікації шкідливого проникнення в систему, тобто автоматично розпізнати сигнатуру зловмисного коду або вхідного інтернет-трафіку, зреагувати на аномальну поведінку користувачів (AbdulNabi et al., 2021). На сьогодні алгоритми машинного навчання широко використовуються для фільтрування спаму, які дозволяють зменшити фішингове навантаження на персонал компанії.

Здебільшого на великі компанії нападають не люди, а алгоритми. Зазвичай людина не здатна адекватно відповісти на цей виклик, адже зловмисні програми постійно видозмінюються. Втім, одному боту можна і потрібно протиставити іншого бота.

У корпоративній кібербезпеці система має одночасно відстежувати багато подій: інтернет-трафік, звернення на сайт тощо. Посеред цього «шуму» легко посилитись і трактувати звичайну поведінку як зловмисну — або навпаки. Наразі це основна проблема кібербезпеки, і генеративний ШІ має великі шанси зменшити кількість неправильно проінтерпретованих сигналів (ШІ у кібербезпеці: Роль, застосування та переваги | Wezom, б. д.).

Фахівці SiliconANGLE проаналізували найбільш перспективні продукти кібербезпеки на основі штучного інтелекту. Наприклад, Palo Alto Networks Inc. впроваджує свою власну велику мовну модель (LLM), яка використовуватиме штучний інтелект для покращення ефективності роботи. SentinelOne Inc. також створює LLM для виявлення потенційної загрози за допомогою простого пошукового запиту без потреби вивчення складної термінології чи синтаксису.

Cloudflare Inc. використовує машинне навчання для швидшого виявлення та нейтралізації ботнетів. Blink Ops і Trend Micro Inc. інтегрують ШІ у свої інструменти з функціями, схожими на копайлота. І це ще не все. Фахівці Darktrace Holdings Ltd. вже використовували штучний інтелект для виявлення кількох кібератак. Наприклад, штучний інтелект виявив за кілька годин спробу нападу на електромережу (Ten et al., 2010).

Підсумовуючи, варто зазначити, що штучний інтелект розвивається дуже стрімко і вже зараз може вирішувати більшість завдань у сфері кібербезпеки швидше, ефективніше та точніше, ніж людина. Безпековий сектор активно освоює засоби штучного інтелекту, оскільки хакери вже використовують ці технології для вчинення злочинів. Крім того, штучний інтелект допомагає організаціям швидко реагувати на загрози, компенсувати нестачу кадрів у сфері кібербезпеки, заздалегідь виявляти вразливості у системах та розробляти ефективні стратегії безпеки.

Список використаних джерел

1. *ШІ у кібербезпеці: Роль, застосування та переваги | Wezom*. (б. д.). IT-компания полного цикла разработки программных продуктов WEZOM - Киев, Украина. https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi

2. *European union agency for cybersecurity (ENISA): Threat landscape 2022 report is released - identity theft observatory system*. (б. д.). Identity Theft Observatory System. https://eithos.eu/european-union-agency-for-cybersecurity-enisa-threat-landscape-2022-report-is-released/

3. Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*. 40, 853–865. https://doi.org/10.1109/TSMCA.2010.2048028

4. Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

5. AbdulNabi, I., & Yaseen, Q. (2021). Spam email detection using deep learning techniques. *Procedia Computer Science*, 184, 853–858. https://doi.org/10.1016/j.procs.2021.03.107

МЕТОДИ ПІДВИЩЕННЯ ЦИФРОВОЇ ОБІЗНАНОСТІ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ: УСПІШНІ ВІТЧИЗНЯНІ ТА ЗАКОРДОННІ КЕЙСИ

METHODS OF INCREASING DIGITAL AWARENESS OF CONSUMERS OF FINANCIAL SERVICES: SUCCESSFUL DOMESTIC AND FOREIGN CASES

***Оголь Дмитро*, студент**
Сумський державний університет, Україна

Сьогодні в цифрову еру, період бурхливого розвитку технологій, впливу на економіку, політику, навчання та щоденне життя засобів масової інформації, Інтернету та технологій обізнаність та компетентність з цифровими засобами та можливостями є ключовими для сучасної людини. З цим пов'язано навчання особистості, її розвиток, вибудовування успішної життєвої траєкторії.

Вперше про цифрову компетентність у Європі заговорили у 2006 році, коли Європейський Союз запропонував вісім ключових сфер компетентності для неперервного навчання, однією з котрих є цифрова компетентність. Європейська система цифрової компетентності громадян, відома також як DigComp (Digital Competence), була розроблена Об'єднаним дослідницьким центром Європейської комісії у 2013 році, і стала орієнтиром для розвитку стратегічного планування ініціатив із цифрової компетентності як на загальноєвропейському рівні, так і на рівні держав-членів ЄС (Урядовий портал, 2019; Європейська Комісія, 2016).

Пандемія COVID-19, вимушений карантин, зміна форм навчання підтвердили важливість і необхідність пришвидшення цифровізації європейського суспільства, в якому цифрові технології пропонують нові шляхи для навчання, роботи, здійснення планів з особистого та професійного розвитку. Сьогодні ЄС окреслює свої пріоритети в освітній діяльності, спрямовуючи їх на: цифрову грамотність населення та підготовку висококваліфікованих фахівців з цифрових технологій, створення безпечних цифрових інфраструктур, цифрову трансформацію бізнесу, цифровізацію державного сектору.

Для того, щоб допомогти політикам окремих країн скласти на макрорівні уявлення про цифрову компетентність громадян, Європейська Комісія розробила Індекс цифрових навичок (DESI). Цей складений показник побудований на чотирьох сферах компетентності системи DigComp (інформація, комунікація, створення контенту та розв'язання проблем). У ньому використовуються дані Обстеження використання

інтернету в домогосподарствах і громадянами в Європейському Союзі (яке охоплює репрезентативну вибірку населення ЄС віком від 16 до 74 років), що проводиться Євростатом.

Щороку в європейських країнах проводиться тиждень цифрової грамотності з метою надихнути та навчити людей цифрових навичок. Кампанія проводиться у коворкінгах, громадських центрах, школах, університетах, бібліотеках та інших місцях по всій Європі. За 2010-2020 роки до Європейського тижня цифрової грамотності долучились більше 1 300 000 учасників. Міністерство цифрової трансформації України традиційно приєднується до заходів, які проводять європейські партнери.

21 січня 2020 року Кабінет міністрів України запустив Національну програму цифрової грамотності, яка мала стати кроком для подолання цифрової нерівності в державі. На момент запуску Програми результати соціологічних досліджень свідчили, що близько 53,5% українців знаходились нижче позначки середній рівень у питаннях цифрової грамотності, не володіли цифровими навичками 15,1% українців, а володіли низьким рівнем цифрових навичок 37,9% громадян. 34% українців у віці 18-70 років за останній рік ставали об'єктом хоча б одного з видів шахрайських дій в Інтернеті, а серед молоді у віці 10-17 років – 49,5% українців ставали жертвами онлайн шахрайства. Найбільш незахищеними сегментами в інтернеті була молодь до 16 років, та люди старше 60 років (Урядовий портал, 2019).

У 2020 році під егідою Міністерства цифрової трансформації України запрацювала національна онлайн-платформа з цифрової грамотності «Дія. Цифрова освіта», через яку кожен українець має безкоштовний доступ до цифрової освіти. Місією платформи є зробити так, щоби сучасні вміння та навички стали доступними для всіх в Україні.

Наразі платформа розвивається і на ній окрім освітніх серіалів також доступні численні тести, симулятори, гайди, вебінари та подкасти, які допомагають користувачам розібратися у світі сучасних технологій та проблем. Платформа має понад 250 освітніх продуктів, 2,1 млн. зареєстрованих користувачів, з час її існування видано 3,1 сертифікатів, до програм з розвитку цифрової грамотності залучено понад 6 млн. осіб (Національної онлайн-платформи з цифрової грамотності).

До розвитку платформи також долучаються різноманітні інституції, зокрема Національний банк бере участь в проектах розвитку цифрових фінансових навиків громадян. Так, у 2020 році спільно з Приватбанком на порталі «Дія. Цифрова освіта» було запущено серіал «Цифрові гроші», в якому простою мовою розповідається все про банківські платіжні картки, платежі онлайн, перекази коштів не виходячи з дому, кредитні ліміти,

накопичення коштів та як убезпечити себе від неприємних ситуацій (Національний банк України, 2020).

Платформа з 2019 року регулярно досліджує рівень цифрової грамотності громадян (за основу було взято методологію Європейської комісії для розрахунку Індексу цифрової економіки та суспільства (DESI)). Відповідно до прийнятої методології, рівень володіння цифровими навичками містить чотири сфери компетенцій: інформаційні навички (information skills); комунікаційні навички (communication skills); навички розв'язання життєвих проблем (problem solving skills); навички створення цифрового контенту (software skills for content manipulation).

Підвищення рівня цифрових навичок серед населення є важливим фактором для стабільного економічного розвитку держави, сприяючи інноваціям, продуктивності та конкурентоспроможності на світовій арені. Цьому можуть слугувати кілька причин:

- підвищення продуктивності праці;
- стимулювання інновацій;
- збільшення конкурентоспроможності країни;
- розвиток цифрових інфраструктур;
- підвищення рівня зайнятості.

За даними Інституту майбутнього цифровізація дасть можливість створювати щонайменше від 11% (у 2021р.) до 95% (2030р.) додаткового ВВП на рік, за 10 років додатково створити до $1 260 млрд ВВП та збільшити надходження в бюджет на $240 млрд, створити 700 тис. нових робочих місць (без урахування експортної ІТ-індустрії) [4].

Наразі варто позитивно оцінити кроки держави, спрямовані на подолання цифрової неграмотності українців, і приділення уваги до розвитку цифрових навичок населення: започаткована національна програма цифрової грамотності, відбувається розробка української рамки цифрових компетентностей громадян та педагогів та популяризація цифрових навичок серед населення.

Список використаних джерел

1. Національний банк України (2020). В Україні запустили освітній серіал "Цифрові гроші". URL: https://bank.gov.ua/ua/news/all/v-ukrayini-zapustili-osvitniy-serial-tsifrovi-groshi (дата звернення: 04.04.2024).

2. Урядовий портал (2019). Національна освітня платформа з цифрової грамотності «Дія: Цифрова освіта» стартує вже 21 січня URL: https://www.kmu.gov.ua/news/oleksij-goncharuk-nacionalna-osvitnya-platforma-z-cifrovoyi-gramotnosti-diya-cifrova-osvita-startuye-vzhe-21-sichnya (дата звернення: 03.04.2024).

3. Офіційна сторінка Національної онлайн-платформи з цифрової грамотності. URL: https://osvita.diia.gov.ua (дата звернення: 04.04.2024).

4. Український Інститут Майбутнього. Україна 2030Е – країна з розвинутою цифровою економікою URL: https://strategy.uifuture.org/kraina-zrozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-1 (дата звернення: 05.04.2024).

5. Європейська Комісія (2016). DigComp 2.0: Система цифрової компетентності громадян URL: http://surl.li/yraajx (дата звернення: 03.04.2024).

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ

ARTIFICIAL INTELLIGENCE AS A TOOL TO TACKLE CYBER THREATS

Анна Шаповалова, студентка
Сумський державний університет, Україна

В умовах стрімкого розвитку цифрових технологій кіберзагрози стають все більш складними, створюючи значні ризики для окремих осіб, компаній і країн. Згідно з даними Cybersecurity Ventures, до 2025 року щорічна шкода від кібератак досягне 10,5 трильйонів доларів, що становить збільшення на 300% з 2015 року (Esentire, 2024).

Традиційні методи кібербезпеки, які часто покладаються на втручання людини та заздалегідь визначені системи, засновані на правилах, не встигають за масштабами та складністю сучасних кібератак. У цьому контексті штучний інтелект стає трансформаційною силою в сфері кібербезпеки. Використовуючи передові алгоритми, машинне навчання та аналіз даних, штучний інтелект дає можливість виявляти, запобігати та реагувати на кіберзагрози з безпрецедентною швидкістю та точністю. За прогнозами експертів до 2027 року обсяг рішень з використанням штучного інтелекту для кібербезпеки досягне 46,3 мільярда доларів США (CEPS, 2021).

Автоматизуючи виявлення загроз, визначаючи аномалії та безперервно навчаючись на нових даних, інтелект підвищує ефективність заходів кібербезпеки, що робить його вирішальним компонентом у боротьбі з кіберзлочинністю. Під час опитування компанії Capgemini, 69% підприємств вважають, що без штучного інтелекту вони не зможуть відреагувати на кіберзагрози. Також, Gartner прогнозує, що до 2025 року 60% підприємств будуть використовувати ШІ для моніторингу загроз і виявлення аномалій у режимі реального часу. Це дозволить суттєво скоротити час виявлення загроз і підвищити ефективність реагування на інциденти.

Фахівці компанії IDC (2024) очікують, що витрати на кібербезпеку з використанням штучного інтелекту зростуть на 15-20% на рік до 2026 року, що підтверджує важливість цієї технології у забезпеченні захисту інформаційних систем

Підприємства, які використовують для кіберзахисту технології штучного інтелекту отримують низку переваг:

– автоматизований аналіз даних, на основі чого розробка прогностичних моделей для ідентифікації підозрілих операцій та активностей в

інформаційному середовищі. Це допомагає в плануванні, управлінні ризиками та розробці стратегій.;

– постійне та швидке адаптування до постійно мінливих кіберзагроз.

– виявлення складних закономірностей, тенденцій та зв'язків у даних, які люди можуть пропустити. Це дає цінні знання та про insights для прийняття ефективних управлінських рішень.

– розпізнавання та блокування шкідливого трафіку, а також адаптивна зміна налаштувань мережі. Інструменти штучного інтелекту дозволяють аналізувати дані про кіберзагрози та автоматично змінювати налаштування мережі для протидії новим загрозам. Це може включати зміну правил брандмауера, оновлення програмного забезпечення або блокування IP-адрес, пов'язаних з шкідливою активністю (European Business Association, 2024).

– автоматичне реагування на кібератаки, що включає блокування шкідливого трафіку, ізоляцію заражених систем або відновлення даних (BDO, 2024) .

Штучний інтелект відіграє центральну роль у сучасних стратегіях протидії кіберзагрозам. Завдяки своїм потужним можливостям автоматизації, ШІ здатний значно покращити процеси виявлення, прогнозування та реагування на кібернетичні атаки. Використовуючи алгоритми машинного навчання та аналіз великих даних, системи на основі ШІ можуть швидко ідентифікувати підозрілу активність та виявляти потенційні загрози в режимі реального часу, що значно перевищує можливості традиційних методів кібербезпеки.

Завдяки постійному розвитку технологій штучного інтелекту, ми можемо очікувати появи ще більш ефективних та надійних систем кібербезпеки в майбутньому. Такі системи будуть здатні не лише оперативно реагувати на загрози, але й проактивно запобігати їм, забезпечуючи тим самим більш високий рівень захисту для бізнесу та приватних користувачів. Штучний інтелект стає незамінним інструментом у боротьбі з кіберзлочинцями, і його роль у сфері кібербезпеки буде тільки зростати з часом.

Список використаних джерел

1. BDO (2024). Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks

2. Esentire (2024). Cybersecurity Ventures Report on Cybercrime. URL: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

3. European Business Association (2024). Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/

4. UNITE (2021). How to Use Cyber Threat Intelligence to Improve Your Cyber Security. URL: https://www.unite.ai/how-to-power-your-cyber-security-with-cyber-threat-intelligence/

5. CEPS (2021). Artificial Intelligence and cybersecurity. URL: https://www.ceps.eu/artificial-intelligence-and-cybersecurity/

6. IDC (2024). 20% of Industrial Operations in Asia to Use AI/ML for Vision-Based Systems and Robotic and Automation Processes by 2026. URL: https://www.idc.com/getdoc.jsp?containerId=prAP51741824

ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ЕФЕКТИВНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ

ARTIFICIAL INTELLIGENCE IN COMBATING CYBERCRIME: EFFECTIVE STRATEGIES AND TOOLS

Еліна Шрамко, студентка
Сумський державний університет, Україна

Науковий керівник:
Вікторія Боженко, к.е.н., доцентка
Сумський державний університет, Україна

У сучасному цифровому світі кібербезпека стає все більш важливою складовою захисту інформації та технологічних систем. З розвитком технологій кількість та складність кіберзлочинів стрімко зростає, ставлячи під загрозу як приватних користувачів, так і великі організації. Традиційні методи захисту стають недостатніми для боротьби з новітніми загрозами, що потребує впровадження передових технологій, таких як штучний інтелект (ШІ).

Актуальність теми обумовлена тим, що штучний інтелект здатний значно підвищити ефективність систем кібербезпеки завдяки своїй здатності до швидкого аналізу великих обсягів даних, виявлення аномалій у реальному часі та адаптації до нових загроз. Використання штучного інтелекту у боротьбі з кіберзлочинністю відкриває нові горизонти у захисті даних та інформаційних систем, дозволяючи створювати більш надійні та ефективні стратегії захисту.

Інтеграція штучного інтелекту у існуючі системи кібербезпеки є першим кроком до підвищення їх ефективності та їх адаптивності до нових загроз. Цей процес розпочинається з оцінки поточних систем для виявлення їхніх слабких місць. Після цього обираються відповідні інструменти ШІ, такі як Splunk, Darktrace, ELK Stack або Cisco Stealthwatch, залежно від потреб організації. Інструменти інтегруються з існуючими системами, налаштовується збір даних і встановлюються зв'язки між різними системами. Далі моделі штучного інтелекту тренуються на історичних даних, щоб навчитися виявляти загрози. Після впровадження системи постійно моніторяться і коригуються для забезпечення їхньої максимальної ефективності. Це дозволяє досягти точного виявлення загроз та швидкого реагування на інциденти, значно підвищуючи рівень кібербезпеки (Holovchak, Holovchak, & Skrypnyk, 2024).

Інтеграція штучного інтелекту в існуючі системи кібербезпеки приносить численні переваги. Вона значно підвищує точність виявлення загроз завдяки здатності штучного інтелекту аналізувати великі обсяги даних і виявляти аномалії, які можуть залишатися непоміченими традиційними методами. Крім того, автоматизація процесів за допомогою штучного інтелекту дозволяє миттєво реагувати на інциденти без затримок, пов'язаних з ручною обробкою. Ще однією перевагою є адаптивність до нових загроз: штучного інтелекту постійно навчається і оновлює свої моделі на основі нових даних, що дозволяє ефективно боротися з новими типами атак. Це робить системи кібербезпеки більш гнучкими і здатними швидко адаптуватися до змін у загрозах (Holovchak et al, 2024).

Втім, інтеграція штучного інтелекту у системи кібербезпеки також стикається з певними викликами. Процеси тренування та застосування моделей штучного інтелекту потребують значних обчислювальних потужностей, що може бути дороговартісним для організацій. Крім того, для ефективного навчання моделей необхідні великі обсяги високоякісних даних, що може бути складно забезпечити. Також інтеграція та підтримка систем ШІ вимагають наявності кваліфікованих фахівців у галузі даних і кібербезпеки, яких не завжди легко знайти. Таким чином, незважаючи на свої численні переваги, інтеграція штучного інтелекту потребує значних ресурсів і добре продуманих підходів для подолання (Holovchak et al, 2024).

Таблиця 1. Опис популярних інструментів з ШІ для інтеграції в системи кібербезпеки (Holovchak et al, 2024).

Інструмент	Особливості	Підтримка ШІ	Типи даних
Splunk	Потужна платформа для збору, аналізу та візуалізації даних	Так	Логи, мережеві дані
Darktrace	Виявлення загроз на основі поведінкових моделей	Так	Мережевий трафік
ELK Stack	Набір інструментів для збору, обробки та візуалізації логів	Так	Логи
Cisco Stealthwatch	Використання аналітики великих даних для виявлення загроз	Так	Мережевий трафік

Автоматизація процесів безпеки є одним із ключових аспектів інтеграції ШІ в системи кібербезпеки. Використання автоматизованих інструментів і технологій на основі ШІ дозволяє значно підвищити ефективність

реагування на загрози та забезпечити проактивний підхід до захисту інформаційних систем (Holovchak et al, 2024).

Основні аспекти автоматизації процесів безпеки:

1. Автоматизація дозволяє здійснювати моніторинг мережевого трафіку та логів у реальному часі. Інструменти на основі ШІ можуть аналізувати великі обсяги даних та виявляти аномалії миттєво, що дозволяє швидко реагувати на потенційні загрози. Це значно зменшує час від виявлення до реагування, мінімізуючи можливі збитки.

2. Завдяки автоматизації, системи безпеки можуть автоматично вживати заходів для усунення загроз. Це включає ізоляцію скомпрометованих систем, блокування підозрілих IP-адрес, застосування патчів та оновлень, а також інформування відповідних фахівців про інциденти. Такі дії можуть бути виконані без втручання людини, що знижує навантаження на IT-персонал.

3. Системи на основі ШІ можуть використовувати прогностичні моделі для виявлення потенційних загроз до їх виникнення. Це дозволяє організаціям бути на крок попереду зловмисників, впроваджуючи заходи безпеки заздалегідь.

4. Однією з проблем традиційних систем безпеки є велика кількість хибнопозитивних спрацювань, що може призводити до зайвих витрат часу та ресурсів. Автоматизація з використанням ШІ дозволяє значно знизити цей показник завдяки точнішому аналізу даних та більш ефективному виявленню реальних загроз (Holovchak et al, 2024).

Прогнозування загроз за допомогою штучного інтелекту є важливою стратегією у сфері кібербезпеки, яка дозволяє організаціям проактивно вживати заходів для захисту своїх інформаційних систем. штучного інтелекту аналізує великі обсяги історичних даних про кіберзагрози, включаючи інформацію про попередні атаки, методи зловмисників та їх поведінкові патерни. Це дозволяє виявляти закономірності та тренди, які можуть вказувати на ймовірність майбутніх атак (Kaur, Gabrijelčič, & Klobučar, 2023).

Основні інструменти для прогнозування загроз використовують алгоритми машинного та глибокого навчання, які навчаються на великій кількості даних, щоб виявляти складні патерни та аномалії. Прогностичні моделі інтегруються з існуючими системами кібербезпеки для постійного моніторингу та аналізу нових даних. На основі прогнозів, системи безпеки можуть автоматично вживати заходів для запобігання атакам, включаючи зміну конфігурацій, оновлення програмного забезпечення, блокування підозрілих IP-адрес або обмеження доступу до критичних ресурсів. Прогнозування загроз дозволяє знизити ризик успішних атак та економити ресурси, зменшуючи кількість інцидентів, які потребують реагування, що

допомагає мінімізувати втрати від кіберзлочинів (Kaur, Gabrijelčič, & Klobučar, 2023).

Виявлення аномалій є одним з найважливіших завдань у сфері кібербезпеки. Штучний інтелект пропонує нові можливості для аналізу великих обсягів даних та ідентифікації нетипової поведінки, що може свідчити про наявність загрози. Розглянемо основні методи та інструменти, що використовуються для виявлення аномалій:

1. Статистичні методи – методи, що базуються на аналізі розподілу даних і виявляють аномалії, порівнюючи поточні дані з попередньо визначеними статистичними моделями. Вони ефективні для виявлення відомих типів аномалій, але можуть бути менш ефективними для нових чи складних загроз.
2. Алгоритми машинного навчання (ML) використовують історичні дані для тренування моделей, здатних виявляти аномалії у нових даних. Найпоширенішими є методи класифікації, кластеризації та нейронні мережі. Вони забезпечують високу точність, але потребують значних обчислювальних ресурсів та попередньої обробки даних.
3. Методи на основі правил – методи, що базуються на встановленні правил або порогових значень, які визначають, чи є подія аномальною. Вони прості у реалізації, але менш гнучкі у порівнянні з іншими методами (Karpyuk & Vengersky, 2021).

Процес виявлення аномалій за допомогою штучного інтелекту починається зі збору великих обсягів даних, таких як мережевий трафік і логи системних подій, які потім очищуються, заповнюються відсутні значення та нормалізуються. Далі, на основі історичних даних, тренуються моделі, зокрема нейронні мережі та методи кластеризації, для вивчення нормальної поведінки системи і виявлення аномалій. Застосовані до нових даних моделі ідентифікують нетипову поведінку та маркують підозрілі події. Останнім етапом є детальний аналіз виявлених аномалій експертами для визначення рівня загрози та вжиття відповідних заходів, таких як ізоляція скомпрометованих систем або блокування доступу (Karpyuk & Vengersky, 2021).

Практичні кейси використання ШІ демонструють його значні переваги та потенціал. Наприклад, компанія Google активно застосовує алгоритми машинного навчання для виявлення та блокування фішингових електронних листів. Це дозволяє ефективно фільтрувати понад 99.9% шкідливих повідомлень, знижуючи ризик компрометації користувачів. Важливість такого підходу підкреслюється в дослідженні, де показано, що машинне навчання є ефективним інструментом для виявлення фішингових атак (Rashid et al., 2020).

Інший приклад – використання прогностичної аналітики для запобігання кібератакам. IBM Watson for Cyber Security аналізує величезні обсяги даних і прогнозує потенційні загрози до їхнього виникнення. Використовуючи природну мову та глибоке навчання, Watson виявляє аномалії та аналізує поведінкові патерни зловмисників. Це дослідження підтверджує, що прогностична аналітика може бути ефективним інструментом для забезпечення кібербезпеки (Freeman & Chio, 2018).

Отже, застосування штучного інтелекту у кібербезпеці значно підвищує ефективність захисту інформаційних систем. ШІ дозволяє швидко аналізувати великі обсяги даних, виявляти аномалії у реальному часі та адаптуватися до нових загроз. Інтеграція штучного інтелекту у існуючі системи кібербезпеки, таких як Splunk, Darktrace, ELK Stack і Cisco Stealthwatch, забезпечує більш надійний та ефективний захист.

Список використаних джерел

1. Holovchak, Y. V., Holovchak, H. V., & Skrypnyk, S. V. (2024). Integration of smart technologies and artificial intelligence in accounting: Key aspects of the digital revolution. Journal "Investments: Practice and Experience", (6), 38-44. https://doi.org/10.32702/2306-6814.2024.6.38

2. Karpyuk, P., & Vengersky, P. (2021). Using machine learning to detect anomalies in cybersecurity to reduce false positives in the daily work of the cyber threat response center. Application Mathematics and Informatics. https://doi.org/10.30970/vam.2021.29.11339

3. Freeman, D., & Chio, C. (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media.

4. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 101804. https://doi.org/10.1016/j.inffus.2023.101804

5. Rashid, J., et al. (2020). Phishing detection using machine learning technique. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, 3-5 November 2020. https://doi.org/10.1109/smart-tech49988.2020.00026

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY

Єлизавета Литюга, студентка
Сумський державний університет, Україна

Поява напряму боротьби з кібератаками виникла через загрози, пов'язані з розвитком Інтернету, а також зростаючого обсягу даних у мережі. Вважається, що дав поштовх до розвитку інцидент 2017 року: під час атаки програми-вимагача WannaCry постраждало понад 200 000 комп'ютерів зі 150 країн. Останніми роками кількість подібних програм і ступінь завданих ними збитків стрімко зростає. У зв'язку з цим комерційні та базові інфраструктури стикаються з підвищеними ризиками витоку даних із супутніми фінансовими втратами.

Зі зростанням кіберзагроз і загроз безпеці в цифровому середовищі важливість ролі штучного інтелекту в кібербезпеці стає дедалі очевиднішою. Автоматичне виявлення інцидентів, аналіз великих обсягів даних, прогнозування потенційних вразливостей - все це є сферою застосування штучного інтелекту в кібербезпеці. Це дає змогу ідентифікувати та відбивати атаки швидше, ніж це можливо для людини. Розглянемо кілька аспектів успішного застосування адаптивних моделей у сфері кібербезпеки:

– адаптивні моделі дозволяють створювати персоналізовані стратегії безпеки. Вони здатні враховувати

– особливості кожної організації, аналізувати її інфраструктуру та історичні дані щодо атак для створення найбільш ефективних заходів безпеки.

– штучний інтелект не тільки зменшує кількість успішних кібератак, а й істотно полегшує робоче навантаження на фахівців у галузі кібербезпеки, звільняючи їхні ресурси для зосередження на інших ключових завданнях.

– штучний інтелект може бути використаний для розробки сильних систем протидії фішингу та шкідливому програмному забезпеченню.

– штучний інтелект може використовуватися для розробки системи моніторингу, яка аналізує активність у мережі та ідентифікує будь-які підозрілі дії.

З появою нових методів атак або зміною поведінки шкідливих програм адаптивні моделі швидко реорганізують свої алгоритми для виявлення цих нових загроз.

Моделі на основі штучного інтелекту мають здатність до контекстного аналізу. Це охоплює аналіз поведінки користувачів, тенденції загроз у

конкретній галузі та особливості системи безпеки організації. Ще однією важливою перевагою адаптивних моделей є те, що вони можуть аналізувати великі обсяги інформації, виділяючи з неї ключові особливості, пов'язані з потенційними загрозами.

Підвищення ефективності алгоритмів штучного інтелекту в кібербезпеці не залишається непоміченим зловмисниками. Разом зі збільшенням кількості відомих вразливостей і дефектів безпеки систем, що реєструються в бібліотеці CVE (Common Vulnerabilities and Exposures), спостерігається зростання застосування технологій штучного інтелекту для створення більш складних кібератак.

Загальна кількість вразливостей, зафіксованих у базі CVE за 2023 рік, досягла 28,961 випадків. Така цифра є рекордною і свідчить про те, що потенціал для розроблення та проведення кібератак, зокрема, заснованих на штучного інтелекту, продовжує розширюватися (CVE (Common Vulnerabilities and Exposures), Metrics, 2024).

Таблиця 1. Статистика вразливостей зафіксованих в бібліотеці CVE (Common Vulnerabilities and Exposures) на період з 2014 по 2023 рік.

Кількість вразливостей	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Загалом	228,96	225,05	220,16	118,37	117,30	116,51	114,64	66,45	66,49	77,94

Джерело: CVE (Common Vulnerabilities and Exposures), Metrics, 2024

Атаки за допомогою систем штучного інтелекту здебільшого пов'язані з плутаниною в базовій моделі машинного навчання і зломом захисту. Наприклад, генеративні змагальні мережі (різновид штучних нейронних мереж) можуть обдурити систему розпізнавання обличь. До того ж такі мережі використовують для атаки на мовні додатки та голосові біометричні системи. Варто також зазначити, що, обдуривши систему штучного інтелекту, шкідливий файл може бути помилково класифікований як безпечний. Тож, можливість атаки на алгоритми штучного інтелекту та спотворення даних може спричинити серйозні наслідки. Такі ризики вимагають розроблення додаткових методів захисту та забезпечення надійності самого штучного інтелекту.

Незважаючи на значні переваги адаптивних моделей, вони також пов'язані з низкою обмежень і викликів, які необхідно враховувати під час їх застосування. Одним з основних викликів є брак якісних даних для навчання. Для ефективної роботи адаптивних моделей потрібен великий обсяг різноманітних даних про кібератаки і загрози. Однак, часто такі дані виявляються обмеженими через конфіденційність або складність їхнього збору.

Наразі кілька інструментів ШІ використовують для розширення можливостей і автоматизації процесу виявлення та запобігання загрозам. Двома найбільш вражаючими з них є Microsoft Security Copilot і платформа Complete Cloud Email Security компанії Tessian. Крім цих двох, іншими інструментами штучного інтелекту для виявлення і запобігання атакам є Cylance, Cybereason і McAfee MVISION. У майбутньому дедалі більше компаній будуть вкладати ресурси в сполучення ШІ з наявними інструментами виявлення і запобігання.

Наразі Microsoft Security Copilot є лідером у галузі з використання штучного інтелекту для автоматичного реагування на інциденти. Однак дедалі більшої популярності набирає інструмент Darktrace. Цей інструмент кібербезпеки побудований на основі безперервного циклу зворотного зв'язку, керованого штучного інтелекту, який приймає вхідні дані ШІ і видає результати ШІ для захисту корпоративних даних від складних кібератак. Антивіруси та засоби виявлення шкідливого ПЗ, як-от Malwarebytes і Kaspersky's Endpoint Security, використовують штучного інтелекту та машинне навчання для точної ідентифікації шкідливих програм, визначення їхньої поведінки та автономного навчання новим методам обходу. Водночас такі плагіни, як BinNet AI, інтегрують ШІ з наявними платформами реверс-інжинірингу, щоб аналітики могли глибше зрозуміти двійковий машинний код із семантичної та синтаксичної точок зору.

Найпопулярніший інструмент штучного інтелекту для вивчення кібербезпеки - ChatGPT від OpenAI. Цей генеративний чат-бот зі штучним інтелектом приймає запитання користувачів, обробляє їх і дає докладні відповіді, використовуючи найсвіжішу інформацію. Він дає змогу вести бесіду в людському стилі та дізнаватися про будь-яку тему кібербезпеки. Можна використовувати власні чат-боти, звані Security GPTs (Generative Pre-Trained Transformers), щоб сфокусувати навчання на конкретних темах.

Нещодавнє опитування головних фахівців CISO з інформаційної безпеки показало такі результати, щодо впровадження ШІ в сферу інформаційної безпеки (Splunk, The CISO Report, Consulted: March, 2024):

– 70 % респондентів вважають, що штучний інтелект дає більше переваг зловмисникам, аніж захисникам, проте 35 % уже експериментують із ним з метою кіберзахисту.

– 83 % респондентів заплатили зловмисникам після атаки ransomware, чи то безпосередньо, чи то через кіберстрахування, чи то за допомогою парламентера.

– 35 % респондентів CISO вже використовують штучний інтелект для забезпечення безпеки.

– 61 % респондентів, ймовірно, будуть використовувати його в найближчі 12 місяців.

– 86 % респондентів вважають, що генеративний штучний інтелект усуне прогалини в навичках безпеки і брак кадрів.

– 96 % респондентів стали жертвами атаки вимагачів за останній рік. Більше половини респондентів заплатили понад 100 000 доларів як викуп.

Отже, взаємодія між штучного інтелекту та людьми стає ключовим фактором для забезпечення кібербезпеки в нашому цифровому суспільстві. Роль штучного інтелекту в кібербезпеці невід'ємна в сучасному цифровому суспільстві. Цей інноваційний засіб дає змогу посилювати захист від кіберзагроз, але також ставить нові виклики, які потребують уваги до аспектів безпеки та етики.

Загалом, адаптивні моделі на основі штучного інтелекту є надійним і ефективним інструментом у боротьбі з сучасними кіберзагрозами. З їхньою допомогою організації можуть підвищити свою кібербезпеку і захистити критично важливі дані від можливих атак.

Список використаних джерел

1. CVE (Common Vulnerabilities and Exposures), Metrics, 2024. URL: https://www.cve.org/About/Metrics

2. Splunk, The CISO Report, Consulted: March, 2024. URL: https://www.splunk.com/en_us/campaigns/ciso-report.html