МАКАРЧУК І. М., ВАСИЛЬЄВ М. К., БІДЕНКО В. І.,
Університет Григорія Сковороди в Переяславі

КІБЕРРИЗИКИ В ЕПОХУ ФІНАНСОВОЇ ДИДЖИТАЛІЗАЦІЇ

Цифрова трансформація фінансового сектору в Україні є ключовим вектором розвитку у післякризовий період. Проте стрімка діджиталізація супроводжується суттєвим зростанням кібер-ризиків. Фінансові установи стають головною ціллю для кіберзлочинців через високий рівень ліквідності, велику кількість персональних даних та вразливість до технологічних атак. У 2023–2024 роках кількість кібер-атак на банки, платіжні сервіси та криптовалютні платформи суттєво зросла, що потребує перегляду традиційних моделей захисту. Кіберризики поділяються на кілька ключових категорій: Фінансові атаки (фішинг, злам акаунтів, маніпуляції з транзакціями) – націлені на пряме викрадення коштів.

Ризики порушення конфіденційності – витоки персональних та платіжних даних клієнтів. DDoS-атаки – блокування доступу до онлайн-сервісів банків та платіжних платформ. Використання шкідливого ПЗ – проникнення у внутрішні системи установ з метою шпигунства або саботажу.

Соціальна інженерія – атаки, що використовують людський фактор, особливо актуальні в умовах дистанційної роботи. Особливої уваги вимагають нові вектори загроз, пов’язані з впровадженням штучного інтелекту, блокчейну та цифрових валют центрального банку (CBDC).

Починаючи з 2022 року, кіберінфраструктура зазнає посилених атак з боку державних та приватних хакерських угрупувань. Банківські системи, сайти держструктур та криптовалютні біржі стали мішенню масових атак. Це спричинило необхідність у посиленні кібероборони, розбудові національного кіберщита, координації з міжнародними партнерами (зокрема ЄС та США) та посиленій підготовці кадрів.Сучасні підходи до управління кібер-ризиками

Технологічні рішення:Мультифакторна автентифікація та ендпоінт-захист;

Системи моніторингу подій безпеки (SIEM); Використання штучного інтелекту та машинного навчання для виявлення аномалій; Хмарні технології з вбудованими протоколами безпеки. Організаційні заходи: Створення відділів з кібербезпеки в установах; Регулярні аудити інформаційної безпеки;

Проведення тренінгів для працівників з протидії фішингу та соціальній інженерії. Регуляторні ініціативи: Закон України «Про основні засади забезпечення кібербезпеки»; Рекомендації НБУ щодо системного управління ІТ-ризиками; Міжнародні стандарти (ISO/IEC 27001, NIST CSF).

Фінансова діджиталізація в Україні відкриває значні можливості для розвитку, але супроводжується зростанням кібер-ризиків. Ефективне управління цими ризиками вимагає поєднання інноваційних технологій, належного регулювання та високого рівня цифрової грамотності. Для зміцнення стійкості фінансового сектору рекомендовано: Впроваджувати комплексні системи управління кібербезпекою. Йдеться про побудову багаторівневої системи захисту, яка включає як технічні (захист мережі, шифрування, виявлення вторгнень), так і організаційні компоненти (інструкції, регламенти, відповідальність персоналу). Особливу увагу варто приділити автоматизованому моніторингу загроз, впровадженню систем реагування на інциденти (CSIRT) та резервному копіюванню даних у захищених середовищах. Такі системи мають враховувати сучасні технології, зокрема хмарну інфраструктуру, блокчейн і нейромережі.

Забезпечити безперервне оновлення політик інформаційної безпеки. У світі, де кіберзагрози постійно еволюціонують, фінансові установи повинні регулярно переглядати та оновлювати внутрішні політики безпеки. Це включає адаптацію до нових нормативних вимог, запровадження нових стандартів (ISO/IEC 27001:2022), врахування змін у бізнес-процесах, а також оновлення вимог до підрядників і партнерів. Важливо проводити щорічні аудити безпеки, тестування на проникнення та аналіз ризиків за сучасними методиками (наприклад, методи OCTAVE, FAIR).Розвивати партнерство з міжнародними організаціями та технологічними лідерами у сфері кіберзахисту. Обмін досвідом, участь у спільних ініціативах, долучення до міжнародних платформ типу Global Forum on Cyber Expertise (GFCE) або FIRST, дозволяє українським установам вчасно реагувати на глобальні загрози та отримувати доступ до передових рішень у сфері безпеки. Також варто співпрацювати з компаніями-лідерами в галузі інформаційної безпеки (Microsoft, Cisco, Palo Alto Networks, Mandiant тощо), які можуть надати як технологічну, так і консультаційну підтримку. Участь в європейських грантових програмах з кібербезпеки, таких як *EU4Digital*, також є перспективним напрямом.

Список використаних джерел

1. Aldasoro I. Cyber risk in the financial sector [Електронний ресурс] / I. Aldasoro, J. Frost, L. Gambacorta. The European Money and Finance Forum, 2020. URI: https:www.suerf.org/policynotes/18421/cyber-risk-in-the-financial-sector
2. Dingel J. How many jobs can be done at home? / J. Dingel, B. Neiman. Journal of Public Economics, 2020. №189.
3. Communiqué: G20 Finance Ministers and Central Bank Governors Meeting [Електронний ресурс]. G20 Information Centre. 2020. URI: http:.www.g20.utoronto.ca/2020/2020-g20-finance-1014.html.

ГУМИНСЬКА М. В.,
Державний торговельно-економічний університет

СТРАХОВИЙ РИНОК УКРАЇНИ В УМОВАХ ВОЄННОЇ ЕКОНОМІКИ

Підвищений ризик для бізнесу та особистого майна в умовах війни створює підвищений попит на страхові послуги. З іншого боку, вплив війни на страховий ринок та зміни в правовому середовищі, що відбулися за останні три роки вимагають від страхових компаній швидких адаптацій. Однак, ці виклики, на наш погляд, одночасно відкривають і нові можливості для розвитку страхового ринку. Дослідження вітчизняного страхового ринку за 2020–2024 рр. вказують на переважно несприятливі зміни, особливо у порівнянні з довоєнними показниками. Зокрема, кількість страхових компаній поступово зменшувалася (абсолютне відхилення в 2023 р. порівняно з 2020 р. становить 109). Спостерігалася також нестабільність у динаміці страхових виплат і премій, але у 2023 р. ситуація почала покращуватися в порівнянні з 2022 р. Зазначена тенденція зберіглась і в 2024 р., – страховий ринок України показав зростання усіх ключових показників – активів, страхових премій та виплат страховиків. Так, валові страхові премії зросли на 12,3% з 34,2 млрд грн до 38,4 млрд грн, рівень виплат склав 41%. Валові премії ризикового страхування за 2024 р. зросли з 30,6 млрд грн до 34,3 млрд грн, збільшення виплат тривало з початку 2023 р. через інфляцію та девальвацію національної валюти, рівень