УДК 004.056

КІБЕРЗАХИСТ БАНКІВСЬКОЇ СИСТЕМИ В УКРАЇНІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Чукалов Кирило Едуардович
Жмуровська Катерина Романівна
Товстик Вадим Олександрович
курсанти факультету № 4
Харківського національного університету внутрішніх справ
Заводний Олександр Олександрович
студент факультету № 6
Харківського національного університету внутрішніх справ
Онищенко Юрій Миколайович
заступник декана з навчально-методичної роботи факультету № 4
Харківського національного університету внутрішніх справ
кандидат наук з державного управління, доцент

Питання забезпечення кіберзахисту світової економічної системи з кожним роком набуває актуальності, адже кібератаки на суб’єктів даного сектору стають більш частішими та вишуканішими, бо зачіпають як приватних осіб, окремих представників бізнесу, державні установи, так і всесвітнє бізнес-співтовариство. Найбільш уразливими перед такими атаками є фінансові установи та інфраструктура фінансового ринку, характер зломів яких змінюється практично щоденно. Поширення криптовалют також збільшило ймовірність виникнення інцидентів у фінансовому секторі. Інформаційні технології вже давно є основою фінансової системи, а пов'язані з нею загрози знаходяться під постійним щоденним контролем банків та уповноважених національних підрозділів.

Тенденція до зростання кіберзлочинності зробила кібербезпеку важливою темою державної політики для регулюючих та наглядових органів. Фінансові установи, особливо банки, стають все більш привабливими цілями для кіберзлочинців, оскільки фінансовий сектор привертає великих інвесторів з галузі інформаційних технологій та виділяє значні фінансові ресурси на різноманітні проєкти. Саме цифрова трансформація в банківській сфері

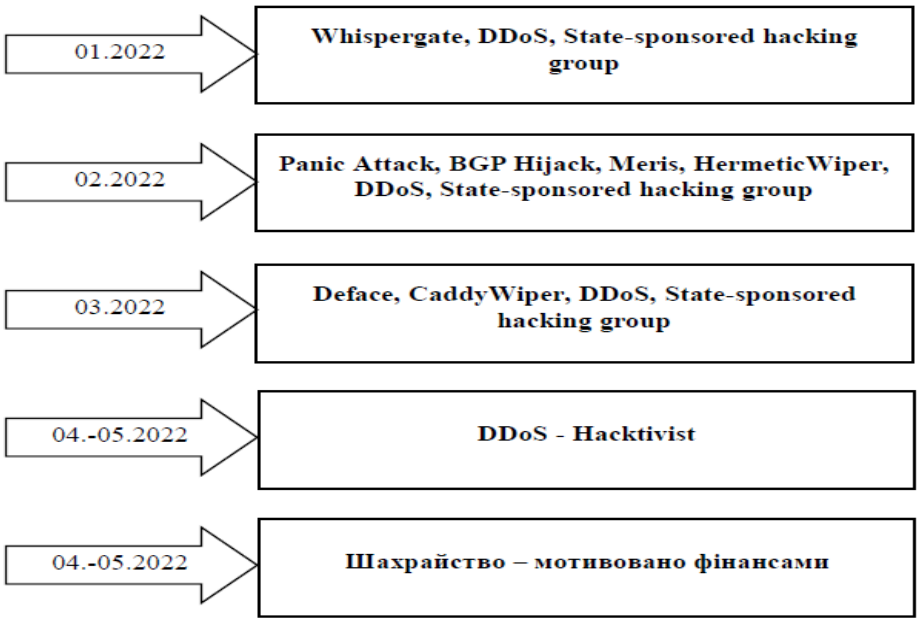
забезпечує розширення можливостей ведення банківської справи, збереження клієнтської бази, покращення позицій на міжнародному фінансовому ринку, зменшення витрат ведення бізнесу, підвищення конкурентоспроможності тощо.

Все це повинно реалізовуватися під щільним контролем виявлення можливих внутрішніх і зовнішніх загроз суб'єктивного та об'єктивного характерів, на тлі яких кіберінциденти стають найнебезпечнішими. Тому дослідження інструментів кіберзахисту фінансової системи, яка працює за допомогою банківської сфери, потребує виваженого та детального вивчення з метою розроблення ефективного механізму кіберзахисту банківської системи [1].

У контексті широкомасштабного вторгнення рф в Україну цифрові (кібер) напади стали неодмінною частиною конфлікту, спрямованими на державні та ключові корпоративні ресурси. Одночасно кіберзлочинці, зокрема рф – держава-терорист, вдосконалюють свої методи для проведення кібернетичних атак. Таким чином, для регуляторів стає важливим завданням збереження системності у протидії кібератакам, а для банківського сектору - активне інвестування у кібербезпеку. На жаль, умови війни змушують банківську систему зосередитися в основному на напрямку забезпечення кіберзахисту, інвестуючи кошти у вдосконалення засобів захисту даних та рахунків своїх клієнтів, а також подолання наслідків проведених кібератак, значно призупинивши розвиток та впровадження інноваційних послуг та інші напрямки роботи довоєнного періоду.

За інформацією НБУ у 2022 році майже усі кібератаки на банківський сектор здійснювались хакерськими угрупованнями, за якими стояла влада країни-агресора (групи хакерів Armageddon, Fancy Bears тощо) [1]. Наразі усі кібернапади рф звелись до двох напрямків: DDoS-атаки різного характеру, від яких страждає вся банківська система України, та фішингові атаки різних типів (різні види шахрайства). Майже усі фішингові атаки, які спрямовані на банківську систему, є виманюванням коштів у клієнтів банків за різними схемами надання допомоги [2]. Шахраї використовують соціальну інженерію,

найпростіші методи створення фейкових мобільних додатків та сторінок банків, де застосовується айдентика справжніх банків.



Хронологія атак на НБУ та банківську систему України у 2022 році [1]

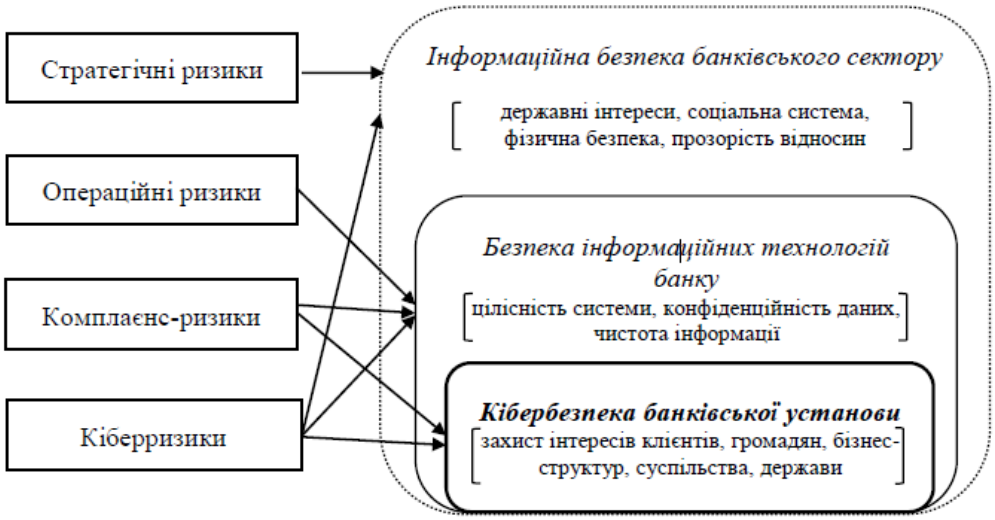
Ключовими тенденціями в цифровізації банківського сектору в Україні на сьогодні є наступні: оптимізація віддаленої праці банківських працівників, збільшення обсягів онлайн-операцій, спрощення доступу до банківських послуг, розширення каналів дистанційного продажу, боротьба з шахраями та хакерами, широке використання технологій штучного інтелекту, перехід до управління на основі даних, реалізація програм тотальної персоніфікації, розвиток екосистем, створення власного програмного забезпечення та нівелювання потреби в IT-фахівцях. Важливим аспектом є акцент на вдосконаленні та розвитку систем захисту, щоб протистояти зростаючим загрозам з боку шахраїв та кіберзлочинців. Разом із тим, банки відзначають важливість надання інноваційних послуг та постійне вдосконалення технологічних рішень для забезпечення високого рівня задоволення клієнтів [2].

Інформаційна безпека банківського сектору – це безпека будь-якої інформації, включаючи паперові документи, голосову інформацію, забезпечення банківської таємниці, цензура, фізична безпека, безперервність роботи банківської установи, протидія соціальній інженерії, компрометації

платіжних інструментів тощо. Найбільшою загрозою для кібербезпеки є людська помилка, так званий «людський фактор». Саме представники персоналу фінансових та комерційних установ зрештою піддають ризику дані та інформаційні системи через те, що їх обманом змусили надати конфіденційну інформацію у руки зловмисників. Відсутність належного захисту паролів, використання «слабких» облікових даних, перехід на підозрілі посилання або відкриття файлів у листах електронної пошти, що містять шкідливе програмне забезпечення – все це становить 85 % усіх порушень кібербезпеки, що є наслідком людської помилки; 94% всіх заражених файлів та програм передаються через електронну пошту [3].

Забезпечення інформаційної безпеки у банківських установах передбачає ефективне керування захистом банківських процесів, включаючи застосування кіберстрахування, дотримання відповідності нормативним вимогам щодо безпеки, гарантування надійності та забезпечення безперервності функціонування банку, виявлення потенційних кіберзагроз. Все це ставить високі вимоги до кваліфікації менеджерів, фінансистів, економістів, аналітиків, маркетологів та юристів, які використовують економіко-математичні методи. Банки повинні детально моніторити потенційні загрози та ризики, чітко розрізняючи об'єкти кібератак. Розглядаючи типові атаки на банківський сектор, можна виділити наступні: порушення конфіденційності та банківської таємниці; атаки на банківську інфраструктуру; небезпека для коштів клієнтів та банку; вплив на вебсайти банків і регуляторів [4].

Банківська система під впливом ризиків цифровізації в першу чергу залежить від кібернетичних ризиків, які здійснюють безпосередній вплив на всю інформаційну систему держави і відтак на її безпеку. Існує багато стандартів, норм і положень, пов’язаних з інформаційною безпекою та кібербезпекою фінансового сектору, зокрема, банківського, які час від часу змінюються. Одним з базових стандартів є ISO/IEC 27001 (ISO/IEC 27001 standard) «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» [5].



Кібербезпека в системі інформаційної безпеки банківського сектору [2]

Система управління кібербезпекою (CSMS), запропонована стандартом IEC 62443 (ISA/IEC 62443 standard), складається з шести основних компонентів: реалізація програми CSMS (з метою надання інформації, необхідної для отримання підтримки керівництва); оцінка високорівневих ризиків (виявлення та визначення пріоритетів загроз); докладна оцінка ризиків (детальний аналіз технічних вразливостей); встановлення правил безпеки, організації та інформування; вибір та реалізація контрзаходів (з метою зменшення ризику для організації); підтримка CSMS (з метою забезпечення ефективності та досягнення цілей організації).

У контексті кібербезпеки важливо враховувати, що стандарт IEC 62443 визначає уніфіковані принципи та вимоги для забезпечення безпеки систем автоматизації та керування; основні етапи впровадження систем управління кібербезпекою, сприяючи створенню ефективних стратегій захисту від кіберзагроз і забезпеченню сталої безпеки організаційних процесів [6].

Отже, ключовим кроком у керуванні кібернетичними ризиками в банківській сфері є розробка та оновлення згідно вимог часу чіткої нормативно-правової бази, на основі якої учасники електронно-дистанційних мереж матимуть формалізовані вимоги до організації захисту інформації. Підбір надійних інвесторів для фінансування заходів, спрямованих на забезпечення ефективного кіберзахисту, використання кіберстрахування,

підготовка кваліфікованого персоналу з кібербезпеки, своєчасне оновлення програмного забезпечення та розвиток міжнародного співробітництва є не менш важливими аспектами кібербезпеки банківського сектору.

Забезпечення кібербезпеки в банківському секторі включає заходи, які здійснюються банками на базі передових цифрових технологій, гарантуючи інформаційну безпеку не лише самого банку, а й всієї країни та міжбанківської мережі загалом. У цьому контексті важливим елементом на кожному етапі захисту від кібернетичних атак є ефективне управління стратегічними, операційними, комплаєнс-ризиками та кіберризиками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифрові технології у банках в умовах війни: кейс IBOX BANK та міжнародний досвід URL: https://ua.news/ua/money/tsyfrovye-tehnologyy-v-bankah-v-uslovyyah-vojny-kejs-ibox-bank-y-mezhdunarodnyj-opyt (дата звернення 01.04.2024).

2. Абрамова А.С. Система ризиків діяльності комерційних банків в умовах цифровізації. Проблеми і перспективи економіки та управління. 2021. № 4(28). С. 186-193 (дата звернення 01.04.2024).

3. Трофіменко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Т. 21, № 3. С. 150-157 (дата звернення 01.04.2024).

4. Forcadell F.J., Aracil E., & Úbeda, F. The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. Global Policy. 2020. № 11 (S1). P. 18-27. URL: https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12761 (дата звернення 01.04.2024).

5. ISO/IEC 27001 and related standards Information security management. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення 11.03.2024).

6. International Society of Automation. ISA/IEC 62443 standard. URL: https://www.isa.org/standards-and-publications/isa-standards/search (дата звернення 01.04.2024).