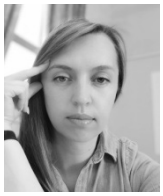
DOI: https://doi.org/10.37634/efp.2023.10.10
УДК 336:330.46:004.056



Ірина Миронівна ***ДОРОШ***
доктор філософії з публічного управління та адміністрування, доцент кафедри, Національний університет "Львівська політехніка"
ORCID: https://orcid.org/0000-0003-1394-5639
e-mail: iryna.m.dorosh@lpnu.ua

КІБЕРБЕЗПЕКА ТА ЇЇ РОЛЬ У ФІНАНСОВОМУ СЕКТОРІ: ЗАГРОЗИ ТА ЗАХОДИ ЗАХИСТУ

У статті розглянуто критичну роль кібербезпеки у фінансовому секторі та виклики, з якими стикаються фінансові установи у сучасному цифровому світі. Досліджено понятійний апарат кібербезпеки як важливого складника національної безпеки держави, а також найбільш поширені кіберзагрози та атаки у фінансовому секторі. Запропоновані у наукових джерелах визначення поняття "кібербезпека" деталізовано основними етапами її забезпечення у фінансових інституціях. Акцентовано увагу на необхідності формування підходу до кібербезпеки як до елемента ризик-менеджменту, що допоможе фінансовим установам зменшити кількість загроз та втрат і зберегти стійкість своєї діяльності в умовах кібервійни. У статті також розглянуто основні заходи захисту, які фінансові установи повинні вживати для забезпечення своєї кібербезпеки. Проаналізовано роль технологій, проактивного моніторингу, створення культури кібербезпеки та інших факторів у забезпеченні безпеки та стійкості фінансових систем.

Ключові слова: *фінансовий сектор, кіберзагрози, культура кібербезпеки, стратегія держави, відповідальність бізнесу*

ВСТУП

Фінансовий сектор – це система фінансових інститутів посередницького характеру, котра виступає з'єднувальною ланкою фінансового забезпечення між фінансовим ринком та реальним сектором економіки, стимулюючи ефективне функціонування фінансової системи, а отже, створюючи передумови для стійкого економічного зростання у країні [11].

Сьогодні фінансовий сектор є одним із найбільш вразливих галузей до кібератак та загроз кібербезпеки. Така вразливість пояснюється значними обсягами фінансових активів, великими масивами персональних даних клієнтів фінустанов, залежністю від інформаційних технологій тощо.

Основними групами мотивів кіберзлочинців, які за результатами досліджень мають різний соціальний статус, а також рівень освіти та виховання є [12]:

– корисливі, пов'язані з фінансово-економічною сферою відносин суб'єктів у кіберпросторі;

– соціально-економічні, пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі;

– антидержавно-політичні, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі;

– ідейні, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі. Саме тому дослідження ролі кібербезпеки у фінансовому секторі є актуальним завданням сьогодення, що сприятиме розумінню потенційних загроз та пошуку нових заходів захисту.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Важливо відмітити, що питання кібербезпеки є доволі широко розкрито у вітчизняних та іноземних наукових публікаціях, що носять більш технічний характер. Водночас бракує досліджень, що сприятимуть імплементації цього поняття у систему менеджменту фінустанов.

Адже, як заначає О.А. Баранов, «*…кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації*» [1]. Тобто це складник ризик-менеджменту організації.

Кібербезпека реалізується шляхом застосування сучасних технологій, процесів та засобів контролю з метою захисту комп'ютерних систем та мереж, програм, пристроїв та даних від кібернетичних атак, а також з метою зниження ризику їх здійснення. Система кібербезпеки складається з низки елементів, координування яких всередині організації має вирішальне значення для успіху всієї програми кібербезпеки [9].

Кібербезпеку фінансової установи чи організації можна визначити також як захищеність її життєво важливих інтересів від внутрішніх і зовнішніх загроз, тобто захист кадрового та інтелектуального потенціалу, інформації, технологій, прибутку, доданої та ринкової вартості, який забезпечується системою заходів спеціального правового, економічного, організаційного, інформаційно-технічного і соціального характеру [3].

Автори Н.Б. Демчишак та А.С. Шкиря виділяють ризики, пов'язані із застосуванням сучасних електронних технологій, що впливають на фінансовий сектор: кібератаки; ризики шахрайства в ІТ-сфері; ризики помилок у програмному забезпеченні; стратегічні ризики, пов'язані зі швидким розвитком інформаційних технологій та зміною умов ведення бізнесу; ризики державного регулювання фінансових інновацій; ризик порушення функціонування складних інформаційних систем. Автори уточнюють види кіберризиків саме у фінансовому секторі: ризик втрати інформації під час злому паролю доступу або внаслідок DDoS атаки; ризик фінансових втрат від фішингових атак; ризик фінансових втрат через порушення роботи комп'ютерних систем; ризик фінансових втрат від кібер-шантажу або вірусного блокування комп'ютерних систем; ризик фінансових втрат через викра-

дення та розголошення персональних даних та інформації [5].

Відповідно до українського законодавства кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час застосування кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [8].

Як зазначають В. Данилишин та С. Синиця, процес діджиталізації на ринку фінансових послуг передбачає впровадження сучасних систем захисту від кібератак та крадіжок, що, зі свого боку, забезпечує надійність та безпеку орієнтованого на клієнта фінансового сектору [4].

Так, деталізуючи запропоновані визначення поняття "кібербезпека", можна виділити основні етапи забезпечення кібербезпеки фінансових інституцій. Це, насамперед, ідентифікування кіберризиків, оцінювання рівня їх загрози, розроблення стратегій управління кіберризиками, впровадження відповідних заходів безпеки, постійний моніторинг мереж та систем, підвищення рівня знань персоналу з кібербезпеки, страхування кіберризиків тощо. Тобто формування підходу до кібербезпеки як до елемента ризик-менеджменту допоможе фінансовим установам зменшити кількість загроз та втрат і зберегти стійкість своєї діяльності в умовах кібервійни.

МЕТА статті – дослідження ролі кібербезпеки у фінансовому секторі, виявлення та аналізування загроз, які становлять небезпеку для фінансових установ, та надання рекомендацій з ефективних заходів захисту.

РЕЗУЛЬТАТИ

Як вже зазначено вище, сектор фінансових послуг є найбільш привабливим для кібератак, що зумовлено можливістю отримання зловмисниками значних фінансових та нефінансових зисків завдяки доступу до конфіденційних фінансових даних значної кількості клієнтів та контрагентів.

Проте, попри найвищий рейтинг кібербезпеки серед усіх галузей та значну увагу установ фінансового сектору до дослідження видів кіберзагроз, ландшафт таких загроз постійно розвивається, призводячи до складнішої кіберекосистеми. Тому настільки важливою сьогодні є система організування кіберзахисту як складника ризик-менеджменту організації.

Розглянемо найбільш поширені кіберзагрози та атаки у фінансовому секторі. Сьогодні це фішинг та соціальна інженерія, віруси та шкідливе програмне забезпечення, DDoS-атаки, викрадення даних (кібершпигунство) тощо.

Соціальна інженерія як технологія управління людьми в Інтернет-просторі стала невід'ємною частиною кібершахрайства. Фішинг є одним з видів соціальної інженерії. Цей метод полягає у створенні підробленої сторінки сайту банку чи іншої фінансової установи з метою отримання у користувача логіну та паролю від його акаунта. Це дає змогу зловмисникам перевести усі гроші з банківського рахунку жертви на власний або розповсюдити віруси та інше шкідливе програмне забезпечення через завантаження різного роду скриптів. Варто зазначити, що фішинг розрахований насамперед на неуважних користувачів, які нехтують основним правилами сучасної кібербезпеки [2].

Ще однією не менш популярною кіберзагрозою є мальваре. Мальваре – це створення та розповсюдження вірусів та шкідливого програмного забезпечення, що перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Це можуть бути віруси, нав'язлива реклама у браузері користувача, шпигунські програми, ботнети, скриптові програми тощо. Шкідливе програмне забезпечення зазвичай поширюється через інфіковані вебсайти, спам-повідомлення, навмисно прикріплені файли тощо.

DDoS-атаки – це вид кібератаки, під час якої зловмисники намагаються порушити роботу вебсайту, мережі чи інших онлайн-сервісів, перевантажуючи їх великою кількістю підроблених або небажаних запитів. Основними характеристиками DDoS-атаки є великий обсяг трафіку, розподілений характер, цільове спрямування, одночасне використання різних видів атак тощо.

Для кращого розуміння необхідності превентивних заходів з попередження кіберризиків наведемо кілька прикладів великих кібератак на фінансові установи [7]:

1. Кібератака на бюро кредитних історій Equifax у США у 2017 р. Атака призвела до витоку персональних даних 143 млн своїх клієнтів внаслідок дій хакерів, включаючи їхні соціальні номери, інформацію про кредитні картки та інші особисті дані.

2. Атака на Bank of Bangladesh у 2016 р. Хакери застосували систему SWIFT, щоб вкрасти більше 81 млн дол. з рахунків Bank of Bangladesh, перевівши їх на рахунки у банках Філіппін і Шрі-Ланки.

3. Використання вірусу WannaCry у 2017 р. можна назвати глобальною атакою великого масштабу, внаслідок якої постраждали фінансові організації Іспанії, Німеччини та інших країн світу. Зловмисники заблокували дані та вимагали викуп, щоб їх розблокувати.

4. Великий американський банк JP Morgan Chase став жертвою кібератаки у 2014 р. Кіберзлочинці отримали доступ до більше ніж 83 млн банківських рахунків клієнтів банку.

Сьогодні Україна функціонує в умовах повномасштабної війни, яка ведеться на різних фронтах, зокрема й в кіберпросторі. Так, у своєму річному звіті за 2022 р. компанія Microsoft назвала найпоширеніші галузі для атак хакерів в Україні [10]: 27% – державні органи; 10% – IT-галузь; 9% – медіа; 8% – енергетика; 7% – транспорт; 7% – телекомунікації; 5% – фінанси; 3% – ритейлери тощо. За прогнозами аналітиків до 2025 р. щорічні збитки бізнесу через кібератаки зростуть до 10,5 трлн. дол. [6]. Саме тому важливо не просто використовувати систему кібербезпеки, а постійно вдосконалювати їх. Коли мова йде про фінансовий сектор, то тут варто формувати проактивну стратегію кібербезпеки, яка включатиме культуру кібербезпеки в організації, застосування новітніх технологій в галузі кібербезпеки, систему постійного моніторингу та ідентифікування загроз, планування відновлення даних після атак тощо.

Отже, кібербезпека – це важливий складник національної безпеки – система стандартів, правил, процедур та відповідальності як держави, так і бізнесу. Діджиталізація бізнес-процесів та системи державного управління – це метод протидії корупційним ризикам, водночас це додаткові кіберризики. І тут повинна бути системна відповідальність і держави, і бізнесу, і громадянського сус-

пільства загалом. Адже на думку експертів в IT-галузі від 90% кібератак захиститися можна, якщо не безкоштовно, то дуже малими витратами, оскільки їх левову частку спрямовано на користувача. Тобто формування культури кібербезпеки – це основний елемент стратегії будь-якої організації фінансового сектору.

Основними етапами формування культури кібербезпеки фінансової установи є:

1. Забезпечення відповідального ставлення до кіберзагроз персоналу та споживачів фінансових послуг шляхом використання ненав'язливих інформаційних повідомлень та інших методів інформування тощо.

2. Організація регулярних тренінгів з кібербезпеки для персоналу та користувачів фінансових застосунків, щоб вони розуміли основні принципи та вміли правильно діяти у випадку загрози.

3. Розроблення й впровадження політики безпеки та правил застосування інформаційних систем, які регулюють поведінку співробітників щодо персональних чи інших конфіденційних даних та обладнання.

Ще одним, не менш важливим, елементом системи кібербезпеки фінансового сектору є застосування передових технологій, що передбачає:

1. Встановлення та постійне оновлення антивірусних та антимальварних програм на всіх комп'ютерах та серверах.

2. Застосування браузерів для моніторингу та фільтрації мережевого трафіку, а також відповідних систем інтерфейсів для виявлення вторгнень.

3. Застосування шифрування для захисту конфіденційної інформації, особливо під час передачі через мережу.

Ще одним складником стратегії кібербезпеки організації фінансового сектору є постійний моніторинг комп'ютерних систем та мереж, який включає в себе встановлення відповідних систем моніторингу, які спостерігають за діяльністю в мережі та на серверах з метою виявлення незвичайних або підозрілих активностей, а також аналізування журналів подій для виявлення потенційно небезпечних ситуацій.

І на випадок кібератаки, яку не вдалося запобігти, організація повинна мати чітко розроблений алгоритм відновлення даних, який передбачає:

1. Резервне копіювання даних – регулярне створення резервних копій даних та забезпечення їх надійного зберігання.

2. Розроблення плану відновлення роботи, включаючи процедури відновлення систем, даних та послуг після кібератаки.

3. Регулярне тестування систем, навчання та випробування плану відновлення з метою визначення його ефективності.

Кіберзагрози не мають кордонів, тому їх вплив відчутний і на міжнародному рівні. Імплементація міжнародних стандартів у сфері кібербезпеки допоможе Україні приєднатися до глобальних зусиль у подоланні кіберзагроз. Так Україна сприятиме підвищенню довіри міжнародних партнерів та іноземних інвесторів до вітчизняного бізнесу. Імплементація міжнародних стандартів у сфері кібербезпеки свідчитиме про зобов'язання країни стосовно захисту інформації та відповідної інфраструктури як важливого елемента національної безпеки. Відповідність міжнародним стандартам сприятиме зміцненню національної безпеки та попередженню кібератак на важливі об'єкти, що є особливо актуальним в умовах війни. До таких стандартів відносять ISO 27001 (міжнародний стандарт з інформаційної безпеки), NIST Cybersecurity Framework (рекомендації з кібербезпеки, які може бути застосовано у фінансовому секторі), PCI DSS (вимоги до забезпечення безпеки даних власників платіжних карток) тощо.

Усі вищезазначені елементи лише у комплексі сприятимуть формуванню системи забезпечення кібербезпеки у фінансовому секторі та дотримання стандартів та вимог до галузі кібербезпеки. Адже кібербезпека у фінансовому секторі має величезне значення, оскільки безпосередньо впливає на всю глобальну економіку.

ВИСНОВКИ

Отже, фінансовий сектор є особливо привабливий для кіберзлочинців, оскільки містить величезні обсяги фінансових активів. Кібератаки можуть призвести до величезних збитків не лише окремої фінустанови, а й економіки загалом. Гарантування безпеки цих активів є вагомим чинником фінансової стабільності. Окрім цього, фінансові установи мають доступ до конфіденційної інформації своїх клієнтів, включаючи персональні та фінансові дані. Витік або втрата цієї інформації може призвести до серйозних юридичних наслідків та втрати довіри клієнтів.

Фінансовий сектор відіграє ключову роль у підтримці економічної ліквідності і функціональності держави. Кібератаки, які створюють перешкоди у системі обслуговування або втрату даних, можуть призвести до непоправних збитків у фінансовій діяльності, котрі матимуть негативний вплив на глобальну економіку.

Довіра у фінансовому секторі є важливою детермінантою. Кібератаки можуть підірвати довіру клієнтів та інвесторів, що, зі свого боку, призведе до відтоку активів і зниження репутації фінансової установи. Саме тому фінансовий сектор підлягає жорсткому правовому регулюванню та стандартизації системи кібербезпеки. Недотримання цих вимог може призвести до санкцій та штрафів, а також втрати відповідних ліцензій та дозволів.

Усі ці фактори підкреслюють важливість кібербезпеки у фінансовому секторі. Фінансові установи повинні вкладати значні зусилля та ресурси у забезпечення безпеки своїх систем та даних, а також співпрацювати з регуляторами та іншими суб'єктами для підвищення рівня кібербезпеки в цій галузі.

Список використаних джерел

1. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. 2014. № 2(42). С. 54-62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf

2. Вишньовський В.В., Ткачук Л.М. Соціальна інженерія як засіб впливу на людську свідомість. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20485/4049.pdf?sequence=3

3. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Випуск № 11. С. 497-502. URL: http://ir.polissiauniver.edu.ua/bitstream/123456789/9969/3/ES_2017_11_497-02.pdf

4. Данилишин В., Синиця С. Діджиталізація на ринку фінансових послуг: сутність та значення для економіки України в умовах

сьогодення. *Трансформаційна економіка*. 2023. № 3 (03). С. 16-20. URL: https://doi.org/10.32782/2786-8141/2023-3-3

5. Демчишак Н.Б., Шкиря А.С. Управління ризиками у фінансовому секторі України в умовах кіберзагроз і постпандемічного відновлення економіки. *Інноваційна економіка*. 2021. № 3-4'. С. 19-27. URL: http://www.inneco.org/index.php/innecoua/article/view/764/839

6. Кібербезпека у Фінтех: Чому це важливо і як цьому сприяє Low-Code. *Mezha.* 2023. URL: https://mezha.media/2023/06/21/kiberbezpeka-u-fintekh-low-code/

7. Перелік кібератак. *Вікіпедія.* URL: https://uk.wikipedia.org/wiki/Перелік_кібератак

8. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 року № 2163-VIII: станом на 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Конституційне та адміністративне право. Юридичний вісник*. 2021. № 2 (59). С. 110-115. URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/I. M. Сопілко.pdf

10. Україна – одна з головних цілей для кібератак у світі. Як захиститися? Розповідаємо з прикладами. URL: https://delo.ua/telecom/ukrayina-odna-z-golovnix-cilei-dlya-kiberatak-u-sviti-yak-zaxistitisya-rozpovidajemo-z-prikladami-412454/

11. Школьник І.О., Семеног А.Ю. Фінансовий сектор України: теоретичний аналіз економічної дефініції. *Вісник Української академії банківської справи*. 2013. № 1(34). С. 31-36. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/69206/1/Semenog_Finsector.pdf;jsessionid=E366805D2AF4FE947C54DD7AB650BEF0

12. Biliavska Y., Mykytenko N., Shestak Y. Cybersecurity and the information protection during the COVID-19 pandemic. *Commodities·and·markets*. 2021. № 37(1). pp. 34–46. URL: https://doi.org/10.31617/tr.knute.2021(37)03

References

1. Baranov O.A. On the interpretation and definition of the concept of "cyber security". *Legal informatics*. 2014. No 2(42). pp. 54-62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf (in Ukrainian).

2. Vyshnovskyi V.V., Tkachuk L.M. Social engineering as a means of influencing human consciousness. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20485/4049.pdf?sequence=3 (in Ukrainian).

3. Viter S.A., Svitlyshyn I.I. Protection of accounting information and cyber security of the enterprise. *Economy and society*. 2017. Issue 11. pp. 497-502. URL: http://ir.polissiauniver.edu.ua/bitstream/123456789/9969/3/ES_2017_11_497-02.pdf (in Ukrainian).

4. Danylyshyn V., Synytsia S. Digitization in the market of financial services: essence and significance for the economy of Ukraine in today's conditions. *Transformational economy*. 2023. No 3 (03). pp. 16-20. URL: https://doi.org/10.32782/2786-8141/2023-3-3 (in Ukrainian).

5. Demchyshak N.B., Shkyria A.S. Risk management in the financial sector of Ukraine in the conditions of cyber threats and post-pandemic economic recovery. *Innovative economy*. 2021. No 3-4'. pp. 19-27. URL: http://www.inneco.org/index.php/innecoua/article/view/764/839 (in Ukrainian).

6. Cybersecurity in Fintech: Why it is important and how Low-Code contributes to it. *Mezha.* 2023. URL: https://mezha.media/2023/06/21/kiberbezpeka-u-fintekh-low-code/ (in Ukrainian).

7. List of cyber attacks. URL: https://en.wikipedia.org/wiki/List_of_cyberattacks

8. On the main principles of ensuring cyber security of Ukraine. Law of Ukraine dated 05.10.2017 No 2163-VIII від: as of 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

9. Sopilko I.M. Information security and cyber security: a comparative legal aspect. *Constitutional and administrative law. Legal Bulletin*. 2021. No 2 (59). pp. 110-115. URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/I. M. Сопілко.pdf (in Ukrainian).

10. Ukraine is one of the main targets for cyber attacks in the world. How to protect yourself? Let's talk with examples. URL: https://delo.ua/telecom/ukrayina-odna-z-golovnix-cilei-dlya-kiberatak-u-sviti-yak-zaxistitisya-rozpovidajemo-z-prikladami-412454/ (in Ukrainian).

11. Shkolnyk I. O., Semenoh A. Yu. Financial sector of Ukraine: theoretical analysis of the economic definition. *Visnyk Ukrainskoi akademii bankivskoi spravy*. 2013. No 1(34). pp. 31-36. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/69206/1/Semenog_Finsector.pdf;jsessionid=E366805D2AF4FE947C54DD7AB650BEF0 (in Ukrainian).

12. Biliavska Y., Mykytenko N., Shestak Y. Cybersecurity and the information protection during the COVID-19 pandemic. *Commodities·and·markets*. 2021. No 37(1). pp. 34–46. URL: https://doi.org/10.31617/tr.knute.2021(37)03

Iryna DOROSH
PhD in Public Management and Administration, Associate Professor, Lviv Polytechnic National University
ORCID: https://orcid.org/0000-0003-1394-5639
e-mail: iryna.m.dorosh@lpnu.ua

CYBER SECURITY AND ITS ROLE IN THE FINANCIAL SECTOR: THREATS AND PROTECTION MEASURES

The paper examines the critical role of cybersecurity in the financial sector and the challenges facing financial institutions in today's digital world. The conceptual apparatus of cyber security as an important component of the national security of the state, as well as the most common cyber threats and attacks in the financial sector, were studied. The definitions of the concept of "cyber security" proposed in scientific sources are detailed with the main stages of its provision in financial institutions. Attention is focused on the need to develop an approach to cyber security as an element of risk management, which will help financial institutions reduce the number of threats and losses and maintain the stability of their activities in the conditions of cyber warfare.

The paper also examines the main safeguards that financial institutions should take to ensure their cyber security. The role of technologies, proactive monitoring, creating a culture of cyber security and other factors in ensuring the safety and stability of financial systems is analyzed. In addition, the paper examines current trends in cyber security and innovative approaches to protecting financial institutions from complex and distributed threats. It highlights the importance of cross-sector collaboration and information sharing for early detection and prevention of cyber threats. An important aspect of the paper is the emphasis on the need to constantly update and improve cyber security strategies, as threats are constantly evolving and financial institutions must be ready to respond to new challenges.

The conclusions emphasize the fact that the financial sector plays a key role in maintaining the economic liquidity and functionality of the state. Cyber-attacks that cause service disruptions or data loss can lead to irreparable losses in financial activity, which will have a negative impact on the global economy. In addition, cyber threats can undermine the confidence of customers and investors, which, in turn, will lead to an outflow of assets and a decrease in the reputation of the financial institution. That is why the financial sector is subject to strict legal regulation and standardization of the cyber security system. Failure to comply with these requirements may result in sanctions and fines, as well as the loss of relevant licenses and permits.

Keywords: *financial sector, cyber threats, cyber security culture, state strategy, business responsibility*