УДК 336:330.46:004.056

С.Д. Лучик
М.В. Лучик

КІБЕРБЕЗПЕКА У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

Харківський національний університет внутрішніх справ
Акціонерне товариство «Креді Агріколь Банк»

Анотація. *У статті досліджені питання кібербезпеки у фінансовому секторі національної економіки, висвітлені основні кіберзагрози, з якими стикаються сьогодні банки та інші фінансові установи, наведені практичні рекомендації щодо захисту фінансової інформації та інформаційних ресурсів, посилення інформаційної безпеки фінустанов.*
Ключові слова: кібербезпека, кіберзагрози, кібератаки, персональні дані, штучний інтелект, хмарні сервіси.

Abstract. *The article examines the issue of cybersecurity in the financial sector of the national economy, highlights the main cyber threats that banks and other financial institutions face today, and provides practical recommendations for protecting financial information and information resources, strengthening the information security of financial institutions.*
Keywords: cybersecurity, cyber threats, cyber attacks, personal data, artificial intelligence, cloud services.

Злочинність в Україні набуває цифрового характеру, тобто стає кіберзлочинністю, яка носить масштабний та різноманітний характер. Негативний вплив на посилення криміногенної ситуації у кіберпросторі Україні справляють, зокрема, такі фактори як збройна агресія рф проти України; поширення глобальних кіберзагроз, таких як атаки на ланцюги постачання (supply chain attacks), кібервикрадення даних (data breaches) та використання штучного інтелекту для вчинення злочинів; масове поширення таких способів вчинення кримінальних правопорушень як фішинг, вішинг, бейтінг, скімінг, злам облікових записів тощо; поширення особистих даних, що сприяє вчиненню майнових злочинів у кіберпросторі; використання сервісів анонімізації під час вчинення кримінальних правопорушень; зростання обсягів використання інтернет-банкінгу. Слід зазначити, що Україна, як частина глобального інформаційного простору, не може уникнути цих ризиків, особливо в контексті інтеграції з ЄС та міжнародними системами обміну даними. [1].

Під кіберзлочином (комп'ютерним злочином) розуміють суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2]. Кіберзлочинність завдає шкоди інформаційним ресурсам, які належать державним органам, підприємствам, установам, особисто громадянам, знижує довіру суспільства до інформаційних та цифрових технологій, призводить до значних репутаційних та матеріальних втрат.

З питаннями кібербезпеки сьогодні стикаються всі підприємства. Для фінансових установ ці питання особливо актуальні. Кіберінценденти, з якими вони стикаються, можуть порушити безпеку інформаційних систем, призвести до втрати цілісності та конфіденційності даних. Це і шкідливе програмне забезпечення, таке як віруси чи трояни, і перевантажені сервери, і спроби викрасти конфіденційні дані шляхом підкупу чи обману працівників компанії. Наслідки реалізованих кіберзагроз можуть поставити під загрозу дані про фінансову установу та її клієнтів, що потенційно може пошкодити довіру останнього та заплямувати репутацію компанії. При цьому фінансові установи та банківські установи, залишаючись головними цілями для кіберзлочинців, продовжують впроваджувати інновації та інтегрувати нові рішення. Все це вимагає стратегії фінансових установ з кібербезпеки, яка враховуватиме нові тенденції та ризики.

Фінансовий сектор української економіки потерпає від фішингових атак. Зловмисники обманом змушують людей розкрити конфіденційну інформацію. Такий обман може переслідувати одразу кілька цілей: або збір персональних даних для створення відповідних баз та "армій" ботів, або крадіжка коштів з банківських карт, або підробка документів. Від імені банківських працівників шахраї розповсюджують серед громадян повідомлення зі шкідливими посиланнями на начебто вебсайт Telegram, щоб отримати несанкціонований доступ до облікових записів, зокрема, і з можливістю

перехоплення одноразового коду з SMS. В Україні за п’ять місяців 2024 року було відкрито рекордну кількість справ про шахрайство − понад 38 тисяч. І це лише ті випадки, коли жертви втрачали кошти і зверталися по допомогу до поліції – реальна кількість спроб різноманітного шахрайства у десятки разів вища. І, за даними Нацбанку, саме фішинг та соціальна інженерія є найпопулярнішими методами маніпуляцій з платіжними картками в Україні (та й загалом у світі) [3].

Для захисту від фішингових загроз фінансовим установам слід використовувати антивірусне програмне забезпечення, постійно його оновлювати. Антивірусні програми можуть допомогти виявити та заблокувати фішингові сайти. Як працівникам фінустанов, так і їх клієнтам, слід обережно працювати з електронною поштою і месенджерами, завжди перевіряти адресу відправника електронної пошти або SMS-повідомлення, не переходити за посиланнями у повідомленнях від незнайомих або підозрілих відправників та не довіряти пропозиціям легкого заробітку. Категорично заборонено вводити свої персональні дані на підозрілих ресурсах, надавати особисту інформацію у відповідь на електронні листи або повідомлення без підтвердження їх автентичності та передавати коди своїх кредитних карток.

Від початку повномасштабної війни росії проти України серед найпоширеніших видів кібератак на фінансовий сектор країни слід виділити DDoS-атаки, які через створення значної кількості зовнішніх запитів знижують доступ до вебресурсів установ, в результаті чого виникають збої в їх роботі або вони взагалі перестають повноцінно працювати. Як DoS-, так і DDoS-атаки здійснюють із метою поширення паніки та дестабілізації, здебільшого не спрямовуються на окремих громадян. Їх задача – зробити важливі інформаційні ресурси недоступними для клієнтів. Причому DDoS-атаки здійснюється не з одного, а з кількох джерел. Від початку 2024 року DDoS-атак зазнали низка сайтів державних органів, телеком-операторів, компаній енергетичного сектору, сайти регіональних органів влади, медіа тощо. Серед найбільших банків слід назвати Monobank, Райффайзен Банк.

Захист від DDoS атак вимагає комплексного підходу і використання різних методів і технологій. Це: фільтрація трафіку на рівні мережевих пристроїв, таких як міжмережеві екрани (firewalls) і маршрутизатори, для блокування підозрілих пакетів даних, що виходять від потенційних джерел DDoS атак; використання CDN (Content Delivery Networks) для розподілу навантаження по серверах, що дає змогу перенаправляти трафік на різні сервери і захищати інформаційні ресурси від DDoS атак; використання апаратних і програмних рішень, таких як Intrusion Prevention Systems (IPS) і DDoS protection appliances, для аналізу трафіку та автоматичного блокування підозрілих запитів; розподілений захист, за якого захисні заходи застосовують на кількох рівнях мережі, включно з рівнем провайдера інтернет-з’єднання і рівнем центру обробки даних. Це дає змогу виявляти та припиняти атаки на більш ранніх етапах, що зменшує вплив на роботу цільового ресурсу.

Оскільки кіберзагрози продовжують розвиватися, очікується, що багато фінансових установ запровадять моделі «Кібербезпека як послуга» (Cybersecurity as a Service, CaaS). Аутсорсинг певних аспектів кібербезпеки, таких як виявлення загроз, управління вразливістю та реагування на інциденти, стане більш поширеним, особливо серед невеликих банків, яким може не вистачати ресурсів для повноцінної внутрішньої команди безпеки.

Хмарні технології надають бізнесу надійне та безпечне середовище для розміщення критично важливих даних та сервісів. Зі збільшенням кількості банківських операцій, фінустанови переходять у хмару. 38% компаній у світі використовують хмарні робочі навантаження, що відповідають трьом критеріям «тріади токсичних хмар»: загальнодоступні, критично вразливі та високопривілейовані. Така комбінація чинників приваблює зловмисників. «Тріада токсичних хмар» спричинює витоки даних, відмову роботи додатків, захоплення систем, та, як один із наслідків, DDoS-атаки, які нерідко супроводжуються вимогами викупу. Це все може нести негативний вплив на бізнес − середня вартість одного витоку даних у 2024 році близька до $5 млн [4].

Основою надійного захисту інформації в хмарі є розуміння відповідальності за безпеку хмари, що розподіляється між оператором та користувачем. Тільки впровадження чітких політик безпеки, надійне шифрування, багатофакторна автентифікація, регулярні аудити, управління вразливостями тощо дозволять захистити інфраструктуру фінансових установ від кіберзагроз і уникнути втрат, які можуть коштувати мільйони.

Сьогодні банки та фінансові компанії активно застосовують штучний інтелект (ШІ) і машинне навчання для покращення взаємодії з клієнтами. Звіт Business Insider показує, що майже 80% банків знають про потенційні переваги ШІ в банківській справі. Інший звіт McKinsey передбачає, що генеративний штучний інтелект може підвищити продуктивність у банківському секторі на 5% і

скоротити глобальні витрати на $300 млрд. Ці цифри вказують на те, що банківський і фінансовий сектори стрімко переходять до штучного інтелекту для підвищення ефективності й продуктивності, покращення обслуговування та зниження витрат [5].

Серед основних напрямків застосування ШІ у банкінгу – запобігання шахрайству та персоналізація послуг. Відомим кейсом є чат-бот зі штучним інтелектом від Ощадбанку «Софія» – голосовий помічник, що консультує клієнтів за широким спектром питань, наприклад, призначення зустрічей у відділеннях і перенаправлення клієнтів до відповідних спеціалістів залежно від їхніх запитів. Завдяки використанню «Софії» 75% клієнтських запитів було автоматизовано, час на їх обробку знизився, загальний рівень задоволеності клієнтів покращився. Кейси успішної інтеграції штучного інтелекту мають й інші українські банки. Це й оптимізація кредитного портфеля через аналіз поведінкових факторів клієнтів, і розробка персоналізованих фінансових продуктів, і моніторинг клієнтських транзакцій для підвищення рівня кібербезпеки.

Однак, незважаючи на те, що ШІ допомагає оперативніше виявляти загрози та реагувати на них швидше, кіберзлочинці також все активніше використовують його для більш складних атак, таких як фішинг із підтримкою штучного інтелекту та шахрайство з дипфейками.

Отже, фінансові установи завжди залишаються в об'єктиві кіберзлочинців. У 2025 році, за прогнозами компанії Gartner, глобальні світові витрати на кібербезпеку становитимуть 212 мільярдів доларів, що на 15,1% більше ніж 2024 року [6]. Тому фінансовим установам в Україні потрібно постійно вкладати інвестиції в сферу власної кібербезпеки, постійно проводити навчання своїх працівників методам протидії кіберзагрозам, нтегрувати в систему безпеки методи MFA нового покоління, щоб покращити взаємодію з користувачем, а також щоб іти в ногу з досвідченими кіберзлочинцями, які постійно розробляють способи обходу традиційних заходів безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. Кіберполіція України. Офіційний сайт.URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 25.02.2025).
2. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text .
3. Україною шириться епідемія фішингових атак: як не потрапити на гачок. *УНІАН.* URL: https://www.unian.ua/society/ukrajinoyu-shiritsya-epidemiya-fishingovih-atak-yak-ne-potrapiti-na-gachok-12672213.html#goog_rewarded (дата звернення: 26.02.2025).
4. Ризики хмарної безпеки: на що звернути увагу та як захиститися. Giga Cloud. URL: https://gigacloud.ua/articles/ryzyky-hmarnoyi-bezpeky-na-shho-zvernuty-uvagu-ta-yak-zahystytysya/ (дата звернення: 28.02.2025).
5. Як ШІ змінює українські банки. *Fintech Insider*. URL: https://fintechinsider.com.ua/yak-shi-zminyuye-ukrayinski-banky/ (дата звернення: 28.02.2025).
6. Тренди кібербезпеки на 2025 рік: як захистити бізнес. Kyivstar Business Hub. URL: https://hub.kyivstar.ua/articles/ostanni-trendy-kiberbezpeky (дата звернення: 01.03.2025).

Лучик Світлана .Дмитрівна, доктор економічних наук, професор, професор кафедри інформаційних систем та технологій, Харківський національний університет внутрішніх справ, Кам'янець-Подільський, luchiksvitlana@gmail.com

Luchyk Svitlana D., Doctor of Economics, Professor, Professor of the Department of Information Systems and Technologies, Kharkiv National University of Internal Affairs, Kamianets-Podilskyi.

Лучик Маргарита Василівна, кандидат економічних наук, керівник напрямку з підтримки зарплатних проєктів, Київ, АТ «Креді Агріколь Банк», luchik-margarita@ukr.net

Luchik Margarita V., Candidate of Economic Sciences, Head of the Salary Project Support Department, Kyiv, Credit Agricole Bank JSC,