УДК 336. 621.391.

М. Ю. Богославський,
здобувач Національної академії управління, м. Київ, Україна

ДОСЛІДЖЕННЯ СТУПЕНЮ ПРОТИДІЇ БАНКІВСЬКИМ КІБЕРАТАКАМ НА СВІТОВОМУ ТА ВІТЧИЗНЯНОМУ РІВНЯХ

N. Bogoslavskij,
Applicant National Academy of Management, Kyiv, Ukraine

STABILITY RESEARCH OF COUNTERVAILING BANKING CIBERATES ON THE WORLD AND DOMESTIC LEVELS

У статті розглянуто світовий досвід та ступінь протидії кібератакам у банківській сфері за рахунок проставлення бальних оцінок здатності регулювати загрозливі ситуації. Наведено приклади транснаціональних фінансових установ та коментарі з цієї тематики від світових фахівців. Методом експертних опитувань було встановлено статистику кіберзлочинності на вітчизняному просторі та запропоновано дієвий механізм протидії загрозам з боку банкірів. Зазначається важливість здійснення посиленого моніторингу за банківськими операціями у відповідності до запропонованих способів в актуальних макроекономічних умовах.

The article examines the world experience and the degree of counteraction to cyberattacks in the banking sector by range assessments on the ability threatening situations regulation. Examples of transnational financial institutions and commentary on this subject from world experts were given. The method of expert surveys has established statistics on cybercrime in the domestic space and proposed an effective mechanism for counteracting threats from bankers. It was noted the importance of implementing enhanced monitoring of banking operations in accordance with the proposed methods in current macroeconomic conditions.

Ключові слова: кіберзлочинність, банківський сектор, ступінь супротиву кібератакам, ключові позиції, світова практика, синергетична модель захисту банківської інформації.

Key words: cybercrime, banking sector, degree of resistance to cyberattacks, key positions, world practice, synergistic model of protection of banking information.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

Проблематика кіберзлочинності в Україні є важливим питанням для стабільної діяльності банківського сектору та забезпечення захисту фінансових даних. За останні роки загрози потужних кібератак зростають з великою швидкістю завдяки інтенсивному розвитку технологій, але за свідчення закордонних джерел інформації їх вдається успішно стримувати. На жаль, сучасний стан вітчизняного банківського сектору вказує на протилежну ситуацію, а 2017 рік знаменувався єдиною широкомасштабною кібератакою в історії України.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Деталізована підбірка статистичних даних щодо світового досвіду протидії кіберзагрозам була сформована на основі досліджень фахівців підрозділів забезпечення ФБ банків з більш ніж 20 країн світу. Основною метою такого звіту було забезпечити організацію Security & Defence Agenda результатами досліджень та показниками готовності банків до кібератак та їх протидії при виникненні.

МЕТА СТАТТІ

Метою статті є проведення огляду сучасного стану розвитку та дослідження практик

Передплатний індекс 21847

Таблиця 1. Бальна оцінка протидії кібератакам

<table>
<tr><td colspan="7">Бальна оцінка протидії кібератакам</td></tr>
<tr><td>5</td><td>4,5</td><td>4</td><td>3,5</td><td>3</td><td>2,5</td><td>2</td></tr>
<tr><td rowspan="8">-</td><td rowspan="2">Ізраїль</td><td>Франція</td><td>Канада</td><td rowspan="2">Італія</td><td rowspan="2">Індія</td><td rowspan="8">Мексика</td></tr>
<tr><td rowspan="2">Нідерланди</td><td rowspan="3">Японія</td></tr>
<tr><td rowspan="2">Польща</td><td rowspan="3">Латвія</td></tr>
<tr><td rowspan="2">Швеція</td><td>Німеччина</td></tr>
<tr><td>Великобританія</td><td rowspan="3">Австралія</td></tr>
<tr><td rowspan="3">Фінляндія</td><td>Росія</td><td rowspan="3">Румунія</td></tr>
<tr><td>США</td><td rowspan="2">Канада</td></tr>
<tr><td>Іспанія</td><td rowspan="2">Австрія</td></tr>
<tr><td>Естонія</td></tr>
</table>

Джерело: складено автором на основі [4, с. 150].

світового досвіду протидії кібератакам для подальшого застосування в умовах вітчизняного банківського сектору.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Завдяки небезпечному становищу циклу діяльності банків під час кібератак, їх основним прагненням є формування більш гнучкого бізнес-плану та створення додаткових інструментів протидії кіберзагрозам у рамках загального забезпечення фінансової безпеки (ФБ) банків, якщо цього не зробити вчасно, то це може підірвати репутацію банку, а разом і з тим спричинити недовіру клієнтів.

На нашу думку, слід зазначити, що на проведення таких досліджень було притягнуто експертів у сферах комп'ютерної діяльності, ІТ-сфери та персоналу з питань захисту комерційних банків від кіберзлочинності. Після наданих результатів, Security & Defence Agenda провела оцінювання комерційних банків різних країн на готовність до протидії кібератакам, таке оцінювання проводиться за шкалою 5 балів. Пропонуємо для ознайомлення з реальними показниками протидії кібератакам різних країн у таблиці 1.

За даними оцінювання вищий за всіх результат, а саме 4,5 бали, здобули всього три країни: Ізраїль, Швеція, Фінляндія. Друге місце посіли комерційні банки таких країн, як: США, Великобританія, Франція та Німеччина.

У рамках дослідження експертів Security & Defence Agenda на базі European Banking Forum's 2017 Technology, Security and Risk Show можна класифікувати такі результати анкетувань: майже 38 % експертів вважають що в світовій фінансовій системі проходить перерозподіл технічних заходів впливу та технологій протиставлення кіберзлочинності", 15% вважають, кіберзагрози є найбільшою проблемою у банківській сфері, 22% відзначили ризик неочікуваності стосовно несанкціонованого заволодіння для будь-якої транзакції чи коштів які перебувають на довгострокових депозитах, 25% опитуваних відповідають, що протидія кібератакам має важливе положення у системі діяльності банків, тому потрібно забезпечувати банки новими кадрами для розвитку нових підходів з протидії кіберзлочинам [5, с. 65].

Зазначимо, що у ході досліджень поведінки підрозділів ФБ банків на виникаючі кіберзагрози, можна виділити ряд таких коментарів від світових фахівців:

— система безпеки фінансової системи та підрозділи ФБ банків потребують обмін інформацією за поточними загрозами у реальному часі;

— більшій частині комерційних банків потрібна постійна фінансова підтримка для забезпечення найліпшого результату боротьби з загрозами;

— важливість методичного доопрацювання та імплементації у процесах протидії кіберзло-

Таблиця 2. Ключові позиції стратегій кібербезпеки

Рівень	Стратегія
Макрорівень	побудова урядової моделі, спрямованої на забезпечення кібербезпеки
	доказ необхідності нової програми освіти в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки
	побудова урядової моделі, спрямованої на забезпечення кібербезпеки
Мікрорівень	підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур
	визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки
	розробка системного та інтегрованого підходу до державного управління ризиками

Джерело: [7, с. 125].

Передплатний індекс 21847

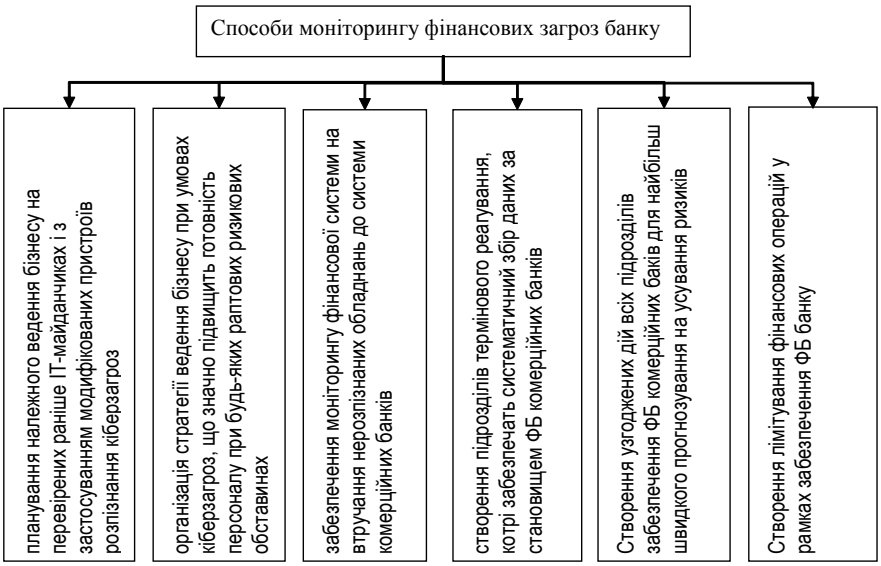

Рис. 1. Способи моніторингу фінансових загроз банку в інформаційній сфері

чинності спільними силами світових органів банківського нагляду та інформаційних технологій;

— необхідність спільної протидії масованим кібератакам на глобальному рівні з міжвідомчою кооперацією;

— системи ФБ банків потребує розширення спектру дій при кібератаках для оперативної допомоги клієнтам.

Для України подібна тенденція розвитку таких взаємовідносин стала би в цілому, позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямі не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним. Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн, можна виділити об'єднуючі ключові позиції (табл. 2).

На нашу думку, найкращі практичні аспекти світових фінансових установ, зокрема у сфері перерозподілу інформаційними ресурсами мають бути імплементовані у вітчизняну систему протидії кіберзагрозам.

Зазначимо, що розширення інформаційного простору банківської діяльності може сприяти створенню слабких ділянок у системі протидії кіберзагрозам, що поступово приведе до дестабілізації банківського сектору.

Прагнення забезпечити вітчизняні комерційні банки та підрозділи захисту їх фінан-

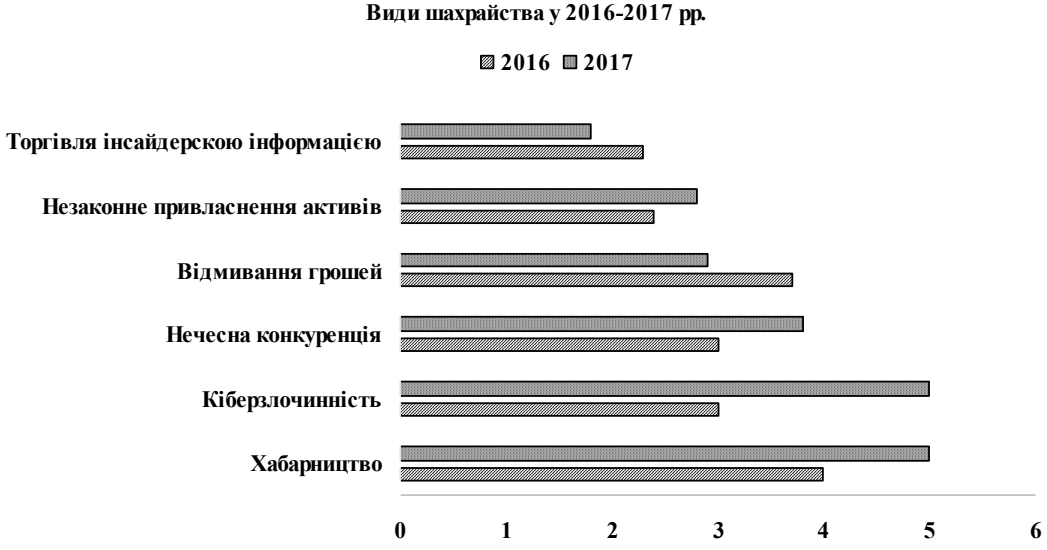

Рис. 2. Статистика видів шахрайства у банківській сфері у 2016—2017 рр.

Передплатний індекс 21847

сової системи новітніми інструментами протидії кібератакам може різко усунути дисбаланс між банками та виникаючими кіберзагрозами під час їх функціонування. Фахівцями у сфері комп'ютерних технологій було зроблено висновок, що через деякий час комерційні банки та підрозділи забезпечення їх ФБ відчуватимуть недостатню кількість кваліфікованих фахівців та груп протидії кібератакам [8, с. 109].

У поточний час головною проблемою є питання щодо формування активних механізмів захисту фінансової системи банків, клієнтської інформаційної бази, даних з клієнтських кредитних карток та системних даних з серверів комерційних банків. На нашу думку, нині має здійснюватися посилений моніторинг об'ємних фінансових операцій саме завдяки таким способів, які вказані на рисунку 1.

Існуючі підходи, як відомо, в основному орієнтуються на компенсування сил і засобів забезпечення безпеки банківської інформації, що часто призводить до неповного перекриття спектру загроз і нераціонального використання ресурсів, виділених на забезпечення безпеки. Зазначено, що розробка принципово нового підходу до забезпечення безпеки банківської інформації, якому присвячена робота, є необхідною умовою надання якісних банківських послуг. У світовому співтоваристві банків імплементовано синергетичну модель загроз безпеки банківської інформації, яка вперше з системних позицій надала змогу розкрити сучасний стан досліджуваної проблеми [1, с. 212].

Доведено, що на сучасному етапі розвитку науки та техніки, забезпечення безпеки банківської інформації має грунтуватися на принципово новому підході, який запропоновано називати синергетичним. Його впровадження надасть змогу одержати синергетичний ефект у разі взаємодії обраних профілів безпеки і, як наслідок, проявити якісно нові та невідомі до цього емерджентні властивості системи безпеки. У межах запропонованого підходу в загальному вигляді формалізовано проблему підвищення рівня захищеності банківської інформації та визначено подальші шляхи її розв'язання. Показано, що відсутність подібних рішень в системах забезпечення банківської інформації визначає актуальність обраної теми для дослідження та її науковий пріоритет [6, с. 105].

За методом експертних опитувань було встановлено таку статистику кіберзлочинності на вітчизняному просторі зображену на рисунку 2.

Односторонні ініціативи з боку банківських підрозділів ФБ можуть забезпечити оперативне реагування на виникаючі ризики, усувати витоки клієнтської інформації, паралельно займатися розробкою нових методів боротьби з кібератаками, залучати менше ресурсів, але з більшим результатом та проводити систематичну профілактику протидії загрозам банку [2, с. 88].

Кіберзлочинність у всій своїй складовій становить суцільну загрозу і стає чинником дестабілізації фінансових систем комерційних установ, є прямою причиною витоку клієнтських даних до мережі Інтернет, також слугує причиною заміни підтверджених даних на штучні та безпосередньо становить собою підривником національної економіки.

ВИСНОВКИ

Розглянуто види шахрайства у 2016—2017 роках та ступінь протидії кіберзагрозам з боку банків, в ході чого встановлено різницю між відповідності та специфікою за територіальною приналежністю, що є суб'єктивним рішення, через масову міграцію фрілансерів, хакерів та відповідно методик банківських атак. На основі світових досліджень засвідчено способи моніторингу фінансових загроз банку в інформаційній сфері, в рамках яких введення та тестування новітніх технологій, інструментів та засобів боротьби з кіберзагрозами комерційних банків можуть спричинити зараження системних даних у разі невдалого тестування та недоцільної розробки тієї чи іншої програми, або механізму і мати негативний вплив на стабільну роботу банку.

Прогрес та розповсюдженість кібератак прогресує з кожним роком, завдяки ще більшому розвитку цифрових технологій та розширення охоплювання нових регіонів мережею інтернет, саме це, на нашу думку, дає змогу злочинцям збільшувати свої сфери діяльності.

Література:

1. Вовчак О.Д. Банківська безпека: навч. посіб. / О.Д. Вовчак, Ю.О. Самура, В.А. Сидоренко, В.А. Вареник. — К.: Знання, 2013. — 237 с.

2. Грюнинг Х. ван. Анализ банковских рисков. Система оценки корпоративного управления и управления финансовым риском [Текст] / Х. ван Грюнинг, С. Брайович Братанович; пер. с англ. — М.: Издательство "Весь Мир", 2007. — 304 с.

3. Єгоричева С.Б. Інноваційна діяльність комерційних банків: стратегічні аспекти: монографія / С.Б. Єгоричева. — Полтава: ТОВ "АСМІ", 2010. — 348 с.

Передплатний індекс 21847

4. Локтев А.В. Зарубежный взгляд на конструктивность государственного регулирования деятельности банковского сектора в условиях мирового экономического кризисна / А.В. Локтев // Социально-экономические явления и процессы. — 2011. — № 1—2. — С. 148—152.

5. Марцин В.С. Економічна безпека як основна складова економічної свободи в період глобалізації. — кн.: Соціально-економічні дослідження в перехідний період. Євроінтеграційний курс України: фінансовий вимір: У 2-х ч. — Львів, 2006. — Вип. 3. — Ч. 1. — С. 95.

6. Крупка І.М. Особливості розвитку фінансового ринку України в умовах глобалізаційних процесів // Національні фінансові системи в умовах глобалізації: монографія / За ред. І.О. Лютого. — Івано-Франківськ: Галицька Академія, 2008. — 306 с. — С. 97—123; Крупка І.М. Фінансовий ринок України та міжнародні фінансові потоки / І.М. Крупка // Фінанси України. — 2009. — № 12. — С. 104—116.

7. Счастная Т.В. IRBAA (Базель II): преимущества и недостатки методологии / Т.В. Счастная, М.В. Дюпина // Вестник Томского государственного университета. — 2012. — № 1. — С. 122—128.

8. Хогарт Г. Разрешение банковских кризисов: основные инструменты и издержки / Г. Хогарт, Дж. Рейдхилл, П. Синклер // Банки: мировой опыт. — 2011. — № 34. — С. 108—109.

9. Щодо інтеграції банківської системи України до банківської системи Європейського Союзу: аналітична записка [Електронний ресурс]. — Режим доступу: http://www.niss.gov.ua

References:

1. Vovchak, O.D. (2013), Bankivs'ka bezpeka [Banking Security], Znannia, Kyiv, Ukraine.

2. Hriunynh, Kh. van. (2007), Analyz bankovskykh ryskov. Systema otsenky korporatyvnoho upravlenyia y upravlenyia fynansovym ryskom [Analysis of banking risks. The system for assessing corporate governance and financial risk management], Yzdatel'stvo "Ves' Myr", Moscow, Russia.

3. Yehorycheva, S.B. (2010), Innovatsijna diial'nist' komertsijnykh bankiv: stratehichni aspekty [Innovative activity of commercial banks: strategic aspects], TOV "ASMI", Poltava, Ukraine.

4. Loktev, A.V. (2011), "Foreign view on the constructiveness of state regulation of the banking sector in the global economic crisis", Sotsyal'no-ekonomycheskye iavlenyia y protsessy, vol. 1—2, pp. 148—152.

5. Martsyn, V.S. (2006), "Economic security as the main component of economic freedom during the period of globalization", Sotsial'no-ekonomichni doslidzhennia v perekhidnyj period. Yevrointehratsijnyj kurs Ukrainy: finansovyj vymir [Socio-economic research in the transition period. Eurointegration course of Ukraine: financial dimension], L'viv, Ukraine.

6. Krupka, I.M. (2009), Osoblyvosti rozvytku finansovoho rynku Ukrainy v umovakh hlobalizatsijnykh protsesiv // Natsional'ni finansovi systemy v umovakh hlobalizatsii: Monohrafiia. / Za red. I. O. Liutoho. - Ivano-Frankivs'k : Halyts'ka Akademiia, 2008, 306 s., pp. 97—123; Krupka I. M. Finansovyj rynok Ukrainy ta mizhnarodni finansovi potoky / I. M. Krupka // Finansy Ukrainy. № 12, pp. 104—116.

7. Schastnaia, T.V. (2012), "IRBAA (Basel II): advantages and disadvantages of methodology", Vestnyk Tomskoho hosudarstvennoho unyversyteta, vol. 1, pp. 122—128.

8. Khohart, H. (2011), "Resolving banking crises: the main tools and costs", Banky: myrovoj opyt, vol. 34, pp. 108—109.

9. Schodo intehratsii bankivs'koi systemy Ukrainy do bankivs'koi systemy Yevropejs'koho Soiuzu : analitychna zapyska [Elektronnyj resurs]. - Rezhym dostupu : http://www.niss.gov.ua

Стаття надійшла до редакції 09.01.2018 р.