УДК: 336.71

Васильчишин О. Б.
д.е.н., професор,
професор кафедри безпеки та
правоохоронної діяльності,
Західноукраїнський національний
університет, адвокат

Цар А. В.
здобувач освіти

Безпека банківської системи в умовах воєнної агресії

Сьогодні розвиток банківської системи супроводжується інтеграційними процесами банківського бізнесу практично в усіх галузях соціально-економічного життя країни шляхом упровадження нових банківських послуг та інновацій. Ураховуючи глибину інтеграції банківського бізнесу в економічні процеси країни, актуальним є питання розробки механізмів, заходів та методів підвищення рівня безпеки банківської системи, адже в разі навіть незначних економічних чи політичних дисбалансів підривається стабільність банківського сектора [1]. В умовах воєнної агресії банківська система держави, на яку спрямована дана агресія особливу увагу повинна спрямовувати на забезпечення безпеки від кіберзагроз для банків та їхніх клієнтів акцентуючи на таких аспектах, як:

- ✓ адаптивість банківського сектора до новітніх кіберзагроз;
- ✓ посилення відповідальності банків, у тому числі й фінансової, перед регулятором;
- ✓ віддалена робота банківських фахівців, що породжує зростання ризиків людського фактора;
- ✓ швидке оновлення шкідливого програмного забезпечення.

Варто врахувати, що жодна банківська установа в банківському секторі України не зацікавлена в поширенні інформації про кібератаку, якої вона зазнала. Причиною такої закритості є насамперед загроза підвищення репутаційних ризиків, оскільки така інформація, навіть у разі відбиття кібератаки, може призвести до відтоку клієнтів, які, мислячи за принципом «диму без вогню не буває», будуть забирати депозити, знижуючи ліквідність банку. Ще одним фактором небажання банків поширювати подібну інформацію є те, що така інформація приверне увагу інших зловмисників, які, маючи досвід і необхідні інструменти, можуть пройти через встановлені патчі і знову здійснити успішну кібератаку на інфраструктуру банку [2].

Запобігання загрозам, не тільки явним, але й потенційним є основою функціонування національної безпеки банківської системи [3] та завданням регулятора банківської системи. Враховуючи сучасні тенденції, Національний банк України сформував окремий інструмент для збору та обміну інформацією про інциденти інформаційної безпеки – MISP-NBU Центру кіберзахисту відповідно до Положенням про організацію кібербезпеки в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України [4]. По суті, це спеціалізований

веб-сайт Національного банку, який побудований на базі відкритої платформи MISP та призначений для організації доступу банків до системи збору, обробки, зберігання та обміну інформацією загального організаційно-технічного характеру в режимі реального часу з урахуванням вимог конфіденційності. Зауважимо, що таким чином, банківський сектор та регулятор знають про всі інциденти інформаційної безпеки.

Регулятор ретельно підійшов до питання формування ефективної системи кібербезпеки. Так, разом із прийняттям Закону України «Про критичну інфраструктуру» було затверджено Положення про організацію кібербезпеки в банківській системі України [5], в якому, серед іншого, описані чіткі вимоги до внутрішньої системи кібербезпеки українських банків, а саме:

- ✓ закріплено основні принципи організації кібербезпеки в банківській системі України;
- ✓ висвітлено принципи організації обміну інформацією між банками та регулятором;
- ✓ визначено заходи щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури банків;
- ✓ окреслено вимоги до проведення незалежного аудиту інформаційної безпеки в банківській системі України та ін.

Варто також зазначити, що регулятор чітко визначив покарання банку за неналежний рівень кіберзахисту. Згідно з чинним Положенням про застосування Національним банком України заходів впливу, кіберризики прирівнюються до ризиків фінансового моніторингу, а штраф за порушення відповідних вимог законодавства становитиме 0,01 відсотка від суми зареєстрованого статутного капіталу банку. Таким чином, збитки банків через порушення вимог безпеки критичної інфраструктури та реалізацію кіберзагроз проти конкретного банку через відповідні недоліки його кіберстійкості можуть проявлятися у втраті значних обсягів фінансових ресурсів, що негативно впливає на банківську діяльність, особливо з огляду на зниження економічної активності банків в умовах проведення військових дій на території України. Банки зобов'язані детально відстежувати потенційні загрози та ризики.

Так, якщо згрупувати найбільш типові кібератаки на банківський сектор, то можна виділити наступні об'єкти атак:

- ✓ конфіденційна або банківська таємниця;
- ✓ банківська інфраструктура;
- ✓ кошти клієнтів та банків;
- ✓ сайти банків та регуляторів.

Слід зауважити, що головною особливістю кібератак є психологічний характер та спрямованість на реалізацію так званого людського фактору. Технічно банки здатні захистити себе та швидко реагувати на кіберзагрози, в той же час фахівець банку може одним кліком відкрити зловмисникам доступ до внутрішнього периметру банку. Так, майже відсутні технічні особливості таких кібератак, а також втрати банків та банківського сектору в цілому від кіберзлочинців. Водночас особливості кіберзагроз можуть кардинально змінитися, оскільки виявлення нових вразливостей банківських програмних систем, пошук нових інструментів вторгнення тощо відкривають перед кібершахраями нові можливості для маніпулювання інформацією.

Підсумовуючи вищезазначене, виокремимо низку обов'язкових заходів

для мінімізації чи уникнення кібератак та кіберзагроз українському банківському сектору в умовах воєнної агресії, а саме: своєчасне оновлення версій програмного забезпечення до актуальних, що дозволить якнайшвидше закрити виявлені вразливості програмного забезпечення та кібербезпеки; проведення тестування на проникнення, що дозволить виявити проблеми взаємодії програмних систем банків, вузькі місця та забезпечить високу ефективність реагування на неочікувані кібератаки.

Водночас цих заходів може бути недостатньо, оскільки кіберзлочинці активно вдосконалюють шкідливий код, а також активно використовують додаткові інструменти для розширення можливостей проникнення у внутрішню інформаційну інфраструктуру банку, що є загрозою національної безпеки України в умовах воєнної агресії.

ЛІТЕРАТУРА:

1. Васильчишин О. Шляхи підвищення рівня фінансової безпеки банківської системи України в умовах політико-економічних дисбалансів. Причорноморські економічні студії. 2016. Випуск 7. С.215-219.
2. Kloba L., Kloba T. Cyber threats of the banking sector in the conditions of the war in Ukraine. URL: https://www.fkd.net.ua/index.php/fkd/article/view/3883/3693
3. Васильчишин О. Б. Економічна сутність фінансової безпеки банківської системи: проблема плюралізму підходів. Науковий вісник Міжнародного гуманітарного університету. 2017. № 28. С. 159-166.
4. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України. Постанова Правління Національного банку України від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
5. Положення про організацію кіберзахисту в банківській системі України. Постанова Правління Національного банку України 12 серпня 2022 року № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text