О.О. Колесник
ст. викладач

УПРАВЛІННЯ КІБЕРРИЗИКАМИ БАНКУ В ЕПОХУ ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА

Питання кібербезпеки потрапили в фокус уваги світової спільноти ще у 2012 р., коли кібератаки ввійшли до п'ятірки найімовірніших ризиків Глобального звіту про ризики Всесвітнього економічного форуму. На сьогодні

питанням кібербезпеки присвячені документи «Великої двадцятки» (G20), Базельського комітету з питань банківського нагляду (BCBS), ЄС включно з Європейським наглядовим органом (EBA), фінансових регуляторів США на чолі з ФРС, Банку Англії, Міжнародної організації комісій з цінних паперів (IOSCO), Міжнародної асоціації страхових наглядів (IAIS) [1] тощо.

Основні цілі кібератак – захоплення даних з інформаційних систем економічних агентів, отримання повного контролю над ресурсами їхніх комп'ютерів або виведення систем із ладу. До негативних наслідків належать прямі фінансові втрати банків, вихід із ладу їхніх IT-систем, перерви в роботі, втрата інтелектуальної власності та репутації, шкода інтересам третіх осіб (клієнтів, акціонерів, співробітників). Крім прямих збитків, кібератаки завдають чимало непрямих, зокрема втрат можливих прибутків, клієнтів, а також падіння курсу акцій та інші. Взаємозалежність між критичними чи не критичними IT-інфраструктурами зазвичай залишається непоміченою до виникнення аварійної ситуації. Україна пережила у 2017 р. кілька масштабних кібератак. Кібератака різновидом вірусу «Petya» виявилася найпотужнішою за весь час. Поширеність програми та швидке розповсюдження вірусу призвели до масштабного одночасного враження підприємств, фінансових установ, органів влади. Уражений сегмент становив 35.0% банківського сектору за чистими активами та 32.4% за депозитами населення. У більшості банків ускладнення в операційній діяльності тривали лише декілька днів, а доходи повернулися до норми менш, ніж за тиждень. Поодинокі банки ставали мішенями кібертатак і раніше, наприклад торік декілька фінансових установ отримали збитки через неправомірне використання хакерами міжнародної системи електронних платежів. Разом з тим чимало банків поки що нехтують питаннями кібербезпеки та не використовують успішний досвід протистояння кіберризикам в Україні та світі.

Беручи до уваги досвід боротьби з попередніми кібератаками та подолання їхніх наслідків, фахівці з інформаційної безпеки необхідно виокремити низку передумов для того, щоб кібератака досягнула мети:

– недостатній контроль за вхідним трафіком електронної пошти;

– відсутність налагодженої системи встановлення критичних оновлень безпеки для операційних систем;

– відсутність належно організованого створення резервних копій критичної інформації;

– використання одного адміністративного облікового запису з широкими привілеями для роботи в різних інформаційних системах.

Цьогорічні кібератаки підтвердили, що проблема має національний масштаб. Її можна вирішити, об'єднавши зусилля держави, фінансового та реального секторів економіки. Інакше кіберризики зростатимуть і можуть

перетворитися на суттєву загрозу для фінансової стабільності. Розуміючи це, НБУ запровадив заходи, що посилять стійкість банків до кібератак та зменшать негативні наслідки від них. 05 жовтня Верховна Рада України прийняла Закон України № 2163 «Про основні засади забезпечення кібербезпеки України», де НБУ названо серед основних суб'єктів національної системи кібербезпеки. Відповідно до ухваленого закону НБУ визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України; створює центр кіберзахисту Національного банку України.

Реагуючи на нові виклики, НБУ запропонував банкам комплексні рішення для мінімізації кіберризиків та усунення наявних кіберзагроз. 28 вересня ухвалено постанову Національного банку України № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». Положення встановлює обов'язкові мінімальні вимоги з організації заходів із забезпечення інформаційної безпеки та кіберзахисту; принципи управління інформаційною безпекою та вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами НБУ. Документ містить як комплексні настанови з розбудови системи інформаційної безпеки, так і вузькі технічні питання захисту банківської інформації [3, с. 56].

Раз у раз держави та міжнародні органи ухвалюють акти, у яких пропонують бізнесу правила управління кіберризиками, настанови для їх оцінки та для забезпечення стійкості до них, вимоги до страхування таких ризиків, а також організацію системи співпраці, щоб їм протистояти. Центробанки дедалі більшої кількості країн світу приділяють увагу кіберризикам та інформаційній безпеці у звітах про фінансову стабільність, а отже можна зробити попередні висновки про суттєвість існуючої загрози та необхідність подальшої розробки інструментів та методів управління кіберризиками комерційних банків.

Література:

1. Global Economic Forum, The Global Risks Report 2017. 12th Edition [Електронний ресурс]. – Режим доступу: http://wef.ch/risks2017. – Назва з екрана.
2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування: Аналітична записка // Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу: www.niss.gov.ua. – Назва з екрана.
3. Найбільші кібератаки в Україні з 2014 року. Інфографіка // Журнал Новое время [Електронний ресурс]. – Режим доступу: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika1438924.html. – Назва з екрана.