Кібербезпека у банківському секторі: чи допоможе IT-outsourcing?

Анастасія ПАВЛОВСЬКА,
юрист Sayenko Kharenko

Заріна ХАЛІМОН,
молодший юрист Sayenko Kharenko

Останнім часом функціонування інформаційних систем у світі виявило проблему недостатньої захищеності від комп'ютерних вірусів. BadRabbit, WannaCry, Petya та інші вражали несподівано, паралізуючи комп'ютерні системи різних установ та підприємств. Їх розробники хоча й мали подекуди різну мету та способи впровадження вірусних програм, однак базувалися на спільному підґрунті – недоліках і слабкостях системи кібербезпеки. Доволі ілюстративним у цьому питанні видається механізм дії вірусу Petya, який за кілька днів завдав мільйонних збитків українському бізнесу та державним установам. Вірус непомітно вражав популярну програму бухгалтерського забезпечення M.E.Doc., отримував доступ до адміністративних прав керування комп'ютерною системою та безперешкодно поширював власні копії.

Не стали винятком банківські установи, які повинні бути захищеними сучасним технічним та системним забезпеченням. Світовий досвід атак вірусів і значних фінансових втрат мав стимулювати, насамперед, саме фінансові установи до пошуку прогалин власних систем кіберзахисту та їх постійного оновлення. Однак 2017 р. показав фактичну неготовність українських банків захисти себе від подібних втручань у роботу їхніх інформаційних систем.

Загальна оцінка подій 27-29.06.2017 р. демонструє, що 70% українських банків так чи інакше постраждали від кібератак вірусу Petya. Видимим наслідком таких атак стала зупинка роботи терміналів, платіжних систем, відділень банків, а також обмежений доступ до інтернет-банкінгу та міжнародних переказів. Хоча банки продовжують стверджувати, що атаки негативно вплинули винятково на інфраструктуру системи Windows, а вірус не отримав доступу до персональних баз даних клієнтів, ніхто вже не може бути впевнений, що більш «витончена» програма не зможе цього зробити.

Той факт, що банки не витримали кібератак, наштовхує на висновок, що проблема криється не лише в IT-департаменті кожного окремого банку. Недооцінка потенційних загроз, відсутність належного програмного забезпечення та нехтування належним бюджетуванням систем кібербезпеки банку – все це свідчить про недостатність системного підходу до забезпечення кібербезпеки.

Постанова НБУ №95 та її наслідки

28.09.2017 р. Національний банк України прийняв Постанову №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» (далі – *Постанова*), якою зобов'язав банки протягом 2018 р. вжити заходів для посилення своєї кібербезпеки. Цей акт об'єднав у собі два етапи:

- до 01.03.2018 р. банки мають провести організаційні зміни – обов'язкове створення колективного органу з питань впровадження та функціонування систем управління інформаційною безпекою («СУІБ»), забезпечити у ньому представництво членів правління банку та призначення відповідальної особи за інформаційну безпеку банку, а також частково чи повністю оновити свої базові системи інформаційної безпеки та привести їх у відповідність до Міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002, PCI DSS, які закладені в основу Постанови;
- до 01.09.2018 р. мають бути впроваджені додаткові заходи посилення інформаційної безпеки – робота з носіями інформації, функціонування серверів банку та використання інструментів централізованого моніторингу.

Найбільш суттєві зміни повинні бути впроваджені вже до 01.03.2018 р. Насамперед, для банків буде важливо забезпечити належний розподіл прав доступу до інформаційних систем банку та періодичність їх контролю, використання механізмів багатофакторної автентифікації та відповідні стандарти шифрування, централізоване управління мережею банку та належний рівень документального оформлення таких процесів захисту інформації.

Таким чином, вже за тиждень банки мають бути готові представити свої оновлені системи кіберзахисту, які повинні відповідати більше ніж сотні вимог Постанови (*стаття підготовлена 23.02.2018 р. – прим. ред.*).

Водночас Постанова не передбачає спеціальних санкцій у разі порушення встановлених вимог. Однак, з огляду на ст. 73 Закону України «Про банки і банківську діяльність», можна виокремити види санкцій за порушення банківського законодавства, які можуть застосовуватися саме у випадку нехтування вимогами щодо вдосконалення систем кіберзахисту: письмове застереження; обмеження, зупинення чи припинення здійснення окремих видів здійснюваних банком операцій, у тому числі операцій з пов'язаними з банком особами; накладення штрафів; тимчасове (до усунення порушення) відсторонення посадової особи банку від посади.

Вірогідно, письмове застереження стане першим видом санкцій, що буде застосовуватися НБУ після виявлення невідповідності положенням Постанови та передбачатиме певний додатковий строк для впровадження нових систем кіберзахисту. У разі подальшого систематичного нехтування своїми обов'язками банки ризикуватимуть обмеженням окремих видів діяльності, які є найбільш вразливими до наслідків кібератак, або тимчасовим відстороненням посадових осіб, прямо відповідальних за впровадження положень Постанови

у діяльності банку. До того ж функціонування таких банків особливо привертатиме увагу НБУ, адже неготовність банку захистити свої інформаційні системи від можливих кібератак становить реальну загрозу для персональних даних клієнтів окремого банку та всієї банківської системи країни.

Впровадження послуг IT-outsourcing

Чи насправді банки готові у такі короткі строки самостійно розробити, профінансувати та запровадити всі необхідні заходити? Адже такі нововведення вимагають значних фінансових затрат і залучення кваліфікованих IT-професіоналів. Хоча пошук та впровадження програмного забезпечення не передбачає значних складнощів, проте знайти спеціалістів, які змогли б провести якісну оцінку недоліків систем та супутніх ризиків кібербезпеки, виявляється набагато складнішим завданням. У той час, коли ринок міжнародних компаній-інтеграторів (наприклад, Windows) володіє повним спектром необхідного програмного і технічного забезпечення, ринок національних спеціалістів у сфері систем кібербезпеки залишається дуже вузьким.

Таким чином, не кожен банк, що має IT-департамент, зможе встояти проти наступної атаки вірусу, адже найсильнішою гарантією безпеки для банку є саме підготовча робота, а також постійне оновлення систем та аналіз недоліків, які вимагають комплексної оцінки більш вузькоспеціалізованих фахівців.

Іншими негативними чинниками, що впливають на неспроможність банків самостійно покращувати власні системи кібербезпеки, є «застарілість» поглядів деяких спеціалістів IT-департаментів щодо впровадження сучасних методів захисту інформаційних систем, значні фінансові затрати на залучення вузькоспеціалізованих працівників, неналежне впровадження міжнародних стандартів ISO та недостатність зовнішньої незалежної оцінки систем безпеки банку.

Саме тому все більшого поширення набирають послуги IT-outsourcing для банків з метою якнайшвидшого приведення методів захисту їхніх інформаційних систем у відповідність до Постанови. Насамперед, такі послуги пропонують деякі IT-компанії, які проводять загальний технічний аудит та перевірку регламентного забезпечення функціонування систем захисту банку. Така перевірка має включати penetration test (тест на проникнення як метод оцінювання захищеності комп'ютерної системи), який допомагає виявити технічні недоліки інформаційних систем та визначити необхідний перелік потрібних систем безпеки. Однак чи є такий аудит достатнім для виявлення всіх потенційних ризиків?

Попередній комплексний аудит насправді є визначальним чинником розуміння недоліків інформаційних систем банку, однак лише першою стадією для оцінки всіх можливих ризиків. Адже поряд з інформаційно-технологічним аспектом також необхідна оцінка ризиків менеджменту та правового регулювання, які впливають на загальну політику банку щодо забезпечення інформаційної безпеки.

На жаль, перевірка лише регламентного забезпечення так само не зможе виявити ризиків неналежної роботи персоналу щодо забезпечення інформаційної безпеки та загалом ставлення адміністрації банку до попередження атак на інформаційні системи.

Отже, кібербезпека банків вимагає комплексного, чітко спланованого, поетапного проекту вдосконалення систем її захисту. Такий комплекс має включати три основні підходи щодо виявлення загроз для функціонування інформаційних систем банку:

• технологічний – першочерговий аудит, впровадження оновлених методів захисту та подальша оптимізація всієї IT-інфраструктури банку з метою не лише позбутися недоліків, але й попередити їх у майбутньому;

• робота з персоналом та адміністрацією банку – на цьому етапі необхідно не лише перевірити належне регламентне забезпечення роботи інформаційних систем, але й провести подальші роз'яснювальні роботи з персоналом; з іншого боку, це робота з керівництвом банку, що має забезпечити розуміння всіх можливих ризиків наступних кібератак та санкцій НБУ за невідповідність положенням Постанови;

• правове забезпечення, яке дозволило б належним чином врегулювати відносини між банком та IT-компанією щодо конфіденційності інформації.

Розробка такого комплексного проекту дозволила б побудувати довгострокові відносини між банками та вузькоспеціалізованими IT-компаніями, що надають послуги у сфері кібербезпеки. Адже якщо впровадження заходів щодо приведення інформаційних систем банків у відповідність до положень Постанови можливе із залученням лише окремих IT-компаній, то подальший захист від можливих кібератак, на жаль, не буде повністю забезпечений, оскільки лише постійна робота щодо запобігання вірусним загрозам зможе убезпечити банки від можливих матеріальних збитків.

Банкам необхідно зрозуміти, що санкції НБУ – це найменша загроза їхній роботі та існуванню, у порівнянні з вірусною атакою, яка наступного разу може вразити персональні бази даних клієнтів і призвести до масштабніших наслідків для функціонування всієї банківської системи. ЮГ

Цифрова Україна без правил гри у майнінг

Олександр ВАСИЛЕВСЬКИЙ,
юрист Asters

Назад у майбутнє

Криптовалюта, блокчейн, біткойн, токен, майнінг – це не слова з майбутнього, а термінологія сучасності, яка заполонила світ та активно розвивається.

Криптовалюта – це різновид цифрових грошей або їх сурогат, в основі якої лежить технологія шифрування даних. Криптовалюта не має фізичного вигляду, а існує лише в електронному. Її основними особливостями є анонімність, децентралізація та захищеність.

Ігнорувати не можна врегулювати

Директор-розпорядник Міжнародного валютного фонду (МВФ) Крістін Лагард назвала неминучим міжнародне регулювання операцій з криптовалютами. «Безперечно, це сфера, в якій необхідне міжнародне регулювання та належний контроль», – заявила Крістін Лагард в інтерв'ю CNN Money.

Наразі в Україні відсутні зрозумілі правила, необхідні для правового врегулювання обігу криптовалюти, проте активний розвиток криптовалютних відносин цього потребує. Адже все, що не заборонено законом – дозволено, а те, що заборонено – не дозволено законом.

Приміром, Республіка Білорусь пішла іншим шляхом. Декретом №8 від 21.12.2017 р. «Про розвиток цифрової економіки» було надано визначення основних термінів, пов'язаних з відносинами обігу криптовалюти, чим створено умови для впровадження в економіку технології реєстру блоків транзакцій (блокчейн).

Реалії сучасності вимагають правового врегулювання криптовалютних відносин в Україні, оскільки вакуум, що наразі існує, неминуче буде заповнюватися небезпечними явищами.

Оподаткування

Купили за одні кошти, продали за інші. Отримали прибуток, а хто сплатить податок? Це питання залишається неврегульованим в Україні, наслідком чого є недонаповнення бюджету. Як повідомлялося на CoinDesk, наприклад, Ізраїль має намір оподатковувати криптовалюту як капітал, а не як валюту. Тобто оподаткування має відбуватися на прибуток від збільшення такого капіталу.

В Україні достатньо власників криптовалюти, яка була куплена за ціною набагато нижчою, ніж її сьогоднішня вартість. Тобто вартість капіталу зросла, однак потреба у сплаті податку відсутня через неврегульованість.

Можливо, законотворцю варто задуматися над оподаткуванням криптовалюти за прикладом Ізраїлю…?

Ризик шахрайства та незаконного обігу

Відсутність чітких правил гри може привести до значних збитків для гравців такого ринку. За матеріалами Мінфіну, Уоррен Баффет вважає, що Bitcoin – це «справжня бульбашка», а ринок криптовалют чекає поганий кінець.

Пропозиція породжує попит, а попит породжує пропозицію. За словами Майка Макглоуна, стратега біржових товарів аналітичного підрозділу Bloomberg Intelligence, вартість найпопулярнішої валюти Bitcoin через постійне її клонування може рухнути на 90%.

Доказом відсутності стабільності вартості криптовалюти та маніпуляцій власниками основної маси наявної криптовалюти є значні коливання Bitcoin, які спостерігалися протягом останнього часу. При цьому учасники ринку криптовалют через відсутність прив'язки до реальних матеріальних активів так чи інакше несуть ризик отримання збитків вартості інвестованого.

Операції з криптовалютою проводяться анонімно, за технологією колективної обробки транзакцій та емісії учасниками мережі, без ідентифікації користувача. Тому з метою запобігання фінансування тероризму чи відмивання коштів ідентифікація сторін операцій з криптовалютою була б доречною.

Водночас ажіотаж криптовалюти базується саме на анонімності та децентралізації, а тому час покаже, чи не знецінить ринок ідентифікація учасників.

І насамкінець...

Хоче цього хтось чи не хоче, але ринок обігу криптовалюти в Україні потребує правового врегулювання. Час не стоїть на місці… В епоху IT не можна залишатися осторонь або ховатися від того, що відбувається. До всього потрібно пристосовуватися. На вказані обставини має звернути увагу, насамперед, законотворець і контролюючий орган та нарешті врегулювати криптовалютні відносини, надавши їх учасникам чіткі та зрозумілі для всіх правила гри. ЮГ