СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРБЕЗПЕКИ БАНКІВСЬКОГО СЕКТОРУ: ВІТЧИЗНЯНІ РЕАЛІЇ ТА ЗАРУБІЖНИЙ ДОСВІД

Паламарчук В. В.
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій Національної академії Служби Безпеки України м. Київ, Україна

Сьогодні поняття кіберзлочину охоплює цілу низку правопорушень, зокрема: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж тощо (так зване «хакерство»); фальшування й шахрайства за допомогою комп'ютера, наприклад, фішинг (незаконний спосіб отримання персональної інформації – паролів, номерів банківських рахунків чи кредитних карт тощо шляхом розсилання від імені банку електронних листів з посиланнями на підроблені сайти, які імітують роботу справжніх, або створення точної копії існуючої банківської веб-сторінки, аби змусити користувача ввести свої особисті фінансові дані) чи його різновид фармінг (при вході на веб-сторінку справжньої установи відбувається переспрямування на підроблену сторінку); правопорушення у сфері інформаційних ресурсів, приміром, дитяча порнографія чи розповсюдження піратського контенту, та ін.

Походження кіберзлочинів пов'язане зі, здавалося б, малошкідливим бажанням хакерів засвідчити свою високу майстерність за допомогою впровадження різних комп'ютерних вірусів. Але доволі швидко зловмисники зрозуміли, що це може приносити великий зиск. Так виникла нова «галузь» злочинного бізнесу, котра знайшла собі застосування в багатьох інших сферах – діяльності розвідок, промисловому шпіонажі, тероризмі та ін. Особливої актуальності ця сфера набула для банківського сектору.

Слід також зазначити, що поширенню кіберзлочинності посприяла недосконалість регуляторних механізмів, створення яких не встигало за стрімким розвитком всесвітньої комп'ютерної мережі. Кіберзлочинці миттєво реагують на всі новації у цій сфері, тоді як неповороткі державні структури й розробники систем інформаційної безпеки роблять це значно повільніше. У той час, коли злочинні кібератаки набувають загрозливої регулярності, стають усе більш складними й витонченими, виявляються вже постфактум або не виявляються зовсім, здійснюються віддалено й анонімно, існуючі системи контролю за несанкціонованим

проникненням та противірусні програми дуже швидко застарівають і не в змозі забезпечити належний захист [1, с. 53].

Загрози, що виникають у кіберпросторі функціонування банківських установ, такі ж численні й різноманітні, як і сам цей простір. Їм притаманні масштабність, взаємозв'язок, швидкість поширення, складність розуміння загроз й реагування на них. При цьому від кібератак, які здійснюються не лише з географічно віддалених місць, а й із-за меж фізичного простору – у цифровому кібернетичному просторі, не існує ідеального захисту. Постійне вдосконалення інтернет-технологій зумовлює відповідне зростання небезпечності, швидкості й руйнівної потужності кібератак, проводити які стає все простіше й дешевше, тоді як захист від них потребує все більших зусиль і витрат. Відтак, сьогодні маємо чимало прикладів, коли один комп'ютерний злодій викрадає більше грошей, ніж великі банди грабіжників банків.

Ситуація ще більше ускладнюється тим, що сама природа Інтернету суперечить традиційним уявленням про те, що і суверенні країни, і бойові дії прив'язані до географії та фізичного місцезнаходження. Компанія може мати головний офіс в одній країні, а мережі й сервери – в іншій. Якщо кібератаку спрямовано проти цих мереж і серверів, хто має реагувати: країна, де розташовано головний офіс, чи країна, де розміщено мережі й сервери? Якщо, не реагуватиме жодна із цих двох країн, а натомість корпорація захищатиметься сама, організувавши власний кібернаступ, то хто ще опиниться втягненим у цю ситуацію? Якщо немає міжнародних норм і договорів, що дають визначення і встановлюють межі кіберконфліктів, то кібервійна може відбуватися між двома країнами, а може – між країною і окремим комерційним банком.

Протягом сотень років пограбування банку передбачало, що в приміщення вдираються озброєні люди, набивають міхи грошима й зникають у невідомому напрямку. Відповідальність за те, щоб знайти, затримати і покарати крадіїв, було покладено на правоохоронців. Нині правоохоронні органи та спец служби зіштовхнулись із запитанням: як уряду трактувати кібератаки, що спустошують рахунки розташованого на їх території комерційного банку, – як напад на їхню державу, як пограбування чи як щось зовсім інше? Відповідно постає необхідність розробки критеріїв трактування подібних інцидентів, з метою їх чіткої класифікації на предмет загроз безпеці людині, суспільству, державі з подальшою їх правовою оцінкою.

Це ж стосується й можливостей терористів, коли лишень один комп'ютер може спричинити більш тяжкі катаклізми, ніж цілий арсенал традиційної зброї. На жаль, така тенденція швидко посилюється, вагомих аргументів до її стримування поки що не видно, й сучасна кіберзлочинність набуває характеру глобальної цифрової епідемії.

Зважаючи безпекові виклики, пов'язані із забезпеченням кібернетичної безпеки банківського сектору, абсолютно слушною убачається теза, що «конструкція Інтернету впливає на соціальні відносини, які виникають навколо глобальної мережі, і сприяє формуванню кіберкультури – специфічної форми культури інформаційного суспільства» [2, с. 23]. Відтак, створена людським розумом і працею віртуальна реальність, глобальна всесвітня мережа Інтернет стають моделлю буття соціуму, чинником соціальної дійсності, який усе більше впливає як на свідомість окремого індивіда, так і на групову, масову, загальносуспільну свідомість. Усе зростаючими темпами відбувається загальна «віртуалізація» індивідуального й суспільного життя, про що, зокрема, свідчить поширення таких явищ, як віртуальні гроші, інтернет-торгівля, віртуальне навчання, електронне урядування і т. д. Тобто феномен віртуальної реальності давно вийшов за межі комп'ютерної техніки й інформаційно-телекомунікаційних мереж, у кіберпросторі закладені й уже реалізуються величезні комунікативні, медійні, пізнавальні, управлінські та інші потенції, широкі можливості керування фінансовими потоками, реалізації демократичних процедур тощо.

Однією з останніх вірусних мутацій і кібератак за її допомогою, що безпосередньо торкнулися банківського сектору, є WannaCry, або Petya (2017 рік). Характерною особливістю цього вірусу було не те, що він шифрував дані, блокував доступ до них і вимагав за відновлення електронні гроші – Біткоїни. Головне, що він на доволі тривалий час зупинив роботу третини банківської системи всієї України. Це вельми негативно позначилося й на роботі авіатранспорту, метрополітену, деяких великих медіа- і промислових компаній. Дію вірусу першими відчули працівники бухгалтерій, котрі працювали з робочою програмою «1С» для подання бухгалтерської звітності, через яку вірус проникав у систему, а потім поширювався через неліцензійне програмне забезпечення. Petya показав, що кібератаки вірусних «мутантів» можуть призвести до тяжких наслідків, до зупинки роботи державних органів та інших об'єктів критичної інфраструктури. Таких масштабних проблем можна було б уникнути, якби об'єкти нападу та їх персонал знали й дотримувалися базових правил кібербезпеки та кібергігієни.

Є всі підстави вважати, що наступні мутації кібератак можуть впливати на безпеку банківського сектру. Приблизно від середини 2010-х років у світі стрімко поширюється новий IT-тренд на розумні пристрої і девайси – розумні годинники, холодильники, пилотяги, фітнес браслети, шоломи віртуальної реальності, окуляри доповненої реальності тощо. У 2016 році в Одесі під час конференції «Black SeaSummi» вперше в Україні людині вживили електронний чіп в руку, котрою вона могла оплачувати рахунки, як банківською картою [3].

Згодом в інших країнах розпочали активно імплантувати чіпи, які замінюють ключі, географічні мапи, ідентифікаційні дані, а в 2019 році проект «xNT» почав розсилати своїм клієнтам чіпи для вживлення в руку. Корпорація Apple започаткувала тренд на FaceID, який дозволяє ідентифікувати людину й розплачуватися на касі просто по обличчю.

Усе це яскраво засвідчує, що електроніка стає все ближчою до тіла, до м'язів, очей, до мозку людини, у прямому сенсі до її змісту. А відтак, існує серйозний ризик, що кібератаки можуть безпосередньо позначитися на фізичному стані людини, її здоров'ї. І чим ближче різноманітна апаратура наближена до тіла і мозку, тим більшого значення набуває захист відповідної інформації та її носіїв. Отже, наступною стадією відповідальності кібербезпеки має стати збереження інформації, процесів і девайсів, котрі щільно пов'язані з тілом і мозком, тобто фізичним життям людини. Ці та ряд інших тенденцій значно розширюють поле кіберзахисту для клієнтів банківського сектору, але одночасно й провокують нові виклики та загрози. У цьому контексті кібербезпека банківського сектору має стати архіважливою складовою політик кібербезпеки держави.

Література:

1. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи; Одеса : Фенікс, 2020. 404 с.
2. Абетка медіа / За загал. ред. В. Ф. Іванов; Переклад з нім. В. Климченка. Київ : Академія української преси, Центр вільної преси, 2015. 177 с.
3. Украине впервые вживили чип в руку человека. Корреспондент.net, 10 сентября 2016. URL: https://korrespondent.net/ukraine/3743253-v-ukrayne-vpervye-vzhyvyly-chyp-v-ruku-cheloveka
4. xNT NFC Chip. URL: https://dangerousthings.com/product/xnt/