УДК 67.401.212.73
DOI: 10.31673/2409-7292.2019.025459

В.М. Ахрамович, В.М. Чегренець

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМЕРЦІЙНОГО БАНКУ

Розглянуті основні компоненти кібербезпеки банків: загрози інформаційній безпеці і вразливості; методи визначення та оцінювання ризиків ІБ; політика безпеки банківських установ; особливості управління інформаційною безпекою; заходи інформаційної безпеки в системі електронних платежів та системи S.W.I.F.T.; забезпечення безпеки мережі банкоматів; вимоги до приміщень банків; побудова системи управління інформаційною безпекою.

Ключові слова: кібербезпека, банки, захист інформації, ризики, інформаційна безпека, політика безпеки, електронні платежі, система S.W.I.F.T, мережі банкоматів, шифрування, програмне забезпечення, витік інформації.

Вступ

Безпека банку визначається як стан стійкої життєдіяльності, при якому забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування.

Тому у процесі розроблення концепції управління банківською діяльністю варто виділити основні процеси функціонування банку і виключити можливість витоку інформації, її несанкціонованого використання, нанесення збитків, упущення вигоди з боку всіх зацікавлених сторін і в напрямі досягнення основних цілей банківської діяльності. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління банківською діяльністю, до якої сьогодні залучаються дедалі більше банків.

Основна частина

1. Загрози інформаційній безпеці банківської установи. Вразливості

В інформаційних взаємовідносинах суб'єктів господарювання (зокрема, банків) можуть виникати два види загроз: загрози, пов'язані з посяганням на їх інформаційні ресурси (переважно ту частину, яка має обмежений доступ) – загрози інформації та загрози, що виникають під час формування інформаційного середовища (умов) діяльності таких суб'єктів – інформаційні загрози.

Як свідчить досвід, основними способами реалізації таких загроз є [4]:

маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);

порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправне збирання і використання інформації;

руйнування та використання з протиправною метою чужих інформаційних ресурсів;

інформаційний тероризм (поширення комп'ютерних "вірусів", установлення програмних та апаратних пристроїв, призначених для несанкціонованого отримання інформації, упровадження радіоелектронних приладів перехоплення інформації, незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

Джерелами загроз інформаційній безпеці банку можуть бути як зовнішніми, так і внутрішніми.

Процес управління ризиками інформаційної безпеки повинен здійснюватися для банку в цілому і зокрема включати:

аналіз та ідентифікацію ризиків;

оцінювання ризиків з точки зору їх впливу на бізнес та ймовірності їх появи;

інформування особи, яка вправі приймати рішення та акціонерів банку про ймовірності та впливи цих ризиків (ймовірність і наслідки ризику мають бути зрозумілими);

встановлення порядку та пріоритетів оброблення ризиків;

становлення пріоритетів виконання дій щодо зниження ризиків;

участь керівництва в процесі прийняття рішень щодо управління ризиками та його поінформованість щодо стану справ в управлінні ризиками;

ефективний моніторинг та регулярний перегляд ризиків і процесу управління ризиками;

інформування керівництва та персоналу щодо ризиків і дій щодо управління ними.

Процес управління ризиками інформаційної безпеки у банку є безперервним процесом і до нього може бути застосована модель ПВПД (плануй – виконуй – перевіряй – дій), наведена у вступі стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Найбільш поширені методи визначення та оцінювання ризиків ІБ, більшість з яких можна застосовувати в банківських структурах.

1. CRAMM (the UK Government Risk Analysis and Management Method).

Метод CRAMM було розроблено службою безпеки Великої Британії та взято на озброєння як державний стандарт.

2. Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінювання ризиків NIST Національного інституту стандартів і технологій США (National Institute of Standards and Technology), зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems).

3. OCTAVE. Методику OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблено в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

4. Наступним програмним забезпеченням є експертна система Risk Watch (розроблено компанією Risk Watch, США), яка презентує себе як потужний засіб аналізу та управління ризиками.

5. Метод COBRA (Consultative Objective and Bi-Functional Risk Analysis, developer – C & A Systems Security Ltd, Велика Британія) орієнтовано на підтримку вимог стандарту ISO 17799.

6. Методика Facilitated Risk Analysis Process (FRAP) передбачає, що на початковому етапі в системі відсутні засоби і механізми захисту. Таким чином, оцінюється рівень ризику для незахищеної інформаційної системи, що надалі дозволяє показати ефект від впровадження системи захисту інформації (СЗІ).

7. ISAMM (Бельгія).

Методику ISAMM було розроблено на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, виражаючи їх через щорічні очікувані збитків в грошових одиницях.

8. Mehari (Франція).

Це модель управління ризиками, з модульними компонентами і процесами. Модуль оцінювання охоплює, крім інформаційної системи, організацію та її місце розташування в цілому, а також умови роботи, правові та нормативні аспекти.

9. EBIOS (Франція).

EBIOS є повним набором посібників: кращі практики, а також додатки до документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як у державному, так і комерційному секторі.

10. Magerit (Іспанія). Magerit є відкритою методологією аналізу та управління ризиками.

2. Політика безпеки банківських установ

Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою правління Національного банку України від 28 вересня 2017 року № 95 зобов'язує банки [1]:

розробити та впровадити політику інформаційної безпеки, яка має містити:

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

4) визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки;

забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік;

затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін;

розробити та затвердити стратегію розвитку інформаційної безпеки. Банк має право затвердити стратегію розвитку інформаційної безпеки банку в документі, яким затверджено загальну стратегію розвитку банку, у вигляді окремого розділу. Зміст стратегії має узгоджуватися з політикою інформаційної безпеки банку, основними стратегічними цілями банку, що пов'язані із впровадженням нових бізнес-процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховувати планування розвитку інфраструктури банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

Відповідно до Методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків за стандартами Національного банку України система управління ризиками банківської діяльності повинна будуватися на основі міжнародного стандарту ISO/IEC 27005 "Information technology – Security techniques – Information security risk management" (Управління ризиками інформаційної безпеки) з урахуванням особливостей діяльності банків України, стандартів і вимог Національного банку України з питань інформаційної безпеки [3,4].

Виділимо такі основні етапи розроблення політики інформаційної безпеки:

визначення та оцінювання інформаційних активів;

визначення загроз безпеці;

оцінка інформаційних ризиків;

визначення відповідальності;

створення комплексного документа;

реалізація;

управління програмою безпеки.

Основою для формування політики інформаційної безпеки банківської установи можна визначити:

характеристику об'єкта застосування;

аналіз поточного стану захисту інформаційної інфраструктури банку;

облік можливих негативних факторів впливу та ймовірність їх реалізації;

створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки.

Політика інформаційної безпеки банку повинна бути затверджена керівництвом банку та доведена до відома всього персоналу та за необхідності до зовнішніх сторін.

3. Побудова системи управління інформаційною безпекою в банківських установах

3.1. Особливості управління інформаційною безпекою в банківських установах

Велику кількість компонентів, які формують банк як об'єкт інформатизації, можна подати сукупністю чотирьох груп: персонал, технічні засоби інформатизації, програмне забезпечення, документи.

Ці групи зазнають впливу різного роду специфічних факторів і, взаємодіючи між собою, впливають одна на одну, формуючи відповідний стан інформаційної безпеки банку. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи, зокрема, щодо захисту інформації призводить до покращення якостей безпеки по одних параметрах і погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки банку.

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави у банківському секторі.

У найзагальнішому розумінні, банки оперують чужими грошима, щоб створити свій прибуток. Тому інцидент інформаційної безпеки в банку в більшості випадків призводить до реальних втрат реальних грошей, тобто до прямих збитків. Не будемо забувати і про репутаційні втрати, штрафні санкції, тощо. Постанова правління Національного банку від 28.08.2017 № 95 дає поняття "критичний бізнес-процес банку", навколо якого і повинна будуватися вся система управління інформаційною безпекою [1].

В кінцевому підсумку, банківська система – це частина критичної інфраструктури держави, збої в роботі якої можуть привести до жахливих наслідків для всієї фінансової системи.

3.2. Заходи інформаційної безпеки в системі електронних платежів (СЕП)

Технологічні засоби контролю, вбудовані в програмно-технічні комплекси СЕП, не можуть бути відключені. У разі виявлення нестандартної ситуації, яка може свідчити про підозру щодо несанкціонованого доступу до СЕП від імені певного учасника СЕП, ЦОСЕП автоматично припиняє приймання початкових електронних розрахункових документів та повідомлень від цього учасника [2].

Основним засобом шифрування файлів (пакетів) СЕП є АКЗІ. Робота АКЗІ контролюється вбудованими в ЦОСЕП і АРМ-СЕП програмними ЗЗІ і забезпечує апаратне шифрування (розшифрування) інформації за алгоритмом, визначеним у національному стандарті України ДСТУ ГОСТ 28147:2009.

Як резервний засіб шифрування в СЕП використовується вбудована в ЦОСЕП і АРМ-СЕП функція програмного шифрування.

Засоби шифрування ЦОСЕП і АРМ-СЕП (як АКЗІ, так і програмне шифрування) забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді.

АРМ-СЕП і ЦОСЕП у режимі реального часу забезпечують додаткову сувору взаємну автентифікацію під час установлення сеансу зв'язку.

Під час роботи АРМ-СЕП створює журнали програмного та апаратного шифрування і захищений від модифікації протокол роботи АРМ-СЕП, у якому фіксуються всі дії, що ним виконуються, із зазначенням дати та часу оброблення електронних банківських документів. Наприкінці банківського дня журнали програмного та апаратного шифрування і протокол роботи АРМ-СЕП підлягають обов'язковому збереженню в архіві.

Банк у разі застосування криптографічного захисту зобов'язаний використовувати криптографічні алгоритми з визначеного НБУ переліку.

Заходи безпеки інформації включають:

1. Контроль доступу до ресурсів АБС (управління доступом)
2. Ідентифікація і аутентифікація АБС (користувачів процесів і т.д.)
3. Реєстрація та аналіз подій, що відбуваються в АБС.
4. Контроль цілісності об'єктів АБС.
5. Шифрування даних.
6. Резервування ресурсів і компонентів АБС.

3.3 Система S.W.I.F.T. та інформаційна безпека

Для поліпшення працездатності і захисту від збоїв в системі S.W.I.F.T. II застосовується дублювання кожного SCP і резервування роботи кожного SP. У будь-який час тільки один SCP є активним і здійснює безпосереднє управління системою. Решта три SCP постійно знаходяться в резерві і безперервно оновлюють свої статки за даними конфігурації активного SCP. У функції управління SCP входить:

дозвіл відкриття нового сеансу і зберігання даних сеансу;

поширення нового програмного забезпечення по системі;

функціональний контроль всіх технічних і програмних засобів;

збір діагностичної інформації про несправності;

управління процесом відновлення після помилки;

динамічний розподіл системних ресурсів.

Комутаційні процесори SP керують маршрутизацією і зберіганням повідомлень. Основні функції SP:

- маршрутизація повідомлень між користувачами через RP;
- надійне зберігання двох копій всіх оброблених даними SP повідомлень (на двох різних носіях) і відповідної їм передісторій доставки;
- формування підтверджень про зберігання, доставку оброблених даними SP повідомлень або їх недоставки;
- обробка вибірки повідомлень.

Регіональний процесор RP здійснює логічне підключення користувачів до мережі S.W.I.F.T. II і, по суті, є вхідною і вихідною точкою системи. Програмне забезпечення RP, взаємодіючи з програмами користувача, здійснює точне і безпечне логічне підключення до S.W.I.F.T. II. У його функції входить:

- перевірка вхідних повідомлень до пересилання в SP;
- обробка протоколів прикладного рівня;
- контроль і перевірка номерів вхідної послідовності (ISN) всіх повідомлень;
- верифікація контрольних сум повідомлень;
- формування позитивних (ACK) і негативних (NAK) підтверджень прийому повідомлень.

Фізична безпека

Здійснюється на основі розмежування і контролю доступу до всіх операційних і адміністративним вузлів S.W.I.F.T. шляхом використання електронних засобів і засобів виявлення несанкціонованого доступу. Застосовується також дистанційне керування для вузлів S.W.I.F.T. II, які управляються автоматично. Якщо користувач запитує центр про доступ до SAP, то в обов'язковому порядку повинен бути зроблений запит до CIO і без його санкції нікому не буде дано дозвіл на доступ до SAP.

Безпека логічного доступу до системи S.W.I.F.T. II

Як вже говорилося вище, користувачі можуть отримати фізичний доступ до системи S.W.I.F.T. II тільки через CBT, що працює з одним або більше LT. Кожному LT призначаються унікальні таблиці безпеки для процедур LOGIN і SELECT (вибір фінансового додатки - FIN), які представляють собою послідовності ключів в табличному вигляді.

3.4 Забезпечення безпеки мережі банкоматів

Принцип дії

Після завантаження карти в кардридер банкомата тримачу карти пропонується ввести секретний код (Пін-код) для авторизації картотримача. Далі пропонується вибір доступних операцій (при виборі операції також може запитуватися Пін-код; це залежить від конкретних налаштувань конкретного банкомата). Після вибору операції банкомат шифрує отриману інформацію (уміст магнітної смуги/чипа, уведений Пін-код, запитану операцію) і передає дані в процесинговий центр банку-банка-еквaєра.

Банк-Екваєр відправляє в платіжну систему запит на проведення операції. Платіжна система маршрутизує запит у банк-емітент (банк, що видав карту) і, одержавши згоду або відмову (код авторизації), передає банкомату команди на виконання або відхилення запиту. При цьому всі дії по відправленню запиту, обробці відповіді на запит, видачі/прийманню грошей з касет фіксуються, що дозволяє провести розслідування у випадку, якщо операція оскаржена.

Тому що Пін-код відомий тільки тримачу карти, операції, підтверджені Пін-кодом, уважаються виконаними безпосередньо тримачем карти.

Велике значення для захисту мереж банкоматів являє дотримання всіх правил безпеки викладених вище та деяких специфічних, наприклад, підсистема «ATM-Інтелект» платформи

«Інтелект» дозволяє включити в комплекс безпеки банку розподілену систему охорони банкоматів. У таку систему входять локальні відеоохоронні системи банкоматів і централізовані робочі місця, що дозволяють оперативно отримувати тривожні повідомлення від банкоматів, повідомлення про технічні неполадки локальних систем і відеокадри. Спеціалізований інтерфейс дозволяє вести претензійну роботу по операціях на будь-якому банкоматі віддалено, без виїзду на об'єкт; локальна відеоохоронна система встановлюється безпосередньо в банкоматі і здійснює запис з відеокамер банкомату. Ця система отримує від ПЗ банкомату інформацію про транзакції і сигнали від датчиків банкомату і синхронізує ці дані з відеозаписом. Система передає на пульт дистанційного відеоконтролю (ПДВ) і пульт контролю технічного стану (ПКТС) тривожні повідомлення, а також дані про технічний стан свого обладнання і устаткування банкомату.

3.6 Вимоги до приміщень банків

Ці вимоги викладені в Правилах з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи N 493 (z0049-08) від 29.12.2007

Вони стосуються приміщень з обмеженим доступом, серверних приміщень, приміщень електронних архівів, екранованих приміщень.

Висновки

Сьогодні успішне функціонування будь-якого банку неможливо без чіткої і організованої системи управління інформаційною безпекою, яка відповідає багатьом стандартам і правовим актам. Це робить рівень інвестицій в інформаційну безпеку дуже високим, рівно як і вимоги до діючих на ринку банкам, однак це єдиний спосіб залишитися на ринку.

Необхідність кібербезпеки банків обумовлена тим, що в реальних умовах роботи банківських установ науковцям необхідно розробляти методи захисту інформації, сучасної криптографії для застосування їх в процесі створення безпечних комп'ютерних систем, віртуальних банків для функціонування електронних грошей (інтелектуальні пластикові картки (смарт-картки), сервер-схеми. Концепція кібербезпеки, банків потребує від науковців вирішити сучасні проблеми: організаційні, правові, технічні і криптографічні методи захисту інформації, криптографічні протоколи, методи цифрового підпису, управління ключами, задачі та ресурси криптографії в мережі Internet.

Кібербезпека є процес, а не результат. Це може означати тільки одне: неможливо «купити» абсолютний захист. Затрати (гроші, ресурси, люди, час) на забезпечення потрібного рівня конфіденційності тільки знижує ймовірність ризиків до визначеної межі, зменшує вартість можливого збитку. Передбачати можливі збитки, управляти інформацією більш розумно і направлено допомагає кібербезпека.

Список використаної літератури

1. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17.

2. Правління Національного банку України. ПОСТАНОВА № 705 Про здійснення операцій з використанням електронних платіжних засобів.2014 р.

3. Національний банк України. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Стандарт організації України. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). Видання офіційне. Київ. Національний банк України. 2010 СОУ Н НБУ 65.1 СУІБ 1.0:2010

4. Національний банк України. СОУ Н НБУ 65.1 СУІБ 2.0:2010. Стандарт організації України. Настанова. Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD). Видання офіційне. Київ. Національний банк України. 2010 СОУ Н НБУ 65.1 СУІБ 1.0:2010

Надійшла: 01.06.2019 Рецензент: к.т.н. Шуклін Г.В.