УДК 004.413.4:004.056:004.738.5:336.71

Сергій Васильович Мартиненко, Григорій Олексійович Кравцов

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ОПЕРАЦІЙНІ РИЗИКИ БЕЗПЕКИ ЕЛЕКТРОННОГО БАНКІНГУ

Анотація: Розглядаються операційні ризики безпеки електронних банківських операцій та послуг. Наводиться ідентифікація цих ризиків, відповідно до рекомендацій Базельського комітету по банківському нагляду. Призначається для аудиторів та спеціалістів з інформаційної безпеки банків.

Розвиток технологій в комп'ютерних і телекомунікаційних системах, застосування їх банківських автоматизованих системах збільшують залежність банків від надійності цих систем. Такий розвиток і більш широке застосування інформаційних технологій (ІТ) в банківській справі мають «дві сторони медалі»:

- з одного боку, дозволяють значно розширити перелік банківських послуг і залучити нових клієнтів тощо;
- з другого боку, шкала банківських ризиків та пошкодження (збитки), які вони можуть нанести, змінюються більш швидкими темпами.

Наприклад, потенційне пошкодження, яке може виникнути від аварійного режиму або пошкодження ІТ, призведе до неможливості виконання технологічних процесів банківського виробництва. Пошкодження конфіденційності даних, пошкодження цілісності (спотворення або фальсифікація даних) тощо – все це може мати негативні наслідки, починаючи від недостовірності даних, некоректних записів на банківському рахунку, аж до змінення інструкцій платежу або наказів з перерахуванням коштів до третьої сторони - шахрая.

Темі управління ризиками інформаційної безпеки присвячено багато публікацій та досліджень. Першим етапом управління ризиками є їх ідентифікація, яка здійснюється на основі аналізу кожної конкретної системи за категоріями ризиків [1]. Враховуючи, що на сьогодні в банківській системі України відсутні стандарти аудиту інформаційних банківських систем, розглянемо тут питання ідентифікації ризиків безпеки, відповідно до рекомендацій Базельського комітету по банківському нагляду (Basle Committee on Banking Supervision).

Базельський комітет по банківському нагляду звертає увагу банків на сучасні проблеми управління ризиками [2]-[8], які пов’язані з автоматизованими технологіями ([3], [4], [6]-[8]). Публікації [2]-[8], які базуються на рекомендаціях інспекторів Базельського комітету та банкірів країн G10, підкреслюють цілий ряд тенденцій і проблем, що пов’язані із зміною профілю банківського ризику [6].

Є багато різних визначень терміну **„**ризик", що відображає те, що під цим терміном різні люди мають на увазі різні речі. Надамо визначення ключових термінів з точки зору інформаційної безпеки:

Електронна банківська справа (електронний банкінг) *(e-banking)* означає здійснення банківських операцій та надання банківських послуг з використанням автоматизованих банківських систем, у тому числі електронними каналами зв'язку (визначення Базельського комітету).

Підкреслимо дві фундаментальні риси e-banking – це характер/природа каналів доставки, через які здійснюються операції, та спосіб/метод для клієнтів отримати доступ до цих каналів. Загальні канали доставки включають „закриті" та „відкриті" мережі. **„Закриті мережі"** обмежують доступ учасникам (фінансові установи, клієнти, торговці та треті особи - сервіс-провайдери), які пов'язані угодами за термінами членства. „**Відкриті мережі"** не мають вимог щодо членства.

Операційний ризик *(Operational Risk)* – ризик втрат/збитків, які можуть виникнути внаслідок неадекватних або невдалих внутрішніх процесів, роботи/дій людей та систем або внаслідок зовнішніх подій. Це визначення може містити законодавчий/юридичний ризик, але виключає стратегічний та системний ризик (визначення Базельського комітету).

Управління ризиками (*Risk Management)* – включає функції: ідентифікації уразливостей та загроз, вимірювання та оцінювання ризиків, які властиві електронній банківській справі, моніторинг таких ризиків та вжиття оперативних заходів щодо їх мінімізації, контроль та аудит ризиків (визначення Базельського комітету).

Ризик *(Risk)***:**

Одне з самих стислих визначень ризику дається Комісією ЄС [9], та стандартом ЄС ETSI (European Telecommunications Standards Institute) [10] - „*Ризик: добуток впливу (impact) та небезпеки (hazard)*".

В цьому визначенні ризик є деякою величиною (значенням) від комбінації загроза-уразливість, тобто це більш є визначенням ***величини (рівня) ризику,*** яка відображає значення вірогідної втрати або збільшення витрат, які можуть відбутися, як результат специфічної комбінації загроза-уразливість. На практиці величина ризику часто визначається якісно, а не кількісно – як ряд рівнів для впливу та небезпеки, наприклад, - максимальний, низький або середній.

Визначення ризику надається Міжнародною Організацією по Стандартизації (ISO) як „*потенційна можливість (ймовірність), що дана загроза експлуатуватиме уразливість активу або групи активів, щоб*

викликати втрату або пошкодження щодо активів. Вплив або відносна небезпека ризику пропорційна бізнес значенню втрати/пошкодження та оціненій частоті загрози." [11].

Найбільш загальний, на нашу думку, термін ризику використовується міжнародною асоціацією аудиторів інформаційної безпеки ISACA (Information Systems Audit and Control Association) як „*можливість (ймовірність) здійснення дії або події, яка мала б несприятливий результат на організацію та її інформаційні системи*. "

Уразливість *(Vulnerability)* - це особливості інформаційних ресурсів, які можуть експлуатуватися загрозою, щоб викликати пошкодження.

Альтернативні визначення:

„*Слабкість (weakness) в процедурах безпеки системи, проекті системи, реалізації системи або внутрішніх засобів контролю, які могли б експлуатуватися, щоб порушити безпеку системи.*" (ISACA)

„*Слабкість в інформаційній системі, яка може дозволити порушення*" (INFOSEC S2001 [9],[10])

Загроза *(Threat)*

„*Будь-яка ситуація або подія, яка має потенційну можливість зашкодити системі*." (ISACA).

Альтернативні визначення:

„*Загроза: потенційний дія або подія, яка може викликати втрату одного або більше аспектів безпеки інформаційних систем*." (INFOSEC S2001 [9])

„*Дія або подія, яка може поставити під сумнів безпеку*." (European ITSEC [12])

„*Потенційне порушення безпеки*." (ISO 7498-2 [13]).

Розглянемо операційні ризики безпеки. Управління операційними ризиками не є новою практикою для банків, - банки завжди намагалися перешкодити шахрайствам, підтримувати цілісність засобів внутрішнього контролю, скоротити помилки в обробці операцій.

Задачею кожного банку є визначення базових засад ідентифікації, оцінки, управління і контролю ризиками безпеки, які пов'язані з електронними технологіями банківської справи [7]. Згідно з вимогами Національного нормативу №6 [14] аудитор повинен оцінити властивий (притаманний) ризик. Отже, розглянемо перший етап управління операційними ризиками безпеки - ідентифікація ризиків та загроз, що включає їх короткий опис.

Загальними класами *загроз* є:

- Помилки
- Зловмисне нанесення шкоди
- Шахрайство

- Крадіжка
- Відмова устаткування/програмного забезпечення

Загрози відбуваються через *уразливість*, пов'язану з використовуванням інформаційних ресурсів. Прикладами *уразливостей* є:

- Відсутність у користувача необхідних знань
- Відсутність функціональності безпеки
- Слабкість паролів
- Невипробувана технологія
- Передача незахищеними комунікаціями
- Тощо.

Розглянемо складові операційного ризику безпеки, виходячи з таких основних задач безпеки в електронній банківській справі:

- не допустити та/або своєчасно виявити підроблення, знищення електронних трансакцій, документів/угод чи записів;
- захистити конфіденційність інформації, що складає банківську та комерційну таємницю (рахунки, обороти, залишки, документи, угоди тощо).

1. Ризики аутентифікації та авторизації

1.1. Несанкціонований доступ

Проблеми систем контролю доступу та аутентифікації можуть призвести до успішних атак зовнішніх зловмисників (хакерів) - хакер може отримати доступ до внутрішніх систем банку; конфіденційна інформація клієнта може бути перехоплена несанкціонованою третьою стороною; банківські системи та дані навмисно можуть бути викривлені чи порушені/знищені.

Оскільки банківські внутрішні мережі залежать від технологій безпеки, що подібні тим, які використовуються для управління їх зовнішніми системами, необхідно ставитись уважно до управління безпекою внутрішніх мереж - компрометація безпеки внутрішньої мережі може скомпрометувати цілісність і конфіденційність банківських записів і даних клієнтів.

1.2. Доступ з перевищенням повноважень

Доступ з перевищенням повноважень означає, що відповідальна особа банку має надлишкові права доступу, що не є необхідними для виконання службових обов’язків. Наявність надлишкових прав може бути використана помилково чи навмисно для здійснення доступу, що не є необхідним для виконання службових обов’язків.

1.3. Помилки при аутентифікації чи невідповідна аутентифікація

Через помилки чи невідповідність (слабкість) процедур аутентифікації особа може отримати несанкціонований доступ чи доступ з перевищенням повноважень.

Фальшиві сертифікати ключів електронного підпису, випущені зловмисником від імені банку, можуть використовуватися для обману клієнтів

чи з метою шахрайства з електронними коштами/угодами. Сертифікати також можуть видаватись особам, які видають себе за банківських клієнтів, без відповідної перевірки достовірності особи.

2. Ризики, пов'язані з людським фактором (працівники банку)

2.1. Зловживання/шахрайство працівника банку

Банківські системи наражаються на операційний ризик безпеки щодо шахрайства працівника банку, який може таємно отримати ідентифікаційні дані (паролі, ключі тощо) з метою доступу до рахунків клієнтів/банку та/або операцій/трансакцій, здійснити крадіжку електронних грошей, карток, які зберігають кошти, чи отримати інформацію про рахунки клієнтів для незаконного її використання тощо.

2.2. Неадекватне чи неправильне використання інформаційних систем та засобів захисту

Неадекватні заходи захисту, які не відповідають наявним ризикам, чи неправильне конфігурування/використання інформаційних систем чи засобів захисту можуть створити умови реалізації ризиків несанкціонованого доступу, доступу з перевищенням повноважень, зловживання службовця тощо.

2.3. Недостатня кваліфікація персоналу

Швидка зміна технологій може призвести до того, що персонал банку не зможе повністю розуміти характер/природу нової технології, яка використовується банком. Це може закінчитись операційними проблемами з новими чи оновленими системами.

3. Ризики проектування, реалізації та експлуатації систем

Банк наражається на ризик, якщо системи, які обираються, розробляються чи супроводжуються, є недостатньо безпечними. Ризики проектування, реалізації та обслуговування систем є важливою складовою операційного ризику (може розглядатися також як елемент *стратегічного ризику*).

3.1. Невідповідність/застарілість системи

Банк схильний до ризику призупинення чи уповільнення роботи його існуючих систем, якщо інформаційна система не відповідає технічним вимогам застосування/експлуатації або реалізація цієї системи, не відповідає технічним вимогам чи недостатньо тестувалась.

Швидкі темпи змін, які характеризують інформаційну технологію, породжують ризик старіння систем банків. Невідповідність чи застарілість систем може бути наслідком стратегічної помилки (реалізація *стратегічного ризику*).

Програмне забезпечення, у тому числі клієнтське, вимагає періодичного оновлення, але канали розповсюдження оновлень несуть у собі ризики для банків щодо можливості зловмисниками перехоплення чи змінення програмного забезпечення.

3.2. Помилки чи шахрайства при програмуванні, супроводженні чи використанні систем

Терміни „*помилка*" та „*шахрайство*" визначені в Нормативі №7 Аудиторської палати України [15].

Помилки програмування можуть призвести до уразливостей, які дозволяють реалізацію різного виду атак на систему – від відмови в обслуговуванні до несанкціонованого доступу. Уразливості можуть спостерігатися як у стандартному програмному забезпеченні, так і в спеціальному.

Шахрайства програмування – це навмисне створення уразливостей системи („люки", „закладки", „троянські коні" тощо).

Можуть мати місце помилки від незнання чи неохайності/халатності службовців при проектуванні, супроводженні чи використанні систем.

Можлива несанкціонована модифікація програм/даних при експлуатації систем, в тому числі конфігураційних даних. При цьому дані можуть бути модифіковані чи підмінені як під час їх зберігання, так і під час транспортування.

3.3. Порушення чи невідповідність взаємодії (інтерфейсу) підсистем

Кожна автоматизована система складається з ряду підсистем. Невідповідність та/чи незахищеність інтерфейсів (каналів обміну даними) між підсистемами може призвести до операційних проблем, починаючи з відмови в обслуговуванні, аж до „підкидання" фальшивих документів/трансакцій.

Другим класом проблем тут є неузгодженість в адмініструванні підсистем, коли зміни в конфігурації однієї (декількох) підсистеми не узгоджуються з іншими, що може призвести до відмови в обслуговуванні, дублювання даних/трансакцій, втрати чи порушення даних.

3.4. Відмова в обслуговуванні

Наявність уразливостей, властивих системі, може призвести до реалізації зловмисником атаки типу „відмова в обслуговуванні". Крім того, невідповідні експлуатаційні умови (температура, пил, відсутність стабільного живлення тощо) можуть призвести до виходу систем з ладу. У кожному з цих випадків банк наражається на операційний ризик *відмови в обслуговуванні*.

3.5. Ризики аутсорсингу *(Outsourcing)*

Деякі послуги можуть надаватися зовнішніми постачальниками послуг (Service providers – сервіс-провайдерами) або зовнішніми спеціалістами з впровадження, експлуатації та підтримання підсистем електронного банкінгу. Такі послуги можуть бути бажані з економічних міркувань чи обов'язкові, у разі, коли банк не має змоги здійснювати їх самостійно.

Разом з цим залежність від зовнішніх постачальників послуг наражає банк на операційні ризики. Постачальники послуг можуть не мати необхідної кваліфікації щодо послуг, які надають, чи можуть бути не здатні своєчасно модернізувати свою технологію згідно з вимогами банку чи розвитком технологій.

Робота постачальників послуг може бути (при)зупинена через поломки системи чи фінансові проблеми, створюючи умови, за яких банк неспроможний постачати банківські продукти чи послуги.

Службовці постачальників послуг також підпадають під *ризики, пов'язані з людським фактором (працівники банку)*, розглянуті вище.

3.6. Помилки чи невідповідність систем захисту

Помилки чи невідповідність системи захисту можуть наражати банк на будь-який із операційних ризиків.

4. Клієнтські ризики

Це категорія ризиків пов'язана з комп'ютерними операціями кінцевого користувача, яким може бути виключно клієнт банку.

4.1. Неправильне застосування клієнтами продуктів та послуг

Неправильне застосування клієнтами банківських продуктів та послуг, навмисно чи з необачності, є складовою операційного ризику. Ризик посилюється, якщо банк не здійснює відповідного навчання та інформування його клієнтів щодо технологічних аспектів та заходів безпеки.

Клієнти, які використовують персональну інформацію (наприклад, ідентифікаційну інформацію, у тому числі паролі чи ключі, номер кредитної картки чи номер банківського рахунку) у небезпечних електронних трансакціях, можуть дозволити зловмисникам отримати несанкціонований доступ до своїх рахунків з метою шахрайства.

4.2. Відмова клієнта від трансакції/угоди

За відсутності адекватних заходів щодо аутентифікації клієнта чи авторизації трансакції, клієнти можуть анулювати трансакції/угоди/документи, які ними ж попередньо були санкціоновані, та завдати тим самим фінансових збитків банку.

5. Ризики кінцевого користувача (клієнта чи службовця банку)

Це категорія ризиків пов'язана з комп'ютерними операціями кінцевого користувача, яким може бути як службовець, так і клієнт банку.

Щодо операцій кінцевого користувача, то слід підкреслити, що створення нових форм доставки інформації і процесів мереженої обробки даних, як правило, випереджає створення елементів безпеки і контролю. Особливу увагу потрібно приділити можливості викривлення (спотворення) або пошкодження даних чи програмного забезпечення, що може зашкодити ефективному функціонуванню операційної мережі установи взагалі.

Крім того, термін „персональний комп'ютер" означає, що фактично одна особа може бути повністю відповідальна за встановлення (інсталяцію), тестування та експлуатацію набору програм, особливо з боку клієнтів. При цьому збільшується можливість використання процедур і обробки даних, відмінних і не сумісних із стандартами, прийнятими в банку.

6. Надзвичайні обставини

Складовою частиною забезпечення безперервної діяльності банку (установи) є створення системи відновлення діяльності у надзвичайних обставинах, пов'язаних із непереборними або стихійними силами (пожежа, повінь тощо), включаючи вихід з ладу обладнання, а також відсутність/втрату персоналу (звільнення, хвороба тощо).

Вищенаведені основні операційні ризики безпеки систем електронного банкінгу, які рекомендується Базельським комітетом для розгляду банківськими фахівцями з управління ризиками. Треба зазначити, що до поряд з операційними ризиками безпеки, необхідно також розглядати й інші ризики – законодавчий ризик, ризик репутації та стратегічний ризик.

Література

1. Стандарт Німеччини: "IT Baseline Protection Manual, Standard security safeguards" - Version: Oktober 2000, Bundesamt für Sicherheit in der Informationstechnik;
2. Risk in Computer and Telecommunication systems. – Basle: Basle Committee on Banking Supervision, July 1989;
3. Risk Management for Electronic Banking and Electronic Money Activities. - Basle: Basle Committee on Banking Supervision, Mart 1998;
4. Operational Risk Management. – Basle: Basle Committee on Banking Supervision, September 1998;
5. Electronic Banking Risk Management Issues for Bank Supervisors. Electronic Banking Group White Paper. – Basle: Basle Committee on Banking Supervision, October 2000;
6. Risk Management Principles for Electronic Banking. – Basle: Basle Committee on Banking Supervision, May 2001;
7. Risk Management Principles for Electronic Banking. – Basle: Basle Committee on Banking Supervision, July 2003;
8. Consultative Document. The New Basel Capital Accord. – Basle: Basle Committee on Banking Supervision, April 2003 (Basel II).
9. Commission of the European Communities (1993a), Glossary of information systems security - DGXIII, INFOSEC Programme/S2001.
10. ETSI TC-NA/STAG. Security Techniques Advisory Group (STAG). Glossary of security terminology - Reference: DTR/NA-002507, ICS: 33.020; ETR 232, ETSI TECHNICAL REPORT, November 1995.
11. ISO/IEC TR 13335-1:1996. Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security.
12. European ITSEC Version 1.2, June 1991.
13. ISO 7498-2:1989. Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

14. Норматив №13. Аудит в умовах електронної обробки даних - Затверджено рішенням Аудиторської палати України від 18 грудня 1998 р. №73.

15. Норматив №7. Помилки та шахрайство - Затверджено рішенням Аудиторської палати України від 18 грудня 1998 р. №73.