УДК 336.71:004.738.5

ПОБУДОВА УЗАГАЛЬНЕНОЇ МОДЕЛІ ЗАГРОЗ ДЛЯ СИСТЕМ ІНТЕРНЕТ-БАНКІНГУ

Марина Миколаївна ВОЙТКО
Головний інженер
Національний банк України
аспірант Університету банківської справи Національного банку України
E-mail: Maryna.Voitko@bank.gov.ua

Анотація. Статтю присвячено дослідженню узагальненої моделі загроз для систем Інтернет-банкінгу, що основана на взаємозв'язку операційних ризиків та ризиків інформаційної безпеки.

Анотация. Статья посвящена исследованию обобщенной модели угроз для систем Интернет-банкинг, которая основана на взаимосвязи операционных рисков и рисков информационной безопасности.

Ключові слова: *Інтернет-банкінг, операційні ризики, ризики інформаційної безпеки, модель загроз, джерела загроз, модель порушника.*

Ключевые слова: *Интернет-банкинг, операционные риски, риски информационной безопасности, модель угроз, источник угроз, модель нарушителя.*

Постановка проблеми. В умовах глобального розвитку ринкової економіки та підвищення рівня конкуренції стало популярним використання відносно нового інструменту для управління банківськими рахунками – системи Інтернет-банкінгу.

Розвиток концепцій вторгнень у системи Інтернет-банкінгу (далі – системи ІБ), засобів і методів їх реалізації обумовлений збільшенням користувачів Інтернет у геометричній прогресії в світі та клієнтів систем ІБ. Засоби захисту, які на сьогодні використовуються в зазначених системах, не здатні повною мірою забезпечити їх захищеність у разі вторгнення порушників.

Завданням цієї роботи є аналіз можливих джерел загроз інформаційної безпеки в системах ІБ та удосконалення на його основі узагальненої моделі загроз для подальшої оцінки захищеності зазначених систем під час виконання банківських розрахунків та розроблення методологічних систем оцінювання ризиків, пов'язаних з ризиками інформаційної безпеки, що є в системах ІБ .

Аналіз останніх досліджень та публікацій. Дослідження проблеми моделювання загроз для систем ІБ перебуває в центрі уваги багатьох вітчизняних та закордонних фахівців. Значні здобутки у висвітленні зазначених проблем мають російські вчені, серед яких необхідно назвати Д. Каленбета, Ю. Н. Юденкова, А. В. Лукацького, П. Ревенкова, А. Вороніна та інших.

Однак на сьогодні створенню узагальненої моделі загроз для систем ІБ, побудованої на взаємозв'язку операційних ризиків та ризиків інформаційної безпеки, не приділяється необхідної уваги. Найчастіше розглядають лише окремі та вибіркові джерела загроз, що не дає змогу узагальнити усіх фактори, які мають вплив на системи ІБ.

Метою статті є дослідження взаємозв'язку операційних ризиків та ризиків інформаційної безпеки в системах ІБ та удосконалення узагальненої моделі загроз для систем ІБ на основі цього взаємозв'язку.

Обґрунтування отриманих наукових результатів. Для розроблення методологічних систем оцінювання ризиків, пов'язаних з ризиками інформаційної безпеки (ІТ-ризики), наявних у системах ІБ, першочерговим завданням є побудова моделі загроз. Модель загроз для систем ІБ – це узагальнена інформація щодо детального аналізу множини можливих загроз, визначення їх характеристик, механізмів і наслідків впливу. Для побудови такої узагальненої моделі системи ІБ будемо розглядати як такі, які складається з клієнтів, веб-серверу банку, серверу застосувань банку, серверу АВС банку та серверу "Клієнт-

банк", розташованих окремо один від одного і забезпечують функціонування систем ІБ.

Перш ніж розглядати модель загроз встановимо взаємопов'язаність операційного ризику та ризику інформаційної безпеки. На основі зазначеної взаємопов'язаності будемо вибудовувати модель загроз для систем ІБ.

Розгляд джерел загроз, що формують операційні ризики та ризики інформаційної безпеки, надасть можливість оцінити існування взаємозв'язку зазначених ризиків (табл. 1).

Таблиця 1

Порівняльна таблиця джерел загроз операційного ризику та ризику інформаційної безпеки

Джерела загроз операційного ризику за визначення з Положення про організацію операційної діяльності в банках України)	Джерела загроз операційного ризику за визначення з «Базель ІІ»	Джерела загроз інформаційної безпеки основані на методичних рекомендаціях щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України
Операційний ризик - це ризик, який пов'язаний з порушенням банківських правил та/або систем контролю за обробленням, проведенням операцій, документацією, що виникаєяк унаслідок…	Операційний ризик – це ризик збитків, що виникають у результаті неадекватних або невдалих…	Ризиком інформаційної безпеки вважається ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду банку.
-	внутрішніх процесів	Часткове/повне пошкодження/втрата обладнання/даних
помилок працівників банку	дій персоналу чи систем	Часткове/повне пошкодження/втрата обладнання/даних; Компрометація інформації
зовнішніх причини	у результаті зовнішніх факторів	Фізичне пошкодження/втрата /будівлі/обладнання/інформації; Викривлення/підробка інформації/даних.

Джерело: складено автором за даними [1, 2, 3]

Відповідно до визначень операційного ризику в Положенні Національного банку України про організацію операційної діяльності в банках України, затвердженого постановою Правління Національного банку України № 254 від 18.06.2003) та Базелі ІІ, а також визначення ризику інформаційної безпеки з листа Департаменту інформатизації Національного банку України від 03.03.2011 № 24-112/365 можна зробити висновок (табл. 1), що вони взаємопов'язані.

Як видно із зазначених у табл. 1 джерел ризику, реалізація будь-яких загроз за їх рахунок може призвести як до виникнення ризиків інформаційної безпеки, так і до операційних ризиків.

Отже, управління ризиками інформаційних технологій надає позитивну динаміку в зниженні операційних ризиків як у цілому, так і частково в системах ІБ кредитних організацій.

Для побудови моделі загроз системи ІБ будемо розглядати як такі, які складається з клієнтів, веб-серверу банку, серверу застосувань банку, серверу АВС банку та серверу "Клієнт-банк" і забезпечують функціонування систем ІБ.

Будемо вважати, що структурно системи ІБ є автоматизованими системами, компоненти яких взаємопов'язані між собою за визначеними правилами та технологіями. Особливістю таких систем є те, що їх компоненти розподілені в просторі й зв'язок між ними фізично здійснюється за допомогою мережних з'єднань.

Проаналізувавши множини можливих типових загроз у системах ІБ, приходимо до висновку того, що системи ІБ є уразливою для багатьох загроз як ненавмисного, так і зловмисного характеру, які можна умовно розділити на чотири основні групи (табл. 2): загрози природного походження, загрози пов'язані з зоною ризиків

клієнтів ІБ, загрози, пов'язані з середовищем взаємодії (Інтернет-провайдер клієнта та банку), та загрози, пов'язані з локальними (або розподіленими) мережами банку.

У запропонованій моделі описані загрози, проведена їх ідентифікація з можливими діями порушників щодо об'єктів захисту, тобто перелік загроз із констатацією можливих дій порушників щодо відповідних об'єктів, виходячи з пріоритетів безпеки та цінності електронних інформаційних ресурсів – порушення конфіденційності інформації (к), цілісності інформації та програмного забезпечення (ц), доступності інформації і сервісів, що надаються системами ІБ (д) інформаційних об'єктів систем ІБ.

Таблиця 2

Модель загроз для систем ІБ

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки
1	2	3	4	5
Загрози природного походження				
1	Катастрофа	Пожежа, повінь, землетрус, техногенні аварії	Зовнішнє середовище	ц, д
Загрози, пов'язані з зоною ризику клієнта				
1	Помилки	Виникнення помилок під час виконання банківських операцій	Клієнт ІБ	к, ц
2	Хакінг	Виконання несанкціонованих дій на кінцевому пристроєві клієнта (на рівні застосувань, web-браузеру, операційної системи)	Зловмисник	к, ц
3	Крадіжка	Крадіжка кінцевого пристрою клієнта	Зловмисник	д
4	Крадіжка	Крадіжка носія з ключовою інформацією клієнта	Зловмисник	к, ц, д
5	Вірусне зараження	Зараження кінцевого пристрою клієнта шкідливим програмним забезпеченням	Зловмисник	ц
6	Соціальна інженерія	Незаконне отримання конфіденційних даних клієнта	Зловмисник	к, ц
7	Перехват	Типові помилки клієнта під час зберігання та зміни інформації персональної ідентифікації	Клієнт ІБ	к, ц
8	Крадіжка	Порушення клієнтами ІБ умов використання системи ІБ	Клієнт ІБ	ц
9	Збої в каналах зв'язку	Забезпечення неможливості відмови (доказ участі в фінансовій операції як клієнта, так і банку)	Середовище взаємодії в системі ІБ	к, ц ,д
Загрози, пов'язані з середовищем взаємодії (Інтернет-провайдер клієнта та банку)				
1	Відмова в обслуговуванні	Виведення з ладу/пошкодження/перехід в нештатний режим роботи інформаційно-телекомунікаційної системи	Персонал, зловмисник, програма	д
2	Відмова в обслуговуванні	Виведення з ладу/пошкодження/ перехід в нештатний режим роботи апаратно-програмного забезпечення	Персонал, зловмисник, програма	д
Загрози, пов'язані з локальними (або розподіленими) мережами банку				
1	Шахрайство	Крадіжка коштів з рахунку клієнтів ІБ	Зловмисник	ц
2	Шахрайство	Незаконне використання системи ІБ з метою відмивання коштів	Клієнт ІБ, зловмисник	ц
3	Недоліки	Відмова в роботі на рівні веб-сервісів	Зловмисник	д
4	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі на рівні веб-серверу	Зловмисник	д
5	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі на рівні операційної системи веб-серверу	Програмне забезпечення, зловмисник	ц, д

1	2	3	4	5
6	Недоліки	Відмова в роботі на рівні XML серверу застосувань	Зловмисник	д
7	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі на рівні серверу застосувань	Зловмисник	д
8	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі на рівні операційної системи серверу-застосувань	Програмне забезпечення, зловмисник	ц, д
9	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі серверу баз даних на рівні SQL	Зловмисник	ц, д
10	Недоліки	Виведення з ладу/перехід у нештатний режим роботи/відмова в роботі серверу баз даних на рівні операційної системи	Програмне забезпечення, зловмисник	ц, д
11	Недоліки	Помилки під час конфігурації, використання та підключення засобів захисті банку (міжмережеві екрани, системи попередження атак)	Апаратно-програмні комплекси	к, д, ц
12	Недоліки	Несанкціоноване сканування як до, так і після мережевих екранів банку	Апаратно-програмні комплекси	д, ц
13	Підміна	Несанкціонована зміна фінансової інформації клієнтів у базах даних ІБ	Персонал, зловмисник	ц
14	Недоліки	Помилки в програмному забезпечені системи ІБ	Розробник, зловмисник	к, ц, д
15	Збої в каналах зв'язку	Перевищення порогу допустимого навантаження на канали зв'язку або ж розрахункові ресурси системи ІБ	Середовище взаємодії	д
16	Нав'язування	Нав'язування хибної інформації від імені авторизованого клієнта системи ІБ	Зловмисник	ц, к
17	Комп'ютерна неграмотність	Помилкові дії персоналу	Персонал	к, ц, д
18	Шахрайство	Злочинні дії персоналу (розголошення банківської та комерційної таємниці, модифікація обладнання, підбір даних аутентифікації)	Персонал	к, ц
19	Імітація	Неправомірне отримання персональних даних клієнтів ІБ з подальшим маскуванням під дійсного клієнта ІБ	Персонал, зловмисник	ц, к, д

Джерело: складено автором за даними [4, 5, 6, 7, 8, 9, 10].

Невід'ємною частиною у разі удосконалення побудови моделі загроз для систем ІБ є модель вірогідного порушника, що має бути адекватною реальному порушнику такого виду систем.

Модель порушника системи ІБ – абстрактний формалізований або неформалізований опис порушника, який складається з опису його вірогідних дій, вектора їх направленості, рівня знань та умінь та первинних знань про систему ІБ.

Загалом модель порушника використовується не тільки в процесі оцінки ризиків, аналізу вразливості системи, а й для підвищення ефективності існуючих і планових заходів захисту.

Відповідно до класифікації порушників в автоматизованих системах [8, с. 62] та до запропонованої моделі загроз (табл. 2) можна зробити висновки, що порушник має два основні вектори направленості своїх дій щодо систем ІБ: опосередковані дії (через засоби зв'язку), прямої дії на елементи систем ІБ та змішаної природи (злочинна домовленість внутрішніх та зовнішніх порушників). Однак таке категоріювання не є достатнім, тому ранжування необхідно проводити з розподілом зазначених категорій на підкатегорії.

Узагальнену модель порушника систем ІБ за зазначеними принципами можна розбити на такі підкатегорії:

а) внутрішні:

працівники, що не мають доступу до системи ІБ;

працівники банку, що безпосередньо працюють з системою ІБ;

прикладні програмісти;

розробники системи ІБ;

б) зовнішні:

клієнти системи ІБ;

розробники системи ІБ;

хакери;

недобросовісні партнери;

кримінальні структури;

конкуренти;

в) злочинна домовленість внутрішніх та зовнішніх порушників.

Окрім категоризації порушника за вектором направленості своїх дій щодо системи ІБ також необхідно врахувати такі фактори:

1) кінцева мета впливу порушника за ступенем небезпеки щодо системи ІБ (зупинка працездатності сервісу, крадіжка коштів з рахунку клієнта, крадіжка персональних даних клієнта);

2) професійний рівень знань та умінь порушника (низький, середній, високий);

3) первинні знання порушника щодо функціонального складу системи ІБ (IP-адреси серверів, версії програмного забезпечення, правило взаємодії елементів системи ІБ);

4) можливості доступу порушника;

5) технічні ресурси та програмно-апаратне забезпечення порушника.

Проаналізувавши структуру вірогідної моделі порушника систем Інтернет-банкінгу, пропонуємо розглянути математичне її зображення:

$$M_O = (O_p, O_{ln}, O_a),$$

де O_p – місце розташування зловмисника;

O_{ln} – професійний рівень знань та умінь порушника; O_{pn} – первинні знання порушника про систему; O_a – сценарії можливого доступу порушника.

Виокремимо три основні місця розташування зловмисника: $O_p \in \{ 1,2,3 \}$, де 1 – порушник зовнішній, 2 – порушник внутрішній; 3 – злочинна домовленість внутрішніх та зовнішніх порушників.

Професійний рівень знань та умінь порушника $O_{ln} \in \{ 1,2,3 \}$, де 1 – низький рівень, 2 – середній рівень; 3 – високий рівень.

Первинні знання порушника про систему ІБ залежать від місця розташування зловмисника відносно неї.

Також необхідно зазначити пряму залежність між O_{ln} та $O_{a.}$ Отже, чим вищий рівень знань зловмисника, тим більше можливих варіантів сценаріїв доступу він може створити.

Сценарії можливого доступу порушника будуються на основі табл. 2.

Для підвищення рівня безпеки в системі в процесі складання моделі порушника в деяких ситуаціях доцільно робити припущення про високий рівень забезпеченості ресурсами та великий досвідом порушника.

Як доповнення до моделі можливе використання статистичної інформації про несанкціоновані проникнення в системи ІБ.

Висновки. Запропонований у статті аналіз множини можливих типових загроз у системах ІБ дає можливість із застосуванням удосконаленої методики побудови моделі таких загроз виявити основні ризики інформаційної безпеки для формування в подальшому методологічних систем оцінювання ризиків пов'язаних з ризиками інформаційної безпеки (IT-ризики), що наявні в системах ІБ та визначення складу необхідних заходів для побудови відповідної моделі захисту для систем ІБ.

Розглядаючи питання моделювання загроз, притаманних системам ІБ, доцільно використовувати чотирирівневу градацію загроз: загрози природного походження, загрози пов'язані з зоною ризиків клієнтів ІБ, загрози пов'язані з середовищем взаємодії (Інтернет-провайдер клієнта та банку) та загрози пов'язані з локальними (або розподіленими) мережами банку.

Список використаних джерел

1. Про затвердження Положення про організацію операційної діяльності в банках України, затверджене Постановою Правління Національного банку України від 18.06.2003 N 254 [Електронний ресурс]. — Режим доступу : http://zakon.nau.ua/doc/?uid=1078.8029.0.

2. Банковские риски: учебное пособие / кол. авторов; под ред. д-ра экономических наук, проф. Н. И. Валенцовой. — 2-е изд., стер. — М. : КНОРУС, 2008. — 232 с.

3. Лист Департаменту інформатизації банках України, затверджене від 03.03.2011 № 24-112/365/ [Електронний ресурс]. — Режим доступу : http://www.zakon.rada.gov.ua.

4. СОУ Н НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для

управління інформаційною безпекою" (ISO/IES 27002:2005, MOD). [Електронний ресурс]. — Режим доступу : http://www.zakon.rada.gov.ua.

5. Постанова Правління Національного банку України від 28.10.2010 № 474 "Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України". [Електронний ресурс]. — Режим доступу : http:// www. zakon.rada.gov.ua.

6. СОУ Н НБУ 65.1 СУІБ 1.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES 27001:2005, MOD). [Електронний ресурс]. — Режим доступу : http://www.zakon.rada.gov.ua.

7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

8. Капустян М. В., Орленко В. С., Хорошко В. О. Створення моделі загроз інформації та механізму її ефективного захисту / М. В. Капустян, В. С. Орленко, В. О. Хорошко // Автоматика, вимірювання та керування: Вісник національного університету "Львівська політехніка". — 2006. — № 551. — С. 58–63.

9. Кудінов В. А. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В. А. Кудінов, В. О. Хорошко // Захист інформації. — № 1. — 2004. — С. 26–36.

10. Лямин Л. В. Анализ факторов риска, связанных с интернет-банкингом / Л. В. Лямин // Расчеты и операционная работа в коммерческом банке. — 2006. — № 5. — С. 52–64.