Загрози інформаційній безпеці у банківських установах

Борисова А.М., студентка гр. УБм-21 юридичного факультету СумДУ
Науковий керівник - Чернадчук О.В.,асистент кафедри права СумДУ

На сьогодні інформація відіграє особливу роль у процесі розвитку цивілізації. Особлива значимість інформації проявляється саме для банківської сфери, що напряму пов'язана із її специфікою, тобто неможливістю здійснення банківської діяльності без інформації. Можна стверджувати, що саме грошові кошти та інформація є «двигуном» усієї банківської діяльності.

А тому ще більш вагомим питанням стає проблема захисту інформації, що є основою для здійснення банківської діяльності.

Проблема забезпечення інформаційної безпеки банківських установ є однією із передових, при цьому, не потрібно навіть бути фахівцем, щоб зрозуміти важливість даного питання. Так як , навіть замислюючись над тим, що кожен з нас має певне відношення, і не раз в житті зіштовхувався із банківськими сегментом послуг, насамперед, зацікавлений у безпеці таких відомостей, та з особливою обережністю ставиться до них.

Так, інформаційна безпека – це формування інформаційних ресурсів банку та організація гарантованого їх захисту. Досягається створенням у банку системи збору та обробки інформації, проведенням відповідних заходів щодо її зберігання та розподілу, визначенням категорій і статусу банківської інформації, порядку і правил доступу до неї, дотриманням усіма працівниками, клієнтами та акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації та їх перетинанням [3, с.5].

Однак для того щоб побудувати збалансовану систему інформаційної безпеки, потрібно спочатку, провести аналіз ризиків у сфері банківської інформаційної безпеки.

Перш за все проблема починається із неправильного розуміння порушень інформаційної банківської безпеки, що пов'язані із такими категоріями як «загроза», «ризики», «джерело загрози», «фактор загрози», «вразливість», «несприятливі чинники впливу», «негативні прояви», «перешкоди». Спільним для них є те, що усі вони характеризують категорію «небезпеки», що є відповідно протилежною «безпеці».

Незважаючи на таку схожість, дані терміни все ж не є тотожними. Так, попри численні дослідження, які проведені у цих напрямках, ще й сьогодні немає чіткого та однозначного їх трактування, особливо це стосується таких понять, як «ризик» та «загроза».

Зазвичай можна зустріти, що термін «загроза» використовують для трактування суті ризиків.

Загроза є специфічною формою ризику, як вважає О.І. Барановський, досліджуючи ризики банківської діяльності, він зупиняється на думці, що перехід ризику в загрозу починається тоді, коли з'являються негативні якісні зміни в економічних системах, що пов'язані зі значними фінансовими втратами, збитками, які спричиняють банкрутство» [1, с. 261]. Крім того є цікавим такий погляд, що: 1) ризик стосовно загрози є первинним, тоді як загроза вторинна і випливає з ризику; 2) ризикуючи, банк може отримати як збитки, так і доходи, тоді як реалізація загрози не приносить доходи чи прибутки; 3) ризик – неминучий супутник банківської діяльності, тоді як загроза може виникати тільки за наявності певних умов [5, с. 237].

Що ж до категорій «джерело» та «фактор» питання є дещо простішим. Так, будь-яке джерело слід розуміти як певне начало, витік, початок. Сама по собі дефініція означає «те, з чого щось бере свій початок».

Відповідно, фа́ктор (лат. «facere» – «діяти», «виробляти», «примножувати») – це умова, рушійна сила будь-якого процесу, явища; чинник [2].

Однак, при цьому слід відмітити, що у випадку, коли мова йде про ризики безпеці (зокрема інформаційній), фактор загрози все ж буде передувати її джерелу. Так, як такий фактор буде певним чинником виникнення джерела, тобто його активі затором, з якого починається увесь «механізм» ризиків інформаційній безпеці банківських установ.

Відповідно, на підставі всього вище зазначеного, можна прийти висновку, що під дією негативного впливу певних факторів (несприятливих чинників впливу, тобто певних дій) джерело загроз через певну вразливість створює певні ризики та загрози системі безпеки.

Така модель інформаційної безпеки має змогу відображувати сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження інформаційних ресурсів.

Таким чином, інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми та внутрішніми.

Водночас, чим більших успіхів досягає людство в боротьбі з зовнішніми загрозами, тим рішучіше на перший план виходять загрози внутрішні, з якими, згідно статистики, пов’язано близько 70% всіх інцидентів безпеки [4, с. 179].

У даному випадку можна навести аналітичні дані та результати дослідження такого ресурсу як російська компанія InfoWatch [7]. Дослідження даної компанії, проведені в період з 20.12.2006 по 25.01.2007 р., в процесі якого були опитані представники 312 російських банків.

Результати показують, що респонденти значно занепокоєні внутрішньою інформаційною безпекою (55%), ніж захистом від зовнішніх загроз (45%).

При цьому, у категорію внутрішніх загроз було віднесено халатність співробітників, саботаж та фінансове шахрайство, а в категорію зовнішніх загроз – віруси, хакери, спами. Разом з тим, необхідно зазначити, що загрози викрадення інформації, різноманітні збої і викрадення обладнання спеціально не були віднесені ні до однієї із груп, так як вони можуть бути реалізовані як в самому банку, так і за його межами [7].

Однак, необхідно враховувати, що такі некласифіковані ризики як, наприклад, викрадення інформації або обладнання, найчастіше відносять до внутрішніх ризиків, і так як в даному випадку вони взагалі не враховані, показники розрахунку свідчать, що зовнішні ризики все ж поступаються внутрішнім загрозам.

Як показали результати дослідження, у списку найнебезпечніших внутрішніх загроз головне місце посідає порушення конфіденційності інформації (78%), на другому місці – втрата інформації (61%), і на третьому – збій в роботі інформаційних систем (52%) [7].

Тому слід відзначити, що зовнішні джерела загроз можуть напряму, або безпосередньо бути пов’язаними із внутрішніми. Тому аналіз зовнішнього та внутрішнього середовища має проводитися комплексно та одночасно.

Також слід пам’ятати, що захист банківської інформації – завдання в рівній мірі як технічне, так і правове, і організаційне.

З метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно виявляти та аналізувати вразливі місця інформаційної системи банку та ресурси, які потребують захисту, а також ймовірні атаки, які можуть відбутися в конкретному оточенні. Після цього потрібно визначити інформаційні ризики для визначеного інформаційного ресурсу та обрати контрзаходи, згідно обраної політики банківської безпеки та забезпечити за допомогою механізмів і сервісів безпеки. Політика банківської безпеки має визначати взаємопов'язану сукупність механізмів і сервісів безпеки, адекватну ресурсам, що захищаються, і оточенню, в якому їх використовують [6, с. 24].

На підставі вище викладеного, можна прийти висновку, що порушення інформаційної безпеки у певній мірі також представляє собою певний «механізм», що починається від негативних чинників (факторів) і закінчується відповідними наслідками. При цьому, слід постійно враховувати джерела потенційних загроз, як зовнішнього, так і внутрішнього середовища, задля стану готовності відвернути можливі ризики. Однак, враховуючи, що останнім часом внутрішні загрози переважають над зовнішніми, не слід їх у чистому вигляді розглядати окремо одне від одного, адже безумовно між ними є взаємозв’язок, що важливо також враховувати. Тому розроблення системи захисту інформаційної безпеки банківських установ має відбуватися комплексно.

Література:

1. Барановський О.І. Фінансові кризи: передумови, наслідки і шляхи запобігання: монографія / О.І. Барановський. – К.: Київ. нац. торг.-екон. ун-т, 2009. – 754 с.

2. Вікіпедія [Електронний ресурс] // Режим доступу: http://uk. wikipedia.org/wiki

3. Зубок М.І. Організаційно-правові основи безпеки банківської діяльності в Україні [Текст]: навч. посіб. / М.І. Зубок, Л.В. Ніколаєва. – 2-ге вид., доп. – К.: Істина, 2000. – 88 с.

4. Перехрест Л.М. Захист економічної інформації банків від внутрішніх загроз [Текст] / Л.М. Перехрест. – Научные труды ДоНТУ. – 2008. – №2. – С. 179-186.

5. Селюченко Н.Є. Ризики та загрози підприємства: підходи до трактування та уточнення їхньої суті [Текст] / Н.Є. Селюченко, В.М. Климаш // Національний університет «Львівська політехніка». – 2011. – С. 234-239.

6. Чернадчук Т.О. Актуальні питання інформаційних правовідносин у банківській сфері [Текст] : монографія / Т.О. Чернадчук; заг. ред. д. ю. н., проф. Арістової І.В. – Суми: «Сумський національний аграрний університет», 2011. – 162 с. –ISBN 978-617-593-017-5.

7. InfoWatch [Електронний ресурс] // Режим доступу : http://www. infowatch.ru/

Міжнародно-правове забезпечення стабільності та безпеки суспільства: матеріали науково-теоретичної конференції викладачів, аспірантів та студ. юридичного фак-ту, м. Суми, 25 травня 2013 р. / Ред.кол.: А.М. Куліш, М.М. Бурбика, М.І. Логвиненко, В.М. Семенов, А.В. Баранова. — Суми: СумДУ, 2013. — С. 127-129.