УДК 004.056.5(045)

ОЦІНКА РИЗИКІВ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Б. Я. Корнієнко, канд. техн. наук, доц.; ***О. К. Юдін***, д-р техн. наук., проф.
Г. В. Наконечна

e-mail: bogdanko@i.ua

Наведено оцінку ризиків інформаційних активів автоматизованої системи. Здійснено їх класифікацію за вартістю та визначено ймовірності реалізації можливих загроз.

Ключові слова: оцінка ризиків, автоматизована система, інформаційна безпека.

In given article it is presented an estimation of risks of information actives of the automated system of bank. It is made their classification and it is defined probabilities of realisation of probable threats.

Keywords: risk assessment, an automated system, information security.

Вступ

На сьогодні питання інформаційної безпеки з кожним днем усе більше загострюється і є одним з найважливіших для будь-якого підприємства чи установи. Інформаційні технології стрімко розвиваються, а тому, крім безперечної користі, зростає і кількість проблем. Кожне підприємство, а серед них і банки, активно дбають про свою безпеку, оскільки від неї залежать їх потенційні прибутки і подальший розвиток.

Так, важливим етапом на початку діяльності будь-якого підприємства є розроблення власної політики безпеки, яка враховуватиме всі можливі шанси в процесі функціонування системи. Суттєвим кроком на шляху до створення сприятливих і безпечних умов роботи організації є аналіз ризиків.

Постановка задачі

Мета даних досліджень — проведення оцінювання ризиків інформаційних активів автоматизованої системи на прикладі банку.

Насамперед у цій роботі необхідно керуватися нормативними документами та стандартами серії ISO, які визначають принципи, правила та рекомендації для створення ефективної та надійної системи управління інформаційною безпекою і, зокрема, аналізу ризиків [1–3].

Аналіз досліджень

Тема аналізу та управління ризиками не є новою, але незважаючи на її досить детальне опрацювання, в процесі побудови системи управління ризиками все ж виникають проблеми. Це пов'язано з різним рівнем зрілості компаній у сфері інформаційної безпеки, з неправильним вибором методик побудови систем або з помилковим вибором джерел інформації для аналізу.

Виклад основного матеріалу дослідження

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» дає означення понять *ризик* та *аналіз ризику*.

Отже, **ризик** (*risk*) — це функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Аналіз ризику (*risk analysis*) — процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеня їх прийнятності для експлуатації АС.

Першим кроком на шляху розрахунку ризиків інформаційної безпеки є визначення ресурсів інформаційної системи та активів організації.

Банківська установа є власником великих економічних, матеріальних та інформаційних активів. У даній статті розглянемо автоматизовану систему банку, визначимо інформаційні ресурси, що до неї належать та розрахуємо ризики, що їй загрожують при втраті, пошкодженні чи компрометації активів.

Автоматизована інформаційна система включає в себе дані, програмні засоби, обладнання, які в сукупності реалізовують технологію обробки інформації, а саме здійснюють її збирання, оброблення та зберігання відповідно до вимог та цілей організації.

Так, до інформаційних ресурсів банківської АС належать: програмне забезпечення, бази даних, файли та різного роду банківська документація (табл. 1). Невід'ємною частиною будь-якого, навіть автоматизованого процесу, є людина, оскільки підтримка, налаштування, обслуговування системи без людського втручання

обійтись не може. Тому кваліфіковані працівники – запорука успіху роботи будь-якої установи.

Таблиця 1

Класифікація інформаційних активів

Інформаційні активи АС банку	Операційні системи
	Програмне забезпечення
	База даних з інформацією про склад персоналу
	База даних з інформацією про клієнтів банку
	База даних з інформацією про валютні операції
	База даних з інформацією про кредитування
	Посадові інструкції співробітників
	Кореспондентські рахунки НБУ та інших банків
	Зразки і бланки заяв
	Цінні папери
	Договори з партнерами
	Кредитні операції
	Платіжна інформація
	Фінансово-аналітичні відомості
	Службова інформація

Наступним етапом у процесі аналізу ризиків є оцінка активів за вартістю.

У роботі вартість ресурсів наведена в термінах потенційних збитків. Ці збитки грунтуються на вартості відновлення, втратах при безпосередньому впливі та наслідках від втрат.

Методика оцінки збитків, яка застосовується в роботі, полягає у використанні якісного ранжування на високі — 5 (збиток від 100 тис. грн), середні — 3 (збиток від 10 тис. грн до 100 тис. грн) та низькі — 1 (збиток до 10 тис. грн) (табл. 2).

Після визначення рівня вартості активів автоматизованої інформаційної системи необхідно описати коло загроз для них та ймовірність (простоту) їх реалізації.

Загрози потенційно можуть завдати шкоди ресурсам автоматизованої системи. Вони можуть мати природні та людські джерела і можуть бути випадковими або навмисними.

До ідентифікації загроз необхідно залучати власників інформаційних банківських активів та користувачів, підрозділи управління персоналом та фізичною безпекою, фахівців з інформаційної безпеки, юридичні підрозділи тощо.

Важливим чинником при оцінюванні ризиків автоматизованої системи є врахування та ідентифікація її вразливостей.

Таблиця 2

Класифікація активів за вартістю

Активи	Рівень вартості
Операційні системи	5
Програмне забезпечення	5
База даних з інформацією про склад персоналу	3
База даних з інформацією про клієнтів банку	5
База даних з інформацією про валютні операції	5
База даних з інформацією про кредитування	5
Посадові інструкції співробітників	1
Кореспондентські рахунки НБУ та інших банків	3
Зразки і бланки заяв	1
Цінні папери	5
Договори з партнерами	5
Кредитні операції	5
Платіжна інформація	3
Фінансово-аналітичні відомості	3
Службова інформація	1

Вразливість — це слабке місце в інформаційній системі, яке може призвести до порушення безпеки шляхом реалізації деякої загрози.

Для загальної оцінки ризику прийнятними будуть абстрактні загрози, оскільки більш детальна оцінка потребується у випадку надання рекомендацій стосовно засобів захисту, які зменшать конкретний ризик.

Отже, в табл. 3 класифіковано загрози для інформаційних активів та, відповідно, зазначено ймовірність реалізації кожної з них. Причому ймовірність має відповідну цифрову градацію:

1 (дуже низька) — виникнення загрози практично неможливо;

2 (низька) — виникнення загрози малоймовірне (не частіше, ніж 1 раз на 1 рік);

3 (середня) — виникнення загрози ймовірне до 1 разу на 3 місяці;

4 (висока) — виникнення загрози ймовірне до 1 разу на тиждень;

5 (дуже висока) — виникнення загрози ймовірне до 1 разу на добу.

Тепер маючи всі необхідні дані можемо розрахувати ризики інформаційних активів автоматизованої системи.

Ризик розраховують за таким принципом:

Ризик = Імовірність * Збиток.

Таблиця 3

Класифікація загроз та ймовірності їх реалізації

Активи	Загрози	Вразливість	Імовірність реалізації загроз
Операційні системи	Фізичне пошкодження апаратури Відмова в роботі обчислювальної техніки Системні збої та помилки Неправильна робота систем захисту	Втрата засобів розмежування доступу (паролів) (розголошення), магнітних носіїв інформації та резервних копій Неправильна настройка та адміністрування системи захисту операційної системи Неправомірне вимкнення засобів захисту Відсутність резервного обладнання Несанкціоноване внесення змін до технічних засобів, у програмне забезпечення, в компоненти інформаційного забезпечення Запуск програм, здатних викликати незворотні зміни в системі	3
Програмне забезпечення	Збої та відмови обладнання та програмного забезпечення Пошкодження ПЗ Руйнування архівної банківської інформації або навмисне її знищення	Можливість використання ПЗ не за призначенням Недосконале або нове ПЗ Несфективне розмежування прав доступу до ПЗ Відсутність системи моніторингу роботи ІТ інфраструктури Відсутність або недосконалість системи резервного копіювання Дія вірусних програм	4
База даних з інформацією про склад персоналу	Здійснення несанкціонованого доступу до баз даних Модифікація, підміна, компрометація інформації	Перехоплення даних Пошкодження даних Помилки в роботі системи Помилки в алгоритмах програм Неправильне використання ПЗ Передавання паролів у відкритому вигляді Здійснення НСД шляхом злому паролів користувачів і адміністратора Помилки користувачів Шпигунство	2
База даних з інформацією про клієнтів банку			3
База даних з інформацією про валютні операції			3
База даних з інформацією про кредитування			3
Посадові інструкції співробітників	Несанкціонована модифікація, знищення	Втрата даних Підміна даних Збої та відмови ПЗ НСД	2
Кореспондентські рахунки НБУ та інших банків	Несанкціоноване ознайомлення Розкрадання, копіювання, модифікація	Крадіжка роздрукованих банківських документів	2

Закінчення табл. 3

Активи	Загрози	Вразливість	Імовірність реалізації загроз
Зразки і бланки заяв	Неможливість використання	Відсутність доступу до даних Збої в ПЗ Відсутні права доступу для певних груп користувачів	2
Цінні папери	Крадіжка, знищення	Ознайомлення банківських службовців з інформацією, до якої вони не повинні мати доступ Заволодіння інформацією з метою власної вигоди	4
Договори з партнерами	Недотримання умов договорів Несвоєчасне реагування на запити партнерів	Недбале зберігання та облік документів, носіїв інформації, даних Збої ПЗ Несумлінне ставлення до роботи працівників банку	3
Кредитні операції	Компрометація	Неправильний підбір персоналу Необізнаність персоналу у справах інформаційної безпеки Відсутність затвердженої процедури поводження з інформацією з обмеженим доступом	4
Платіжна інформація	Несанкціонована модифікація Знищення	Неефективність процедур контролю прав доступу Умисне пошкодження або знищення інформації зацікавленими особами	4
Фінансово-аналітичні відомості	Підміна даних	Неефективне розмежування права доступу до ПЗ Доступність інформації особам, що не мають відповідних повноважень	2
Службова інформація	Модифікація	Необізнаність персоналу у справах інформаційної безпеки Неефективне розмежування прав доступу	2

Для наочності в табл. 4 зображено градацію ризиків за ступенем їх важливості відносно до автоматизованої системи. Відповідно, темнішим кольором позначений високий рівень ризику, а світлішими — середній та низький. У табл. 5 наведено результати розрахунків ризиків відповідно до загроз інформаційним активам згідно з одержаними вище даними.

Отже, оцінивши ризики інформаційних активів автоматизованої системи банку та визначивши ступінь їх небезпечності, можна починати будувати систему захисту.

Для прийняття рішення щодо оброблення конкретних ризиків слід керуватися розрахованими даними, оскільки вони дозволяють чітко виявити найбільші ризики, показують які ресурси потребують більшої уваги при виборі засобів захисту.

Таблиця 4

Рівні ризиків

Імовірність / Збиток	Дуже низька	Низька	Середня	Висока	Дуже висока
Низький	1	2	3	4	5
Середній	3	6	9	12	15
Високий	5	10	15	20	25

Таблиця 5

Результати оцінки ризиків

Активи	Імовірність реалізації загрози	Збитки	Ризик
Операційні системи	3	5	15
Програмне забезпечення	4	5	20
База даних з інформацією про склад персоналу	2	3	6
База даних з інформацією про клієнтів банку	3	5	15
База даних з інформацією про валютні операції	3	5	15
База даних з інформацією про кредитування	3	5	15
Посадові інструкції співробітників	2	1	2
Кореспондентські рахунки НБУ та інших банків	2	3	6
Зразки і бланки заяв	2	1	2
Цінні папери	4	5	20
Договори з партнерами	3	5	15
Кредитні операції	4	5	20
Платіжна інформація	4	3	12
Фінансово-аналітичні відомості	2	3	6
Службова інформація	2	1	2

Висновки

У результаті дослідження було здійснено розрахунок ризиків інформаційних активів автоматизованої системи безпеки банку.

У процесі роботи було класифіковано інформаційні активи банківської АС, визначено загрози та оцінено ймовірність їх реалізації.

Проте під час здійснення аналізу ризиків безпосередньо в банку необхідно здійснити детальніший опис інформаційної системи та оцінювання активів усіх рівнів: матеріальних, нематеріальних, економічних, інформаційних.

Також необхідно врахувати людські ресурси, сервіси, що забезпечують роботу організації (електроенергія, телефонний зв'язок та ін.) та відповідно до визначених ризиків обрати засоби і заходи захисту системи.

ЛІТЕРАТУРА

1. *Информационная* технология. Рекомендации по менеджменту безопасности информационных технологий. Ч. 3. Методы менеджмента безопасности информационных технологий (ИСО/МЭК ТО 13335-3:1998) : ИСО/МЭК ТО 13335-3-2007. — [Дата введения 2007-09-01]. — М. : Стандартинформ, 2007. — 49 с. (Национальный стандарт Российской Федерации).

2. *Информационные* технологии. Свод правил по управлению защитой информации (ISO/IEC 27002:2005) : ИСО/МЭК 27002:2005. — [Дата введения 2005-10-15]. — М. : Технонорматив, 2007. — 183 с. (Международный стандарт).

3. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99. – [Чинний від 1999-07-01]. – К. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 24 с. (Нормативний документ).

Стаття надійшла до редакції 15.03.2012