УДК 004.725.5
DOI: 10.31673/2409-7292.2023.010004

Котенко А. М., Щебланін О. Ю.

МЕТОДИКА ОЦІНЮВАННЯ СИСТЕМИ ЗАХИСТУ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМЕРЦІЙНОГО БАНКУ

Розглянуто існуючі системи захисту автоматизованих систем. Зроблено аналіз загроз інформаційним ресурсам комерційного банку. Визначені складові інформаційної безпеки банківської установи. Показано склад автоматизованої банківської системи та її ядра – підсистеми "Операційний день банку". Розроблено рекомендації по побудові системи захисту інформаційних ресурсів комерційного банку.

Ключові слова: об'єкт інформаційної діяльності, автоматизована банківська система, операційний день банку, комплексна система захисту інформації, активні методи захисту, пасивні методи захисту.

Вступ

В сучасному суспільстві важливим ресурсом є інформація. Виходячи зі ступеню володіння інформацією можливо ефективно будувати будь-яку діяльність. Природньо, що зловмиснику для заволодіння доступом до інформації, що його цікавить, потрібно застосувати технічні та інші засоби. Тобто існують загрози інформації, а саме загрози несанкціонованого доступу до інформації та загрози її витоку технічними каналами. Це стосується також і банківської сфери. Тому питання захисту інформації банківської системи є актуальною задачею.

Основна частина

Взагалі нормативні документи технічного захисту інформації в Україні визначають, що для захисту інформації в автоматизованих системах (АС) створюється комплексна система захисту інформації (КСЗІ). Комплексна система захисту інформації - це взаємопов'язана сукупність організаційних, інженерних, технічних, криптографічних та інших заходів, засобів і методів для забезпечення безпеки інформації [1].

Комплексна система захисту інформації призначена для захисту інформації в АС від:

- витоку технічними каналами (електричний, радіоканал, оптичний, акустичний, матеріально-речовий;
- несанкціонованих дій з інформацією (порушення встановлених в АС правил розмежування доступу до інформації);
- спеціального фізичного впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і наслідком якого є порушення цілісності інформації та несанкціоноване блокування.

Також існує ще одна система захисту інформації – комплекс технічного захисту інформації (КТЗІ) від витоку технічними каналами. Цей комплекс може створюватися у вигляді самостійної системи, у випадку коли немає необхідності захищати інформацію від несанкціонованих дій, а також КТЗІ входить до складу КСЗІ.

Порядок створення КСЗІ викладено у НД ТЗІ 3.7-003-05. Створення КТЗІ визначено у НД ТЗІ 36-003-2016, а також іншими допоміжними нормативними документами ТЗІ.

Результатом дії КСЗІ та КТЗІ є забезпечення критерієв інформаційної безпеки – цілісності, конфіденційності, доступності.

Стосовно банківської системи. Враховуючи предметну специфічність АС банківської системи називається – автоматизована банківська система (АБС). АБС використовує ЕОМ і інших технічні засоби для збору даних, реєстрації їх, передачі, обробки, збереженні, тощо при управлінні банківською діяльністю.

АБС є інтегрованою системою. До її складу входять такі основні функціональні підсистеми АБС (рис. 1) [2]:

- операційний день банку (ОДБ);
- управління кредитними ресурсами (Кредити);

- управління валютними операціями (Валютні операції);
- управління депозитами (Депозити);
- управління цінними паперами (Цінні папери);
- управління касою (Каса);
- внутрибанківський облік (Внутрішній облік);
- управління розрахунками з використанням пластикових карток (Карткові операції);
- звітність, аналіз діяльності банку (Аналіз).

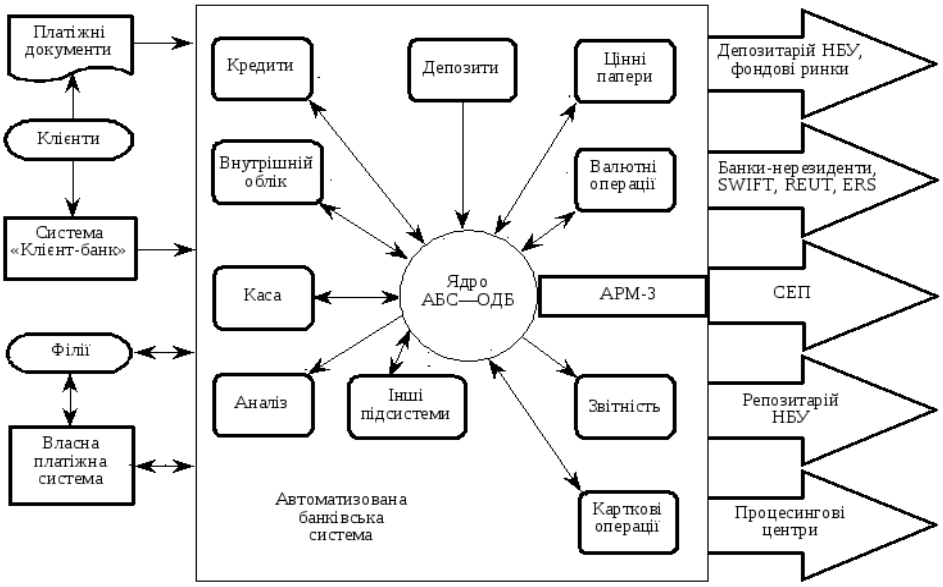

Рис. 1. Структура автоматизованої банківської системи

АБС – це високо технологічна система, яка інформаційно забезпечує функціонування банківської установи. Ядром АБС є підсистема "Операційний день банку" (ОДБ).

Усі загрози безпеці інформації АБС класифікуються наступним чином: програмно-математичні, інформаційні, фізичні, організаційно-правові, радіоелектронні. Дамо пояснення деяким конкретним загрозам.

Несанкціонований доступ – стосується комп'ютерних систем. Причина - порушення правил розмежування доступу до інформації в системі.

Маніпулювання даними – свідома дезінформація, приховування, фальсифікація даних у системі.

Встановлення програмних закладок – приховане встановлення у АС спеціальних програм. Мета – надання зловмиснику доступу до захищених інформаційних ресурсів АС.

Неправильне розмежування прав доступу – це надання визначених повноважень особам, які не є являються відповідальними, за конкретну технологічну операцію. Усі захищені АС містять засоби, які використовуються в критичних ситуаціях, у випадку коли користувачу потрібно мати доступ до усіх наборів системи. Звичайно ці засоби використовуються адміністраторами, системними програмістами, операторами та іншими користувачами. Надання таких повноважень більш широкому колу працівників є великою загрозою безпеці системи. Кожен користувач АС повинен мати обмежені його посадовими обов'язками права доступу до ресурсів АС. Набори прав доступу необхідно охороняти системою захисту від несанкціонованого їх захоплення.

Відомо, що у міжбанківських платежах в Україні у якості платіжного документу використовується електронний платіжний документ. Він має певну форму і свої засоби захисту, які надає НБУ кожному учаснику системи електронних платежів (СЕП). Основні задачі системи захисту СЕП наступні:

- захист від зловживань (неконтрольоване розшифрування повідомлень, наявнісьб зфальсифікованих повідомлень);
- автоматичне протоколювання користування банківською мережою для локалізації всіх порушників технології роботи у СЕП;
- захист від технічних пошкоджень і збоїв у роботі обладнання (поламки апаратних та програмних засобів, перешкоди у каналах зв'язку).

Вимоги які враховуються при розробці системи безпеки СЕП:

- система захисту СЕП охоплює усі етапи розробки, впровадження та експлуатації усього програмно-технічного комплексу СЕП;
- система безпеки поєднує організаційні, технічні, криптографічні засоби захисту;
- у системі конкретно розподілена відповідальність за усі різні етапи обробки та виконання платежів.

Оскільки робота СЕП забезпечується АБС ядром якої є підсистема ОДБ, можна визначитись зі складовими інформаційної безпеки АБС (рис. 2).

Рис. 2. Складові інформаційної безпеки банківської установи

Питання оцінки захищеності інформаційних систем (ІС) в Україні виникло на початку 2000 років зпід час появи міжнародних стандартів з управління інформаційною безпекою (ІБ). Стандарти містять вимоги до оцінювання стану ІБ.

Дана методика ґрунтується на дослідженнях в області ІБ [4], вітчизняні та міжнародні стандарти з управління ІБ [5]. Для практичної реалізації даної методики застосована система управління ІБ «Матриця» [5].

Процедура даної методики грунтується на оцінці ризиків ІБ і є наступною:

- первинне опитування клієнта;
- визначення активів;
- визначення важливості активів за словесною шкалою;
- пошук вразливостей визначених активів;
- визначення загроз, що походять від знайдених вразливостей;
- визначення ступеня небезпеки знайдених загроз за словесною шкалою;
- перевод важливості активів та ступеня небезпеки загроз у кількісні оцінки;
- підрахування оцінок ризиків;
- ранжування за сумарними оцінкам ризиків. Визначення найбільш вразливих активів та найбільш небезпечних загроз;
- ранжування вразливостей кожного активу;
- складання рекомендацій щодо усунення вразливостей та оформлення звіту.

Первинне опитування клієнта розуміє аналіз структури мережі, загроз ІБ у ній, перелік загроз, ранжування важливості активів для клієнта та облікові записи.

Визначення активів визначає складання списку активів клієнта (фізичні та інформаційні).

Визначення важливості активів за словесною шкалою. Кожному активу визначається словесна оцінка важливості. Приклад ступенів важливості: критичний, важливий, рядовий, маловажливий, неважливий.

Пошук вразливостей визначених активів робиться у відповідності з перевірками: перевірити на проникнення; визначити зловмисників серед співробітників даної організації; проаналізувати налаштування; проаналізувати можливість фізичного доступу до засобів комп'ютерної мережі і т.ін.

Визначення загроз, що походять від знайдених вразливостей. Необхідно визначити загрози для кожної з вразливості. Результатом цього етапу є складений перелік загроз.

Визначення ступеня небезпеки знайдених загроз за словесною шкалою. Дані первинного опитування клієнта аналізуються експертами перевіряючої сторони з урахуванням стандартів ІБ або бюлетенів Microsoft. Результатом кожній загрозі ставиться словесна оцінка рівня небезпеки. Рекомендовані оцінки: критична, важлива, середня, низька, малоймовірна.

Перевод важливості активів та ступеня небезпеки загроз у кількісні оцінки. З метою автоматизації оцінки ризиків необхідно перевести отримані словесні оцінки активів і загроз у кількісні. У таблицях 1 та 2 приведені рекомендовані шкали оцінок. Приклад результату даного етапу показано у таблицях 3 та 4.

Таблиця 1

Рекомендована шкала оцінок важливості активів

Важливість активу	Збиток при реалізації загроз (умовна оцінка)
Критичний	5
Важливий	4
Рядовий	3
Маловажливий	2
Неважливий	1

Таблиця 2

Рекомендована шкала оцінок ступеня небезпеки загроз

Рівень небезпеки загрози	Вірогідність реалізації (умовна оцінка)
Критичний	5
Важливий	4
Середній	3
Низький	2
Малоймовірний	1

Таблиця 3

Приклад оцінок важливості активів

Актив	Важливість	Збиток
Сервер доступу до Інтернет	Критичний	5
Сервер 1С:Підприємство, термінал.сервер	Критичний	5
Головний контролер домену	Критичний	5
Поштовий сервер	Важливий	4
Запасний контролер домену, сервер БД	Важливий	4

Таблиця 4

Приклад оцінок рівня небезпеки загроз

Загроза	Рівень небезпеки	Частота
Переповнення буфера	Критичний	5
Несанкціоноване отримання прав	Важливий	4
Виток інформації	Важливий	4
Віддалене виконання коду	Середній	3
Відмова в обслуговуванні	Низький	2

© Котенко, А. М., & Щебланін, О. Ю. (2023). Методика оцінювання системи захисту автоматизованих інформаційних ресурсів комерційного банку. Сучасний захист інформації, 1(53), 34–38. https://doi.org/10.31673/2409-7292.2023.010004.

Підрахування оцінок ризиків. Даний пункт виконується автоматизовано в СУІБ «Матриця». Виконуються певні дії у пункті головного меню «Списки елементів». Математичне підгрунття підрахування оцінки ризиків основано на множенні значення збитку активу на значення частоти загрози:

$$R = W \times n$$

де: R – ризик, W – збиток, n – частота загрози.

Визначення найбільш вразливих активів та найбільш небезпечних загроз робиться з використанням результату попереднього етапу ранжуванням полів даних.

Ранжування вразливостей кожного активу робиться щляхом групування вразливості по активах і вирахуванням сумарної оцінки ризику для кожної вразливості кожного активу. Математично числова сумарна оцінка ризику для вразливості конкретного активу обчислюється як сума оцінок ризиків від кожної загрози, джерелом якої є ця вразливість для цього активу:

$$V_a = \sum R_a = W_a \times \sum n_a$$

де: V_a – вразливість активу, R_a – ризик активу, W_a – збиток активу, n_a – частота загрози.

Складання рекомендацій щодо усунення вразливостей та оформлення звіту є заключним етапом Методики. Необхідно: скласти типові рекомендації по усуненню виявлених вразливостей ґрунтуючись на стандартах ІБ або бюлетенів Microsoft.

Скласти таблиці вразливостей для кожного активу з колонками: Вразливість, Загрози, Важливість (словесна оцінка сумарного ризику вразливості), Рекомендації.

Потім скласти звіт з таких розділів: терміни, визначення і скорочення, використані в звіті; цілі та сфера дослідження; дослідження вразливостей: виявлені уразливості та зведені дані щодо оцінок ризиків; рекомендації щодо усунення вразливостей; додаткові розділи (за потреби); загальні висновки. Дані розділи будуть відображати основні етапи оцінювання ризиків ІБ за Методикою.

Висновок

У статті показана структура автоматизованої банківської системи. Визначені загрози автоматизованої банківської системи. Проведено огляд способів забезпечення інформаційної безпеки автоматизованої банківської системи. Розроблена методика визначення ефективності системи забезпечення інформаційної безпеки автоматизованої банківської системи. Напрямом подальших досліджень може бути удосконалення даної Методики, обумовлене появою нових видів загроз інформаційної безпеки і, відповідно, появою нових методів та засобів захисту від них.

Перелік посилань

1. НД ТЗІ 3.7-003-05 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – 08 листопада 2005 р.

2. Г.А. Титоренко, В.І. Суворова, І.Ф. Возгілевич та ін. / Ред. Г.А. Титоренко. Автоматизовані інформаційні технології у банківській діяльності: Учб. посібник для ВНЗ / — М.: Фінстатінформ, 1997. – 268 с.

3. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с. ISBN 966-7992-36-5

4. Domarev D.V. Information security management system "Matrix" based on system approach // Проблемиінформатизаціїтауправління: Зб. наук. пр. – К.: НАУ, 2011. – Вип. 2(34). – С. 36 - 39. ISSN 2073-4751.

Надійшла: 27.12.2022 Рецензент: д.т.н., професор Кожухівський А.Д.