УДК 621.39

ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ РИЗИКІВ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Мокій А.В., Горицький В.М.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: andreymokiy@gmail.com

RESEARCH OF RISK MANAGEMENT METHODS IN THE INFORMATION SECURITY MANAGEMENT SYSTEM

The basic concept for ISMS on the basis of ISO 27001: 2013 is the risk of information security, and the toolkit is the risk management of the IB. The article deals with the methods of risk management IB based on the normative legal acts of the National Bank of Ukraine and international standards of the ISO 27K series.

Однією з важливих складових сучасних систем інформаційної безпеки (ІБ) є системи управління інформаційною безпекою (СУІБ). В концентрованому вигляді основні положення та вимоги щодо побудови СУІБ, які в подальшому можуть бути оцінені акредитованими органами з оцінки відповідності, викладені в серії міжнародних стандартів ISO 27K. Стандарт ISO 27001:2013 безпосередньо встановлює вимоги до СУІБ. Базовим поняттям для СУІБ на основі ISO 27001:2013 є ризик інформаційної безпеки, а інструментарієм – обробка ризиків ІБ. В статті розглядаються методи обробки ризиків ІБ на основі нормативно-правових актів Національного банку України та міжнародних стандартів серії ISO 27K.

Методологія оцінки ризиків може бути кількісною або якісною, або їх комбінацією.

На практиці якісна оцінка часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків.

Кількісна оцінка ризиків є більш складною та потребує більше часу та ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки. Якісна методика оцінки ризиків використовує шкалу атрибутів для опису

величини потенціальних наслідків реалізації загроз і вірогідність того, що такі наслідки виникнуть. Перевагою якісної методики є її простота розуміння всім персоналом. Недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз разом із вразливостями, з виникненням яких ці загрози можуть реалізуватися, та оцінки ймовірності їх реалізації для кожного бізнес-процесу/банківського продукту, мережі, обладнання, програмного забезпечення, які забезпечують функціонування цього бізнес-процесу/банківського продукту, мережі банку в цілому,

Можливими варіантами оброблення ризиків можуть бути:

- зниження ризиків шляхом застосування належних заходів безпеки;

- свідоме та об'єктивне прийняття ризиків за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;

- уникнення ризиків;

- перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

Для прийняття рішення щодо оброблення конкретних ризиків рекомендується визначити критерії стосовно кожного окремого ризику (низький ризик, середній ризик, високий ризик).

Застосування належних заходів безпеки дозволить зменшити ризики. Під час вибору цих додаткових заходів безпеки повинні бути враховані всі вимоги законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів, політики та стратегії банку.

Крім того, цей вибір також повинен враховувати вартість додаткових заходів безпеки, час їх впровадження, вплив на технологію операційної роботи, інтерфейс користувача тощо.

З урахуванням цих факторів складається план оброблення ризиків. У разі необхідності тривалої підготовки до впровадження додаткових заходів безпеки деякі ризики можуть бути тимчасово прийняти як залишкові з включенням до

наступного плану оброблення ризиків після перегляду оцінки ризиків. Прийняття всіх залишкових ризиків повинно бути задокументовано і затверджено керівництвом банку. Це стосується середніх та високих ризиків і повинно бути ретельно розглянуто. У документах стосовно прийняття залишкових ризиків має бути надана причина прийняття ризику та, за необхідністю, строки впровадження додаткових заходів безпеки для зниження ризику. Наприклад, якщо банком використовується програмно-технічний комплекс із застарілими технологіями, який має великий ризик реалізації однієї або декількох загроз і який планується замінити на новий більш сучасний комплекс протягом 2 років, то ці ризики можуть бути прийняти як тимчасове рішення до заміни цього програмно-технічного комплексу з наданням терміну впровадження нового.

Деякі ризики є властивістю існуючого бізнес-процесу/банківського продукту/програмно-технічного комплексу. Особливу увагу слід звернути на вразливості саме програмно-технічних комплексів, які використовують застарілі або новітні незахищені технології. В деяких випадках слід розглянути питання щодо уникнення ризиків за рахунок зміни операційного середовища, баз даних, програмно-технічного комплексу, технології оброблення та зберігання інформації, оскільки це буде вимагати менших витрат, ніж впровадження додаткових заходів безпеки.

Сучасні системи вразливі до ряду мережевих загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття, викривлення або модифікації інформації. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи управління безпекою та обробкою ризиків з послідуючою сертифікацією СУІБ в акредитованому органі з оцінки відповідності.

Література

1. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України від 01.03.2011.
2. ГАЛУЗЕВИЙ СТАНДАРТ УКРАЇНИ. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010.