УДК 004.056

ПІДХОДИ ДО БЕЗПЕРЕВНОГО УДОСКОНАЛЕННЯ МОДЕЛІ ЗАГРОЗ В ІНТЕРЕСАХ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40

The report analyzes the problem of constantly updating the threat model while ensuring the functioning of the information security management system. It is proposed to draw up a threat model in a Google-sheet, and to calculate information security risk according to the SRAMM methodology.

Однією з системних вимог до системи управління інформаційною безпекою (СУІБ, Information Security Management System, ISMS) є вимога постійного покращення якості даної системи. Логіка реалізації даної вимоги ще в стандарті ISO/IEC 27001-2005 була представлена у вигляді моделі PDCA (або моделі Шухарта-Демінга) - моделі як основи для всіх процедур управління інформаційною безпекою. Сутність даної моделі полягає в реалізації взаємопов'язаних процесів на етапі планування СУІБ, впровадження та функціонуванні її, моніторингу та покращення. Такими процесами є оцінка та обробка ризиків інформаційної безпеки (ІБ), обробка інцидентів ІБ, аудит, аналіз системи з боку менеджменту компанії та інші. Необхідність реалізації даної моделі була пов'язана з тим, що після розробки та в процесі функціонування СУІБ в компанії, яка її експлуатувала, могли бути зміни в бізнес-процесах, а також з'являтися нові загрози та вразливості. В умовах значних змін в безпековій ситуації навколо компанії необхідна була переоцінка ризиків ІБ з удосконаленням заходів захисту критичних інформаційних активів.

Для необхідності якісної реалізації процесу переоцінки ризиків необхідна постійна оцінки загроз та вразливостей, тобто постійна переоцінка моделі загроз для компанії з урахуванням безпекової ситуації як з компанією, так і в регіоні, країні та світі [1].

Для постійного удосконалення моделі загроз необхідно використовувати ресурси, в які можна оперативно вносити зміни для тих загроз, які вже були проаналізовані, та вносити нові загрози, надавати допуск для експертів інформаційної безпеки, а також менеджменту компанії. На наш погляд, ефективною технологією для рішення цього завдання є Google Таблиці.

Google Таблиці – це онлайн-додаток, за допомогою якого можна створювати та форматувати таблиці, а також працювати над ними спільно з іншими користувачами [2]. При роботі з цими таблицями можна додавати до таблиць текст, цифри та формули, а також редагувати та форматувати ці дані. Google Таблиці відповідають тим самим вимогам щодо забезпечення конфіденційності та захисту даних, які застосовуються до інших корпоративних сервісів Google Cloud. Корпорація Google використовує передові технології для захисту даних, у тому числі від шкідливого програмного забезпечення. Таблиці Google дозволяють зберігати файли в хмарі, а не локально, що знижує ризики для пристроїв компанії. Всі файли, завантажені на Google Диск або створені в Таблицях, шифруються не тільки під час передачі, але й при зберіганні.

Яка структура таблиці може бути та які сервіси в ній мають бути при побудові та корекції моделі загроз? Якщо аналізувати тільки модель навмисних загроз – модель порушника, то основними складовими даної таблиці мають бути: перелік критичних активів, перелік потенційних загроз для кожного з активів, опис загроз, опис вразливостей для даних активів, рівень загрози та рівень вразливості відповідно тієї методики, яка використовується. Дана таблиця може бути удосконалена розрахунком ризику ІБ. В доповіді приведений приклад Google-Таблиці загроз для навчальної ситуації, приведені приклади оцінки рівнів загроз та вразливостей для методики CRAMM, та приведений приклад оцінки ризику ІБ відповідно механізму розрахунку згідно даної методики.

Методика CRAMM спочатку був розроблена CCTA (Central Computer and Telecommunications Agency) у 1985 році у відповідь на зростаючу потребу в безпеці інформаційних систем. Дана методика на даний час є кращою методикою для використання в урядових департаментах Великобританії та прийнятий багатьма комерційними організаціями та іншими державними адміністраціями по всьому світу [3].

В доповіді запропоновані рішення дозволяють здійснювати постійне оновлення моделі загроз з урахуванням вразливостей, через які ці загрози здійснюють вплив з автоматизованим розрахунком ризику ІБ по методиці CRAMM.

Список використаних джерел:

1. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iso.org/standard/80585.html.

2. Приймайте обґрунтовані рішення, аналізуючи дані в Google Sheets [Електронний ресурс]. // Google – Режим доступу до ресурсу: https://www.google.com/intl/ru_ua/sheets/about/.

3. CRAMM (CCTA Risk Analysis and Management Method) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.