УДК 005.7:519.8

ШЛЯХИ ПОБУДОВИ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

Борисенко Леся Андріївна
студентка V курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті відображена важливість розробки та впровадження системи менеджменту інформаційної безпеки. Визначено доцільний математичний апарат для прийняття рішень в умовах апріорної невизначеності. Запропоновано підхід до побудови системи менеджменту інформаційної безпеки в умовах апріорної невизначеності.

Ключові слова: інформаційна безпека, невизначеність, оптимальна стратегія, система менеджменту інформаційної безпеки, теорія ігор.

Забезпечення системи захисту інформації є однією з найважливіших актуальних проблем сьогодення. Стрімкий розвиток суспільства призвів до широкого використання в усіх сферах діяльності швидкодіючих інформаційних систем та технологій. Одночасно збільшилися загрози для інформації, тяжкість наслідків реалізації яких посприяли оновленню розуміння захисту інформації, який полягає у забезпеченні цілісності, доступності та конфіденційності інформації. Сучасне підприємство має на увазі не тільки організацію робочого процесу та документообігу, а й захист конфіденційної інформації, що циркулює у певному приміщенні. Її витік може призвести до серйозних наслідків: втрата таємниць компанії, санкції контролюючих органів, погіршення іміджу компанії, втрата особливо важливої інформації. Саме тому для попередження витоку конфіденційної інформації та уникнення вищеперерахованих наслідків, кожна компанія та підприємство має подумати про проблему витоку інформації та організувати на своїй території систему протидії намірам зловмисників.

Впровадження системи менеджменту інформаційної безпеки (далі – СМІБ) є стратегічним рішенням організації. На проектування СМІБ компанії впливають потреби та цілі підприємства, вимоги безпеки, використовувані процеси, а також масштаби діяльності і структура організації. Загальноприйнятим є факт, що стандарт ISO/IEC 27001:2013 містить кращі практики і принципи з управління інформаційною безпекою компанії, впровадження яких дозволить забезпечити захист від сучасних інформаційних ризиків. Проте ті організації, які не стикались із загрозами втрати конфіденційних даних, мають повну невизначеність у побудові СМІБ. З огляду на це, метою статті була поставлена розробка шляху побудови систем менеджменту інформаційної безпеки в умовах апріорної невизначеності.

Система менеджменту інформаційної безпеки – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Вона повинна забезпечувати гарантію досягнення таких цілей, як забезпечення конфіденційності критичної інформації, неможливості виникнення несанкціонованого доступу до критичної інформації, цілісності інформації та пов’язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей [1].

Незамінним елементом на шляху створення цілісної системи менеджменту інформаційної безпеки виступає сімейство міжнародних стандартів ISO 27000, а саме ISO/IEC 27001:2013 та ISO/IEC 27003:2017. Вони забезпечують такі питання, як політика та організація інформаційної безпеки, процеси СМІБ, визначення статусу заходів щодо забезпечення інформаційної безпеки, використання зовнішніх та внутрішніх аудитів для визначення відповідності СМІБ, а також розглядають підходи до управління ризиками, активами та інформаційною безпекою відповідно до законодавства.

Взагалі розробка та впровадження системи менеджменту інформаційної безпеки – відповідальний та достатньо довготривалий процес, що охоплює декілька етапів, перелічені нижче.

1) Прийняття рішення керівництвом компанії про створення системи менеджменту інформаційної безпеки.

2) Підготовка до створення СМІБ. Цей етап включає в себе створення команди, яка буде відповідати за впровадження системи менеджменту інформаційної безпеки, ознайомлення цих співробітників з нормативно-методичним забезпеченням, а далі – вибір галузі діяльності компанії, яка буде охоплена системою менеджменту інформаційної безпеки.

3) Аналіз різноманітних ризиків. Цей етап повинен відображати результати проведення таких процесів:

- ідентифікація активів у межах обраної частини діяльності;
- визначення цінності ідентифікованих активів;
- ідентифікація загроз та вразливостей для ідентифікованих активів;
- оцінка ризиків для можливих випадків успішної реалізації загроз інформаційній безпеці щодо ідентифікованих активів;
- вибір критеріїв прийняття ризиків;
- підготовка плану обробки ризиків [2].

Отже, зазначений етап включає процес оцінки ризиків інформаційної безпеки, спрямований на ідентифікацію ризиків, пов'язаних із втратою конфіденційності, цілісності та можливості застосування інформації в рамках галузі дії системи менеджменту інформаційної безпеки.

4) Розробка політики системи менеджменту інформаційної безпеки на основі результатів аналізу попередніх етапів.

5) Впровадження системи менеджменту інформаційної безпеки в експлуатацію. При впровадженні СМІБ у роботу компанії повинні бути задіяні всі розроблені методи та методики, які здатні реалізувати та досягти первинно обрані цілі.

Очевидно, що етап аналізу ризиків є найважливішим для розробки ефективної системи менеджменту інформаційної безпеки, але в умовах апріорної невизначеності, з якою стикається доволі широкий пласт компаній, майже неможливо правильно та чітко оцінити ризики виникнення тієї чи іншої загрози. Отже, однією з головних проблем прийняття рішень у умовах апріорної невизначеності є її власне розкриття. У дослідженні операцій розроблено спеціальні математичні методи, призначені для кількісного обґрунтування рішень в умовах невизначеності.

Вагомим внеском у виборі засобів захисту конфіденційних даних при розробці системи менеджменту інформаційної безпеки є результати математичних перетворень. Перелік останніх, в свою чергу, визначається за допомогою підсумку аналізу наявних ризиків та уразливостей активів.

Для того, щоб знайти оптимальний математичний апарат, який може стати в нагоді у пошуку найкращої стратегії при побудові СМІБ в умовах апріорної невизначеності, досліджено метод аналізу ієрархій, теорію корисності, а також теорію ігор, яка має досить широку класифікацію. Перелічені математичні методи мають безліч переваг та можуть бути застосовані при прийнятті рішень у розробці системи

менеджменту інформаційної безпеки. Але слід відмітити, що вищезазначені теорії, окрім однієї, засновані на виборі певних критеріїв, на знаннях про визначені ризики та загрози, що має організація. Таким чином, при дослідженні теорії ігор був відокремлений розділ, що стосується ігор з природою, в яких усвідомлено діє тільки один гравець, а інший – навмання. Природа не має на меті отримання виграшу, що і відрізняє цей тип ігор від інших. Отже, в якості шляху побудови СМІБ в умовах апріорної невизначеності, буде використана теорія ігор ходом природи. Слід зазначити, що природа – узагальнене поняття супротивника, який не переслідує власних цілей у конфлікті. Відповідно, в іграх з природою задача вибору оптимальної стратегії для гравця з одного боку полегшується, а з іншого – ускладнюється через дефіцит інформації про поведінку природи.

Взагалі, управління інформаційною безпекою певною мірою і є грою – уповноважена особа компанії захищається від атак зловмисника, а той, в свою чергу, шукає слабкі сторони в системі захисту інформації організації для отримання власної вигоди. Як правило, при побудові СМІБ переважна кількість рішень приймається в умовах невизначеності. Саме тому є важливим дослідження математичних апаратів, які можуть надати інформацію для прийняття доцільних рішень.

Прийняття рішення в умовах апріорної невизначеності полягає у визначенні найбільш оптимальної стратегії, успіх реалізації якої залежить від певних невизначених факторів, що не відомі в момент прийняття рішення. Як було визначено, допоміжним математичним апаратом в цьому питанні виступає теорія ігор ходом природи. Її використання передбачає застосування таких критеріїв оптимальності, як критерій оптимізму, песимізму, Лапласа, Вальда, Севіджа та Гурвіца [3]. Обґрунтувати використання критеріїв оптимальності досить легко, оскільки причина полягає в неможливості передбачити наслідки вибору певного засобу захисту адміністратором безпеки в умовах апріорної невизначеності. Вибір комбінацій критеріїв оптимальності залежить від політики компанії, для якої розробляється система менеджменту інформаційної безпеки, яка може бути більш оптимістична або більш песимістична з елементами обережності вибору.

Отже, запропонований підхід може бути використаний компаніями, які мають на меті захистити свої активи для знаходження балансу інтересів бізнесу та інформаційної безпеки, а також для підвищення довіри зацікавлених сторін, але стикнулися зі станом невизначеності при побудові СМІБ.

Список джерел:

1. Система управління інформаційною безпекою як ключовий чинник успішності організації [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://ua.ikmj.com/isms/.

2. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.iso.org/standard/54534.html.

3. Критерії опимальності в умовах повної невизначеності [Електронний ресурс] – Режим доступу до ресурсу: https://lubbook.org/book_411_glava_7_Tema_7._Pravove_reguljuvannja_.html.

4. Ігри з природою в умовах невизначеності [Електронний ресурс] – Режим доступу до ресурсу: https://moodle.kstu.ru/mod/book/view.php?id=11481.

5. Сааті Т. Прийняття рішень. Метод аналізу ієрархій / Т. Сааті. – М.: Радио и связь, 1993. – 278 с.

6. Вертакова Ю. В. Теорія корисності та її використання для пошуку рішення [Електронний ресурс] / Ю. В. Вертакова. – 2005. – Режим доступу до ресурсу: https://laws.studio/upravlencheskie-resheniya-uch/teoriya-poleznosti-ispolzovanie-dlya-poiska-25828.html.