

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналізу інформаційних ризиків в нашій країні традиційно не приділяли належної уваги до прийняття рішення «Про Доктрину інформаційної безпеки України» в 2017 році [1]. Проте, за останні роки проблематика за цією темою активно досліджується і деякі рішення впроваджуються на практиці фахівцями в області інформаційної безпеки (ІБ). При цьому особлива увага приділяється практичному застосуванню існуючих методологій аналізу ризиків та їх вдосконаленню.

На сьогоднішній день в наявності є безліч методик аналізу ризиків. Деякі з них засновані на досить простих табличних методах і не припускають використання спеціалізованого програмного інструментарію, інші, навпаки, активно його застосовують. Незважаючи на підвищення інтересу до управління ризиками, методики, що використовуються в даний час, відносно неефективні, оскільки цей процес у багатьох організаціях здійснюється кожним підрозділом незалежно. Централізований контроль над їхніми діями часто відсутній, що виключає можливість реалізації єдиного і цілісного підходу до управління ризиками у всій організації.

Для розв'язання задачі оцінки ризиків інформаційної безпеки в даний час найбільш часто використовуються наступні програмні комплекси: CCTA Risk Analysis and Management Method (CRAMM), розроблений агентством з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency); Facilitated Risk Analysis Process (FRAP); RiskWatch; Microsoft Security Assessment Tool (MSAT); ГРИФ; CORAS; Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE); Oracle Crystal Ball; SecureWatch; Information Security Risk Analysis Method (ISRAM) і ряд інших [2, 3]. Всі відомі методики можна розділити на три групи:

- методики, що використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»), до таких методик, зокрема, відноситься CRAMM, FRAP, MSAT, CORAS;
- кількісні методики (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат), до цього класу належать методики Oracle Crystal Ball, SecureWatch, ISRAM;

– методики, що використовують змішані оцінки (такий підхід використовується в RiskWatch, OCTAVE, та ГРИФ).

Для оцінки та порівняння представлених методів аналізу та управління ІТ-ризиками використовується стандарт «Control Objectives for Information and Related Technologies» (COBIT) [4] – пакет документів, що описують універсальну модель управління інформаційними технологіями. В COBIT детально описані цілі і принципи управління, об'єкти управління, чітко визначені всі ІТ-процеси (завдання), що протікають в компанії, і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі ІТ-процесів також приведені практичні рекомендації по управлінню ІТ-безпекою.

Аналіз представлених методів показав ряд недоліків: відсутні механізми управління ризиками залишкового рівня, а також не проводиться оцінка якості процесу реагування на інциденти в області інформаційної безпеки. Крім того, жоден з методів не дає докладних рекомендацій стосовно періодичності проведення оцінок ІТ-ризиків.

У тих випадках, коли потрібно виконати тільки разову оцінку рівня ризиків в організації середнього розміру, доцільно рекомендувати використання методики CORAS. Для управління ризиками на базі періодичних оцінок на технічному рівні найкраще підходить CRAMM. Методики MSAT і RiskWatch кращі для використання у великих організаціях, де передбачається впровадження управління ризиками ІБ на базі регулярних оцінок, на рівні не нижче організаційного і потрібна розробка обґрунтованого плану заходів щодо їх зниження.

До прийняття рішення про впровадження тієї чи іншої методики управління ризиками ІБ слід переконатися, що вона досить повно враховує бізнес-потреби організації, її масштаби, а також відповідає кращим світовим практикам і має ґрунтовний опис процесів і необхідних дій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. Дата оновлення: 28.02.2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 12.04.2020).
2. Agrawal V. A Comparative Study on Information Security Risk Analysis Methods. Journal of Computers. 2017. Vol. 12, No. 1. P. 57–67.
3. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1(49). С. 15–26.

4. Метод COBIT. URL: <https://www.isaca.org/resources/cobit> (дата
звернення: 12.04.2020).