УДК 004.056
О. Б. Король,
Тернопільський національний технічний університет імені Івана Пулюя, Україна

УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

O.B. Korol

INFORMATION RISK MANAGEMENT

Із стрімким розвитком інформаційних технологій, найважливішим ресурсом у світі стала інформація. Та чим важливіший ресурс тим більше він потребує захисту. Адже інформація зберігає свою цінність до тих пір, поки вона секретна. Для забезпечення інформаційної безпеки використовується управління та оцінка ризиками.

Метою процесу управління ризиками інформаційної безпеки є виявлення, контроль та мінімізація невизначеності впливу чинників дестабілізації. Виділяється чотири основні етапи управління ризиками інформаційної безпеки, яке здійснюється з метою забезпечення неперервності функціонування корпоративної мережі зв'язку, зокрема підсистеми систем захисту інформації:

1. Аналіз ризику. Виявлення та оцінка чинників дестабілізації, які можуть скомпрометувати важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення чинників дестабілізації і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.
2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності вразливостей, величини завданого збитку.
3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування систем захисту інформації.
4. Оцінка вразливостей та контролів. Аналіз основних властивостей корпоративної мережі зв'язку та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів інформаційної безпеки та виявлення недоліків в її реалізації. Представимо графічне зображення життєвого циклу процесу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування.

Нижче наведені короткі описи ряду поширених методи аналізу ризиків. Їх можна розділити на:

1. Методики, які використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»). До таких методи, зокрема, відноситься FRAP;
2. Кількісні методики (ризик оцінюється через числове значення, наприклад розмір очікуваних річних втрат). До цього класу належить методика RiskWatch;
3. Методики, які використовують змішані оцінки (такий підхід використовується в CRAMM, та такою методикою користується корпорація Microsoft).

Отже, аналіз ризиків потребує терпіння, чесності та досвіду роботи системного аналітика. У свою чергу це вимагає наполегливості, самонавчання та постійного моніторингу сучасних методик та технологій оцінки ризиків. Завдяки цьому – управління та оцінка ризиків інформаційної системи забезпечуватиме цінність, захист та безпеку інформації, котра обробляється, використовується та циркулює у межах організації.