Д. Е. Вельков, Я. И. Фролов

ПРОГРАММНЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ

Объектом анализа являются программные методы оценки рисков, такие как CRAM, FRAP и RiskWatch

Введение

Оценка риска – это совокупность аналитических методов, позволяющих прогнозировать возможность получения дополнительного дохода или определенной величины ущерба. Это позволяет минимизировать последствия рисковой ситуации и своевременно принять меры по предотвращению риска. Потерями будем считать случайное отклонение прибыли, дохода, выручки в сторону снижения. в сравнении с ожидаемыми величинами. Предпринимательские потери - это в первую очередь случайное снижение предпринимательского дохода. Именно величина таких потерь и характеризует степень риска. Отсюда анализ риска прежде всего связан с изучением потерь. Риск-ориентированный подход к решению задач управления информационной безопасностью лежит в основе таких стандартов на системы менеджмента, как ISO 27001, ГОСТ Р 27001, СТО БР ИББС, Basel II, UK Turnbull Guidance, SOX и др.

I. Программные методики оценки рисков

Распространённые программные методики анализа рисков можно разделить на:

- методики, использующие оценку риска на качественном уровне. Пример: FRAP;
- количественные методики. Пример: методика RiskWatch;
- методики, использующие смешанные оценки. Пример: CRAMM, методика Microsoft.

Методика "Facilitated Risk Analysis Process (FRAP)"предлагается компанией Peltier and Associates.В методике обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере ИБ - процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом. Компания RiskWatch разработала собственную методику анализа рисков и семейство программный средств, в которых она в той либо иной мере реализуется.

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный профиль (Government profile).

Заключение

Оценка рисков является неотъемлемой часть любого вида деятельности. Внедрение системы менеджмента качества ISO 31000 убедительно доказало, что оценка рисков является неотъемлемой частью успешного развития науки, технологий и инновационной экономики.

В то же время существует множество разнообразных методов и алгоритмов для оценки рисков. Выбор методики оценки рисков каждом конкретном случае является наукоемким и требует больших материальных ресурсов.

Список литературы

1. Bjorn, A. G. CORAS, A Platform for Risk Analysis on Security Critical Systems: Model-based Risk Analysis Targeting Security / A. G. Bjorn// – 2002. – P. 5–8.
2. OCTAVE Method Implementation Guide Version 2.0 / Carnegie Mellon University // Mode of access: http://www.cert.org. – Date of access: 14.05.2021.

Вельков Дмитрий Евгеньевич, студент 3 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлекстроники, velkov2000@list.ru.

Фролов Ярослав Ильич, студент 3 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлекстроники, iaroslav_frolov@mail.ru.

Научный руководитель: Гуринович Алевтина Борисовна, доцент кафедры вычислительных методов и программирования Белорусского государственного университета, кандидат технических наук, gurinovich@bsuir.by.