СПЕЦИФИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Анищенко В.А.

Анищенко Виктор Александрович – студент магистратуры,
факультет прикладной математики и информатики,
Московский авиационный институт,
Учебный центр «Интеграция», г. Серпухов

Аннотация: *в статье рассмотрены основные моменты, влияющие на оценку рисков для информационной безопасности предприятий.*
Ключевые слова: *оценка рисков, информационная безопасность, защита.*

Современные отделы стратегического управления организацией не способны обойтись без оценки наиболее вероятных и критичных рисков информационной безопасности (ИБ), т.к. от этого зависит успешность деятельности компании [1]. Существует ряд методологий, посредством которых производится оценка рисков (ОР), в частности:

- CRAMM - методология, используемая в правительстве Великобритании;
- OCTAVE – методология оценки уязвимости ИБ;
- NIST SP800-30 – методология УР в системе информационных технологий;
- ИБ - ISO / IEC 27005: 2011 – стандарт, определяющий количественные и качественные методы управления рисками (УР);
- ENISA – свод правил по ОР ИБ.

С помощью методов ОР ИБ организации, можно выявить и рассчитать:

- объемы информационных активов (ИА);
- денежную ценность активов;
- угрозы, которые критично отражаются на ИА;
- средства защиты приоритетных активов;
- угрозы возможных потерь.

Специалисты в области ОР ИБ осуществляют такой комплекс работ:

- точную и регулярную инвентаризацию ИА и их стоимости;
- обоснование и использование методологии, позволяющей осуществлять эффективную ОР для конкретных сценариев развития риска в отдельной компании;
- анализ наиболее вероятных уязвимостей и угроз;
- планирование мер, нацеленных на поддержку и повышение уровня ИБ;
- разработку матриц рисков;
- ОР общей безопасности хранения и обработки информации;
- формирование отчетов о результатах работы;
- разработка плана по минимизации уровней рисков.

Результатом работ по ОР являются:

- подготовка общей карты ИА компании;
- разработка концептуальной карты рисков;
- создание отчетно-графических документов по результатам проведенной ОР;
- разработка плана по дальнейшей обработке рисков.

Проведение ОР ИБ организации позволяет:

- обратить внимание руководства на наиболее актуальных и приоритетных проблемах;
- разработать превентивные меры для предотвращения возможного вреда компании [2].

Обеспечение ИБ организации часто дополнительно осуществляется посредством разработки и применения методов защиты информации, для чего создается отдельная система - комплексная система защиты информации (КСЗИ).

В ряде случаев, когда организация разрабатывает собственную политику обеспечения ИБ, она может руководствоваться:

- международными стандартами ISO / IEC 17799: 2005, ISO / IEC 27001: 2005, что особенно эффективно на основе COBIT. В таком случае в организации имплементируется существующая система управления ИБ согласно установленным стандартам;
- собственными сертифицированными разработками.

Для того чтобы обеспечить достаточный уровень ИБ организации на практике разрабатывается унифицированная система обеспечения ИБ. Она включает в себя некоторую совокупность мер программно-технического (ПТ) и организационного уровней, которые направлены на обеспечение

защиты ИА, от потенциальных, наиболее вероятных и критичных, угроз. Меры, направленные на защиту организационного уровня, применяются на базе соответствующих мероприятий, которые предусмотрены используемой политикой ИБ. Меры защиты ПТ уровня как правило включают адаптацию математических методов защиты информации и интеграцию технических аппаратных средств защиты [3].

Экономический эффект от внедрения подобной системы выражается в виде уменьшения значений возможного репутационного и материального видов ущерба, которое наносится предприятию, за счет применения мер для поддержания режима ИБ.

Эффективно идентифицировать весь перечень нужных мер по защите информации, выбрать перспективную стратегию развития информационной архитектуры и инфраструктуры организации и постоянно поддерживать на высоком уровне ИБ организации становиться возможным лишь после проведения аудита уязвимостей и анализа рисков.

Наиболее часто используемой на практике методикой ОР ИБ является –NIST, разработанная в США [3]. Она охватывают достаточно значительный ряд вопросов, которые связаны со стратегией УР, однако, не имплементирует никаких средств НЛ, что не позволяет в полной мере учесть специфику взаимосвязи факторов влияния и неопределенностей.

Список литературы

1. *Акимов В.А.* Нечеткие модели в природе, техносфере, обществе и экономике / В.А. Акимов, В.В. Лесных, Н.Н. Раднаев. М.: Деловой экспресс, 2004. 352 с.
2. *Аронов И.З.* Современные проблемы безопасности технических систем и анализа риска / Аронов И.З. // Стандарты и качество, 1998. № 3. С. 451.
3. *Борисов В.В.* Нечеткие модели и сети. / В.В. Борисов, В.В. Круглов, А.С. Федулов, М.: Горячая линия-Телеком, 2007. 284 с.