Анализ рисков информационной безопасности, или Как обосновать затраты на информационную безопасность.

/Артемий ПОНОМАРЕВ, ведущий специалист НИИ ЭИТТ, Астана, ponart@mail.ru/

Как правильно обосновать затраты на информационную безопасность (ИБ) в коммерческой организации? На какие угрозы ИБ следует в первую очередь обратить внимание? Ответы на эти вопросы должен дать анализ рисков ИБ.

Табл. 1 Матрица уровня риска

Вероятность угрозы	Ущерб		
	Низкий	Средний	Высокий
Низкая	Низкий	Низкий	Низкий
Средняя	Низкий	Средний	Средний
Высокая	Низкий	Средний	Высокий

Система защиты информации (СЗИ) создается с целью противодействия угрозам безопасности информации, которые носят вероятностный характер. Результатом проявления угрозы является ущерб собственнику информационного ресурса. Таким образом, можно говорить о том, что собственник информационного ресурса действует в условиях риска. В информационной безопасности под риском информационного ресурса понимается мера ожидаемых потерь информационного ресурса от угрозы. Создание СЗИ и совершенствование существующей СЗИ предполагает применение методологии анализа рисков ИБ. Под анализом рисков ИБ будем понимать систематическое исследование информационных процессов с целью выявления угроз информации, оценки рисков ИБ, выработки стратегии по управлению рисками ИБ.

Анализ рисков является основой для управления ИБ в американском стандарте национального института по стандартам и технологиям NIST [1], британском стандарте по управлению ИБ BS ISO/IEC 27001:2005, где приводится общая методология анализа рисков для организаций.

Кроме того, в настоящее время, существуют коммерческие программные продукты, которые так же оценивают риски для организаций и выдают некоторые рекомендации по усовершенствованию существующих систем. Обычно такие программные продукты строятся на основе вопросных листов, после ответа на вопросы, программа решает, какие меры следует предпринять. Можно выделить три программных продукта CRAMM, RiskWatch, ГРИФ. Но не следует думать, что данные программные продукты предназначены для неподготовленных людей, они ориентированы на пользователей, обладающих специальной подготовкой и высокой квалификацией. Так, например, в качестве входных данных программного продукта CRAMM, используется следующая информация: ресурсы системы (оценка их стоимости), угрозы (идентифицируются и оцениваются) и уязвимости [2]. Оценка производится согласно выбранной шкале. Далее программа предлагает варианты мер противодействия выявленным рискам.

Можно выделить три сформировавшихся направления анализа рисков ИБ[3, 4]:

- качественная оценка рисков;
- количественная оценка рисков;
- методики и коммерческие программные продукты, в которых может быть реализована количествен-

ная либо качественная оценка рисков, или оба подхода сразу.

КАЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ

Качественная оценка обычно сводится к введению некоторых качественных шкал оценки показателей для оценки вероятности угрозы (например, низкая, средняя, высокая) и оценки ущерба от угрозы (низкий, средний, высокий). После оценки уровня риска (Табл. 1) должны быть приняты решения по принятию либо дальнейшему снижению низкого уровня риска, разработан план по устранению угроз со средним уровнем риска и немедленно приняты меры по снижению высокого уровня риска *(см. табл.1).*

Достоинствами качественной оценки рисков являются:

- ускорение и упрощение анализа рисков;
- отсутствие необходимости оценивать в денежных единицах стоимость ресурса;
- отсутствие необходимости вычислять вероятности проявления угрозы;
- отсутствие необходимости вычислять соответствие применяемых мер угрозам.

КОЛИЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ

Количественная модель рисков оперирует такими понятиями как [3]:

- годовая частота происшествия (англ. Annualized Rate of Occurrence – ARO);
- ожидаемый единичный ущерб (англ. Single Loss Expectancy – SLE);
- ожидаемый годовой ущерб (англ. Annualized Loss Expectancy – ALE), величина, равная произведению ARO на SLE:

$$ALE=ARO \times SLE, \quad (1)$$

где: ARO – это частота появления события, приносящего ущерб в год; SLE – показатель, который рассчитывается как произведение стоимости информации (Asset Value – AV) на фактор воздействия (англ.Exposure Factor – EF)

$$SLE=AV \times EF, \quad (2)$$

где: фактор воздействия (EF) - это размер ущерба или влияния на значение актива (от 0 до 1), т. е. часть значения, которую актив потеряет в результате осуществления угрозы.

Управление рисками считается эффективным, если расходы на безопасность в год не превышают ожидаемый годовой ущерб.

СТРАТЕГИИ УПРАВЛЕНИЯ РИСКАМИ

Этап управления рисками следует, после того как оценены частные риски, т. е. риски по каждой угрозе. Управление должно заключаться в применении некоторой стратегии управления рисками с целью минимизации общего риска.

Управление рисками предполагает принятие мер, направленных на снижение частоты реализации угроз и снижение ущерба от них. В зависимости от полученных показателей рисков собственник информационных ресурсов должен выбрать стратегию управления рисками. Существуют следующие стратегии:

1). Принятие риска – собственник информационных ресурсов считает, что риск мал и не предпринимает никаких мер;

2). Снижение (уменьшение) риска – собственник информации осуществляет меры по снижению показателя риска для информационных ресурсов;

3.Исключение риска – собственник информационного ресурса предпринимает меры, которые позволяют полностью исключить частный риск;
4). Передача риска третьим лицам – меры, предпринимаемые собственником с целью возмещения возможных последствий наступления риска (страхование).

МИНИМИЗАЦИЯ ОБЩЕГО РИСКА

Общий риск для информационных ресурсов организации складывается из всех существующих угроз безопасности информации; управление общим риском должно заключать в себе меры, направленные на его снижение:

$$R_o = \sum_1^n R_1, R_2, ..., R_n \rightarrow \min \quad (3)$$

где: R_o – общий риск, $\sum_1^n R_1, R_2, ..., R_n$ – сумма всех частных рисков (рисков по каждой угрозе). Поэтому иногда следует пренебречь некоторым частным риском, чтобы снизить общий риск за счет снижения других рисков с большими показателями.

Таким образом, целью проведения анализа рисков должно стать снижение общего риска ИБ, которое достигается выбором эффективной стратегии управления частными рисками по каждой угрозе ИБ.

Литература:

1. NIST Special Publication 800-30 Rev A. Risk management Guide for information Technology Systems / G. Stoneburner, A. Goguen, A. Feringa, recommendation of the National institute of standards and technology, Washington: U.S. Government printing office, 2002. – 58p.

2. Методы и средства анализа рисков и управление ими в ИС [Электронный ресурс] / www.bytemag.ru // журнал BYTE-Россия, – 2005. –№12, – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=9076, свободный. - Электрон. версия печ. публикации.

3. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия / И. Р . Конев, А. В. Беляев. – СПб.: БХВ-Петербург, 2003. – 752: ил.

4. Симонов, С. В. Методология и технологии анализа рисков / С. В. Симонов // Вопросы защиты информации. Научно-практический журнал. – М. – 2003. –№ 1. – С. 25- 33.