*Александр КАМИНСКИЙ, МЭА*

# ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

*This work describes the methods and techniques Assessment and risk management information systems, their classification and species.*

Понятия «оценка рисков» (Risk Assessment) и «управление рисками» (Risk Management) появились сравнительно недавно и сегодня вызывают постоянный интерес специалистов в области обеспечения непрерывности бизнеса (Business Continuity) и сетевой безопасности (Network Security). Управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании.

Риск –возможность возникновения некоторой угрозы, связанной с текущей деятельностью компании. Также риск –это комбинация вероятности события и его последствий (ISO/IEC 27001:2005). Риск отражает возможные прямые или косвенные финансовые потери.

Оценка рисков: оценка угроз для информации и средств ее обработки, возможного ущерба для них в случае нарушения безопасности, их уязвимостей а также возможности их возникновения.(ISO/IEC 17799)

Управление рисками: процесс определения, контроля и уменьшения или полного устранения (с приемлемыми затратами) рисков для информационной безопасности, которые могут повлиять на информационные системы.(ISO/IEC 17799)

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценка (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты – минимальными. Управление рисками в жизненом цикле ИС:

1. На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

2. На этапе закупки (разработки) знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.
3. На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.
4. На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.
5. При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Методики и технологии управления информационными рисками.

Определение требований к безопасности производится путем методической оценки рисков. Методы оценки рисков могут применяться ко всей организации или лишь к ее частям, а также к отдельным информационным системам, системным компонентам и сервисам, в зависимости от того, что окажется наиболее практичным, реалистичным и полезным.

Оценка рисков – это систематический анализ следующих показателей:

- ущерб для бизнеса, который может возникнуть при нарушении безопасности. При этом следует учитывать возможные последствия утраты конфиденциальности, целостности или доступности информации и других ресурсов;
- оценка вероятности такого нарушения с учетом известных опасностей, уязвимостей и реализованных средств защиты.

Результаты такой оценки помогут определить необходимые действия и приоритеты для управления рисками, связанными с информационной безопасностью, и для реализации выбранных средств защиты от этих рисков. Процесс оценки рисков и выбора средств защиты может потребоваться выполнить несколько раз, чтобы охватить различные части организации или отдельные информационные системы.

Для эффективного управления информационными рисками разработаны специальные методики, например методики международных стандартов ISO 15408, ISO 17799 (BS7799), BSI; а также национальных стандартов NIST 80030, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им. В соответствие с этими методиками управление информационными рисками любой компании предполагает следующее. Во-первых, определение основных целей и задач защиты информационных активов компании. Во-вторых, создание эффективной системы оценки и управления информационными рисками. В-третьих, расчет совокупности детализированных не только качественных, но и количественных оценок рисков, адекватных заявленным целям

бизнеса. В-четвертых, применение специального инструментария оценивания и управления рисками.

Существуют качественные и количественные международные методики, а на их основе и средства управления информационными рисками. Качественные методики управления рисками достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 177992002, к ним относятся COBRA и RA Software Tool. К количественным методикам относят методику CRAMM и MethodWare, также на основании стандартов (AS/NZS 4360:1999 и ISO17799).

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть и количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками – типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении.

Для решения данной задачи были разработаны программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания Digital Security).

Методика учёта расходов на управление информационными рисками.

При подсчете полных расходов на управление информационными рисками могут быть использованы положения методики определения совокупной стоимости владения (ТСО). Показателем ТСО являются полные расходы на эксплуатацию системы управления информационными рисками предприятия в течение года, а это: учёт и оценка всех активов предприятия, капитальных и переменных затрат на технические и программные средства, помещения, персонал и т.д. Предлагается производить разделение расходов на управление информационными рисками на группы в соответствии с целями исследования.

Кроме этого в ТСО для ИБ необходимо учитывать еще и угрозы и риски, связанные с функционированием информационной системы предприятия, а также негативных внешних факторов, способных привести к осуществлению угрозы ИБ, используя уязвимости ресурсов информационной системы предприятия.

Лучшие мировые практики и ведущие международные стандарты в области информационной безопасности требуют для эффективного управления безопасностью информационной системы внедрения системы анализа и управления рисками. Подготовлено более десятка различных стандартов и спецификаций, детально

регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты ISO 177992002 (BS 7799), GAO и FISCAM, SCIP, NIST, SAS 78/94 и COBIT.

При этом можно использовать любые удобные инструментальные средства, но, главное – всегда четко понимать, что система информационной безопасности создана на основе анализа информационных рисков, проверена и обоснована. Анализ, оценка и управление информационными рисками – ключевой фактор для построения эффективной защиты информационной системы.

**Литература:**


1. «Защита от компьютерного терроризма», (А. Соколов, О. Степанюк), Арлит 2002.
2. «Методики и технологии управления информационными рисками», (Сергей Петренко, Сергей Симонов, «IT Manager»), http://citforum.ru/security/articles/risk/
3. «Учет расходов на управление информационными рисками», (Завгородний В.И.), http://www.1c.ru/rus/partners/training/edu/tez_pdf/zavv2.pdf
4. «Международный стандарт безопасности ISO/IEC 17799»
5. «Построение системы управления рисками IT-безопасности», (Андрей Коптелов), http://citcity.ru/14986/
6. «Основы информационной безопасности (Управление рисками)», http://www.INTUIT.ru