Обзор методик анализа рисков информационной безопасности информационной системы предприятия

Сегодня существует большое количество разнообразных и повсеместно распространенных методик анализа рисков, которые в свою очередь делятся на ряд групп. Авторы статьи предлагают рассмотреть эти методики более подробно на примере конкретных продуктов западных компаний. Методика "Facilitated Risk Analysis Process (FRAP)"[5] согласно данной методике риски оцениваются на качественном уровне. По данной методике оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации. Компания RiskWatch разработала собственную количественную методику, где риск оценивается через числовое значение, например размер ожидаемых годовых потерь и оценка возврата инвестиций. Методика компании RiskWatch позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. CRAMM использует комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций. Аналогичная смешанная методика оценки рисков используется и в продуктах компании Microsoft. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) — методика поведения оценки рисков в организации особенностью которой является то, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов.[6] В OCTAVE при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности. В отличие от прочих методик, OCTAVE вся документация по OCTAVE общедоступна и бесплатна.

Ключевые слова: *информационная безопасность, Facilitated Risk Analysis Process, Operationally Critical Threat, Asset, and Vulnerability Evaluation.*

Пугин В.В.,
к.т.н., доцент ФГОБУ ВПО ПГУТИ,
pugin@psati.ru

Губарева О.Ю.,
аспирант ФГОБУ ВПО ПГУТИ,
OlgaGubareva@inbox.ru

По данной тематике написано достаточно много трудов, но ее актуальность в настоящее время заставляет обращать на них своё внимание новых авторов. Это связано с тем, что на практике приходится часто сталкиваться с различными проблемами в процессе построения систем управления рисками. Зачастую это связано с разным уровнем зрелости компаний в сфере информационной безопасности (ИБ), с неправильным выбором методик построения систем или с ошибочным выбором источников информации для анализа, базирующихся на неправильных прогнозах и умозаключениях, а не на фактах, относящихся к реальной деятельности компании.

На Западе большинство компаний имеет опыт анализа рисков, но в России данная практика, особенно в области информационных рисков, недостаточно развита. Зачастую анализом риска называют любые, полученные в ходе работы, данные, используя это словосочетание в качестве "модного". При этом используются "правильные" термины, которым даются собственные определения. Чаще всего это связано с отсутствием подготовленных кадров в компании и нежеланием самой службы безопасности попадать в зону ответственности подразделения "рисков" [1].

Существует множество случаев, когда целесообразно проводить аудит безопасности. Это делается, в частности, при подготовке технического задания на проектирование и разработку системы защиты информации и после внедрения системы безопасности для оценки уровня ее эффективности. Возможен аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства. Аудит может также предназначаться для систематизации и упорядочения существующих мер защиты информации или для расследования произошедшего инцидента, связанного с нарушением информационной безопасности [2].

Сегодня существует большое количество разнообразных и повсеместно распространенных методик анализа рисков. Их можно разделить на несколько групп:[4]

- методики, использующие оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). К таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

В основе метода CRAMM [7] 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). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC ("Оранжевая книга").

Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса — потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация — рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка инфор-

мации, доставка по неверному адресу.

Согласно методу CRAMM для оценки возможного ущерба рекомендуется использовать следующие параметры:

- ущерб репутации организации;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Затем для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10. В описаниях CRAMM в качестве примера приводится такая шкала оценки по критерию "Финансовые потери, связанные с восстановлением ресурсов":

- 2 балла — менее $1000;
- 6 баллов — от $1000 до $10 000;
- 8 баллов — от $10 000 до $100 000;
- 10 баллов — свыше $100 000.

Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ. Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий. Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий.

CRAMM — пример методики расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Методика "Facilitated Risk Analysis Process (FRAP)" предлагаемая компанией Peltier and Associates [5] рассматривает обеспечение ИБ ИС в рамках процесса управления рисками. Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы.

После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта (англ. cost/benefit analysis), который позволяет определить те средства защиты, которые нужны для снижения риска до приемлемого уровня.

В FRAP более подробно раскрываются пути получения данных о системе и ее уязвимостях.

При проведении анализа, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом, оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации (СЗИ).

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) — методика поведения оценки рисков в организации, разрабатываемая институтом Software Engineering Institute (SEI) при университете Карнеги Меллон (Carnegie Mellon University).[6] Данной методике посвящено много научных и научно-технических статей.

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

OCTAVE предполагает три фазы анализа:

- разработка профиля угроз, связанных с активом;
- идентификация инфраструктурных уязвимостей;
- разработка стратегии и планов безопасности.

При описании профиля в методике OCTAVE предлагается использовать "деревья вариантов" рис. 1. При создании профиля угроз рекомендуется избегать обилия технических деталей — это задача второго этапа исследования. Главная задача текущей стадии — стандартизованным образом описать сочетание угрозы и ресурса.

В OCTAVE при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности, в виде шкалы: высокий (high), средний (middle), низкий (low). Оценивается финансовый ущерб, ущерб репутации компании, жизни и здоровью клиентов и сотрудников, ущерб, который может вызвать судебное преследование в результате того или иного инцидента. Описываются значения, соответствующие каждой градации шкалы (например, для малого предприятия финансовый ущерб в $10000 — высокий, для более крупного — средний).

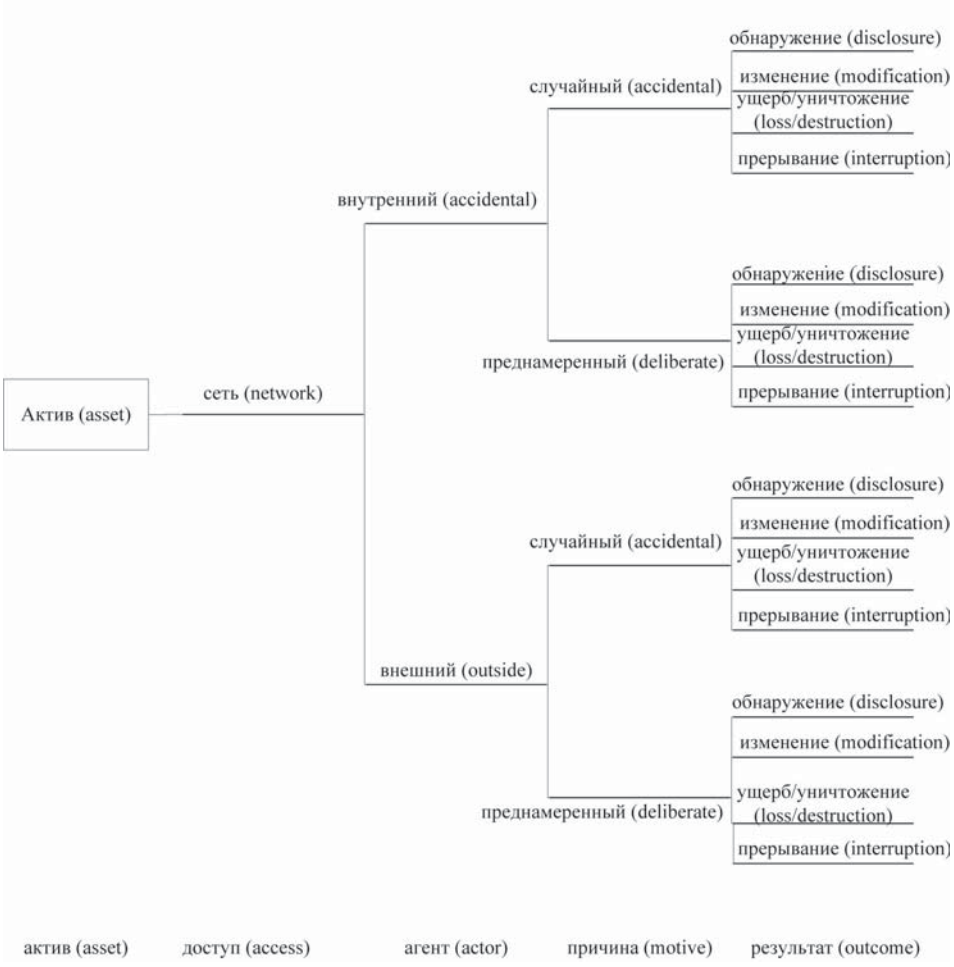

Рис.1. Дерево вариантов, использующееся при описании профиля в методике OCTAVE

Для определения мер противодействия угрозам в методике предлагаются каталоги средств.

В отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

Компания RiskWatch [8] разработала собственную методику анализа рисков и семейство программных средств, в которых она в той либо иной мере реализуется.

В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности:

• RiskWatch for Physical Security — для анализа физической защиты ИС;

• RiskWatch for Information Systems — для информационных рисков;

• HIPAA-WATCH for Healthcare Industry — для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США;

• RiskWatch RW17799 for ISO 17799 — для оценки соответствия ИС требованиям международного стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

На первом этапе определяется предмет исследования. Описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Второй этап — ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе, в частности, подробно описываются ресурсы, потери и классы инцидентов, получаемые путем сопоставления категории потерь и категории ресурсов.

Третий этап — количественная оценка риска. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. В целом, риск оценивается с помощью математического ожидания потерь за год.

На четвертом этапе генерируются отчеты.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Процесс управления рисками, предлагаемый корпорацией Майкрософт, разбивает этап оценки рисков на следующие три шага:

• Планирование. Разработка основы для успешной оценки рисков.

• Координированный сбор данных. Сбор информации о рисках в ходе координированных обсуждений рисков.

• Приоритизация рисков. Ранжирование выявленных рисков на основе непротиворечивого и повторяемого процесса.

Для проведения оценки требуется собрать данные о: активах организации, угрозах безопасности, уязвимостях, текущей среде контроля, предлагаемые элементы контроля.

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие качественные классы активов: — высокое, среднее и низкое влияние на бизнес.

Для угроз указывается уровень воздействия в соответствии с концепцией многоуровневой защиты (уровни — физический, сети, хоста, приложения, данных).

Следующий шаг этапа оценки рисков — приоритизация рисков, т.е. создание упорядоченного по приоритетам списка рисков. Формирование данного списка сначала предлагается выполнить на обобщенном уровне, после чего описания наиболее существенных рисков детализируются. Итоговый уровень риска определяется исходя из уровня влияния и оценки частоты возникновения риска.

Формирование перечня рисков на уровне детализации является последней задачей процесса оценки рисков. В этом перечне каждому риску в итоге сопоставляется оценка в числовой (денежной) форме.

Далее определяется уровень подверженности воздействию, а затем производится оценка величины влияния. Каждому уровню подверженности воздействию сопоставляется значение в процентах, отражающее величину ущерба, причиненного активу, и называемое фактором подверженности воздействию. Майкрософт, рекомендует использовать линейную шкалу подверженности воздействию от 100 до 20%, которая может изменяться в соответствии с требованиями организации. Кроме того, каждой величине влияния сопоставляется качественная оценка: высокая, средняя или низкая.

Результирующий уровень вероятности определяется на основании двух значений: вероятности существования уязвимости в текущей среде и вероятности существования уязвимости, исходя из эффективности текущих элементов контроля. Каждое значение изменяется в диапазоне от 1 до 5. Определение оценки проводится на основе ответов на вопросы.

Уровень риска определяется как произведение оценок уровня влияния (от 1 до 10) и уровня вероятности (от 0 до 10). В результате уровень риска может принимать значения от 0 до 100.

В заключение процедуры оценки рисков, проводится количественный анализ.

Количественную оценку предлагается начать с активов, соответствующих описанию класса высокого влияния на бизнес. Для каждого актива определяется денежная стоимость с точки зрения его материальной и нематериальной ценности для организации. Для определения степени ущерба, которая может быть причинен активу, предлагается использовать ранее определенный уровень подверженности воздействию, на основе которого определяется одноименный фактор.

Последний шаг состоит в получении количественной оценки влияния путем умножения стоимости актива на фактор подверженности воздействию.

Подводя итог, перечислим те преимущества, которые дает проведение анализа рисков в сфере ИБ:

• выявление проблем в сфере безопасности (не только уязвимостей компонент системы, но и недостатков политик безопасности и т.д.);

• анализ рисков позволяет нетехническим специалистам (в частности, руководству организации) оценить выгоды от внедрения средств и механизмов защиты и принять участие в процессе определения требуемого уровня защищенности КС;

• проведение оценки рисков добавляет обоснованность рекомендациям по безопасности;

• ранжирование рисков по приоритетам позволяет выделить наиболее приоритетные направления для внедрения новых СЗИ, мер и процедур обеспечения ИБ;

• подробно описанные методики анализа рисков позволяет людям, не являющимся экспертами в данной области, воспользоваться аккумулированными в методике знаниями, чтобы получить заслуживающие доверия результаты анализа.

В то же время, необходимо отметить, что оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение ИБ и получаемую от них отдачу (в виде снижения суммарного риска). Поэтому более предпочтительными представляются количественные методики. Но они требуют наличия оценок вероятности возникновения для каждой из рассматриваемых угроз безопасности. Кроме того, использование интегральных показателей, таких как ALE, опасно тем, что неправильная оценка вероятности угрозы в отношении очень дорогостоящего актива может кардинально изменить оцениваемое значение суммарной стоимости рисков.

Одной из областей, важных с практической точки зрения и хорошо проработанных в плане управления рисками, является аутсорсинг по управлению информационной системой (в частности, контроль ее информационной безопасности). Но здесь владелец компании или специалист по ИБ может столкнуться со следующими угрозами:

1. Непредвиденно высокие затраты на переход на новую дисциплину управления ИС. "Уязвимостями" — отсутствие у организации опыта аутсорсинга, неопределенность в законодательстве.

2. Затраты на переход на обслуживание другой организацией (включая попадание в заложники обслуживающей организации, возврат к исходному состоянию и переход на обслуживание новой организацией). Уязвимости: специфичность ИС, узкий выбор обслуживающих организаций, размеры и сложность ИС, взаимосвязь разных видов деятельности.

3. Дорогостоящие поправки к контракту. Уязвимости: неопределенность, технологический разрыв, сложность задачи.

4. Споры и тяжбы с обслуживающей организацией. Уязвимости: проблемы измеримости, недостаток опыта (у одной или обеих сторон) по заключению контрактов на аутсорсинг, неопределенность законодательства, недостаток культуры.

5. Снижение качества обслуживания. Уязвимости: взаимосвязь разных видов деятельности, недостаток опыта, слишком большой размер и/или финансовая нестабильность обслуживающей организации, проблемы измеримости.

6. Превышение затрат. Уязвимости: недостаток опыта по управлению контрактом на аутсорсинг, проблемы измеримости, недостаток опыта у поставщика услуг.

7. Потеря компетенции. Уязвимости: размеры и сложность ИС, близость к основной деятельности организации, взаимосвязь разных видов деятельности.

8. Скрытые затраты на обслуживание. Уязвимости: сложность разных видов деятельности, проблемы измеримости.

Формирование и ранжирование требований безопасности для анализируемой конфигурации системы необходимо для того, чтобы определить понятие успешной атаки. Обычно требования выражаются в терминах доступности, конфиденциальности и целостности.

При выборе мер для повышения уровня защиты ИС учитывается одно принципиальное ограничение — стоимость реализации этих мер не должна превышать стоимости защищаемых информационных ресурсов, а также убытков компании от возможного нарушения конфиденциальности, целостности или доступности информации [3].

Большинство организаций на собственном опыте осознали актуальность и важность проблем ИБ. Следующим шагом должен стать количественный подход к их решению, основанный на управлении рисками.

Первым этапом в этом процессе является сбор данных о расходах на безопасность, об имевших место нарушениях ИБ и ущербе от них. Базируясь на этих данных, организация может построить количественную модель рисков для своей ИС, запланировать меры по усилению защиты слабых мест, сформировать обоснованный бюджет для защитных мероприятий.

Регулярная переоценка рисков позволит поддерживать данные о безопасности ИС организации в актуальном состоянии, оперативно выявлять новые опасные риски и находить пути для их нейтрализации экономически целесообразным способом.

Литература

1. http://www.buhgalteria.ru/article/n44826.
2. Скрёхин Сергей Викторович http://www.bytemag.ru/articles/detail.php?ID=6781.
3. security.meganet.md http://bre.ru/security/13985.html.
4. http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/upravlenie-riskami-obzor-upotrebitelnyh-podhodov.
5. http://www.peltierassociates.com.
6. www.cert.org/octave.
7. http://www.cramm.com.
8. www.riskwatch.com.

Review of methods for the analysis of information security risk information system

V.V. Pugin, *pugin@psati.ru,* **O.Yu. Gubareva,** *OlgaGubareva@inbox.ru*

Abstract

Today there is a large number of wide-spread risk analysis techniques that can be divided into a number of groups. The authors of this article suggest reviewing these techniques in detail using as an example following specific products developed by western companies. FACILITATED RISK ANALYSIS PROCESS (FRAP) technique implies qualitative risk analysis. This method evaluates the risk level of an unprotected Information System. This is later used to demonstrate the effect of implementation of an information security tool. RISKWATCH has developed proprietary quantitative method, where the level of risk is presented in the form of numbers, such as expected losses and return of investment. This method evaluates current risks and prospective gains that could be obtained after implementation of physical, technical, software and other information security tools. CRAMM applies an integrated method, using both qualitative and quantitative techniques. It is comprehensive and applicable for both large and small companies. Similar method is employed in Microsoft products. OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION) — is a risk evaluation method that implies that the evaluation process is conducted in the company internally, without external consultants. OCTAVE provides only the estimate of the expected loss, while the probability is not evaluated. OCTAVE is a freeware product in contrast to the others.

Keywords: *FACILITATED RISK ANALYSIS PROCESS, RISKWATCH, CRAMM, OCTAVE.*