**Тема 8: "МЕТОДИКИ И ТЕХНОЛОГИИ УПРАВЛЕНИЯ РИСКАМИ"**

В настоящее время 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.**

Поэтому под термином «управление информационными рисками» обычно понимается *системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности*.

Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Не секрет, что сегодня наблюдается повсеместное усиление зависимости успешной бизнес деятельности отечественных компаний от используемых организационных мер и технических средств контроля и уменьшения риска.

Для эффективного управления информационными рисками разработаны специальные методики, например методики международных стандартов ISO 15408, ISO17799 (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. Давайте рассмотрим некоторые качественные и количественные международные методики управления информационными рисками, обращая основное внимание на возможность их адаптации и применения в отечественных условиях.

***8.1 Качественные методики управления рисками***

Качественные методики управления рисками приняты на вооружение в технологически развитых странах многочисленной армией внутренних и внешних IT-аудиторов. Эти методики достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 17799. В сентябре 2002 года основные положения ISO17799 были пересмотрены и дополнены с учетом развития современных информационных технологий и требований к организации режима ИБ. Сегодня это наиболее распространенный стандарт во всем мире среди организаций и предприятий, которые используют подобные стандарты на добровольной основе.

К качественным методикам управления рисками на основе требований ISO 17799 относятся методики *COBRA* и *RA Software Tool* (Инструмент Программного Обеспечения). Кратко рассмотрим названные методики.

**COBRA**

Во второй половине 90х годов компания *C & A Systems Security Ltd*. разработала одноименные методику и соответствующий инструментарий для анализа и управления информационными рисками под названием *COBRA*. Эта методика позволяет выполнить в автоматизированном режиме простейший вариант оценивания информационных рисков любой компании. Для этого предлагается использовать специальные электронные базы знаний и процедуры логического вывода, ориентированные на требования ISO17799. Существенно, что при желании перечень учитываемых требований можно дополнить различными требованиями отечественных нормативно-регулирующих органов, например, требованиями НД ТЗИ.

Методика *COBRA* представляет требования стандарта ISO 17799 в виде тематических вопросников (*check list’s*), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнес транзакций компании.

Далее введенные ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет c текущими оценками информационных рисков компании и рекомендациями по их управлению.

Достоинство методики – в ее простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

Этот программный продукт может применяться при проведении аудита ИБ или для работы специалистов служб, ответственных за обеспечение информационной безопасности.

Простота, соответствие международному стандарту, сравнительно небольшое число вопросов позволяют легко адаптировать этот метод для работы в отечественных условиях.

**RA Software Tool**

Методика и одноименное инструментальное средство *RA Software Tool* основаны на требованиях международных стандартов ISO 17799 и ISO 13335 (части 3 и 4), а также на требованиях некоторых руководств Британского национального института стандартов (BSI), например, PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты) и пр.

Эта методика позволяет выполнять оценку информационных рисков (модули 4 и 5) в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов.

***8.2 Количественные методики управления рисками. Метод CRAMM***

Вторую группу методик управления рисками составляют количественные методики, актуальность которых обусловлена необходимостью решения различных оптимизационных задач, которые часто возникают в реальной жизни. **Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих**. *Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?*» или «Какую из альтернатив построения корпоративной защиты информации (защищенного *WWW* сайта или корпоративной *Email*) выбрать с учетом известных ограничений бизнес ресурсов компании?» Для решения этих задач и разрабатываются методы и методики количественной оценки и управления рисками на основе структурных и реже объектно-ориентированных методов системного анализа и проектирования (SSADM – Structured Systems Analysis and Design). На практике такие методики управления рисками позволяют:

* Создавать модели информационных активов компании с точки зрения безопасности;
* Классифицировать и оценивать ценности активов;
* Составлять списки наиболее значимых угроз и уязвимостей безопасности;
* Ранжировать угрозы и уязвимости безопасности;
* Обосновывать средства и меры контроля рисков;
* Оценивать эффективность/стоимость различных вариантов защиты;
* Формализовать и автоматизировать процедуры оценивания и управления рисками.

Одной из наиболее известных методик этого класса является методика CRAMM.

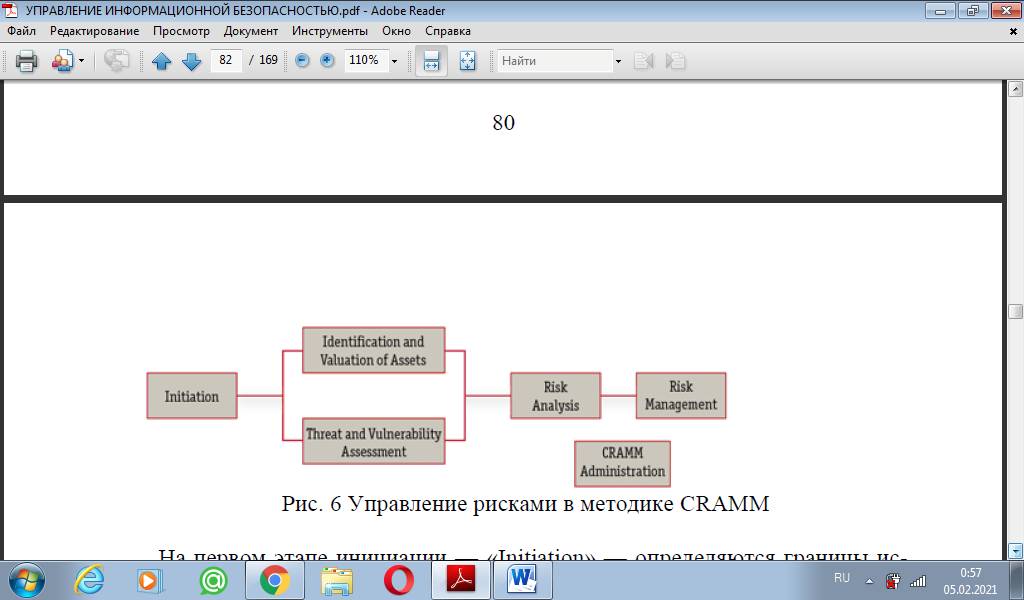
Метод **CRAMM**

В 1985 году Центральное агентство по компьютерам и телекоммуникациям (CCTA) Великобритании начало исследования существующих методов управления информационной безопасностью для выдачи рекомендаций по их использованию в правительственных организациях, обрабатывающих конфиденциальную информацию. Ни один из рассмотренных методов не подошел. Поэтому сначала был создан метод, а затем одноименная методика CRAMM (анализа и контроля рисков), соответствующая требованиям CCTA. Затем появилось несколько версий методики, ориентированных на требования различных государственных и коммерческих организаций и структур. Одна из версий «коммерческого профиля» широко распространилась на рынке средств защиты информации.

**Основными целями методики CRAMM являются:**

* Формализация и автоматизация процедур анализа и управления рисками;
* Оптимизация расходов на средства контроля и защиты;
* Комплексное планирование и управление рисками на всех стадиях жизненного цикла информационных систем;
* Сокращение времени на разработку и сопровождение корпоративной системы защиты информации;
* Обоснование эффективности предлагаемых мер защиты и средств контроля;
* Управление изменениями и инцидентами;
* Поддержка непрерывности бизнеса;
* Оперативное принятие решений по вопросам управления безопасностью и пр.

Управление рисками в методике СRAMM осуществляется в несколько этапов (рис. 6).



***Рис. 6 Управление рисками в методике СRAMM***

На первом этапе инициации - «Initiation» - определяются границы исследуемой информационной системы компании, состав и структура ее основных информационных активов и транзакций.

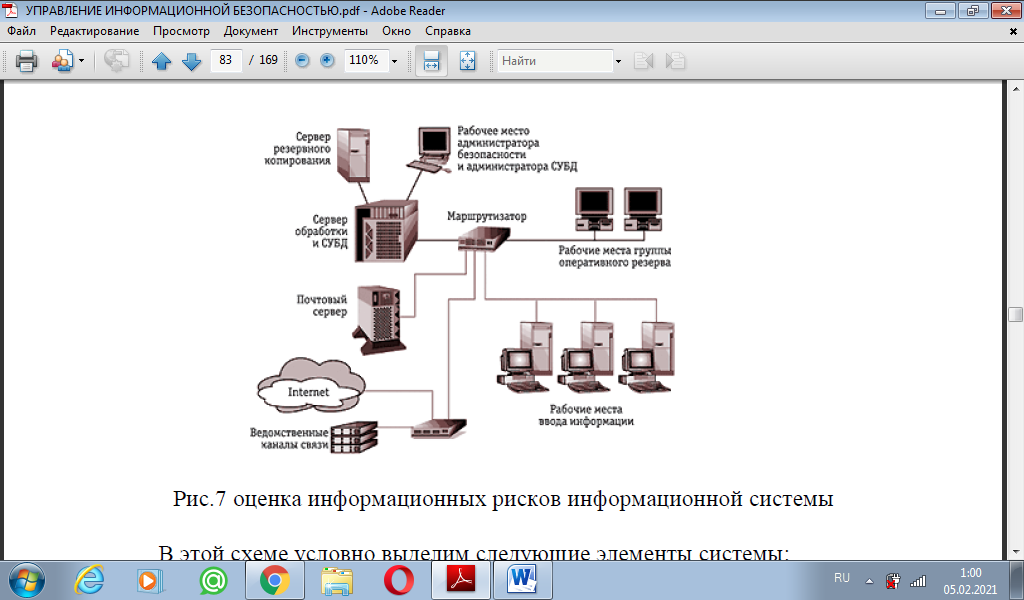
На этапе идентификации и оценки ресурсов - «Identification and Valuation of Assets» - четко идентифицируются активы, и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На этапе оценивания угроз и уязвимостей - «Threat and Vulnerability Assessment» - идентифицируются и оцениваются угрозы и уязвимости информационных активов компании.

Этап анализа рисков - «Risk Analysis» - позволяет получить качественные и количественные оценки рисков.

На этапе управления рисками - «Risk management» - предлагаются меры и средства уменьшения или уклонения от риска.

Рассмотрим возможности CRAMM на следующем примере. Пусть проводится оценка информационных рисков следующей корпоративной информационной системы (рис. 7).



***Рис.7 Оценка информационных рисков информационной системы***

В этой схеме условно выделим следующие элементы системы:

- рабочие места, на которых операторы вводят информацию, поступающую из внешнего мира;

- почтовый сервер, на который информация поступает с удаленных узлов сети через Интернет;

- сервер обработки, на котором установлена СУБД;

- сервер резервного копирования;

- рабочие места группы оперативного реагирования;

- рабочее место администратора безопасности;

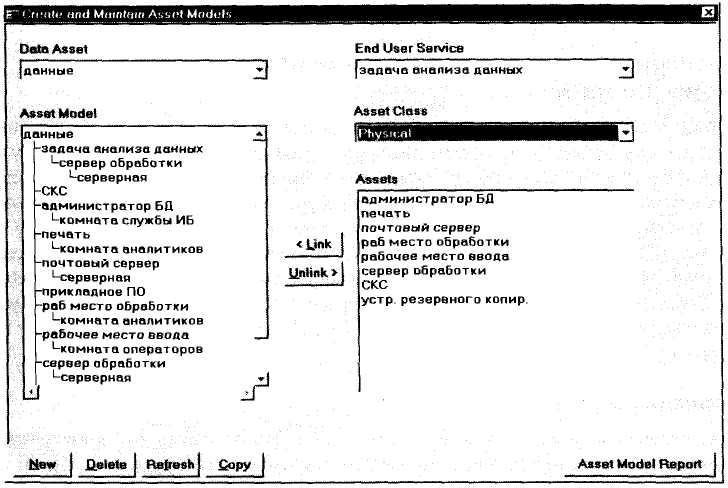
- рабочее место администратора БД.

Функционирование системы осуществляется следующим образом. Данные, введенные с рабочих мест пользователей и поступившие на почтовый сервер, направляются на сервер корпоративной обработки данных. Затем данные поступают на рабочие места группы оперативного реагирования и там принимаются соответствующие решения.

Давайте теперь проведем анализ рисков с помощью методики CRAMM и предложим некоторые средства контроля и управления рисками, адекватные целям и задачам бизнеса компании.

**Определение границ исследования**. Этап начинается с решения задачи определения границ исследуемой системы. Для этого собирается следующая информация: ответственные за физические и программные ресурсы; кто является пользователем и как пользователи применяют или будут использовать систему; конфигурация системы. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

**Идентификация ресурсов и построение модели системы с точки зрения ИБ.** Проводится идентификация ресурсов: материальных, программных и информационных, содержащихся внутри границ системы. Каждый ресурс необходимо отнести к одному из предопределенных классов. Классификация физических ресурсов приводится в приложении. Затем строится модель информационной системы с точки зрения ИБ. Для каждого информационного процесса, имеющего самостоятельное значение с точки зрения пользователя и называемого пользовательским сервисом (*EndUserService*), строится дерево связей используемых ресурсов. В рассматриваемом примере будет единственный подобный сервис (рис. 8). Построенная модель позволяет выделить критичные элементы.



***Рис.8 Дерево связей используемых ресурсов***

**Ценность ресурсов**. Методика позволяет определить ценность ресурсов. Этот шаг является обязательным в полном варианте анализа рисков. Ценность физических ресурсов в данном методе определяется ценой 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 информации, доставка по неверному адресу.

Для оценки возможного ущерба предлагается использовать следующие критерии:

- 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.

Приведенная совокупность критериев используется в коммерческом варианте метода (профиль *Standard*). В других версиях совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10. К примеру, если данные содержат подробности коммерческой конфиденциальной (критичной) информации, эксперт, проводящий исследование, задает вопрос: как может повлиять на организацию несанкционированный доступ посторонних лиц к этой информации?

Возможен такой ответ: провал сразу по нескольким параметрам из перечисленных выше, причем каждый аспект следовало бы рассмотреть подробнее и присвоить самую высокую из возможных оценок.

Затем разрабатываются шкалы для выбранной системы параметров. Они могут выглядеть следующим образом.

Ущерб репутации организации:

2 – негативная реакция отдельных чиновников, общественных деятелей;

4 – критика в средствах массовой информации, не имеющая широкого общественного резонанса;

6 – негативная реакция отдельных депутатов Верховной Рады Украины;

8 – критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т. п.;

10 – негативная реакция на уровне Президента и Правительства.

Ущерб для здоровья персонала:

2 – минимальный ущерб (последствия не связаны с госпитализаций или длительным лечением);

4 – ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);

6 – серьезные последствия (длительная госпитализация, инвалидность одного или нескольких сотрудников);

10 – гибель людей.

Финансовые потери, связанные с восстановлением ресурсов:

2 – менее $1000;

6 – от $1000 до $10 000;

8 – от $10000 до $100000 ;

10 – свыше $100000.

Дезорганизация деятельности в связи с недоступностью данных:

2 – отсутствие доступа к информации до 15 минут;

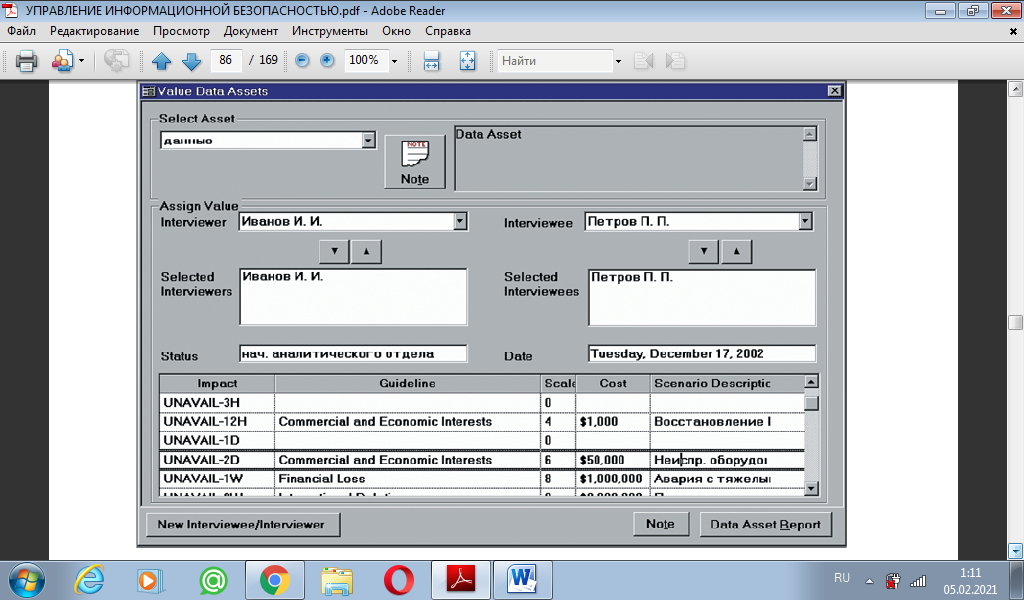
4 – отсутствие доступа к информации до 1 часа;

6 – отсутствие доступа к информации до 3 часов;

8 – отсутствие доступа к информации от 12 часов;

10 – отсутствие доступа к информации более суток.

Далее рассматриваются основные сценарии, приводящие к различным негативным последствиям, описываемым в терминах выбранных параметров (рис.9. - Оценка ценности информационных ресурсов).



***Рис.9 Оценка ценности информационных ресурсов***

На этом этапе может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов). Если ценности ресурсов низкие, можно использовать базовый вариант защиты. В таком случае исследователь может перейти от этой стадии сразу к стадии анализа рисков. Однако для адекватного учета потенциального воздействия какой-либо угрозы, уязвимости или комбинации угроз и уязвимостей, которые имеют высокие уровни, следует использовать сокращенную версию стадии оценки угроз и уязвимостей. Это позволяет разработать более эффективную систему защиты информации компании.

На этапе оценивания угроз и уязвимостей оцениваются зависимости пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей.

Далее активы компании группируются с точки зрения угроз и уязвимостей. Например, в случае наличия угрозы пожара или кражи, в качестве группы ресурсов разумно рассмотреть все ресурсы, находящиеся в одном месте (серверный зал, комната средств связи и т. д.).

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.

На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком.

CRAMM объединяет угрозы и уязвимости в матрице риска. Рассмотрим, как получается эта матрица, и что каждый из уровней риска означает.

Основной подход, для решения этой проблемы состоит в рассмотрении:

- уровня угрозы (шкала приведена в табл. 1);

- уровня уязвимости (шкала приведена в табл. 2);

- размера ожидаемых финансовых потерь (пример на рис. 10).

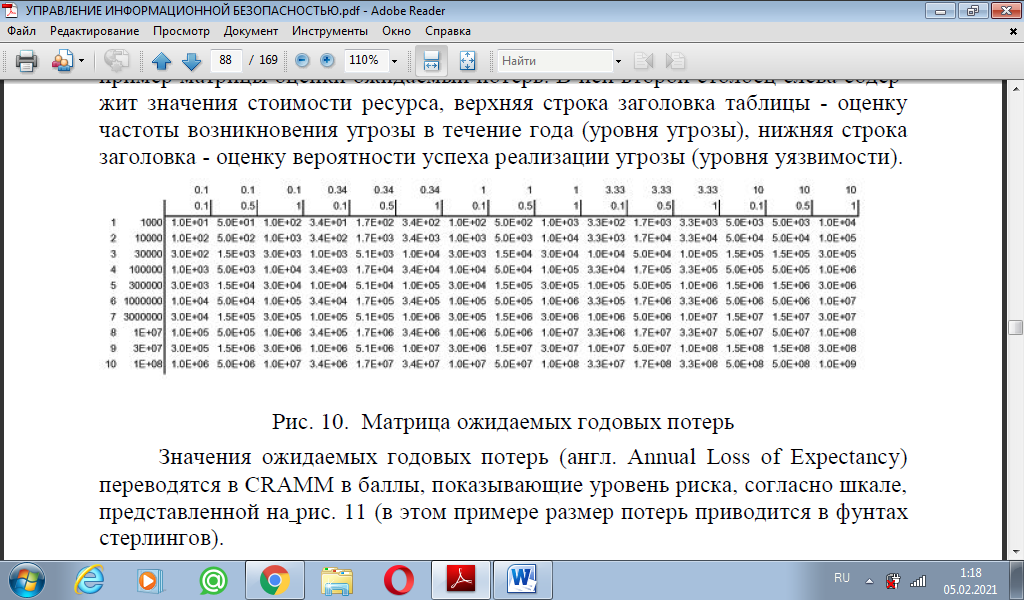
*Таблица 1. Шкала оценки уровней угрозы (частота возникновения).*

|  |  |
| --- | --- |
| ***Описание*** | ***Значение*** |
| инцидент происходит в среднем, не чаще, чем каждые 10 лет | очень низкий |
| инцидент происходит в среднем один раз в 3 года | низкий |
| инцидент происходит в среднем раз в год | средний |
| инцидент происходит в среднем один раз в 4 месяца | высокий |
| инцидент происходит в среднем раз в месяц | очень высокий |

*Таблица 2. Шкала оценки уровня уязвимости (вероятность успешной реализации угрозы).*

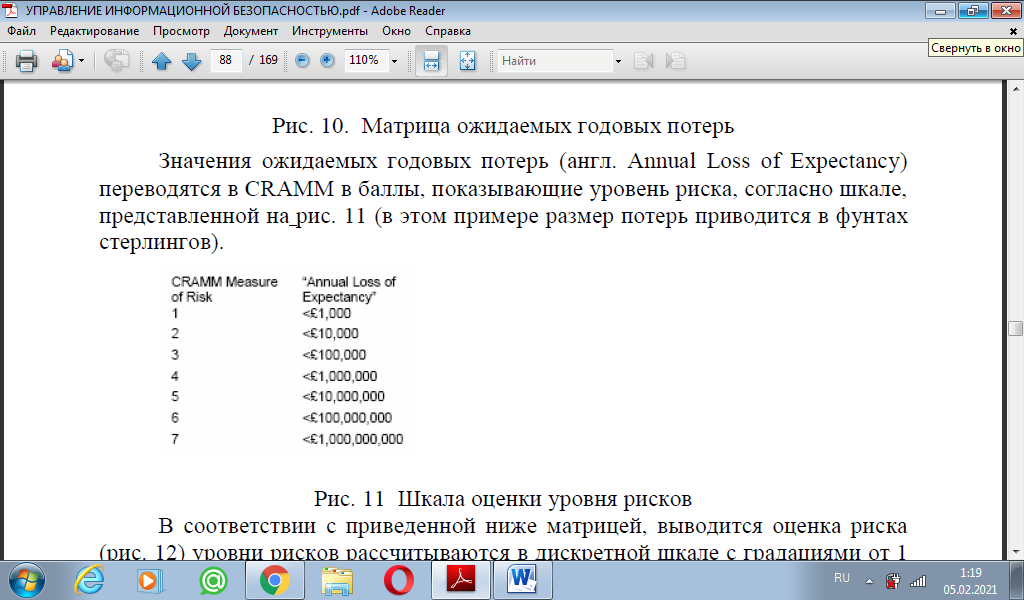
|  |  |
| --- | --- |
| ***Описание*** | ***Значение*** |
| В случае возникновения инцидента, вероятность развития событий низ по наихудшему сценарию меньше 0,33 | низкий |
| В случае возникновения инцидента, вероятность развития событий сре по наихудшему сценарию от 0,33 до 0,66 | средний |
| В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию выше 0,66 | высокий |

Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются "ожидаемые годовые потери". На рис. 10 приведен пример матрицы оценки ожидаемый потерь. В ней второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы - оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка - оценку вероятности успеха реализации угрозы (уровня уязвимости).



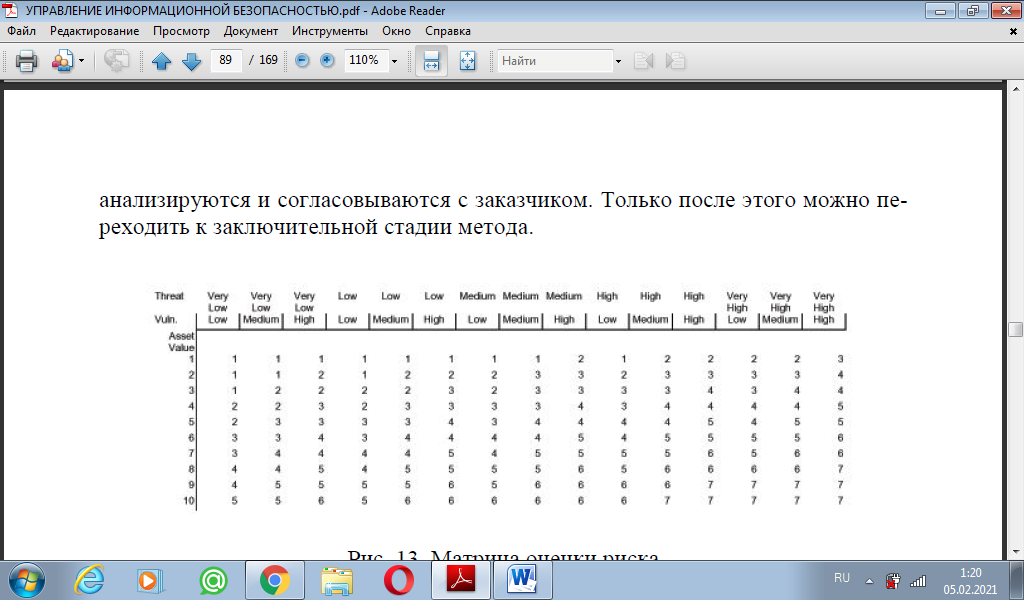
***Рис. 10. Матрица ожидаемых годовых потерь***

Значения ожидаемых годовых потерь (англ. Annual Loss of Expectancy) переводятся в CRAMM в баллы, показывающие уровень риска, согласно шкале, представленной на рис. 11 (в этом примере размер потерь приводится в фунтах стерлингов).



***Рис. 11 Шкала оценки уровня рисков***

В соответствии с приведенной ниже матрицей, выводится оценка риска (рис. 12) уровни рисков рассчитываются в дискретной шкале с градациями от 1 до 7 (этап анализа рисков). Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.



***Рис. 13 Матрица оценки риска***

Третья стадия исследования заключается в поиске адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

На этом этапе CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

* Обеспечение безопасности на сетевом уровне.
* Обеспечение физической безопасности.
* Обеспечение безопасности поддерживающей инфраструктуры.
* Меры безопасности на уровне системного администратора.

В результате выполнения данного этапа формируется несколько видов отчетов.

Таким образом, рассмотренная методика анализа и управления рисками полностью применима и в наших условиях, несмотря на то, что показатели защищенности от НСД к информации и требования по защите информации различаются в украинских нормативных документах и зарубежных стандартах. Особенно полезным представляется использование инструментальных средств типа метода CRAMM при проведении анализа рисков информационных систем с повышенными требованиями в области ИБ. Это позволяет получать обоснованные оценки существующих и допустимых уровней угроз, уязвимостей, эффективности защиты.

**CRAMM как инструментарий аудитора**

CRAMM имеет средства генерации отчетов, необходимые при проведении аудита информационной безопасности в соответствии с BS 7799 (ISO 17799).

Это следующие отчеты:

- политика информационной безопасности;

- система управления информационной безопасностью;

- план обеспечения бесперебойной работы;

- ведомость соответствия.

Метод CRAMM в настоящее время применяется наиболее часто, если требуется провести аудит в соответствии с требованиями Британского стандарта.

Его достоинства заключаются в использовании технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, удобной системе моделирования информационной системы с позиции безопасности, обширной базе данных по контрмерам. Этот метод - самый «мощный» и самый трудоемкий из рассмотренных в настоящем обзоре, он позволяет весьма детально оценить риски и различные варианты контрмер.

Его недостаток с позиции отечественного потребителя состоит в сложности русификации и большом объеме выходных документов (сотни страниц). Аналитик (аудитор) обычно вынужден на основе полученных документов сам писать отчет для заказчика.

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