

И.В. Аникин

**УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

И.В. Аникин

**УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Учебное пособие

*Рекомендовано к изданию
Учебно-методическим управлением КНИТУ-КАИ*

Казань
2018

УДК 004.056.5

ББК 32.973.26-018.2

A 95

Рецензенты:

Кафедра «Информационная безопасность» (Казанский национальный исследовательский технологический университет)

Ш.Т. Ишмухаметов – доктор физ.-мат. наук, профессор кафедры Системного анализа и информационных технологий Казанского (Приволжского) федерального университета.

Аникин И.В.

A 95

Управление рисками информационной безопасности: учебное пособие – Казань: Редакционно-издательский центр «Школа», 2018. – 149 с., ил.

ISBN 978-5-906935-93-9

Предлагаемое учебное пособие предназначено для организации учебного процесса при изучении дисциплины «Управление рисками» студентами направления 10.03.01 «Информационная безопасность» и дисциплины «Экономика защиты информации» студентами специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

УДК 004.056.5

ББК 32.973.26-018.2

ISBN 978-5-906935-93-9

© Аникин И.В., 2018

СПИСОК СОКРАЩЕНИЙ

АС	–	Автоматизированная система
ИБ	–	Информационная безопасность;
ИТ	–	Информационные технологии;
НСД	–	Несанкционированный доступ
ОЗУ	–	Оперативное запоминающее устройство
ОС	–	Операционная система
ПЗУ	–	Постоянное запоминающее устройство
ПО	–	Программное обеспечение
СЗПО	–	Система защиты программного обеспечения
СВТ	–	Средство вычислительной техники
ЭВМ	–	Электронно-вычислительная машина

ВВЕДЕНИЕ

Предлагаемое учебное пособие предназначено для организации учебного процесса при изучении дисциплины «Управление рисками» для направления 10.03.01 «Информационная безопасность» и дисциплины «Экономика защиты информации» для специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

В разделе 1 даются основные термины и определения, определяется актуальность проблемы оценки и управления рисками ИБ, дается классификация существующих методов оценки рисков.

В разделе 2 приводятся основные Российские и зарубежные стандарты и руководства оценки и управления рисками ИБ. Приводятся методы качественной оценки, количественной оценки и смешенной оценки и управления рисками ИБ.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ. АНАЛИЗ ОСНОВНЫХ ПОДХОДОВ К ОЦЕНКЕ И УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной главе даются основные термины и определения, определяется актуальность проблемы оценки и управления рисками ИБ, дается классификация существующих методов оценки рисков.

1.1. Актуальность

Бурное развитие вычислительной техники привело к значительному увеличению степени автоматизации современных предприятий. Повсеместное применение информационных технологий (ИТ) позволило им, с одной стороны, выйти на качественно новый уровень производства, с другой — это привело к чрезвычайной уязвимости их бизнес-процессов по отношению угроз информационной безопасности (ИБ).

Роль деструктивных факторов для современных информационных систем значительно возросла в связи с тем, что данные факторы могут напрямую влиять на выполнение бизнес-процессов. Это приводит к значительному увеличению количества угроз ИБ, которые выражаются не только в умышленном хищении или уничтожении информации, но и в повреждении информации в результате естественных факторов: аварийного отключения электричества, неисправности вычислительной техники, случайного изменения и т.п.

Растущая сложность информационных систем только усугубляет ситуацию. Увеличение объемов информации, хранимой в электронном виде, приводит к тому, что ее потеря или разглашение может нанести существенные убыт-

ки предприятию. Нарушение работоспособности ИТ-сервисов может привести к остановке бизнес-процессов, что также наносит непоправимый ущерб. Наносимые убытки могут выражаться в виде прямого финансового ущерба, в виде ущерба авторитету предприятия, ухудшении морального климата в коллективе и т.д.

Можно утверждать, что в современных условиях эффективность функционирования предприятий напрямую зависит от степени защищенности их информационных систем и сетей, посредством которых осуществляется автоматизация бизнес-процессов.

На рисунке 1.1. представлена аналитическая информация, характеризующая мировую географию кибератак в 2017 году где видно, что Россия является одной из основных целей, что требует адекватного противодействия с позиций повышения защищенности. Современные тенденции также показывают постоянное увеличение количества уязвимостей и уязвимых компонентов современных информационных систем. Все это приводит к повышению требований по защите информации, то есть к увеличению затрат на предупредительные мероприятия.

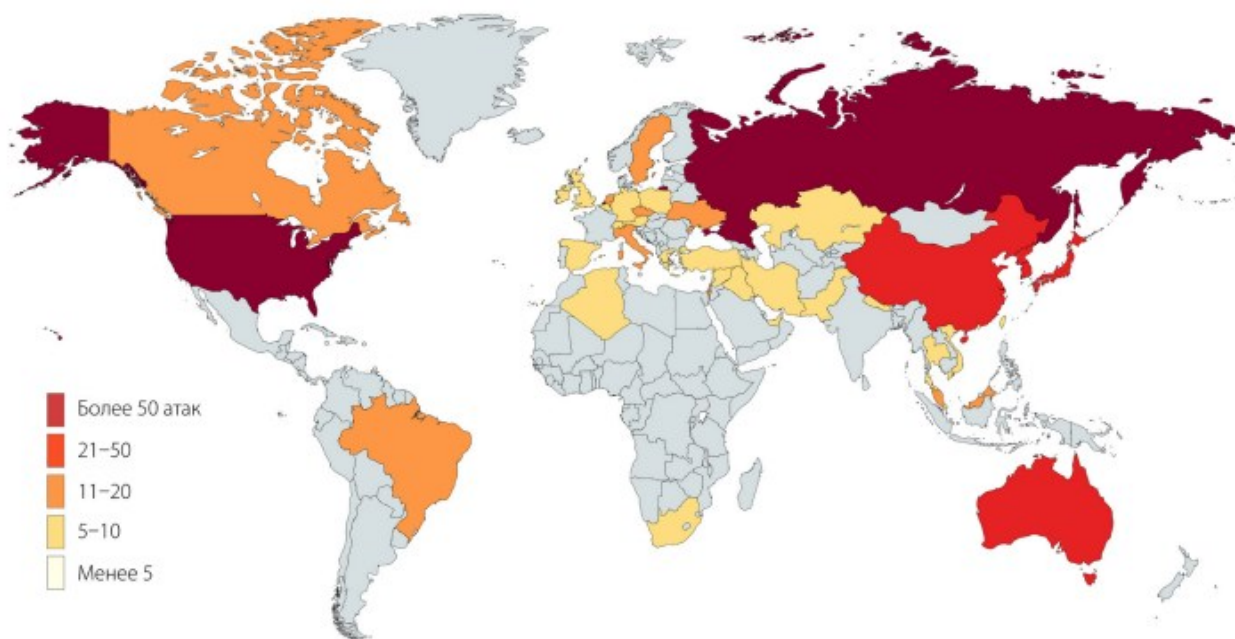


Рисунок 1.1. География кибератак в IV кв. 2017 года
(аналитика Positive Technologies)

В настоящее время существует два основных подхода к обеспечению информационной безопасности.

1. Реализация базового уровня ИБ. В настоящее время в России и за рубежом известно множество руководящих документов и стандартов, используемых для обеспечения ИБ на базовом уровне. При этом ставятся и решаются следующие основные задачи:

- убедиться в том, что рассматриваемые компоненты удовлетворяют всем обязательным требованиям стандартов и руководящих документов;
- убедиться в том, что рассматриваемые компоненты защищены от всех видов основных угроз.

2. Подход, основанный на оценке и управлении рисками ИБ. Данный подход реализуется, как правило, после обеспечения базового уровня ИБ. При этом ставятся и решаются следующие основные задачи:

- анализ угроз и уязвимостей объекта защиты, оценка возможности их реализации и возможного ущерба;
- оценка рисков ИБ и определение актуальных угроз для объекта защиты;
- формирование множества защитных мер и снижение рисков ИБ до приемлемого уровня.

Анализ экономической составляющей защиты информации говорит о том, что затраты на ИБ складываются из двух основных частей – затрат на предупредительные мероприятия и затрат на компенсацию потерь в случае реализации угроз это актуализирует необходимость нахождения баланса между достигаемым уровнем защищенности и стоимостью защитных мероприятий, исследованию экономической составляющей данного процесса. Данную задачу эффективно позволяет решить подход к обеспечению ИБ, основанный на оценке и управлении рисками. В связи с этим, для современных информационных систем и сетей применение данного подхода приобретает все большую актуальность. Об этом свидетельствует и то, что, начиная с 2005 года, большинство стандартов в области информационной безопасности компьютерных систем и

сетей включают в себя разделы, связанные с оценкой и управлением рисками ИБ.

1.2. Основные термины и определения

Рассмотрим основные термины и определения предметной области.

Под защищаемым активом понимают все то, что имеет ценность для организации и требует защиты. В качестве основных видов активов, требующих защиты в современных информационных системах и сетях, рассматриваются те из них, которые находятся на уровне технического, информационного и программного обеспечения. К таким активам относятся: автоматизированные рабочие места (АРМ), сервера, телекоммуникационное оборудование, информационные активы и ИТ-сервисы.

Под *ИТ-сервисами* будем понимать процессы предоставления пользователям ресурсов информационных технологий для обеспечения выполнения ими своих бизнес функций. ИТ-сервисы могут предоставляться одной организацией для другой или одним подразделением организации другому подразделению. Можно выделить следующие основные классы ИТ-сервисов:

1) Платформенные – являющиеся платформой построения ИТ-инфраструктуры организации и основой предоставления сервисов всех остальных типов (Active Directory, IP-телефония, DNS и т.д.).

2) Операционные – предназначенные для автоматизации деятельности ИТ-специалистов (резервное копирование, программно-аппаратные средства защиты информации, удаленный доступ и т.д.).

3) Стандартные, предоставляемые пользователям, - являются основной группой ИТ-сервисов, предоставляемых их потребителям (электронная почта, доступ к ресурсам Интернет, сервис печати, доступ к корпоративным ресурсам и т.д.).

4) Обеспечивающие производственно-хозяйственную деятельность предприятия. Примерами таких сервисов является электронный документооборот

предприятия, информационно-справочные системы, системы управления персоналом, ведения бухгалтерии и т.д.

5) Обеспечивающие технологический процесс предприятия. Данные сервисы автоматизируют технологическую деятельность предприятия и достаточно распространены в автоматизированных системах управления технологическими процессами.

На рисунке 1.2. представлена общая схема взаимодействия различных активов, которую следует принимать во внимание при формировании модели угроз.

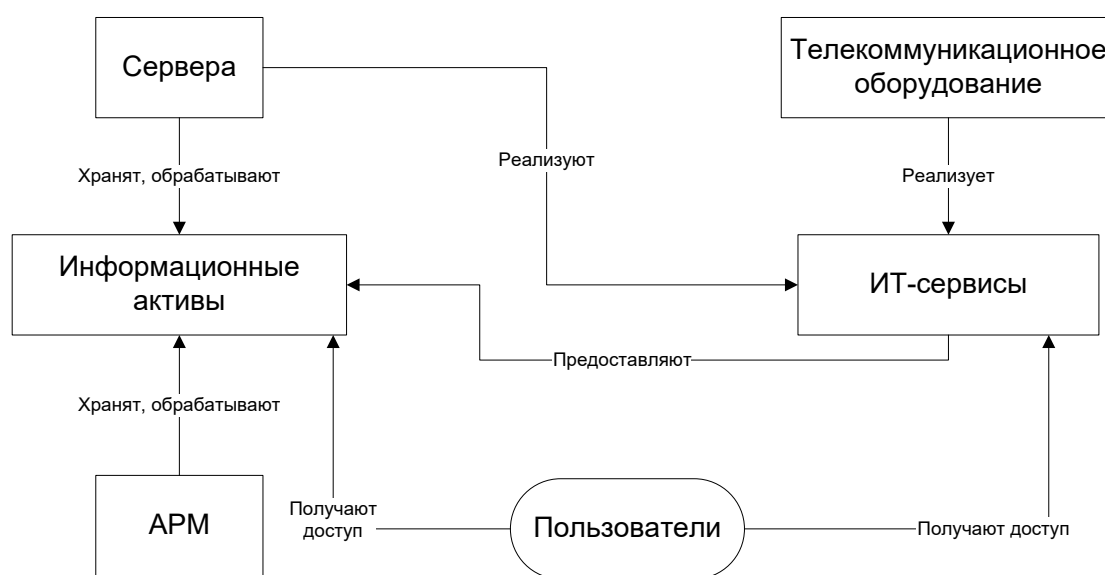


Рисунок 1.2. Общая схема взаимодействия активов

Эксплуатация любых информационных систем и сетей осуществляется в условиях потенциально опасных воздействий искусственного и естественного характера. Данные воздействия являются проявлениями угроз ИБ. Под *угрозой ИБ* понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Непосредственную реализацию угрозы ИБ называют *инцидентом ИБ*. Угрозы ИБ реализуются через определенные *уязвимости* – свойства информационной системы, предоставляющие возможность реализации угроз информационной безопасности для обрабатываемой в ней информации. Субъекта (физическое лицо, материальный объект или физическое явление), являющегося непосред-

ственной причиной возникновения угрозы безопасности называют *источником угрозы*. На рисунке 1.3. представлена возможная классификация угроз ИБ.

Особо опасными угрозами ИБ в КИС являются антропогенные угрозы, источником которых является человеческий фактор. Среди них особое внимание с точки зрения защиты необходимо уделять внутренним нарушителям или «инсайдерам». Большинство предприятий относят внутренние угрозы к наиболее опасным, о чем свидетельствуют аналитические отчеты таких компаний известных компаний, как Perimetrix, Ernst&Young. Статистика показывает, что объем инцидентов ИБ, связанных с внутренними сотрудниками, для современных компаний составляет более 85 процентов общего числа.

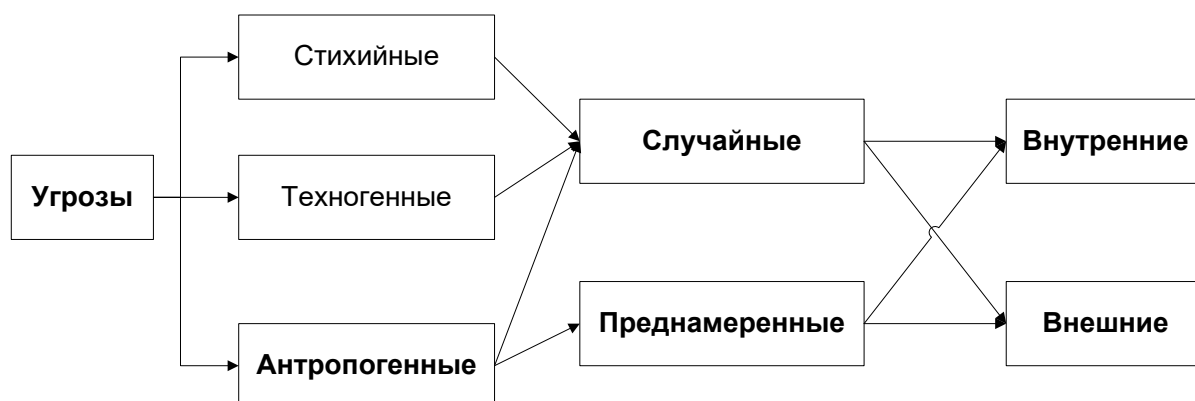


Рисунок 1.3. Возможная классификация угроз ИБ

Рассматривая угрозы ИБ во взаимосвязи с защищаемыми активами, следует отметить различный характер возможных угроз. Например, информационные ресурсы могут быть подвержены угрозам нарушения конфиденциальности, целостности, доступности. Те же угрозы следует рассматривать для АРМ и серверов, являющихся хранилищем и местом обработки информационных активов. С другой стороны, для ИТ-сервисов в качестве основных угроз следует рассматривать снижение их производительности или нарушение доступности, которые напрямую отражаются на эффективности выполнения бизнес-функции и бизнес-процесса, реализуемого ИТ-сервисом. На рисунке 1.4. приведены возможные временные затраты, связанные с простаиванием или снижением производительности ИТ-сервиса в результате реализации угроз, приведших к инциденту ИБ.

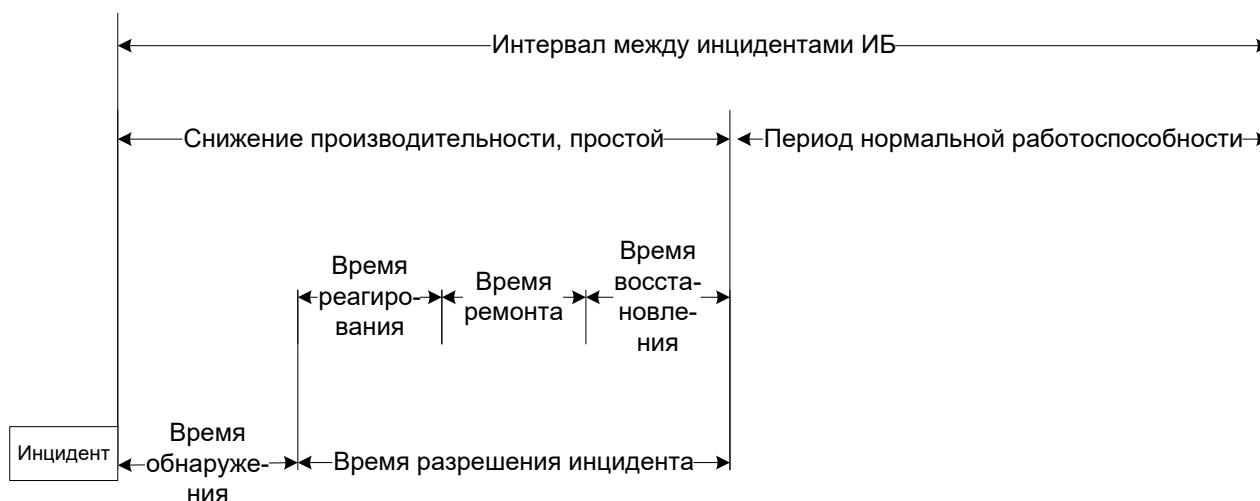


Рисунок 1.4. Временные затраты, связанные с влиянием инцидента на ИТ-сервис

В настоящее время известно множество российских и международных стандартов, предназначенных для обеспечения базового уровня защищенности обозначенных активов корпоративных информационных сетей. Однако для многих современных информационных систем и сетей целесообразно рассматривать защищенность с позиций оценки и управления рисками ИБ, связанных с угрозами, нацеленными на данные активы. Это приводит к необходимости исследования понятия риска ИБ и способов его оценки.

Понятие риска в различных предметных областях зачастую определяется по-разному, в связи с чем использование данного термина требует уточнения исследуемой области. Понятие риска, инвариантное к предметной области определено в стандарте ГОСТ Р 51897-2011/Руководство ИСО 73:2009. «Менеджмент риска. Термины и определения», согласно которому под *риском* следует понимать «следствие влияния неопределенности на достижение поставленных целей». При этом с точки зрения информационной безопасности КИС важны следующие примечания, которые оговариваются в данном стандарте:

- величина риска часто характеризуется «путем описания возможного события и его последствий, или их сочетания»;
- событие может быть названо терминами «угроза возникновения опасного события», «угроза инцидента»;
- последствием является «результат воздействия события на объект».

В РФ применительно к области информационной безопасности понятие риска определено в ряде (в том числе отраслевых) стандартов:

- ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», согласно которому под *риском информационной безопасности* понимается «возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации».
- ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология», согласно которому под *риском информационной безопасности* понимается *потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации*.
- ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения»: *Риск нарушения безопасности сети электросвязи это вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи;*
- ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности организаций. Основные термины и определения»: *Риск это влияние неопределенностей на процесс достижения поставленных целей, часто выражаемый в терминах комбинаций последствий события или изменения обстоятельств и их вероятности;*
- ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»: *Риск это потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием*

уязвимости актива или группы активов. Определяется как сочетание вероятности события и его последствий

- РС БР ИББС-2.2-2009 «Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организации банковской сферы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»: *Риск нарушения ИБ это риск, связанный с угрозой ИБ, – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.*

Кроме этого, проводя анализ зарубежных стандартов и руководств по оценке и управлению рисками ИБ, можно выделить следующие основные определения:

- NIST SP 800-30 Revision 1 «Information Security. Guide for Conducting Risk Assessments»: *Риск информационной безопасности это оценка возможного ущерба, наносимого организации либо активу в результате реализации некоторой угрозы;*
- Руководство Microsoft «The Security Risk Management Guide»: *Риск информационной безопасности это сочетание вероятности события и его последствий;*
- OCTAVE: *Риск это возможность получения ущерба или возникновения негативных последствий*

Анализ данных определений, а также соответствующих им стандартов и руководств позволяет сформировать следующую диаграмму возникновения риска ИБ (рисунок 1.5). Согласно данной диаграмме, риск возникает при наличии источника угрозы и наличии эксплуатируемой уязвимости, через которую может реализовываться данная угроза.

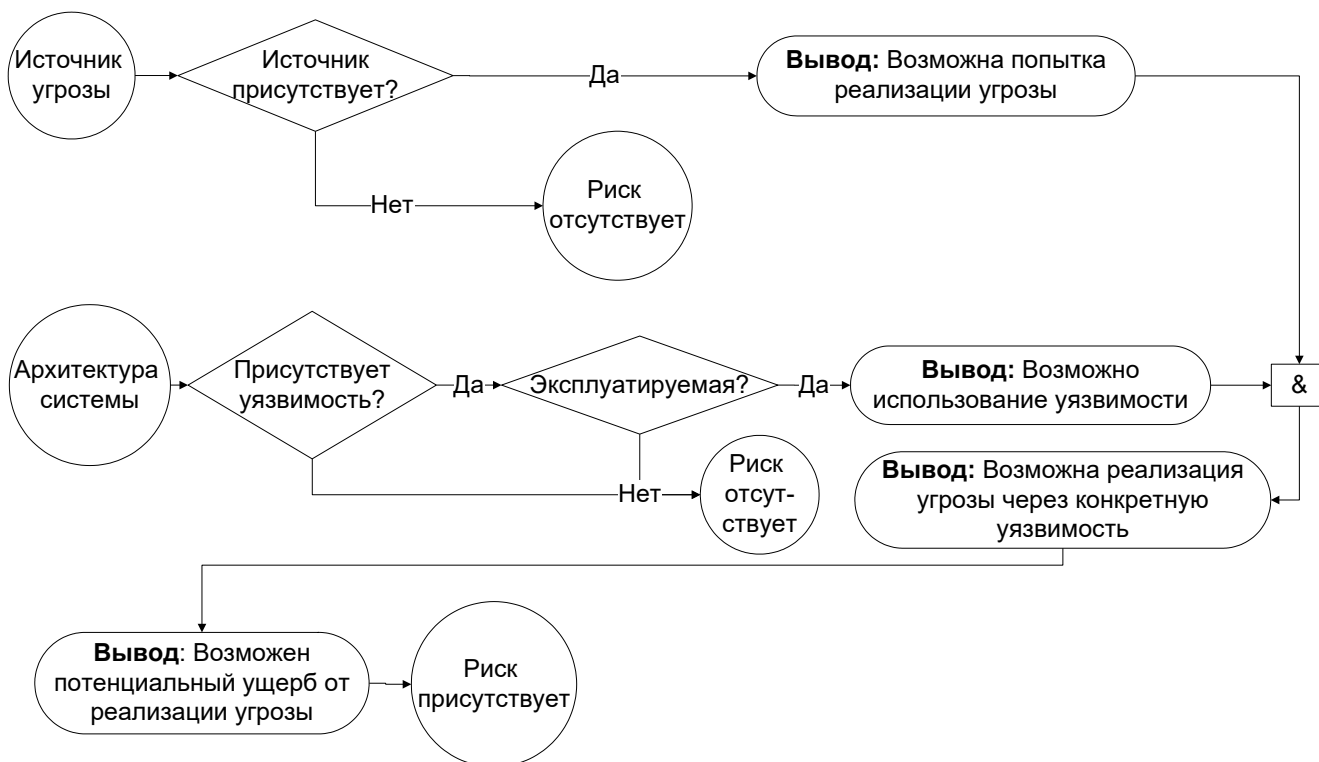


Рисунок 1.5. Диаграмма возникновения риска информационной безопасности

В результате проведенного анализа определений риска ИБ, а также диаграммы, представленной на рисунке 1.5, будем рассматривать следующее определение риска информационной безопасности.

Риск информационной безопасности – возможный ущерб организации в результате реализации некоторой угрозы через уязвимость.

Исходя из данного определения и рисунка 1.5, можно выделить следующие основные факторы риска ИБ:

- возможность реализации угрозы,
- возможность использования уязвимости,
- ущерб от реализации угрозы.

Основываясь на этом, выделяют два основных способа оценки рисков ИБ – двухфакторный и трехфакторный. При использовании двухфакторного подхода риск ИБ определяется согласно выражению (1.1) через возможность реализации угрозы T , используя заданную уязвимость V и ущерб от реализации угрозы T . Данный подход используют такие стандарты и руководства, как NIST SP 800-30, OCTAVE, Digital Security, Risk Watch. При использовании трехфакторного подхода уровень риска ИБ определяется согласно выражению (1.2) че-

рез возможность использования уязвимости V , возможность реализации угрозы T , используя заданную уязвимость V и ущерб от реализации угрозы T . Данный подход используют такие стандарты, как Microsoft Methodology «The Security Risk Management Guide», CRAMM, ISRAM.

$$R(T) = PossT(T) \cdot Impact(T), \quad (1.1)$$

$$R(V, T) = PossV(V) \cdot PossT(T) \cdot Impact(T), \quad (1.2)$$

где $PossV(V)$ – возможность использования уязвимости V , $PossT(T)$ – возможность реализации угрозы T , $Impact(T)$ – ущерб от реализации угрозы T .

1.3. Классификация существующих методов оценки рисков и основные проблемы

На рисунке 1.6. представлены основные группы методов оценки и управления рисками информационной безопасности.



Рисунок 1.6. Основные группы методов оценки и управления рисками информационной безопасности

Методы качественной оценки и управления рисками ИБ используются для экспресс-оценки рисков с целью быстрого определения актуальных угроз. Основным способом оценки рисков в данном случае является введение порядковых шкал для оценки факторов риска, а также матриц для оценки уровней риска ИБ.

К основным преимуществам данных методов следует отнести следующие:

- простота практического использования;
- возможность учесть качественный характер факторов риска информационной безопасности;
- более высокая согласованность формируемых оценок риска за счет использования небольшого количества градаций качественных шкал.

К основным недостаткам данных методов следует отнести следующие:

- плохая интерпретируемость формируемых оценок риска ИБ в рамках экономических моделей;
- трудоемкость применения математического аппарата для формирования оптимальной совокупности защитных мероприятий;
- оценки риска ИБ в рамках одной градации не различаются, что осложняет анализ полученных оценок (исследователю приходится иметь дело с «грубыми», неточными категориями риска);
- поверхностный характер оценок.

Методы количественной оценки и управления рисками ИБ предполагают детальный анализ процессов, происходящих в информационных системах и сетях, формирование экономических оценок на основе оценок риска ИБ. Основным способом оценки рисков в данном случае является использование непрерывных числовых интервалов для оценки факторов риска ИБ.

К основным преимуществам методов количественной оценки и управления рисками ИБ следует отнести следующие:

- хорошая интерпретируемость формируемых оценок риска ИБ в рамках экономических моделей;
- простота применения математического аппарата для формирования оптимальной совокупности защитных мероприятий;
- возможность формирования более детально проработанных оценок риска, основываясь на аналитическом описании отдельных процессов, происходящих в информационных системах и сетях;
- формируемые оценки риска получаются менее «грубыми», в отличие от качественных оценок, что позволяет легко их различать.

Основные недостатки и сложности практического использования методов количественной оценки рисков ИБ связаны со следующими особенностями исходных данных:

- качественным (не количественным) характером большинства частных показателей факторов риска ИБ, влияющих на возможность реализации угроз и использования уязвимостей, а также определяющих ущерб (например, возможный ущерб организации в результате реализации угрозы может выражаться в таких «чисто качественных» показателях, как «Ущерб ее авторитету», «Публикации негативных материалов в прессе», «Ухудшении эмоционального климата в коллективе» и т.д.);
- недостаточным объемом или полным отсутствием статистической информации об отдельных угрозах и уязвимостях;
- отсутствием или нечеткостью исходной информации об угрозах и уязвимостях;
- противоречивостью оценок факторов риска, формируемых экспертами.

К основным недостаткам методов количественной оценки и управления рисками ИБ следует отнести следующие:

- более высокая сложность практического использования;
- необходимость обеспечения согласованности и достоверности формируемых оценок;
- факторы риска часто имеют не количественный, а качественный характер (их сложно оценить в количественном виде);
- недостаточный объем или полное отсутствие статистической информации по ряду угроз, в связи с чем возникают сложности применения аналитических методов для оценки факторов риска ИБ;
- практическая сложность либо невозможность формирования экспертом точных оценок факторов риска (в связи с этим методы, основанные на использовании нечетких оценок, становятся более актуальными).

Тем не менее, практическое применение методов количественной оценки рисков ИБ при построении экономически эффективных систем защиты инфор-

мации является более предпочтительным. Однако, при этом возникает ряд выше перечисленных сложностей, требующих решения.

Среди количественных подходов к оценке и управлению рисками ИБ выделяют аналитические и экспертные. Однако, в связи с ранее отмеченными сложностями, связанными с отсутствием статистики по реализации угроз, неопределенностью исходной информации, на практике более широкое распространение получили экспертные методы.

Смешанные методы оценки и управления рисками ИБ могут использовать как качественный, так и элементы количественного подхода к оценке и управлению рисками.

Также необходимо отметить, что несмотря на значительное количество проводимых исследований и опубликованных работ, а также несмотря на наличие современной нормативной базы оценки и управления рисками ИБ, в настоящее время в данной области существует ряд сложностей, несоответствий и даже противоречий.

На рисунке 1.7 представлены основные современные руководства и стандарты оценки и управления рисками ИБ.

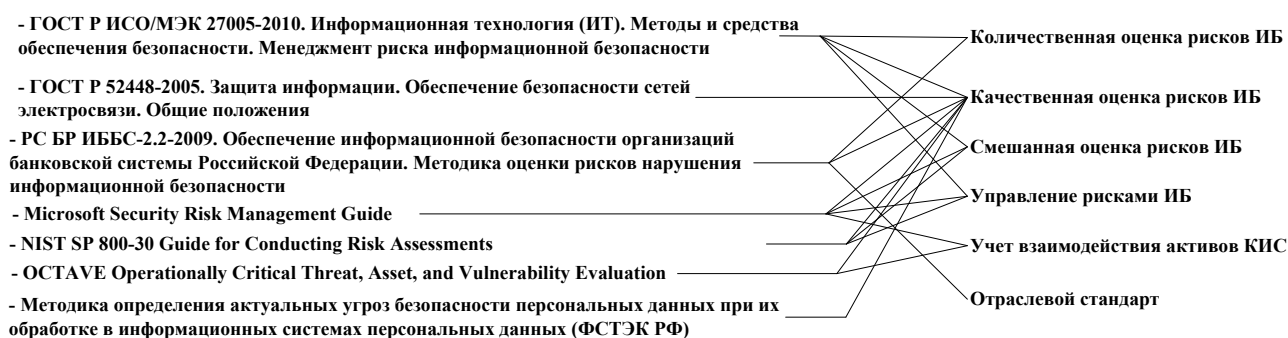


Рисунок 1.7. Основные современные руководства и стандарты оценки и управления рисками ИБ

Анализ данных руководств и стандартов позволяет выявить отдельные их недостатки:

- отсутствие единого подхода к оценке факторов риска;

- отсутствие единых требований к определению частных показателей ущерба от реализации угроз, возможности их активизации;
- отсутствие либо неполный учет взаимодействия активов с позиции оценки наносимого им ущерба.

Существующие методы оценки риска достаточно подробно представлены в стандарте ГОСТ ИСО/МЭК 31010 – 2011. Их анализ представлен на рисунке 1.8.

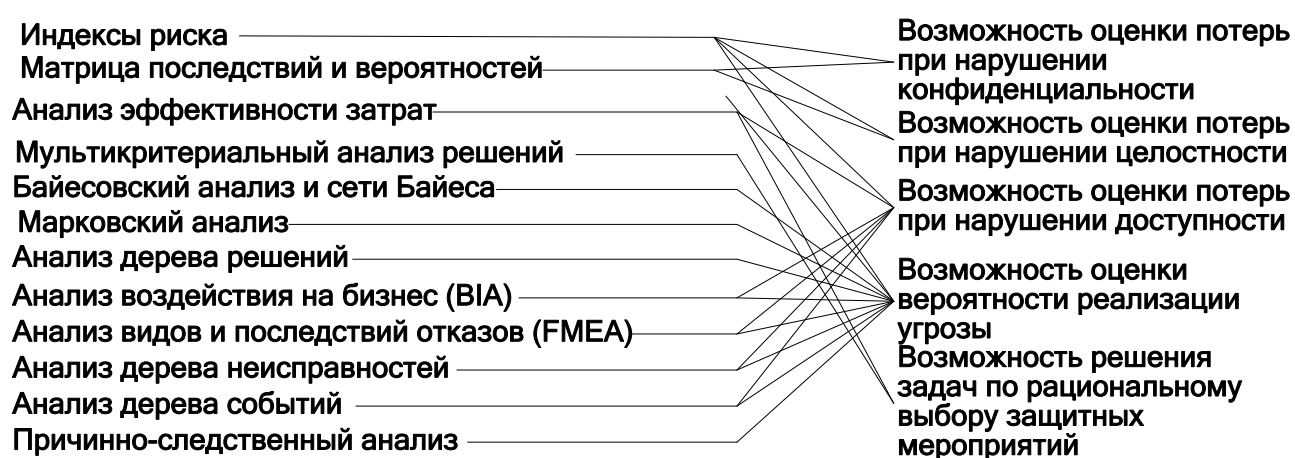


Рисунок 1.8. Сравнительный анализ методов оценки рисков
(ГОСТ ИСО/МЭК 31010 – 2011)

Рассмотрим более подробно отдельные стандарты и руководства по оценке и управлению рисками ИБ.

1.4. Контрольные вопросы

1. В чем заключается актуальность проблемы оценки и управления рисками информационной безопасности?
2. Охарактеризуйте базовый подход к обеспечению информационной безопасности.

3. Охарактеризуйте подход к обеспечению информационной безопасности, основанный на оценке и управлению рисками.
4. Что понимают под защищаемыми активами?
5. Что понимают под ИТ-сервисами?
6. Перечислите виды ИТ-сервисов.
7. Дайте определение угрозы и уязвимости.
8. Перечислите несколько видов источников угроз.
9. Дайте классификацию угроз ИБ по источнику их возникновения.
10. Дайте определение риска.
11. В чем заключается специфика качественного подхода к оценке и управлению рисками ИБ.
12. В чем заключается специфика количественного подхода к оценке и управлению рисками ИБ.
13. В чем заключается специфика смешанного подхода к оценке и управлению рисками ИБ.
14. Перечислите основные достоинства и недостатки качественного подхода к оценке и управлению рисками ИБ.
15. Перечислите основные достоинства и недостатки количественного подхода к оценке и управлению рисками ИБ.

2. СТАНДАРТЫ И РУКОВОДСТВА ОЦЕНКИ И УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной главе приводятся основные Российские и зарубежные стандарты и руководства оценки и управления рисками ИБ. Приводятся методы качественной оценки, количественной оценки и смешенной оценки и управления рисками ИБ.

2.1. Качественная оценка и управление рисками информационной безопасности

2.1.1. NIST SP 800-30 «Guide for Conducting Risk Assessments»

Рассмотрим подход к оценке и управлению рисками ИБ согласно стандартам США и более ее ранней версии. Данные документы позволяют достаточно хорошо описать общий подход решению рассматриваемых задач.

Согласно методология оценки рисков включает в себя 9 основных шагов (рисунок 2.1):

- 1) определение характеристик системы;
- 2) определение уязвимостей;
- 3) определение угроз;
- 4) анализ мер безопасности;
- 5) определение вероятности;
- 6) анализ влияния;
- 7) определение риска;

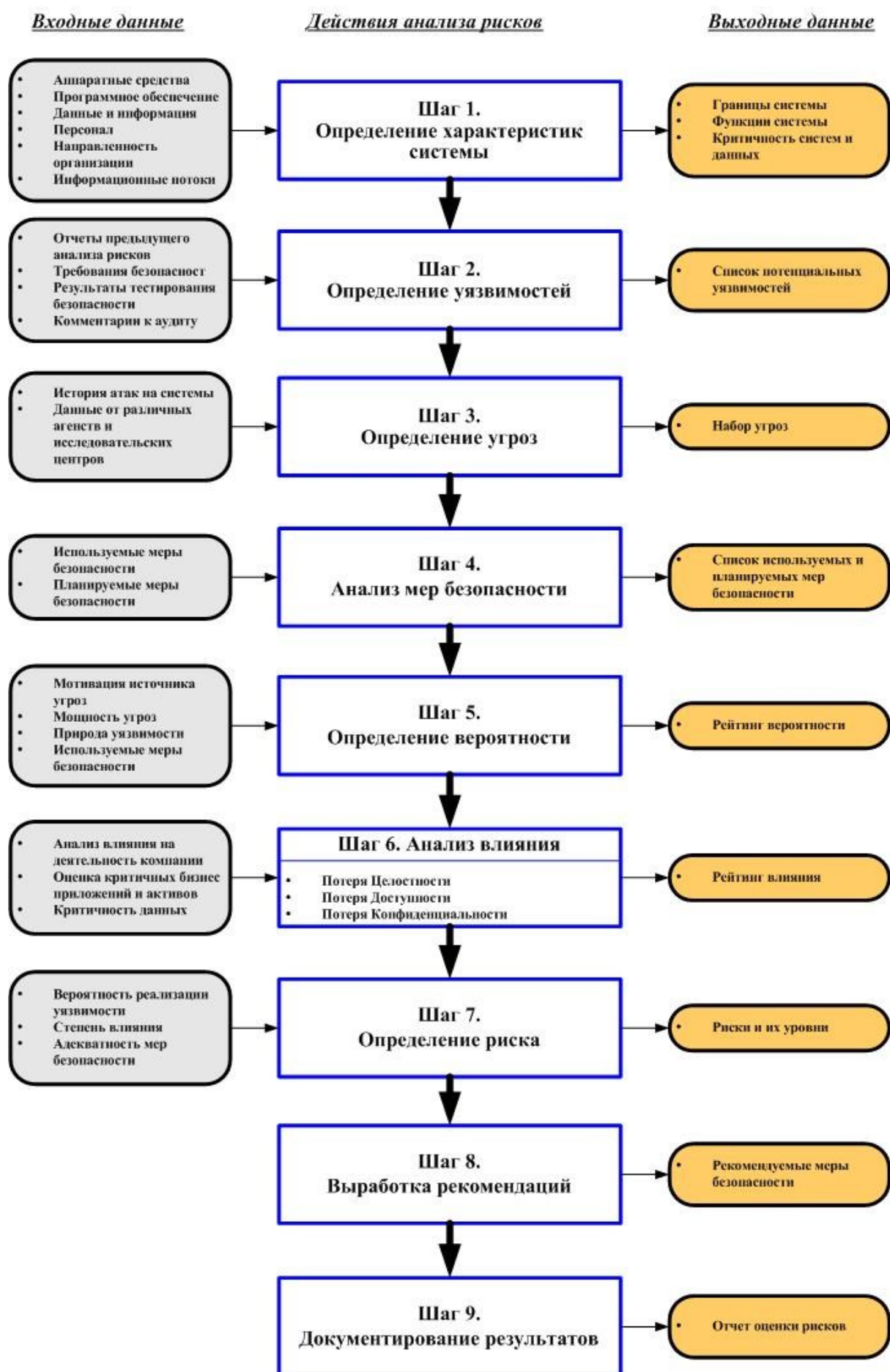


Рисунок 2.1. Оценка рисков ИБ согласно руководству NIST SP 800-30

- 8) выработка рекомендаций;
- 9) документирование результатов.

Шаг 1. Определение характеристик системы

Лицо или лица, которые выполняют оценку рисков, должны произвести детальный анализ системы, для чего провести сбор следующей информации:

- сведения об аппаратном обеспечении;
- сведения о программном обеспечении;
- взаимодействие системы (например, внешние и внутренние связи);
- сведения о хранимых и обрабатываемых данных и информации;
- сведения о лицах, которые поддерживают и используют информационную систему;
- назначение системы;
- сведения о критичности информационных ресурсов (конфиденциальность, целостность, доступность);
- функциональные требования к информационной системе;
- пользовательские роли;
- правила безопасности для информационной системы;
- архитектура безопасности системы;
- текущая сетевая топология;
- механизмы безопасности, которые обеспечивают конфиденциальность, целостность и доступность данных и системы;
- информационные потоки, принадлежащие информационной системе;
- механизмы управления, используемые в информационной системе;
- операционные механизмы, используемые в информационной системе;
- способы обеспечения физической безопасности информационной системы;
- механизмы обеспечения безопасности среды функционирования информационной системы (например, механизмы контроля влажности, воды, энергии, выбросов, температуры и химических веществ).

Для сбора информации о системе может быть использована одна из следующих техник, или их комбинация.

Опросные листы. Для сбора необходимой информации персонал, выполняющий оценку рисков, может разработать опросные листы, касающиеся управленческих и операционных механизмов, планируемых к использованию или используемых в информационной системе. Эти опросные листы должны распространяться в технической и нетехнической форме персоналу, который занимается проектированием, поддержкой или использованием информационной системы. Опросные листы могут также использоваться непосредственно в течение интервьюирования.

Интервьюирование с персоналом, который поддерживает работу информационной системы. NIST SP 800-30 содержит примеры вопросов, задаваемых в течении интервьюирования. Образцы вопросов:

- Кто являются авторизованными пользователями?
- Какие задачи решает система в отношении деятельности организации?
- Какова важность системы для решения пользователями своих задач?
- Какие требования доступности системы?
- Какая информация (входная и выходная) важна для организации?
- Какая информация создается, потребляется, обрабатывается, хранится или принимается системой?
- Как распределены информационные потоки?
- Какие виды информационных ресурсов обрабатываются и хранятся в системе?
- Каков уровень конфиденциальности информации, обрабатываемой в системе?
- Где конкретно обрабатывается и хранится информация?
- Каковы требования по доступности и целостности к информации?
- Каково допустимое время простоя системы для организации? К каким иным способом пользователи могут получить доступ к системе?

Обзор документов – политик безопасности, системной документации, документации по безопасности системы и т.д.

Использование автоматизированных средств сканирования – средств картографирования сети, сканеров портов и сканеров безопасности, средств автоматического сбора информации о конфигурации узлов. Использование данных средств позволяет получить в автоматизированном режиме карту информационной системы, перечень активного оборудования и реализуемых ИТ-сервисов, используемых ОС, а в идеале и полную конфигурацию узлов информационной системы.

На этапе определения характеристик системы желательно иметь или построить формализованные описания бизнес-процессов, реализуемых в информационной системе.

Шаг 2. Определение уязвимостей

Цель данного шага – определение перечня уязвимостей, которые могут быть использованы и привести к реализации угроз ИБ. Рекомендуемые методы для определения уязвимостей системы:

Анализ источников, публикующих информацию об уязвимостях: CVE Project, SecurityTracker, CERT, SecurityFocus, SecurityLab и др.

Тестирование безопасности системы, включающее в себя использование сканеров безопасности, специализированных тестов и оценок безопасности, тестов на проникновение.

Использование проверочных листов для анализа выполнения требований безопасности.

Наиболее известными сканерами безопасности, позволяющих выполнять поиск уязвимостей в автоматизированном режиме, являются NESSUS, XSpider, IBM AppScan, СКАНЕР-BC, Burp Suite и Acunetix WVS (используемые для поиска уязвимостей в WEB-приложениях). В работе предлагается подход к автоматизации процесса валидации уязвимостей, найденных автоматическими сканерами безопасности.

В приложении F документа представлена шкала для оценки степени опасности найденных уязвимостей в информационной системе.

Шаг 3. Определение угроз

На данном шаге строится модель угроз, включающая в себя источник угрозы и используемую уязвимость. Включение в модель антропогенных угроз и мотивации их источника позволяет делать в дальнейшем более обоснованные выводы относительно возможности их реализации.

В приложении D документа представлена классификация источников угроз, а в приложении E – перечень возможных угроз. Данные приложения могут быть эффективно использованы для построения модели угроз КИС.

В качестве возможных источников реализации угроз рассматриваются следующие:

– Преднамеренные

- Исходящие от индивидуального нарушителя
 - Внешнего нарушителя
 - Внутреннего нарушителя (инсайдера)
 - Инсайдера (доверенного сотрудника)
 - Привилегированного инсайдера
- Исходящие от группы нарушителей
 - Официальной
 - Временно созданной
- Исходящие от организации
 - Конкурентов
 - Поставщиков
 - Партнеров
 - Клиентов
- Исходящие от государства

– Случайные

- Исходящие от пользователей
- Исходящие от привилегированных пользователей/администраторов

– **Связанных с активами КИС**

- Связанные с ИТ-активами
 - Хранения информации
 - Обработки информации
 - Передачи информации
 - Отображения информации
 - Датчиками
 - Управления
- Связанные с управляющим оборудованием
 - Управления температурой/влажностью
 - Бесперебойного питания
- Связанные с программным обеспечением
 - Операционными системами
 - Компьютерными сетями
 - ПО, реализующего основные бизнес-процессы
 - ПО, реализующего не основные бизнес-процессы

– **Связанные с окружающей средой**

- Природные катаклизмы или исходящие от человека бедствия
 - Пожар
 - Затопление/цунами
 - Шторм/торнадо
 - Ураган
 - Землетрясение
 - Бомбардировка
 - Опустошение
- Необычные природные события
- Сбой в работе или простой инфраструктуры
 - Телекоммуникаций
 - Электричества

В качестве перечня возможных преднамеренных угроз рассматриваются следующие:

- Разведка и сбор информации
 - Разведка/сканирование периметра сети
 - Прослушивание каналов связи
 - Разведка/наблюдение за работой организации
 - Использование вредоносных программ с целью внутренней разведки
 - Сбор информации об организации на основе открытых источников
- Мошенничество
 - Мошенничество с помощью фишинг-атак
 - Фишинговые атаки, направленные на высшее руководство организации
 - Мошенничество, использующее специально развернутое в организации оборудование
 - Создание фальшивых сайтов
 - Создание фальшивых сертификатов
 - Поставка вредоносных компонентов в организацию через организаций-поставщиков
- Доставка/внедрение/установка вредоносных компонентов
 - Доставка/внедрение/установка известных вредоносных программ во внутренние системы организации
 - Доставка/внедрение/установка новых версий вредоносных программ во внутренние системы организации
 - Целевое внедрение вредоносных программ для управления информационными системами и хищения данных
 - Заражение вредоносными программами через сменные носители
 - Заражение вредоносными программами через загружаемое из сети ПО или коммерческие продукты

- Целенаправленное внедрение вредоносных программ в компоненты информационных систем
 - Внедрение специализированных вредоносных программ в информационные системы, основываясь на ошибках системной конфигурации
 - Поставка поддельного оборудования в организацию
 - Подделка критичных компонентов в информационных системах
 - Использование снифферов общего вида
 - Использование специализированных снифферов
 - Внедрение заинтересованных лиц в организацию
 - Внедрение заинтересованных лиц в качестве привилегированных персон в организацию
- Компрометация и использование в своих интересах
- Использование в своих интересах авторизованных сотрудников для того, чтобы получить доступ к объектам организации
 - Использование в своих интересах плохо сконфигурированных или несанкционированных информационных систем, получающих доступ в интернет
 - Использование в своих интересах многостороннего договора аренды в облачных средах
 - Использование известных уязвимостей в мобильных системах
 - Использование недавно обнаруженных уязвимостей
 - Использование уязвимостей информационных систем организации
 - Использование уязвимостей через «zero-day» атаки
 - Использование уязвимостей бизнес-процессов организации
 - Использование небезопасного или неполного удаления данных при многопользовательском использовании оборудования
 - Нарушение изоляции в многопользовательской среде
 - Компрометация критичных информационных систем, используя физический доступ

- Компрометация критичных информационных систем, используя внешний доступ
 - Компрометация программного обеспечения критичных информационных систем
 - Компрометация критически важной информации
 - Компрометация компонентов информационных систем в процессе проектирования, разработки и/или распространения
- Атака на системы
- Проведение атак, направленных на перехват информации, передаваемой по каналам связи
 - Создание помех в беспроводных сетях
 - Проведение атак, используя несанкционированные порты, протоколы и сервисы
 - Проведение атак, используя данные об организации, полученные путем внешнего сканирования
 - Реализация простых DoS атак
 - Реализация распределенных DoS атак
 - Реализация целевых DoS атак
 - Физическое нападение на объекты организации
 - Физическое нападение на инфраструктуру, поддерживающую работу объектов организации
 - Кибер-атаки на объекты организации
 - Восстановление удаленных данных в облачных средах
 - Полный перебор паролей для учетных записей
 - Проведение нецелевых zero-day атак
 - Внешний захват сессии
 - Внутренний захват сессии
 - Внешняя модификация сетевого трафика (man in the middle)
 - Внутренняя модификация сетевого трафика (man in the middle)
 - Внешняя социальная инженерия

- Внутренняя социальная инженерия
- Компрометация личных устройств у критичных работников
- Угрозы получения ценной информации или реализации неблагоприятных последствий
 - Получение ценной информации путем прослушивания внешних сетей
 - Получение ценной информации через утечку данных
 - Снижение производительности или отказ в доступе к определенным сервисам
 - Снижение производительности или разрушение компонентов и функций критичных информационных систем
 - Нарушение целостности публично доступной информации (в т.ч. дефейс web-сайта)
 - Нарушение целостности критичных данных
 - Нарушение целостности путем введения ложных (но правдоподобных) данных в информационные системы организации
 - Утечка критичной информации через авторизованных пользователей
 - Реализация утечки информации путем ее «расщепления»
 - Внешний перехват трафика, передаваемого по беспроводной сети организации
 - Несанкционированный доступ со стороны авторизованного пользователя путем расширения своих полномочий
 - Получение критичной информации из публично опубликованной
 - Кража информации или компонентов КИС, которые были оставлены без присмотра за пределами периметра организации
- Управляемые атаки
 - Атаки, реализуемые в несколько шагов
 - Атаки, требующие как физического, так и внешнего доступа
 - Атаки, требующие воздействия на несколько организаций

- Распространение воздействия одной информационной системы организации на другую
- Управление атакой на основе детального наблюдения за системой
- Одновременное воздействие на организацию со стороны инсайдера, аутсайдера и поставщика

В качестве перечня возможных непреднамеренных угроз рассматриваются следующие.

- Случайная пересылка конфиденциальной информации неавторизованному пользователю
- Некорректное воздействие или использование критичной информации авторизованным пользователем
- Некорректная установка привилегий
- Снижение производительности каналов связи в силу соперничества
- Неотображаемая информация
- Землетрясение
- Пожар в головном здании
- Пожар в резервном здании
- Воздействие наводнения на головное здание
- Воздействие наводнения на резервное здание
- Воздействие урагана на головное здание
- Воздействие урагана на резервное здание
- Воздействие торнадо на головное здание
- Воздействие торнадо на резервное здание
- Истощение ресурсов
- Уязвимости разрабатываемого программного обеспечения
- Ошибка дискового устройства (носителя информации)
- Многократная ошибка дискового устройства

Шаг 4. Анализ мер безопасности

Цель этого шага – анализ мер безопасности, которые реализованы или планируются к реализации организацией для уменьшения рисков ИБ. В документах можно найти исчерпывающий набор мер безопасности, которые могут быть использованы для защиты информационной системы. На основании данных документов можно формировать опросные листы, которые использовать на этапе анализа мер безопасности.

Шаг 5. Определение вероятности

Для получения общего рейтинга вероятности, который показывает возможность реализации угрозы через потенциальную уязвимость, должны рассматриваться следующие факторы:

- Мотивация и возможности источника угрозы,
- Природа уязвимости,
- Наличие и эффективность действующих мер безопасности.

В для определения данной вероятности, предлагается использовать качественную шкалу, представленную в таблице 2.1.

Таблица 2.1. Определение вероятности

Уровень вероятности	Определение вероятности
Высокий	Источник угрозы высоко мотивирован и имеет достаточные возможности, и механизмы безопасности не эффективны.
Средний	Источник угрозы мотивирован и имеет возможности, но действующие механизмы безопасности могут быть помехой в реализации уязвимости.
Низкий	Источник угрозы недостаточно мотивирован или имеет недостаточные возможности, или действующие механизмы безопасности могут предотвратить или значительно снизить возможность реализации уязвимо-

	сти.
--	------

В для оценки вероятности реализации угроз предпринимаются следующие шаги:

1. Определяется возможность инициации или возникновения угрозы согласно таблицам 2.2, 2.3.

Таблица 2.2. Возможность инициации угрозы (источник - человеческий фактор)

Качественные значения	Количественные значения		Характеристика
Очень высокая	96-100	10	Злоумышленник почти определенно попытается реализовать угрозу
Высокая	80-95	8	Злоумышленник очень вероятно попытается реализовать угрозу
Средняя	21-79	5	Злоумышленник достаточно вероятно попытается реализовать угрозу
Низкая	5-20	2	Вряд ли злоумышленник попытается реализовать угрозу
Очень низкая	0-4	0	Злоумышленник очень вероятно не будет пытаться реализовать угрозу

Таблица 2.3. Возможность возникновения угрозы (техногенные и стихийные)

Качественные значения	Количественные значения		Характеристика
Очень высокая	96-100	10	Ошибка, авария, или природное явление почти определенно реализуется;

			появление более 100 раз в год
Высокая	80-95	8	Ошибка, авария, или природное явление очень вероятно реализуется; появление 10-100 раз в год
Средняя	21-79	5	Ошибка, авария, или природное явление достаточно вероятно реализуется; появление 1-10 раз в год
Низкая	5-20	2	Ошибка, авария, или природное явление вряд ли реализуется; появление реже, чем 1 раз в год, но чаще чем 1 раз в 10 лет
Очень низкая	0-4	0	Ошибка, авария, или природное явление очень вероятно не реализуется; появление реже, чем 1 раз в 10 лет

2. Определяется возможность того, что реализация угрозы приведет к негативным последствиям на качественной шкале (таблица 2.4)

Таблица 2.4. Возможность нанесения негативных последствий

Качественные значения	Количественные значения		Характеристика
Очень высокая	96-100	10	Если угроза инициируется или возникнет, то почти определенно возникнет негативный эффект
Высокая	80-95	8	Если угроза инициируется или возникнет, то очень вероятно возникнет

			негативный эффект
Средняя	21-79	5	Если угроза инициируется или возникнет, то достаточно вероятно возникнет негативный эффект
Низкая	5-20	2	Если угроза инициируется или возникнет, то вряд ли возникнет негативный эффект
Очень низкая	0-4	0	Если угроза инициируется или возникнет, то почти очень вероятно не будет нанесен негативный эффект

3. Используя матрицу (таблица 2.5) определяется общая вероятность нанесения угрозой ущерба

Таблица 2.5. Общая вероятность нанесения угрозой ущерба

Возможность инициации или возникновения угрозы	Возможность нанесения негативных последствий				
	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Очень высокая	Низкая	Средняя	Высокая	Очень высокая	Очень высокая
Высокая	Низкая	Средняя	Средняя	Высокая	Очень высокая
Средняя	Низкая	Низкая	Средняя	Средняя	Высокая
Низкая	Очень низкая	Низкая	Низкая	Средняя	Средняя
Очень низкая	Очень	Очень	Низкая	Низкая	Низкая

	низкая	низкая			
--	--------	--------	--	--	--

Шаг 6. Анализ влияния

При оценке влияния угрозы необходимо принимать в рассмотрение целевое назначение системы, критичность данных, набор существующих мер безопасности и их эффективность.

В для оценки влияния угрозы предлагается использовать качественную шкалу (таблица 2.6).

Таблица 1.7. Оценка влияния угрозы

Величина влияния	Определение влияния
Высокое	<p>Потеря конфиденциальности, целостности или доступности может привести к тяжелым или катастрофичным неблагоприятным последствиям, которые отразятся на функционировании организации, а также на активы или персонал этой организации.</p> <p>Тяжелые или катастрофичные неблагоприятные последствия означают, что потеря конфиденциальности, целостности или доступности может: (1) вызвать невосполнимую деградацию целевых показателей, в результате чего организация не способна выполнять свои функции; (2) привести к невосполнимым повреждениям активов организации; (3) привести к невосполнимым финансовым потерям; или (4) привести к тяжелым последствиям в отношении персонала, включая потерю жизни или серьезные раны, которые могут угрожать жизни.</p>
Среднее	<p>Потеря конфиденциальности, целостности или доступности может привести к серьезным неблагоприятным последствиям, которые отразятся на функцио-</p>

	<p>нировании организации, а также на активах или персонале к организации.</p> <p>Серьезные неблагоприятные последствия означают, что потеря конфиденциальности, целостности или доступности может: (1) вызвать значительную деградацию целевых показателей организации, при этом организация способна выполнять свои основные функции, но эффективность этих функций значительно снижена; (2) привести к значительным повреждениям активов организации; (3) привести к значительным финансовым потерям; или (4) привести к значительным повреждениям персоналу, исключая потерю жизни и серьезные раны, угрожающие жизни.</p>
Низкое	<p>Потеря конфиденциальности, целостности или доступности может вызвать ограниченные неблагоприятные последствия, которые отразятся на функционировании организации, а также активах или персонале организации.</p> <p>Ограниченные неблагоприятные последствия означают, что потеря конфиденциальности, целостности или доступности может: (1) вызвать деградацию целевых показателей организации, при этом организация способна выполнять свои основные функции, но эффективность этих функций заметно снижена; (2) привести к незначительным повреждениям активов организации; (3) привести к незначительным финансовым потерям; или (4) привести к незначительным повреждениям персоналу.</p>

В для оценки влияния предлагается рассматривать различные виды ущерба, а также оценивать влияние на следующей качественной шкале (таблица 2.7).

Таблица 2.7. Оценка влияния угрозы

Качественные значения	Количественные значения		Характеристика
Очень высокая	96-100	10	Реализация угрозы может привести к множественным тяжелым или катастрофичным неблагоприятным последствиям, которые отразятся на функционировании организации, а также на активы или персонал этой организации.
Высокая	80-95	8	Реализация угрозы может привести к тяжелым или катастрофичным неблагоприятным последствиям, которые отразятся на функционировании организации, а также на активы или персонал этой организации.
Средняя	21-79	5	Потеря конфиденциальности, целостности или доступности может привести к серьезным неблагоприятным последствиям, которые отразятся на функционировании организации, а также на активах или персонале к организации.
Низкая	5-20	2	Потеря конфиденциальности, целостности или доступности мо-

			жет вызвать ограниченные неблагоприятные последствия, которые отразятся на функционировании организации, а также активах или персонале организации.
Очень низкая	0-4	0	Потеря конфиденциальности, целостности или доступности может вызвать незначительные неблагоприятные последствия, которые отразятся на функционировании организации, а также активах или персонале организации.

Шаг 6. Определение риска

Оценка риска осуществляется на основе полученных оценок вероятности реализации угрозы и ее влияния. Это делается с помощью матриц риска. В таблице 2.8 приводится матрица рисков, предлагаемая в.

Таблица 2.8. Матрица рисков

Возможность	Уровень влияния				
	Очень низкий	Низкий	Средний	Высокий	Очень высокий
Очень высокая	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Высокая	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Средняя	Очень низкая	Низкая	Средняя	Средняя	Высокая

Низкая	Очень низкая	Низкая	Низкая	Низкая	Средняя
Очень низкая	Очень низкая	Очень низкая	Очень низкая	Низкая	Низкая

Шаг 8. Выработка рекомендаций

На данном шаге определяются меры безопасности, которые могут снизить определенные риски исследуемой организации. Цель рекомендуемых мер – снизить уровень риска информационной системы до приемлемого уровня.

Необходимо заметить, что не все рекомендуемые меры безопасности могут быть реализуемы для снижения возможных потерь. На практике необходимо выполнять их анализ по критерию «стоимость/эффективность». Также должно быть тщательно оценено влияние мер безопасности на функционирование системы (например, снижение производительности системы в результате внедрения защитных мер), а также возможность реализации рекомендуемых мер безопасности (например, технические требования, пользовательское одобрение).

Шаг 9. Документирование результатов

По результатам оценки рисков необходимо их документировать в виде официального отчета. В приложениях документов представлена рекомендуемая форма отчета по результатам оценки рисков.

По результатам оценки рисков необходимо предпринимать корректирующие мероприятия и действия по управлению рисками ИБ. Управление рисками представляет собой целенаправленный процесс, направленный на уменьшение уровня рисков и доведение его до приемлемого уровня. По результатам оценки рисков могут быть предприняты следующие действия по отношению к каждому риску:

- Принятие риска. Принять потенциальный риск и продолжать функционирование ИС.

- Уход от риска. Уход от риска с помощью устранения причин и/или последствия риска.
- Снижение риска. Снизить риск путем реализации мер безопасности, которые минимизируют неблагоприятное влияние угрозы или возможность ее возникновения.
- Передача риска. Передать риск, используя такие меры компенсации потерь, как страхование или заключение договора на обслуживание с поставщиком решения.

При внедрении мер безопасности должно применяться следующее правило: меры безопасности направлены в отношении наибольшего риска и стремятся к достаточному снижению этого уровня риска за наименьшую стоимость, при этом внедрение мер оказывает минимальное влияние на возможности функционирования организации.

Диаграмма снижения уровней рисков представлена на рисунке 2.2.

Шаг 1. Определение приоритетов действий. В соответствии с уровнями риска производится определение приоритетов действий по реализации рекомендуемых мер безопасности. Наибольший приоритет следует отдавать действиям, которые отвечают неприемлемо высоким рискам.

Шаг 2. Оценка рекомендуемых мер безопасности. Меры безопасности, рекомендуемые в процессе оценки риска, могут не обладать необходимыми свойствами или функциями для конкретной организации и информационной системы. В течение данного шага выполняется анализ свойств: пригодности (например, совместимость, дружелюбие интерфейса пользователя) и эффективности (например, степень защищенности и уровень снижения риска) рекомендуемых мер. Целью этого шага является выбор наиболее пригодных для минимизации риска мер безопасности.

Шаг 3. Выполнение оценки стоимости/эффективность мер безопасности. Наиболее предпочтительными мерами безопасности являются те, которые за меньшую стоимость будут давать большую эффективность.

Шаг 4. Выбор мер безопасности. В соответствии с результатами анализа мер безопасности по критерию «стоимость/эффективность», определяются наиболее пригодные для снижения риска меры безопасности. Для обеспечения адекватного уровня защиты ИС и организации выбранные меры должны включать в себя организационные, технические, физические и другие меры.

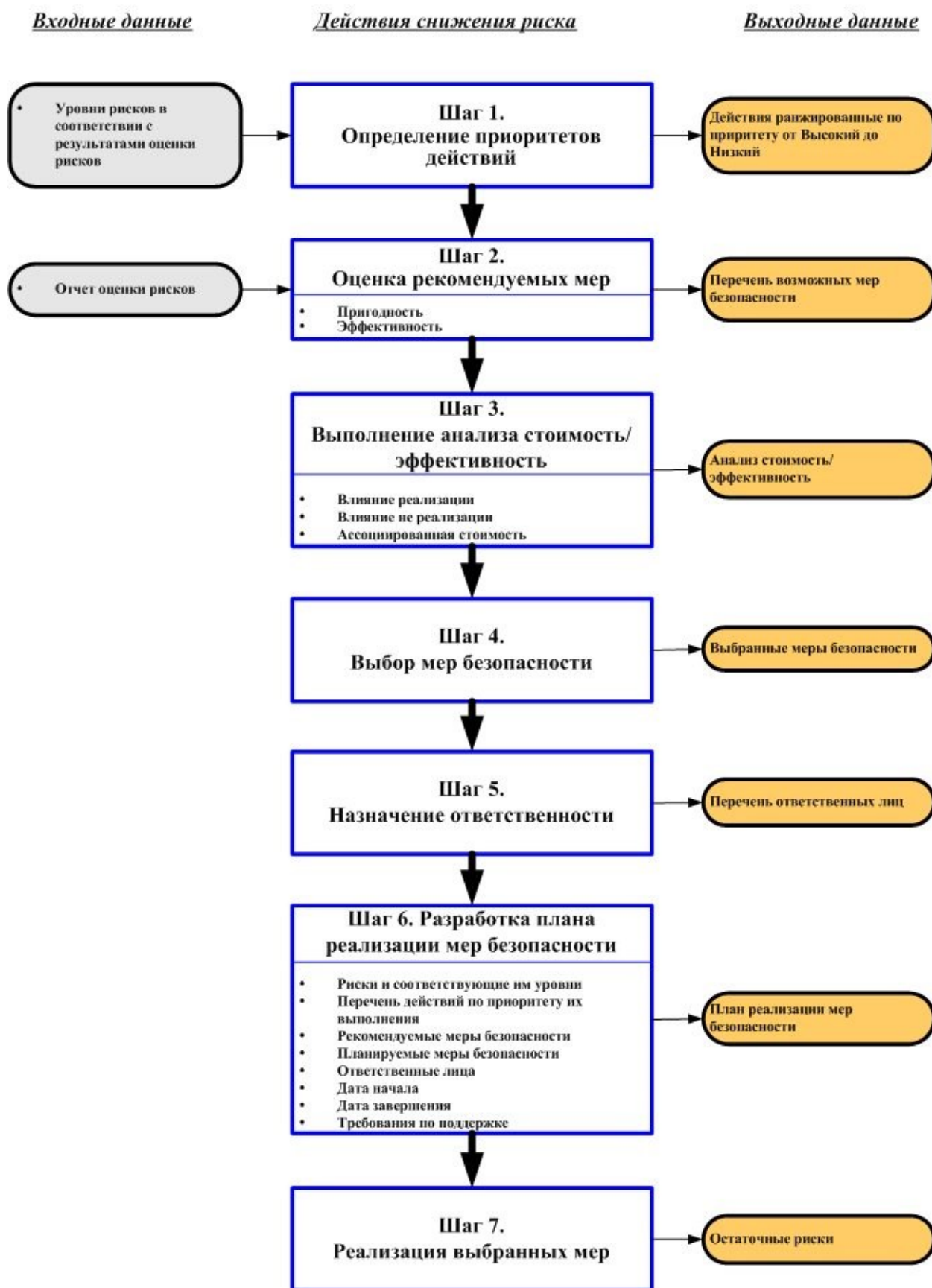


Рис. 2.2. Диаграмма снижения уровней рисков

Шаг 5. Назначение ответственных лиц. Производится определение персонала, который обладает соответствующими навыками и опытом для реализации выбранных защитных мер. Этот персонал определяется как ответственный за их реализацию.

Шаг 6. Разработка плана реализации мер безопасности. План реализации мер безопасности определяет приоритеты реализации действий, а также даты начала и завершения проектов, заключающихся в их выполнении. Этот план будет использоваться для направления и контроля процесса снижения рисков. В приложениях документов представлен образец заполнения данного плана,

Шаг 7. Реализация выбранных мер безопасности. Реализованные меры безопасности могут снизить уровень риска, но не исключить риск. В любом случае в информационной системе будет какой-то уровень остаточных рисков, но этот уровень должен быть приемлемым для организации.

2.1.2. OCTAVE

Метод OCTAVE был разработан координационным центром CERT и достаточно часто используется для внутренней оценки рисков ИБ организациями. Подход, предлагаемый в методе OCTAVE, позволяет решить множество важных задач для организации:

- идентифицировать и ранжировать ключевые информационные активы;
- получить взвешенные оценки угроз для данных активов;
- провести анализ уязвимостей;
- оценить риски информационной безопасности.

Метод OCTAVE предполагает организацию работ по оценке рисков в несколько этапов (фаз). Каждая фаза включает в себя несколько процессов, которые в свою очередь включают в себя ряд симпозиумов, проводимых командой анализа. На симпозиумах происходит обсуждение важных вопросов, выработка стратегии работы.

Фаза 1 предполагает построение профиля угрозы на основе активов. Команда анализа определяет, какие активы организации являются самыми важными для организации и определяют, что делается в настоящее время для защиты данных активов.

Фаза 2 предполагает идентификацию уязвимостей инфраструктуры. Для каждого из выбранных на фазе 1 активов определяются ключевые компоненты информационных систем. Команда анализа исследует эти ключевые компоненты на наличие уязвимостей (организационных, технологических, технических, программных, связанных с человеческим фактором).

Фаза 3 предполагает разработку стратегии защиты и планов по уменьшению рисков информационной безопасности. Команда анализа идентифицирует все угрозы информационной безопасности, определяет возможный ущерб от реализации каждой угрозы, создает критерии оценки рисков информационной безопасности, по которым строится профиль риска для каждого критического актива. На основе этого вырабатывается стратегия защиты и планы по уменьшению рисков.

Метод OSTAVE использует каталог защитных мер и профиль угрозы, а в ходе оценки рисков строится профиль актива.

Каталог защитных мер представляет собой набор лучших практик, использование которых позволяет обеспечить высокий уровень ИБ для организации. Каталог используется для сравнения текущего состояния дел по обеспечению ИБ в организации с желаемым состоянием. Структура данного каталога представлена в таблице 2.9.

Таблица 2.9. Структура каталога защитных мер

Организационные меры защиты	
SP1	Осведомленность и обучение персонала в области ИБ
SP2	Стратегия безопасности
SP3	Управление безопасностью
SP4	Политика безопасности

SP5	Обеспечение безопасности при работе с внешними организациями
SP6	Управление непрерывностью ведения бизнеса
Операционные меры защиты	
OP1	Физическая безопасность
OP1.1	Планы и процедуры физической безопасности
OP1.2	Физический контроль доступа
OP1.3	Мониторинг и аудит физической безопасности
OP2	Безопасность информационных технологий
OP2.1	Управление безопасностью систем и сетей
OP2.2	Администрирование систем
OP2.3	Мониторинг и аудит информационной безопасности
OP2.4	Аутентификация и авторизация
OP2.5	Управление уязвимостями
OP2.6	Криптография
OP2.7	Проектирование и архитектура безопасности
OP3	Кадровая безопасность
OP3.1	Управление инцидентами
OP3.2	Общие методы обеспечения кадровой безопасности

Профили угроз представляют собой деревья, вид которых зависит от источника угроз. На рисунке 2.3. представлен пример дерева угроз, источником которых является человек, получающий доступ по сети или имеющий физический доступ к объекту (базе данных). На рисунке 2.4. представлен пример дерева угроз, источник которой представляет собой системную или иного вида проблему. Активом, подверженным угрозе, также является база данных.

Ниже рассмотрены процессы, реализуемые в ходе оценки рисков в методе OCTAVE.

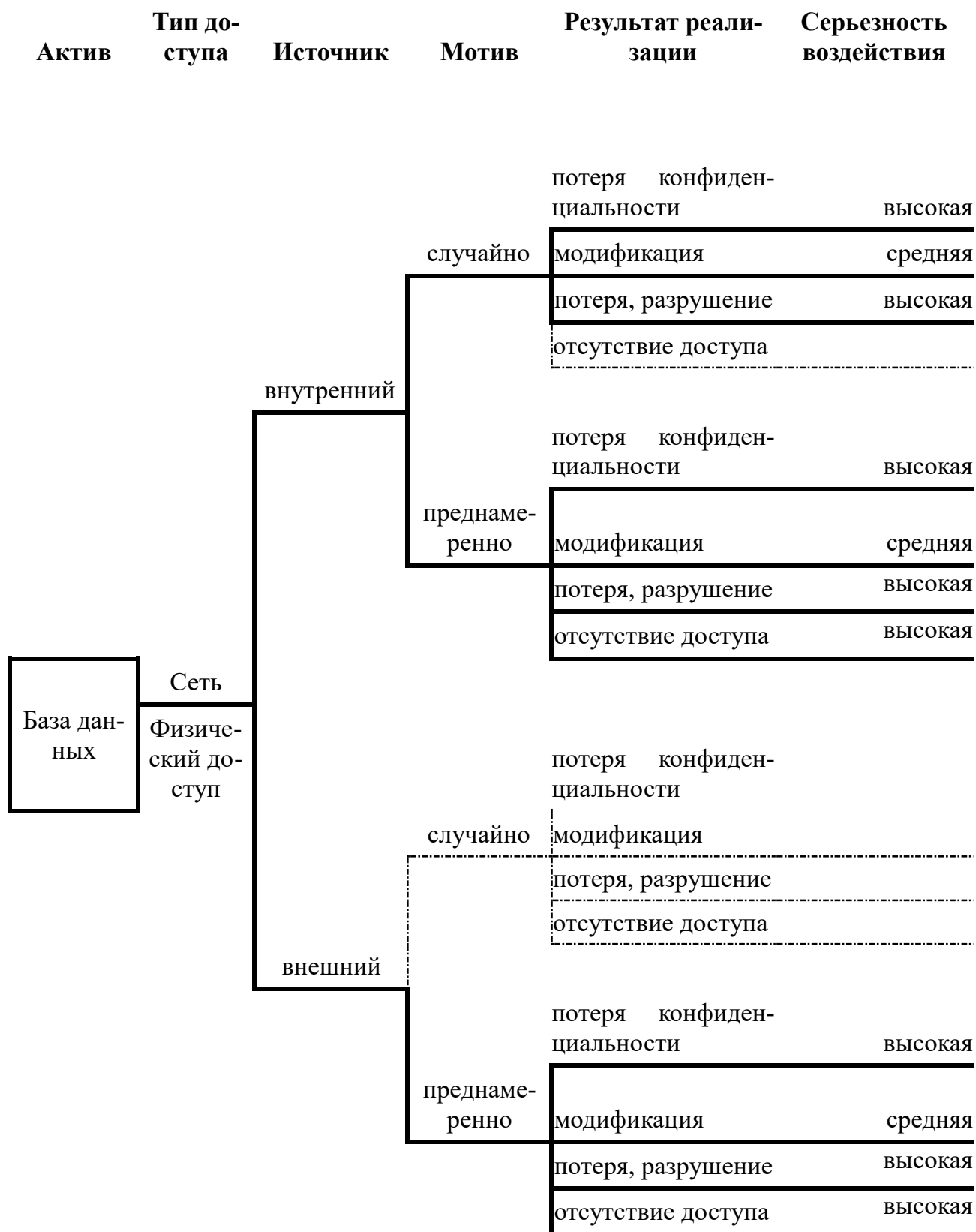


Рисунок 2.3. Пример дерева угроз для источников в виде человека, имеющего доступ по сети или физический доступ.

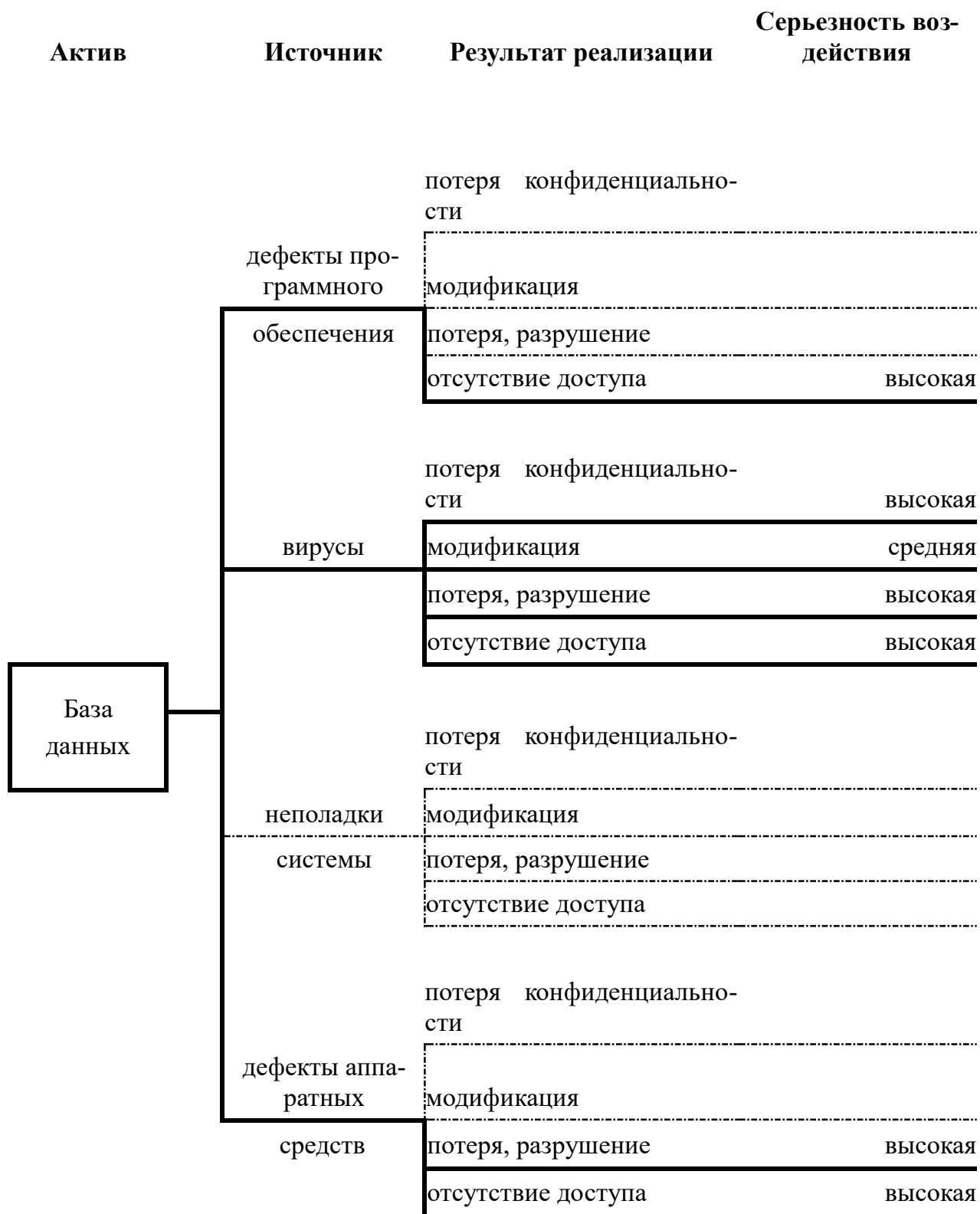


Рисунок 2.4. Пример дерева угроз для источников угроз, представляющих собой системные или иного вида проблемы

Процессы 1-3 включают в себя серию семинаров (для высшего руководства, руководителей среднего звена и сотрудников организации), направленных на получение информации о критичных активах, областях беспокойства, требований по безопасности для наиболее критичных активов.

Процесс 4 предполагает создание профилей угроз для критичных активов. Данные профили строятся в виде рисунка 2.3 или рисунка 2.4.

Процесс 5 предполагает идентификацию ключевых компонентов информационной системы, которые будут проверены на наличие уязвимостей.

Процесс 6 предполагает поиск уязвимостей для выбранных компонентов.

Процесс 7 предполагает выполнение анализа рисков. Для этого определяется уровень воздействия угроз на критичные активы (рассматриваются различные виды ущерба), а также уровень возможности реализации угроз. Данные оценки осуществляются на качественных шкалах. Для каждой угрозы строится профиль риска в виде дерева, аналогичного рисункам 2.3, 2.4 с добавлением оценок уровня воздействия и уровня возможности реализации.

Процесс 8 предполагает разработку стратегии защиты на основе анализа рисков.

2.1.3. CRAMM

Метод CRAMM (CCTA Risk Analysis and Managment Method) был разработан Агентством по компьютерам и телекоммуникациям Великобритании и используется в качестве государственного стандарта. В настоящее время существует несколько версий метода, ориентированных на требования Министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций.

На предварительном этапе работы метода выявляется целесообразность оценки рисков. В случае отсутствия достаточно критичных активов в КИС, к

ней применяется стандартный набор механизмов контроля, которые базируются, как правило, на стандарте BS7799.

На первом этапе метода CRAMM строится модель активов информационной системы. Данная модель описывает взаимодействие между информационными, программными и техническими активами. Далее определяется ценность активов исходя из возможного ущерба, которая организация может понести в результате их компрометации. Используются следующие критерии определения ценности ресурсов:

- Ущерб репутации организации
- Безопасность персонала
- Разглашение персональных сведений
- Разглашение коммерческих сведений
- Неприятности со стороны правоохранительных органов
- Финансовые потери
- Невозможность нормальной работы организации

Определение ценности ресурсов осуществляется по десятибалльной шкале. В качестве примера можно привести следующую шкалу оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов»:

- 2 балла – менее \$1000;
- 6 баллов – от \$1000 до \$10000;
- 8 баллов – от \$10000 до \$100000;
- 10 баллов – свыше \$100000.

При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты (для этого уровня не требуется детальной оценки угроз ИБ) и второй этап метода не реализуется.

На втором этапе метода CRAMM производится оценка рисков в трехфакторном виде. При этом производится идентификация и оценка вероятности угроз, оценка величины уязвимостей и определение рисков для каждой тройки

элементов «актив-угроза-уязвимость». Оценка рисков производится без учета реализованных мер безопасности.

Уровень угроз оценивается по шкале: очень высокий, высокий, средний, низкий, очень низкий. Уровень уязвимости оценивается как высокий, средний или низкий. На основе этой информации оцениваются уровни риска по семи-бальной шкале.

На третьем этапе метода CRAMM определяется набор мер безопасности, направленных на минимизацию полученных рисков. Производится сравнение рекомендуемых и существующих контрмер. CRAMM имеет обширную базу, содержащую описание около 1000 примеров реализации подсистем защиты для различных компьютерных систем. Данные примеры можно использовать в качестве шаблонов. База данных контрмер CRAMM охватывает все аспекты информационной безопасности и множество стандартов, включая BS7799 и ISO 15408.

Решение о внедрении в систему новых мер безопасности и модификации старых принимает руководство организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для бизнеса.

2.1.4.ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

Данный стандарт идентичен международному стандарту ISO/IEC 27005:2008 “Information technology – Security techniques – Information security risk management”. В данном стандарте представлено общее руководство по управлению риска информационной безопасности. В частности, поддерживаются требования к системе менеджмента информационной безопасности (СМИБ) в соответствии ИСО/МЭК 27001. Однако, в отличие от других стан-

дартов, в нем не рассматривается конкретной методологии. Выбор подхода к управлению риску ИБ осуществляется каждой организацией самостоятельно.

На рисунке 2.5 представлен процесс менеджмента риска ИБ в соответствии с рассматриваемым стандартом.

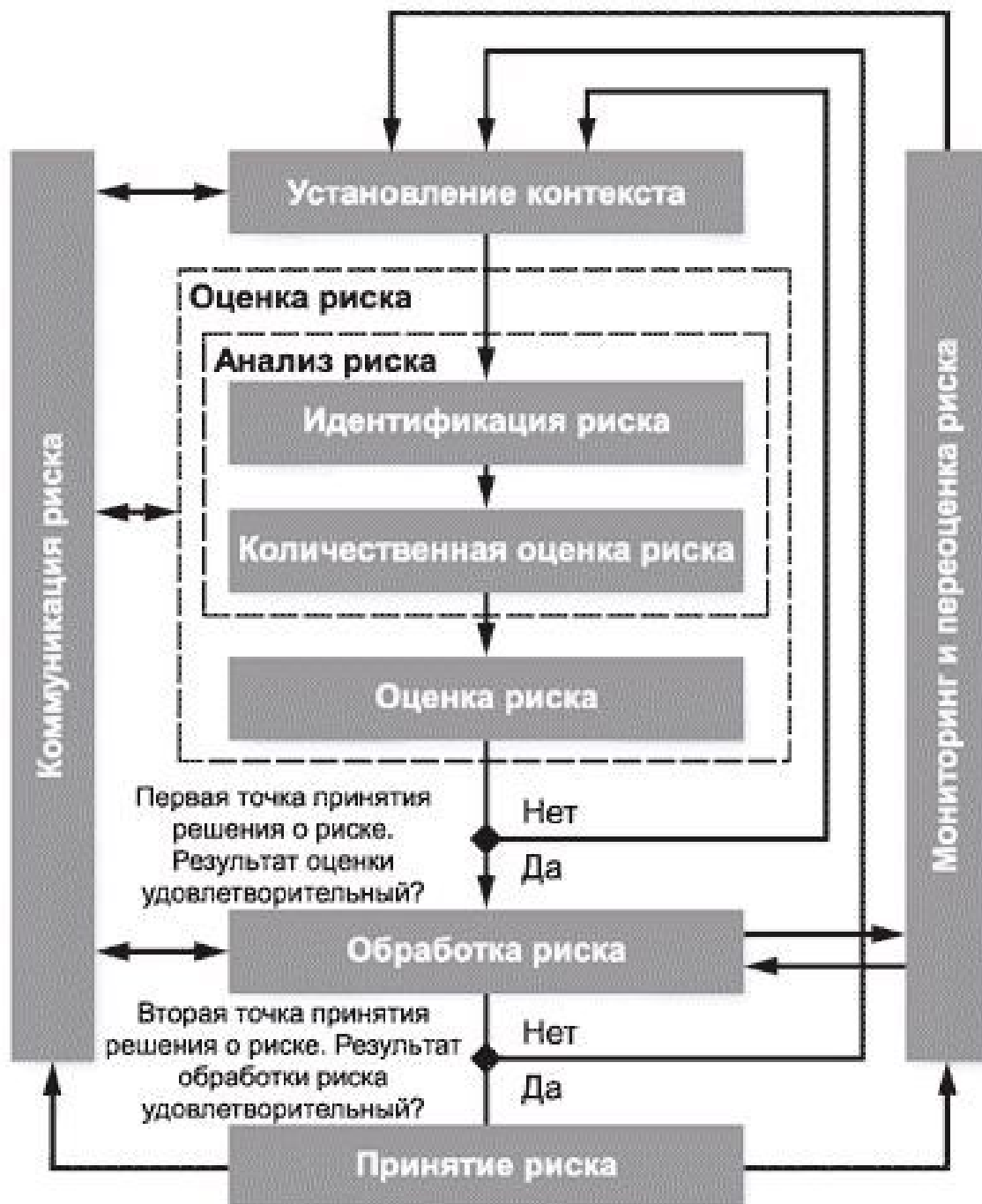


Рисунок 2.5. Процесс менеджмента риска ИБ

Сначала устанавливается контекст, а затем проводится оценка риска. Если при этом удастся получить достаточную информацию для эффективного определения действий, требуемых для снижения риска до приемлемого уровня,

то задача выполнена, после чего следует обработка риска. Если информация является недостаточной, то проводится очередная итерация оценки риска в условиях пересмотренного контекста (например, критериев оценки рисков, критериев принятия рисков или критериев влияния), возможно в ограниченной части полной предметной области (см. рисунок 2.5, первая точка принятия решения).

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

Оценка риска часто проводится за две (или более) итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, служащих основанием для дальнейшей оценки. Следующая итерация может включать дальнейшее углубленное рассмотрение потенциально высоких рисков. В тех случаях, когда полученная информация недостаточна для оценки риска, проводится более детальный анализ, возможно, по отдельным частям сферы действия, и, возможно, с использованием иного метода.

Методология установления значения риска может быть качественной, количественной или комбинированной, в зависимости от обстоятельств. На практике установление качественного значения часто используется вначале для получения общих сведений об уровне риска и выявления основных значений рисков. Позднее может возникнуть необходимость в осуществлении более специфичного установления количественного анализа основных значений рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и затратным.

Для установления ценности активов организация должна в первую очередь определить все свои активы на соответствующем уровне детализации. В стандарте выделяется два вида активов:

- основные активы, включающие бизнес-процессы, бизнес-деятельность и информацию;
- вспомогательные (поддерживающие) активы, от которых зависят основные составные части области применения всех типов, включающие аппаратные средства, программное обеспечение, сеть, персонал, место функционирования организации, структуру организации.

Данный стандарт следует рассматривать только как руководство, на основе которого должны применяться конкретные подходы к оценке и управлению рисками ИБ.

2.2. Количественная оценка и управление рисками информационной безопасности

2.2.1. RiskWatch

Метод RiskWatch является одним из методов количественного анализа и управления рисками. Данный метод включает в себя такие решения, как:

- RiskWatch for Information Systems & ISO 17799 – для информационных рисков.
- RiskWatch for Financial Institution – для банков.
- RiskWatch for Credit Unions – для кредитных организаций.
- RiskWatch for PCI – для банковских информационных систем, использующих пластиковые карты.
- RiskWatch for Federal Systems – для федеральных информационных систем США.
- RiskWatch for HIPAA Compliance – для оценки соответствия требованиям стандарта HIPAA, используемого в здравоохранении.

- RiskWatch for Healthcare Security – для здравоохранения.
- RiskWatch for Electrical Utilities (NERC) – для организаций энергетической сферы.
- RiskWatch for Nuclear Power (NEI-NRC) – для атомной энергетики.
- RiskWatch for Physical & Homeland Security – для физической и домашней безопасности.

В методе RiskWatch производится количественная оценка общих годовых потерь (Annual Loss Expectancy, ALE) и коэффициента возврата от инвестиций (Return on Investment, ROI) при внедрении средств защиты информации.

Метод RiskWatch включает в себя четыре этапа.

Первый этап - определение предмета исследования. Здесь исследуются такие параметры, как тип организации, общий состав исследуемой системы, базовые требования в области информационной безопасности. В методе присутствуют шаблоны, соответствующие типу организации (например, "коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты информации. Из них следует выбрать те параметры, которые соответствуют исследуемой организации.

Второй этап - ввод данных, описывающих конкретные характеристики системы. На данном этапе подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов формируются путем сопоставления категории потерь и категории ресурсов. Определяется частота возникновения каждой из выделенных угроз (рисунок 2.6). RiskWatch включает в себя базы с оценками частот LAFE и SAFE. LAFE (Local Annual Frequency Estimate) - показывает, сколько раз в среднем в год исследуемая угроза реализуется в исследуемом месте (например, в городе). SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в среднем в год исследуемая угроза реализуется в исследуемой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации

угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Определение множества уязвимостей и степеней их опасности осуществляется на основе различных стандартов (ISO 17799, NIST SP 800-26, PCI DSS, HIPAA и т.д.) (рисунок 2.7), а также опросного листа с обширной базой вопросов (рисунок 2.8).

Phase II - Threat Frequencies

Listed below are the Threats and their corresponding Standard Annual Frequency Estimate (SAFE). The Local Annual Frequency Estimate (LAFE) reflects this case's estimate and is the value that will be used in the calculations. Initially, the SAFE and LAFE are the same value.

Selected Threats	LAFE	SAFE
Chemical/Biological Contaminat	0.05	0.05
Cold/Frost/Snow	2.00	2.00
Communications Loss	12.00	12.00
Computer Intrusion	2.00	2.00
Computer Misuse	5.00	5.00
Data Destruction	8.00	8.00
Data Disclosure	3.00	3.00
Data Integrity Loss	3.00	3.00
Denial of Service Attacks	3.00	3.00
Earthquakes	0.05	0.05
Eavesdropping/Interception	1.00	1.00
Errors, Configuration	3.00	3.00
Errors, Data Entry	20.00	20.00

Selected LAFE: 3.00

Threat Description: DENIAL OF SERVICE (DOS) ATTACKS - refers to distributed DOS attacks and is an effective and easily

Рисунок 2.6. Оценка частоты возникновения угроз

[Help](#) [Exit](#)

Question 26 of 28

Question Number[1450] Have plans been developed and implemented to maintain or restore operations?

Your Rating:

☐ 0
Never

☐ 1
Rarely

☐ 2
Sometimes

☐ 3
Mostly

☐ 4
Always

☐ N/A

☐ I Don't Know

Your Comment:

[Next Question](#)

Control Standard:

Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes (A.14.1.3).

Рисунок 2.7. Пример вопроса RiskWatch

Question Category: ISO 17799 Access Control (4.7)

Question Title: AC - Node Authentication

Question: #671

Are connections to remote computer systems authenticated?

Control Standard:

Connections to remote computer systems shall be authenticated (4.7.4.4).

Vulnerability:

Connections are not authenticated.

[Add](#) [Delete](#)

Vulnerability Area:

Access Control

Functional Areas:

- ☐ Human Resources/Personnel Se
- ☐ Information Owners
- ☒ Information Security Officer (ISO
- ☐ Information Technology (IT) Man
- ☐ Internal Audit
- ☒ Network Management

Question Weight - 1

Jump To Question ID:

1000
1000
 1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019

[OK](#)
[Cancel](#)
[Help](#)

Рисунок 2.8. Составление/корректировка опросного листа RiskWatch

Третий этап – количественная оценка рисков. На данном этапе определяются количественные значения рисков и выбираются меры обеспечения без-

опасности. Для каждой из контрмер определяется стоимость внедрения, стоимость поддержки, время жизни и текущий процент реализации (рисунок 2.9).

Phase II - Safeguard Details

Selected Safeguards

- Application Controls
- Audit Trails
- Authentication & Access Controls**
- Change Control
- Contingency Plan
- Continuity Planning
- Detection Systems
- Documentation
- Electrical Power
- Emergency Response
- Encryption
- File/Program Control
- Fire Suppression
- Incident Response
- Insurance

Safeguard Definition

Authentication & Access Controls refers to the verification of identity by a system based on the presentation of unique credentials to that system, and access rights.

Implementation Cost: \$35,000

Annual Maintenance Cost: \$5,000

Percentage Implemented: 100 %

Lifetime (in years): 2

Threat LAFE Reduction

Vulnerability Reduction

OK Cancel Help

Рисунок 2.9. Определение количественных характеристик контрмер

В методе устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования (риск описывается совокупностью этих четырех параметров) (рисунок 2.10). Программное обеспечение RiskWatch может автоматически анализировать более 3 млн. подобных связей.

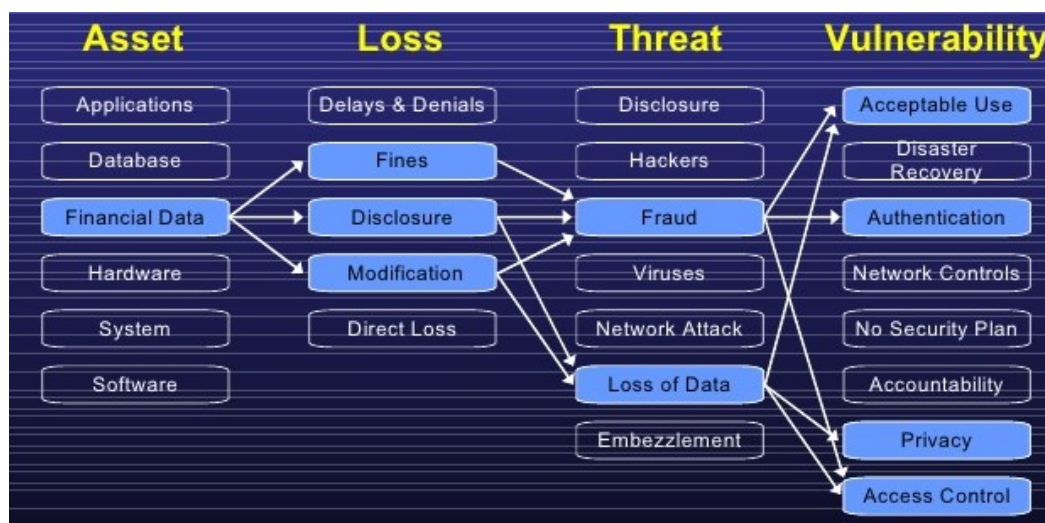


Рисунок 2.10. Установка связей

Риск информационной безопасности оценивается как стоимость актива, умноженная на вероятность реализации угрозы.

Эффект от внедрения средств защиты информации количественно определяется с помощью коэффициента возврата инвестиций ROI, который показывает отдачу от сделанных инвестиций за определенный период времени. Данный коэффициент рассчитывается по следующей формуле:

$$ROI = \sum_i NPV(Benefits_i) - \sum_i NPV(Cost_i)$$

где $Benefits_i$ - оценка полезности внедрения i -ой меры защиты (например, уровень снижения риска), $Cost_i$ - затраты на внедрение и поддержание данной меры, NPV - приведенная стоимость затрат, которая в частности учитывает инфляцию.

На заключительном этапе метода строятся различные виды отчетов по результатам оценки рисков.

2.2.2. Digital Security

Компанией Digital Security предложено две основных модели оценки рисков: модель информационных потоков и модель анализа угроз и уязвимостей. Данные модели реализованы в продукте DS Office 2006.

1.3.2.1. Модель информационных потоков

В данной модели оценка рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Рассматриваются средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, права доступа групп пользователей, организационные меры.

В первую очередь владелец информационной системы описывает архитектуру информационной системы, включая в это описание следующую информацию:

- все ресурсы, на которых хранится ценная информация;
- все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз (нарушение конфиденциальности, целостности, доступности);
- бизнес-процессы, в которых обрабатывается информация;
- группы пользователей, имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Исходя из данной информации, в методе строится полная модель КИС компании.

Риск оценивается отдельно по каждой связке «группа пользователей – информация», т.е. модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики.

Риск реализации угрозы ИБ для каждого вида информации рассчитывается по трем основным угрозам: нарушения конфиденциальности, целостности и доступности. Владелец информации задает ущерб отдельно по трем угрозам.

Расчет рисков по угрозам нарушения конфиденциальности и целостности.

1. Определяется вид доступа группы пользователей к информации. От этого будет зависеть количество средств защиты, т.к. для локального и удаленного доступа применяются разные средства.

2. Определяются права доступа группы пользователей к информации. Это важно для целостности, т.к. при доступе «только чтение» целостность и доступность информации нарушить нельзя. Установленные права доступа сказываются непосредственно на выбор средств защиты информации.

3. Вероятность реализации угрозы зависит от класса группы пользователей. Например, анонимные Интернет-пользователи представляют наибольшую угрозу для ценной информации компании, значит, если данная группа имеет доступ к информации, риск реализации угрозы увеличивается. Также, в зависимости от класса группы пользователей меняется выбор их средств защиты.

4. Особым видом средства защиты является антивирусное программное обеспечение. Отсутствие антивирусного программного обеспечения на ресурсе необходимо принимать во внимание отдельно. Если на ресурсе не установлен антивирус, то вероятность реализации угроз конфиденциальности, целостности и доступности резко возрастает.

5. На основании полученной информации определяются средства защиты информации. Просуммировав веса средств защиты, получим суммарный коэффициент. Для угрозы нарушения целостности учитываются специфические средства защиты – средства резервирования и контроля целостности информации. Если к ресурсу осуществляется локальный и удаленный доступ, то на данном этапе будут определены три коэффициента: коэффициент локальной защищенности информации на ресурсе, коэффициент удаленной защищенности информации на ресурсе и коэффициент локальной защищенности рабочего места группы пользователей. Из полученных коэффициентов выбирается минимальный. Чем меньше коэффициент защищенности, тем слабее защита, т.е. важно учесть наименее защищенное (наиболее уязвимое) место в информационной системе.

6. Вводится понятие наследования коэффициентов защищенности и базовых вероятностей. Например, на ресурсе, входящем в сетевую группу, содержится информация, к которой осуществляется доступ групп пользователей (анонимных, авторизованных или мобильных) из Интернет. Для этой связи «информация – группа Интернет-пользователей» рассчитывается только коэффициент удаленной защищенности информации на ресурсе, т.к. оценить защищенность групп пользователей мы не можем. Далее этот коэффициент защищенности сравнивается с коэффициентами защищенности, полученными для нашей связи «информация – группа пользователей». Таким образом учитывается влияние других ресурсов системы на наш ресурс и информацию. В реальной информационной системе все ресурсы, взаимосвязанные между собой, оказывают друг на друга влияние. Т.е. злоумышленник, проникнув на один ресурс информационной системы (например, получив доступ к информации ресурса), может без труда получить доступ к ресурсам, физически связанным с взломанным. Явным преимуществом данной модели является то, что она учитывает взаимосвязи между ресурсами информационной системы.

7. Отдельно учитывается наличие криптографической защиты данных при удаленном доступе. Если пользователи могут получить удаленный доступ к ценным данным не используя систему шифрования, это может сильно повлиять на целостность и конфиденциальность данных.

8. На последнем этапе перед получением итогового коэффициента защищенности связи «информация – группа пользователей» анализируется количество человек в группе пользователей и наличие у группы пользователей выхода в Интернет. Все эти параметры сказываются на защищенности информации.

9. Вычисляется конечный, итоговый коэффициент защищенности для нашей связки «информация – группа пользователей».

10. Далее полученный итоговый коэффициент умножается на базовую вероятность реализации угрозы ИБ. Базовая вероятность определяется на осно-

ве метода экспертных оценок. Группа экспертов, исходя из классов групп пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец информационной системы, при желании, может задать этот параметр самостоятельно. Умножив базовую вероятность на итоговый коэффициент защищенности, получим итоговую вероятность реализации угрозы. Для каждой из трех угроз информационной безопасности отдельно рассчитывается вероятность реализации.

11. Значение полученной итоговой вероятности накладывается на ущерб от реализации угрозы и получается риск угрозы информационной безопасности для связи «вид информации – группа пользователей».

12. Чтобы получить риск P_{inf} для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), вначале суммируются итоговые вероятности реализации угрозы по следующей формуле:

$$P_{inf} = 1 - \prod_{i=1}^n (1 - P_{ug,n}),$$

где $P_{ug,n}$ - риск для связи «информация – группа пользователя»

Затем полученная итоговая вероятность для информации умножается на ущерб от реализации угрозы. При этом получается риск от реализации угрозы для данной информации.

13. Чтобы получить риск для ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

Расчет рисков по угрозе отказа в обслуживании

Если для целостности и конфиденциальности вероятность реализации угрозы рассчитывается в процентах, то для доступности аналогом вероятности является время простоя ресурса, содержащего информацию. Однако риск по угрозе отказ в обслуживании все равно считается для связки «информация -

группа пользователей», т.к. существует ряд параметров, которые влияют не на ресурс в целом, а на отдельный вид информации.

1. На первом этапе определяется базовое время простоя для информации.

2. Далее рассчитывается коэффициент защищенности связки «информация - группы пользователя». Для угрозы отказ в обслуживании коэффициент защищенности определяется, учитывая права доступа группы пользователей к информации и средства резервирования.

3. Так же, как для угроз нарушения конфиденциальности и целостности, наличие антивирусного программного обеспечения является особым средством защиты и учитывается отдельно.

4. Накладывая коэффициент защищенности на время простоя информации, получается время простоя информации, учитывая средства защиты информации. Оно рассчитывается в часах простоя в год.

5. Специфичный параметр для связки «информация – группа пользователей» - время простоя сетевого оборудования. Доступ к ресурсу может осуществляться разными группами пользователей, используя разное сетевое оборудование. Для сетевого оборудования время простоя задает владелец информационной системы. Время простоя сетевого оборудования суммируется со временем простоя информации, полученным в результате работы алгоритма, таким образом, формируется итоговое время простоя для связи «информация – группа пользователей».

6. Значение времени простоя для информации (T_{inf}), учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{inf} = \left(1 - \prod_{i=1}^n \left(1 - \frac{T_{ug,n}}{T_{max}} \right) \right) \times T_{max}$$

где T_{max} – максимальное критичное время простоя;

$T_{ug,n}$ – время простоя для связи «информация – группа пользователя».

7. Ущерб для угрозы отказ в обслуживании задается в час. Перемножив итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы отказ в обслуживании для связи «информация - группа пользователей».

Эффективность контрмеры рассчитывается по следующей формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

где R_{old} - уровень риска без учета контрмеры, R_{new} - уровень риска с учетом контрмеры.

1.3.2.2. Модель анализа угроз и уязвимостей

Для оценки рисков информационной системы защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

Входными данными для работы данного метода являются:

- Ресурсы;
- Критичность ресурса;
- Отделы, к которым относятся ресурсы;
- Угрозы, действующие на ресурсы;
- Уязвимости, через которые реализуются угрозы;
- Вероятность реализации угрозы через данную уязвимость;
- Критичность реализации угрозы через данную уязвимость.

С точки зрения базовых угроз информационной безопасности существует два режима работы метода:

- Одна базовая угроза (суммарная);

- Три базовые угрозы.

При работе с алгоритмом используется шкала от 0 до 100%. Максимальное число уровней – 100, т.е. шкалу можно разбить на 100 уровней. При разбиении шкалы на меньшее число уровней, каждый уровень занимает определенный интервал на шкале. Причем, возможно два варианта разбиения:

- равномерное (рисунок 2.11);
- логарифмическое (рисунок 2.12);

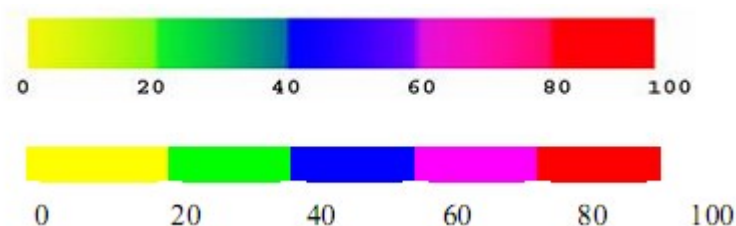


Рисунок 2.11. Равномерное разбиение шкалы

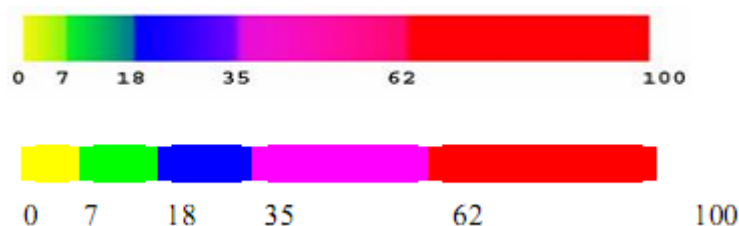


Рисунок 2.12. Логарифмическое разбиение шкалы

1. На первом этапе рассчитывается уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$Th_{c,I,a} = \frac{ER_{c,I,a}}{100} \times \frac{P(V)_{c,I,a}}{100},$$

где $ER_{c,I,a}$ - критичность реализации угрозы конфиденциальности, целостности или доступности (указывается в %); $P(V)_{c,I,a}$ - вероятность реализации угрозы через данную уязвимость (указывается в %).

Вычисляется одно или три значения в зависимости от количества базовых угроз. Получаем значение уровня угрозы по уязвимости в интервале от 0 до 1.

2. Чтобы рассчитать уровень угрозы по всем уязвимостям CTh , через которые возможна реализация данной угрозы на ресурсе, суммируются полученные уровни угроз через конкретные уязвимости по следующей формуле:

2.1. Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^n (1 - Th)$$

2.2. Для режима с тремя базовыми угрозами:

$$CTh_c = 1 - \prod_{i=1}^n (1 - Th_c)$$

$$CTh_I = 1 - \prod_{i=1}^n (1 - Th_I)$$

$$CTh_a = 1 - \prod_{i=1}^n (1 - Th_a)$$

Значения уровня угрозы по всем уязвимостям получаются в интервале от 0 до 1.

3. Аналогично рассчитывается общий уровень угроз по ресурсу $CThR$ (учитывая все угрозы, действующие на ресурс):

3.1. Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^n (1 - CTh)$$

3.2. Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{i=1}^n (1 - CTh_c)$$

$$CThR_I = 1 - \prod_{i=1}^n (1 - CTh_I)$$

$$CThR_a = 1 - \prod_{i=1}^n (1 - CTh_a)$$

Значение общего уровня угрозы получается в интервале от 0 до 1.

4. Риск по ресурсу R рассчитывается следующим образом:

4.1. Для режима с одной базовой угрозой:

$$R = CThR \times D$$

где D – критичность ресурса. Задается в деньгах или уровнях.

Для угрозы отказа в обслуживании критичность ресурса в год вычисляется по следующей формуле:

$$D_{a/\text{год}} = D_{a/\text{мес}} \times T$$

Для остальных угроз критичность ресурса задается в год.

4.2. Для режима с тремя базовыми угрозами:

$$R_c = CThR_c \times D_c$$

$$R_I = CThR_I \times D_I$$

$$R_a = CThR_a \times D_a$$

$$R = \left(1 - \prod_{i=c,I,a} \left(1 - \frac{R_i}{100} \right) \right) \times 100$$

$D_{c,I,a}$ - критичность ресурса по трем угрозам. Задается в деньгах или уровнях. R - суммарный риск по трем угрозам. Таким образом, получим значение риска по ресурсу в уровнях (заданных пользователем) или деньгах.

5. Риск по информационной системе CR рассчитывается по формуле:

5.1. Для режима с одной базовой угрозой:

5.1.1. Для режима работы в деньгах:

$$CR = \sum_{i=1}^n R_i$$

5.1.2. Для режима работы в уровнях:

$$CR = \left(1 - \prod_{i=1}^n \left(1 - \frac{R_i}{100} \right) \right) \times 100$$

5.2. Для режима работы с тремя угрозами:

5.2.1. Для режима работы в деньгах:

$$CR_{c,I,a} = \sum_{i=1}^n R_i$$

$$CR = \sum_{i=c,I,a} CR_i$$

где CR - риск по системе суммарно по трем видам угроз.

5.2.2. Для режима работы в уровнях:

$$CR_{c,I,a} = \left(1 - \prod_{i=1}^n \left(1 - \frac{R_i}{100} \right) \right) \times 100$$

$$CR = \left(1 - \prod_{i=c,I,a} \left(1 - \frac{R_i}{100} \right) \right) \times 100$$

2.2.3. ISRAM (Information Security Risk Analysis Method)

Метод ISRAM был разработан Институтом Электроники и Криптографии совместно с Турецким Технологическим институтом Гебзе. Данный метод использует опросные листы для оценки факторов риска и вычисляет уровень риска в виде произведения вероятности реализации угрозы и ее последствий. Данный уровень риска находится в диапазоне от 1 до 25 и вычисляется по следующей формуле.

$$Risk = \left(\frac{\sum_m T_1 \left(\sum_i w_i p_i \right)}{m} \right) \cdot \left(\frac{\sum_n T_{21} \left(\sum_j w_j p_j \right)}{n} \right)$$

В (1.4) значение i показывает номер вопроса, используемого для оценки вероятности реализации угрозы, j – номер вопроса, используемого для оценки последствий от реализации угрозы, m и n – количество экспертов, участвующих в опросе, w_i и w_j – веса вопросов, p_i и p_j – количественные значения выбранных ответов на вопросы с номерами i и j , T_1 и T_2 – порядковые шкалы для оценки вероятности реализации угроз и последствий.

2.2.4. FAIR (Factor analysis of information risk)

FAIR предлагает таксономию частных показателей, которые влияют на факторы риска – ущерб от реализации угроз и вероятность их наступления. Подход FAIR не является самостоятельной методикой оценки и управления рисками ИБ, однако может быть использован совместно с многими из таких методик. Подход FAIR рассматривает вероятностную природу риска.

В FAIR определяется шесть видов возможного ущерба ресурсам:

- Productivity - потеря производительности.
- Response – расходы на восстановление от неблагоприятного события.
- Replacement – расходы на замену/ремонт пострадавшего актива.
- F/J - штрафы и судебные издержки.
- CA – упущенные возможности при конкурентной борьбе.
- Reputation – падение корпоративной репутации.

FAIR определяет ценность активов через следующие показатели:

- Критичность – влияние на производительность организации.
- Цена – чистая стоимость актива (например, его замены).
- Чувствительность (Sensitivity) – цена утечки информации, которая включает в себя:
 - Затруднение – принятие неадекватных решений руководством организации.

- Стоимость, связанная с потерей конкурентного преимущества.
- Стоимость, связанная с возможным нарушением законодательства.
- Другие затраты.

2.2.5. iRisk

iRisk предлагает достаточно простой метод количественной оценки рисков ИБ в организациях. Данный метод может быть легко использован внутри различных моделей управления рисками.

В общем виде, оценка риска ИБ в данном методе осуществляется с помощью формулы (2.1)

$$iRisk = (Vulnerability \times Threat) - Control, \quad (2.1)$$

где *Vulnerability* - оценка уязвимости, *Threat* - оценка угрозы, *Control* - оценка мер безопасности.

Оценка уязвимости осуществляется на базе известного метода CVSS V3 «A Complete Guide to the Common Vulnerability Scoring System» используя только базовые метрики. Структура оценки уязвимости представлена на рисунке 2.13. Для выполнения оценки может быть использован он-лайн калькулятор CVSS.

При оценке угрозы выполняют оценку возможности реализации угрозы (likelihood) и степени ее влияния (impact). Структура оценки угрозы представлена на рисунке 2.14.

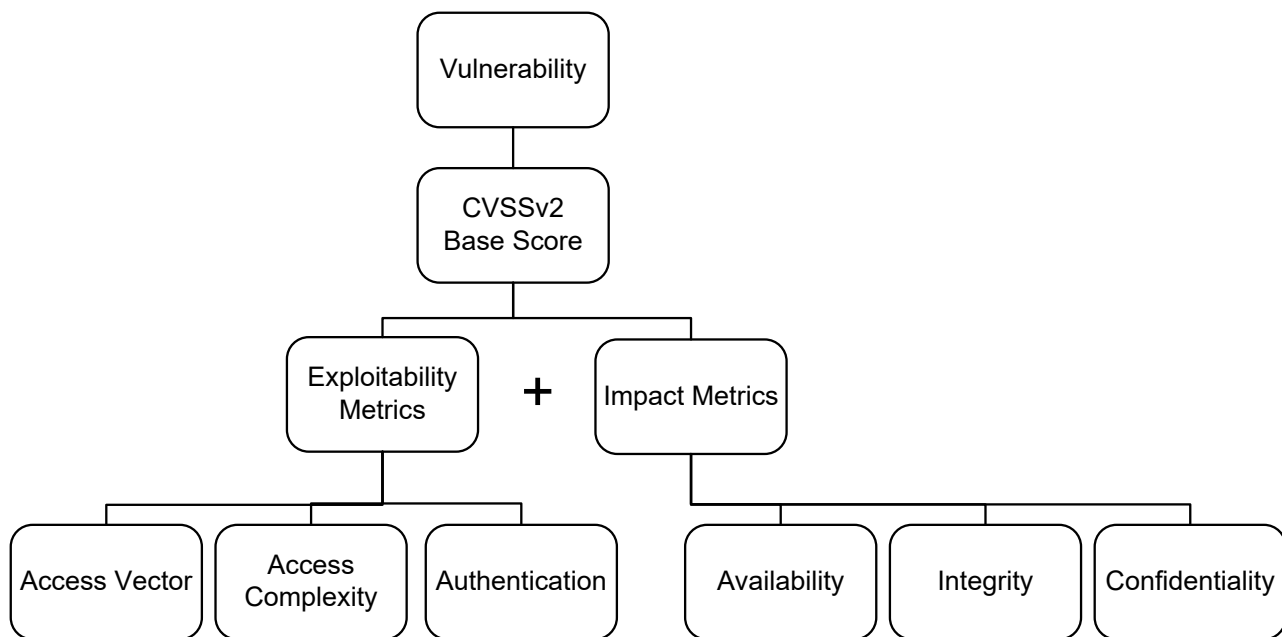


Рисунок 2.13. Структура оценки уязвимости

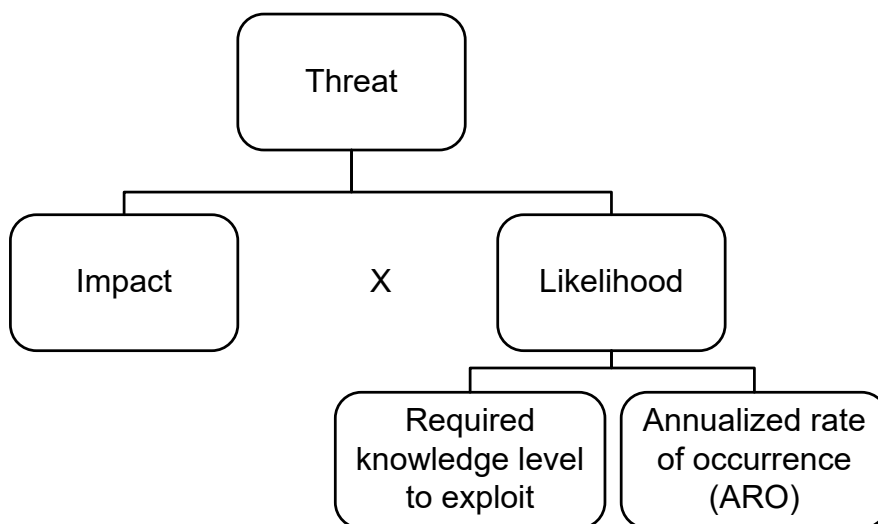


Рисунок 2.14. Структура оценки угрозы

Степень влияния угрозы оценивается следующим образом (оценки суммируются и могут быть изменены):

- Срываються денежные поступления (impact=25).
- Срываються стратегические инициативы (impact=15).
- Остановка бизнеса (impact=25).
- Нарушение требований регуляторов и стандартов (impact=25)

– Ущерб репутации (impact=10)

Для оценки возможности реализации угрозы используют оценки двух показателей: ARO (ожидаемое количество реализаций рассматриваемой угрозы в течении года), а также уровень знаний и необходимый уровень доступа злоумышленника. Способ оценки возможности реализации угрозы представлен в таблице 2.10.

Таблица 2.10. Способ оценки возможности реализации угрозы

Уровень знаний и необходимый уровень доступа злоумышленника в КИС	ARO			
	Очень частый (1.0-0.81)	Частый (0.8-0.51)	Нечастый (0.5-0.21)	Редкий (0-0.2)
Аутсайдер, Отсутствуют технические навыки (1.0)	1.0-0.81	0.8-0.51	0.5-0.21	0-0.2
Аутсайдер, Некоторые технические навыки (0.9)	0.9-0.729	0.72-0.459	0.45-0.189	0-0.18
Инсайдер, Повседневный пользователь (0.9)	0.9-0.729	0.72-0.459	0.45-0.189	0-0.18
Аутсайдер, Продвинутый пользователь (0.8)	0.8-0.648	0.64-0.408	0.4-0.168	0-0.16
Аутсайдер, Навыки пентестера (0.7)	0.7-0.567	0.56-0.357	0.35-0.147	0.014
Аутсайдер, Профессиональный пентестер систем безопасности (0.6)	0.6-0.486	0.48-0.306	0.3-0.126	0-0.12
Организованная группа с государственной поддержкой (0.5)	0.5-0.405	0.4-0.255	0.25-0.105	0-0.1
Инсайдер, Привилегированный доступ (0.5)	0.5-0.405	0.4-0.255	0.25-0.105	0-0.1

Инсайдер, Администратор (0.2)	0.2-0.162	0.16-0.102	0.1-0.042	0-0.04
Инсайдер, Профессиональный пентестер систем безопасности (0.1)	0.1-0.081	0.08-0.051	0.1-0.042	0-0.02

Оценка мер безопасности осуществляется с помощью определения типов и оценки эффективности используемых или планируемых мер безопасности. Структура оценки мер безопасности представлена на рисунке 2.15.

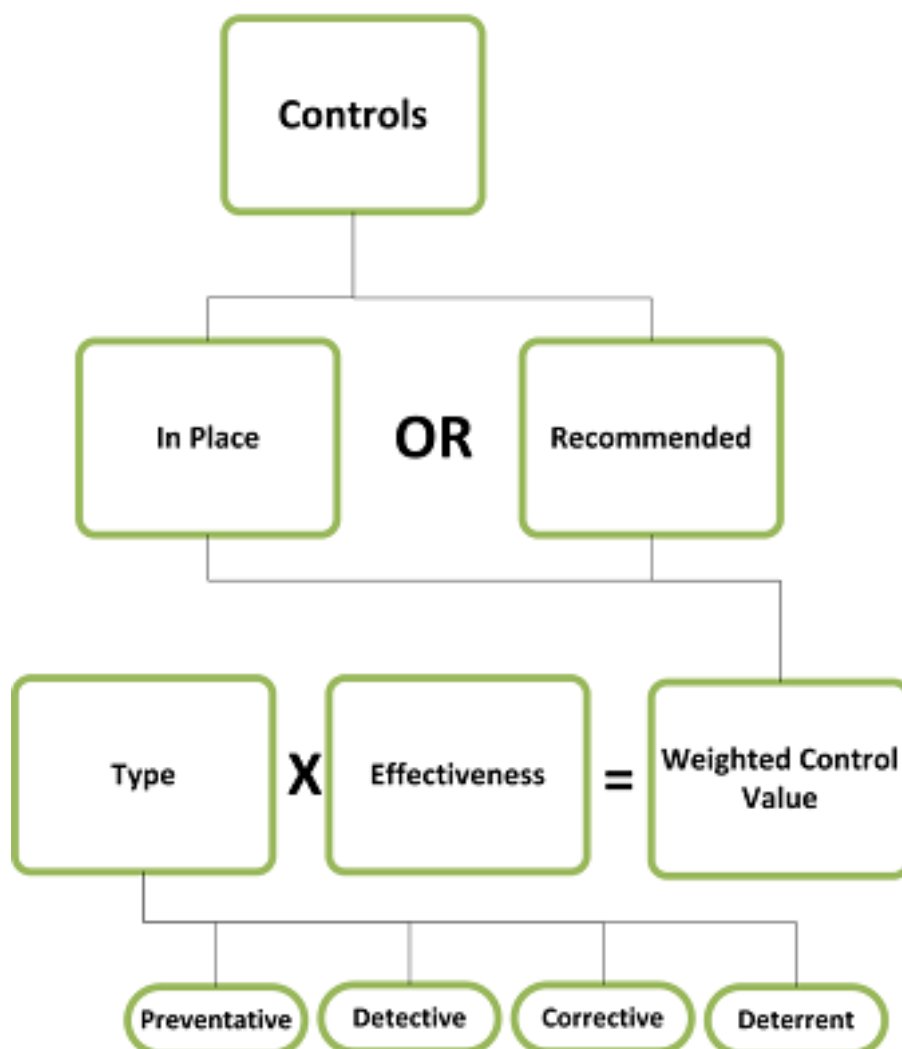


Рисунок 2.15. Структура оценки мер безопасности

В первую очередь определяется тип защитной меры:

- Превентивная (*type=5*)
- Детектирующая (*type=4*)
- Корректирующая (*type=3*)
- Сдерживающая (*type=2*)

Далее определяется эффективность меры безопасности:

- Очень эффективная (*effectiveness=5*)
- Эффективная (*effectiveness=4*)
- Адекватная (*effectiveness=3*)
- Не эффективная (*effectiveness=2*)
- Очень не эффективная (*effectiveness=1*)

На основе типа и эффективности меры безопасности определяется общая оценка защитной меры от 0 до 1000, используя СММІ:

- Оптимизированная (801-1000)
- Управляемая (601-800)
- Документированная (401-600)
- Ранняя стадия внедрения (1-200)
- Отсутствует (0)

Далее по формуле (2.1) оценивается риск ИБ для исследуемой угрозы, реализуемой через конкретную уязвимость.

2.3. Смешанные методы оценки и управления рисками информационной безопасности

2.3.1. Microsoft Methodology «The Security Risk Management Guide»

В методологии управления рисками Microsoft реализуется как качественный, так и количественный подход к управлению рисками ИБ. Перед внедрением методологии управления рисками осуществляется самооценка уровня зрелости организации с точки зрения управления рисками. Для этого осуществляется

оценка от 0 до 5 уровня реализации каждого из ниже перечисленных признаков организации:

- Политика информационной безопасности и процедуры ясны, понимаемы, и хорошо документируемы
- Все сотрудники, вовлеченные в обеспечение ИБ, четко понимают свои роли и обязанности
- Политики и процедуры, относящиеся к доступу сторонних лиц, хорошо документированы.
- Производится инвентаризация всех защищаемых ИТ-активов. Данная инвентаризация является актуальной.
- Присутствуют адекватные меры контроля для инсайдеров и аутсайдеров.
- Производится регулярное и эффективное обучение пользователей правилам ИБ.
- Физический доступ к сети и другим ИТ-активам ограничивается используя эффективные защитные мероприятия.
- Реализуется постоянный мониторинг и установка обновлений от вендоров.
- Реализуется эффективное реагирование на инциденты. Все инциденты расследуются до тех пор, пока их корневая причина не будет обнаружена.
- Реализуется эффективная защита от вирусов.
- Реализуется эффективное управление учетными записями. При увольнении сотрудников их учетные записи немедленно блокируются.
- Реализуется строгая аутентификация, авторизация, контроль доступа к данным и аудит.
- При разработке программного обеспечения программисты руководствуются стандартами безопасной разработки. Осуществляется тестирование безопасности программного кода.
- Реализуется управление непрерывностью ведения бизнеса.

– Реализуется периодический внешний аудит компании на соответствие требованиям по информационной безопасности.

Если полученная суммарная оценка 51 или выше, то это означает, что организация хорошо подготовлена для внедрения методики Microsoft управления рисками ИБ. Оценка от 34 до 50 означает, что организация должна реализовать много серьезных шагов, для того, чтобы внедрить методику. Оценка ниже 34 означает, что организация пока не готова «воспринимать» методику. Необходимо внедрять методику управления рисками очень осторожно, начав с одного подразделения и последовательно распространяя ее на остальные.

Реализация методики осуществляется в несколько шагов:

1. Сбор данных. На данном этапе решаются следующие задачи:

- идентификация и классификация активов;
- идентификация угроз;
- идентификация уязвимостей.

Выделяются следующие виды активов – физические, сетевые, узлы, приложения, данные. Выделяются следующие категории активов: high business impact (HBI), moderate business impact (MBI), low business impact (LBI).

2. Оценка рисков. На данном этапе решаются следующие задачи:

- оценка степени влияния угрозы на активы;
- оценка возможности реализации угроз;
- детальный анализ рисков.

Оценка степени воздействия угрозы на конкретный актив осуществляется на качественной шкале (высокая, средняя, низкая). Оценка степени влияния угрозы на конкретный актив осуществляется с помощью матрицы, приведенной в таблице 2.11.

Таблица 2.11. Оценка степени влияния угрозы на актив

Класс актива	HBI	Средняя	Высокая	Высокая
	MBI	Низкая	Средняя	Высокая

	LBI	Низкая	Низкая	Средняя
		Низкая	Средняя	Высокая
		Степень воздействия угрозы на актив		

Оценка возможности реализации угрозы осуществляется на качественной шкале: Высокая (один или несколько раз в год), Средняя (один раз в два года или три года), Низкая (вероятность появления в течении 3 лет очень мала).

Далее оценка уровня рисков осуществляется в качественном виде с помощью матрицы, приведенной в таблице 2.12

Таблица 2.12 Матрица оценки уровня рисков

Степень влияния угрозы на актив	Высокая	Средняя	Высокая	Высокая
	Средняя	Низкая	Средняя	Высокая
	Низкая	Низкая	Низкая	Средняя
		Низкая	Средняя	Высокая
		Возможность реализации угрозы		

Далее осуществляется детальная оценка рисков для угроз, показавших высокий уровень риска, противоречивые или пограничные риски. В ходе детальной оценки рисков решаются следующие задачи:

- оценка степени влияния угрозы на актив;
- определение перечня защитных мер;
- определение возможности реализации угроз;
- детальная оценка рисков.

Оценка степени воздействия угрозы на актив при нарушении его конфиденциальности или целостности осуществляется на качественной шкале (таблица 2.13). Оценка степени воздействия угрозы на актив при нарушении его доступности осуществляется согласно таблице 2.14.

Табл. 2.13. Оценка степени воздействия угрозы на актив при нарушении
конфиденциальности или целостности

Сила воздействия на актив	Конфиденциальность или целостность
5	Полное разрушение актива. Величина воздействия на бизнес очень значительная и видна извне
4	Серьезное, но не полное разрушение актива. Величина воздействия на бизнес значительная, может быть видна извне
3	Средние потери. Воздействие на внутренние бизнес-процессы. Выражается в увеличении операционных затрат
2	Низкие потери. Воздействие на внутренние бизнес-процессы. Выражается в небольшом увеличении операционных затрат
1	Минимальное воздействие

Табл. 2.14. Оценка степени воздействия угрозы на актив при нарушении
доступности

Сила воздействия на актив	Доступность	Описание
5	Остановка работы	Полное разрушение актива. Величина воздействия на бизнес очень значительная и видна извне
4	Прерывание работы	Серьезное, но не полное разрушение актива. Величина воздействия на бизнес значительная, может быть видна извне
3	Задержка в выполнении работы	Средние потери. Воздействие на внутренние бизнес-процессы. Выражается в увеличении операционных затрат

2	Небольшая задержка в выполнении работы	Низкие потери. Воздействие на внутренние бизнес-процессы. Выражается в небольшом увеличении операционных затрат
1	Перекрывается обычными не автоматизированными бизнес-операциями	Минимальное воздействие

Для оценки степени влияния угрозы на актив выполняются следующие действия:

- категория актива переводится в численный эквивалент (Impact Class Value – V): HBI – 10, MBI – 5, LBI – 2;
- степень воздействия угрозы на актив переводится в проценты (Exposure Factor – EF): 5 – 100%, 4 – 80%, 3 – 60%, 2 – 40%, 1 – 20%.
- Степень влияния угрозы на актив вычисляется следующим образом:

$$\text{Impact Rating} = V * EF.$$

После определения перечня защитных мер, реализованных в КИС, определяется возможность реализации угроз. При этом определяется два значения:

- возможность реализации уязвимостей, основанная на атрибутах уязвимостей или возможных эксплойтах (таблица 2.15);
- возможность реализации угрозы, основанная на применяемых защитных мерах (таблица 2.16).

Таблица 2.15. Определение возможности реализации уязвимостей на основе их атрибутов

Вероятность реализации уязвимости	Описание
-----------------------------------	----------

5 (HIGH)	Эксплойт может быть использован большим количеством нарушителей (присутствует «детский» скрипт)
	Эксплойт может быть реализован удаленно
	Для запуска эксплойта необходимы привилегии анонимного пользователя
	Эксплойт свободно опубликован
3 (MEDIUM)	Для использования эксплойта необходим средний уровень атакующего, требуется дописывать эксплойт
	Эксплойт не может быть запущен удаленно
	Для запуска эксплойта требуются привилегии пользователя
	Эксплойт свободно не опубликован
1 (LOW)	Эксплойт могут использовать очень ограниченное количество злоумышленников, как правило, требуется знание инсайдерской информации
	Эксплойт не может быть запущен удаленно
	Для запуска эксплойта требуются привилегии уровня администратора
	Эксплойт свободно не опубликован

Таблица 2.16. Определение возможности реализации угрозы на основе оценки эффективности защитных мер

Вопрос	ДА=0, НЕТ=1
Управление учетными записями присутствует и оно эффективно?	
Пользователи осведомляются об угрозах ИБ?	
Все процессы документированы и функционируют эффективно?	
Существующие защитные меры способны эффективно противостоять угрозам?	
Используется ли практика аудита?	

ИТОГО	0-5
--------------	------------

Каждое из значений, полученное из таблиц 2.15 и 2.16 оценивается числом от 0 до 5. Возможность реализации угрозы определяется путем суммирования данных значений. Исходя из способа задания таблиц 2.15 и 2.16, возможность реализации угрозы представляет собой целое число от 1 до 10.

Риск ИБ, полученный по результатам детального анализа, оценивается в виде произведения возможности реализации угроз и степени влияния угрозы на актив (таблица 2.17). В результате, риск ИБ представляет собой целое число от 0 до 100. Риски со значениями от 0 до 19 определяются как низкие, от 20 до 40 – как средние, выше 40 – высокие.

Таблица 2.17. Оценка риска ИБ

Степень влияния угрозы	10	10	20	30	40	50	60	70	80	90	100
	9	9	18	27	36	45	54	63	72	81	90
	8	8	16	24	32	40	48	56	64	72	80
	7	7	14	21	28	35	42	49	56	63	70
	6	6	12	18	24	30	36	42	48	54	60
	5	5	10	15	20	25	30	35	40	45	50
	4	4	8	12	16	20	24	28	32	36	40
	3	3	6	8	12	15	18	21	24	27	30
	2	2	4	6	8	10	12	14	16	18	20
	1	1	2	3	4	5	6	7	8	9	10
	0	0	0	0	0	0	0	0	0	0	0
		1	2	3	4	5	6	7	8	9	10
Возможность реализации угрозы											

Количественная оценка рисков ИБ

Количественная оценка рисков ИБ осуществляется на основании информации, полученной при качественной оценке рисков. При этом реализуется следующая последовательность шагов.

1. Назначается денежный эквивалент $\$M$ для ресурсов категории HBI. Тогда для ресурсов MBI будет назначен денежный эквивалент $\$M/2$, для LBI - $\$M/4$.

2. Для каждого актива полученный денежный эквивалент умножается на Exposure Factor EF (степень воздействия угрозы на актив), выраженный в процентах. В результате этого получается показатель SLE (Single Loss Expectancy Value).

3. Для угрозы экспертным путем определяется показатель ARO (Annual Rate of Occurrence), показывающий количество реализаций данной угрозы в год.

Риск определяется через показатель ALE (Annualized Loss Expectancy).
 $ALE = SLE * ARO$.

2.3.2. Отраслевые и корпоративные руководства и стандарты оценки и управления рисками ИБ

Большинство отраслевых и корпоративных стандартов оценки и управления рисками ИБ также используют экспертные оценки и качественные подходы в силу удобства их применения. Ниже указаны наиболее известные из подобных отраслевых и корпоративных стандартов.

В [4] представлено руководство по оценке рисков для банковских платежных систем, использующих пластиковые карты. Для таких систем применяется стандарт безопасности PCI DSS. В [1] представлен подход к управлению рисками ИБ в АСУТП критичных информационных систем Австралии. В [3] представлено руководство по управлению рисками информационной безопасности в энергетической сфере. В представлен стандарт РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». Рассмотрим ее более подробно.

РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»

Данная методика распространяется на организации банковской сферы (БС) РФ, проводящие оценку рисков нарушения ИБ в рамках построения/совершенствования системы обеспечения информационной безопасности (СОИБ) в соответствии с требованиями стандарта СТО БР ИББС 1.0

Для оценки рисков нарушения ИБ предварительно определяются и документально оформляются:

- полный перечень типов информационных активов, входящих в область оценки;
- полный перечень типов объектов среды, соответствующих каждому из типов информационных активов области оценки;
- модель угроз ИБ, описывающую угрозы ИБ для всех выделенных в организации БС РФ типов объектов среды на всех уровнях иерархии информационной инфраструктуры организации БС РФ.

В качестве примера можно использовать следующий перечень типов информационных активов в организации БС РФ ограниченного доступа:

- информация, содержащая сведения, составляющие банковскую тайну;
- платежная информация (информация, предназначенная для проведения расчетных, кассовых и других банковских операций и учетных операций);
- = информация, содержащая сведения, составляющие коммерческую тайну;
- персональные данные;
- управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации).

Можно выделить следующие объекты среды:

- линии связи и сети передачи данных;

- сетевые программные и аппаратные средства, в том числе сетевые серверы;

- файлы данных, базы данных, хранилища данных;
- носители информации, в том числе бумажные носители;
- прикладные и общесистемные программные средства;
- программнотехнические компоненты автоматизированных систем;
- помещения, здания, сооружения;
- платежные и информационные технологические процессы.

Оценка рисков ИБ базируется на экспертной оценке, выполняемой сотрудниками службы ИБ организации БС РФ с привлечением сотрудников подразделений информатизации.

Для проведения оценки рисков нарушения ИБ выполняются следующие процедуры.

Процедура 1. Определение перечня типов информационных активов, для которых выполняются процедуры оценки рисков нарушения ИБ.

Для каждого из типов информационных активов определяется перечень свойств ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации БС РФ. Основными свойствами ИБ являются: конфиденциальность, целостность, доступность. При необходимости для конкретных типов информационных активов в организации БС РФ могут определяться другие дополнительные свойства ИБ.

Процедура 2. Определение перечня типов объектов среды, соответствующих каждому из типов информационных активов области оценки рисков нарушения ИБ.

Процедура 3. Определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения процедуры 2.

Процедура 4. Определение степени возможности реализации (СВР) угроз ИБ применительно к типам объектов среды, определенных в рамках выполнения процедуры 3.

Основными факторами для оценки СВР угроз ИБ являются:

- данные о расположении источника угрозы относительно соответствующих типов объектов среды;
- информация о мотивации источника угрозы (для источников угроз антропогенного характера);
- предположения о квалификации и (или) ресурсах источника угрозы;
- статистические данные о частоте реализации угрозы ее источником в прошлом;
- информация о способах реализации угроз ИБ;
- информация о сложности обнаружения реализации угрозы рассматриваемым источником;
- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер.

Для оценки СВР угроз ИБ используется следующая качественная шкала степеней:

- нереализуемая;
- минимальная;
- средняя;
- высокая;
- критическая.

При привлечении к оценке отдельных СВР угроз ИБ нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СВР угроз ИБ принимать равной экспертной оценке, определяющей наибольшую СВР угрозы ИБ.

Процедура 5. Определение степени тяжести последствий (СТП) нарушения ИБ для типов информационных активов об ласти оценки рисков нарушения ИБ.

Основными факторами для оценки СТП нарушения ИБ являются:

- степень влияния на непрерывность деятельности организации БС РФ;
- степень влияния на деловую репутацию;
- объем финансовых и материальных потерь;

- объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;

- объем людских ресурсов, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;

- объем временных затрат, необходимых для восстановления свойств ИБ для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;

- степень нарушения законодательных требований и (или) договорных обязательств организации БС РФ;

- степень нарушения требований регулирующих и контролирующих (надзорных) органов в области ИБ, а также требований нормативных актов Банка России;

- объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;

- данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих апостериорных защитных мер.

Для оценки СТП нарушения ИБ вследствие реализации угроз ИБ используется следующая качественная шкала степеней:

- минимальная;

- средняя;

- высокая;

- критическая.

При привлечении к оценке отдельных СТП нарушения ИБ нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СТП нарушения ИБ принимать равной экспертной оценке, определяющей наибольшую СТП нарушения ИБ.

Процедура 6. Оценка рисков нарушения ИБ.

Оценка рисков проводится с помощью матриц рисков для всех свойств ИБ выделенных типов информационных активов и всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз.

Для оценки рисков нарушения ИБ используется следующая качественная шкала:

- допустимый;
- недопустимый.

Оценка рисков в денежной форме

Риски нарушения ИБ могут быть оценены в количественной (денежной) форме. Оценка рисков нарушения ИБ в количественной форме проводится с целью формирования резервов на возможные потери, связанные с инцидентами ИБ и определяется на основании количественных оценок:

- СВР угроз ИБ, выраженной в количественной форме (процентах) ($СВР_{кол}$);
- СТП нарушения ИБ, выраженной в количественной (денежной) форме ($СТП_{кол}$).

Данные оценки формируются экспертно путем перевода качественных оценок в количественную форму согласно таблицам 2.18 и 2.19.

Таблица 2.18. Шкала соответствия СВР и $СВР_{кол}$

Величина СВР	Величина $СВР_{кол}$
Нереализуемая	0%
Минимальная	От 1% до 20%
Средняя	От 21% до 50%
Высокая	От 51% до 100%
Критическая	100%

Таблица 2.18. Шкала соответствия СТП и $СТП_{кол}$

Величина СТП	Величина $СТП_{кол}$
--------------	----------------------

Минимальная	До 0,5% от величины капитала организации
Средняя	От 0,5% до 1,5% от величины капитала организации
Высокая	От 1,5% до 3% от величины капитала организации
Критическая	Более 3% от величины капитала организации

Количественные оценки рисков нарушения ИБ вычисляются путем перемножения оценок $СВР_{кол}$ и $СТП_{кол}$ нарушения ИБ.

Суммарная количественная оценка риска нарушения ИБ организации БС РФ вычисляется как сумма количественных оценок по всем отдельным рискам нарушения ИБ. Размер резерва на возможные потери, связанные с инцидентами ИБ, рекомендуется принимать равным суммарной количественной оценке риска нарушения ИБ.

2.4. Контрольные вопросы

1. Приведите примеры стандартов и руководств, предполагающих оценку рисков на качественных шкалах.
2. Приведите примеры стандартов и руководств, предполагающих оценку рисков в количественном виде.
3. Приведите примеры стандартов и руководств, предполагающих оценку рисков как на качественных шкалах, так и в количественном виде.
4. Перечислите и охарактеризуйте шаги оценки рисков в рамках методологии NIST SP 800-30 «Guide for Conducting Risk Assessments».
5. Что понимается под определением характеристик системы. Какая информация и каким образом должна быть собрана на данном этапе?

6. Приведите примеры качественных шкал для оценки вероятности угрозы и ущерба.
7. Что понимается под анализом стоимость/эффективность?
8. Охарактеризуйте фазы стандарта OCTAVE.
9. Что понимается под деревом угроз в стандарте OCTAVE.
10. Что понимается под установлением контекста в стандарте ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»?
11. Охарактеризуйте модель информационных потоков оценки рисков.
12. Охарактеризуйте модель анализа угроз и уязвимостей оценки рисков.
13. Каким образом осуществляется оценка уязвимостей в руководстве по управлению рисками Microsoft?
14. Каким образом осуществляется оценка уровня зрелости организации в руководстве по управлению рисками Microsoft?

3. СПИСОК ЛИТЕРАТУРЫ

1. Нестеров С.А. Информационная безопасность: Учебник и практикум / С. А. Нестеров. - М: Издательство Юрайт, 2018. - 321 с.
2. Мельников В.П. Защита информации: учебник / В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе – М.:Академия, 2014. – 304 с.
3. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев; под редакцией Борисова В.И. – Москва: Радио-Софт, 2011. – 232 с.
4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия, 2009. – 416 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия, 2009. – 336 с.
6. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А. Введение в информационную безопасность: Учебное пособие для вузов. – М.: Горячая линия- Телеком, 2014. – 288 с.
7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «Форум», ИНФРА-М, 2014. - 416с.
8. Астахов, А. Искусство управления информационными рисками / А. Астахов. – М: ДМК Пресс, 2010. – 312 с.
9. Баранов, А.П. Теоретические основы информационной безопасности (дополнительные главы). Учебное пособие / А.П. Баранов, Д.П. Зегжда, П.Д. Зегжда, А.М. Ивашко, С.С. Корт. – СПб.: СПбГТУ, 1998. – 173 с.

10. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учебное пособие / Ю.И. Коваленко. – М.: Горячая линия–Телеком, 2012. – 140 с.
11. Куканова, Н. Современные методы и средства анализа и управление рисками информационных систем компаний / Н. Куканова // CIT FORUM [Электронный ресурс]. – Режим доступа: <http://citforum.ru/products/dsec/cramm> (дата обращения 18.04.2017).
12. Курило, А.П. Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М. Горячая линия – Телеком, 2013. – 244 с.
13. Милославская, Н.Г. Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 130 с.
14. Саати, Т. Принятие решение решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993. – 278 с.

СОДЕРЖАНИЕ

Введение	5
1. Термины и определения. Анализ основных подходов к оценке и управлению рисками информационной безопасности	6
1.1. Актуальность	6
1.2. Основные термины и определения.....	9
1.3. Классификация существующих методов оценки рисков и основные проблемы	16
1.4. Контрольные вопросы	20
2. Стандарты и руководства оценки и управления рисками информационной безопасности	22
2.1. Качественная оценка и управление рисками информационной безопасности	22
2.1.1. NIST SP 800-30 «Guide for Conducting Risk Assessments»	22
2.1.2. OCTAVE.....	46
2.1.3. CRAMM.....	51
2.1.4. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»	53
2.2. Количественная оценка и управление рисками информационной безопасности	56
2.2.1. RiskWatch	56
2.2.2. Digital Security.....	61
1.3.2.1. Модель информационных потоков.....	61
1.3.2.2. Модель анализа угроз и уязвимостей.....	67
2.2.3. ISRAM (Information Security Risk Analysis Method)	71
2.2.4. FAIR (Factor analysis of information risk).....	72
2.2.5. iRisk.....	73
2.3. Смешанные методы оценки и управления рисками информационной безопасности	77
2.3.1. Microsoft Methodology «The Security Risk Management Guide»....	77
2.3.2. Отраслевые и корпоративные руководства и стандарты оценки и управления рисками ИБ.....	85
2.4. Контрольные вопросы	91
3. Список литературы	93

ДЛЯ ЗАМЕТОК

Игорь Вячеславович Аникин

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Редактор Яруллина Г.Х.

Техническое редактирование Гапсаламов А.

Сдано в набор 25.08.2018. Подписано к печати 28.08.2018.

Формат 60х84 ^{1/16}. Бумага офсетная.

Гарнитура «Таймс». Печать цифровая.

Усл. печ. л. 9,30. Печ. л. 10. Тираж 500 экз. Заказ № 117.

420111, Казань, Дзержинского, 9/1. Тел.: 8-917-264-84-83

Отпечатано в РИЦ «Школа».