**СОДЕРЖАНИЕ**

## Введение

В постановлении Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий" от 21 марта 2012 год, № ПП-1730 [1] особое внимание уделено вопросам "Совершенствования системы регулирования в сфере информационно-коммуникационных технологий с учетом состояния развития информационных ресурсов технологий и систем...".

В настоящее время организация эффективной системы защиты информационной системы становится критически важным стратегическим фактором развития любой компании. По сути, информация является одним из ключевых элементов бизнеса. При этом под информацией понимаются не только статические информационные ресурсы (базы данных, текущие настройки оборудования и другие), но и динамические информационные процессы обработки данных.

Информационная среда организации, вне зависимости от своего состава, должна предусматривать систему защиты. Однако затраты на обеспечение высокого уровня безопасности могут быть не оправданны. Нахождение разумного компромисса и выбор приемлемого уровня защиты при допустимых затратах является важным условием постановки задачи обеспечения ИБ. Для решения этого вопроса необходимо проводить анализ рисков ИБ, позволяющий оценить существующий уровень защищенности ресурсов организации. Значение риска, являющееся произведением вероятности реализации угрозы по отношению к защищаемому ресурсу на ущерб от реализации данной угрозы, служит показателем полноты, комплексности и эффективности системы ИБ организации, а также позволяет выявить ее слабые места.

Существуют различные способы проведения оценки рисков. Они отличаются методами оценивания их составляющих - вероятности и ущерба. Наиболее распространено использование экспертных оценок в совокупности

с балльными шкалами значений, что затрудняет трактовку результатов расчетов. Эффективность анализа рисков снижает также рассмотрение типовых угроз ИБ применительно к конкретной организации с характерными для нее информационными ресурсами. В связи с этим обстоятельством актуальной является задача разработки метода анализа и управления рисками, опирающегося на показатели, пригодные для количественной экспертной оценки. При этом оценки необходимо получать в денежном выражении, что позволило бы использовать строгие формулы для расчетов и адекватно интерпретировать результаты.

Все вышеперечисленные факторы и обусловили актуальность нашего исследования.

ВКР состоит из введения, трех глав, заключения, списка использованной литературы и приложения.

Во введении обосновывается актуальность избранной темы.

В обзорной части рассмотрены классификации и анализ угроз конфиденциальной информации, существующие виды систем анализа информационных рисков, вопросы анализа рисков и управления ими и многофакторный анализ рисков информационной безопасности.

В основной части рассмотрена методология матричного подхода анализа рисков, исследованы алгоритмы построения математической модели управления рисков от внешних угроз и алгоритмизация формирования автоматизированных средств анализа информационных рисков. Описана методика разработки оценивания рисков при обеспечении информационной безопасности.

Третий раздел включает в себя безопасность жизнедеятельности.

В заключении приводятся основные результаты и выводы, полученные автором в ходе выполнения работы.

# 1. ОБЗОРНАЯ ЧАСТЬ. АНАЛИЗ МЕТОДЫ И СПОСОБЫ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ РИСКОВ

## 1.1. Классификация и анализ угроз конфиденциальной информации

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению даже лицензионное программное обеспечение не лишено уязвимостей).

История развития информационных систем показывает, что новые уязвимые места появляются постоянно. С такой же регулярностью, но с небольшим отставанием, появляются и средства защиты.

В этой связи более приемлемым является другой способ – способ упреждающей защиты, заключающийся в разработке механизмов защиты от возможных, предполагаемых и потенциальных угроз [2].

Некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты, необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

– по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;

– по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);

– по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);

– по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние.

Внешние угрозы исходят также от субъектов, не входящих в состав пользователей и обслуживающего персонала системы, разработчиков системы, и не имеющих непосредственного контакта с информационными системами и ресурсами.

Внутренние угрозы исходят от пользователей и обслуживающего персонала системы, разработчиков системы, других субъектов, вовлеченных в информационные процессы и имеющих непосредственный контакт с информационными системами и ресурсами, как допущенных, так и не имеющих доступа к информации.

Источниками внешних угроз являются:

– недобросовестные конкуренты;

– преступные группировки и формирования;

– отдельные лица и организации административно–управленческого аппарата.

Источниками внутренних угроз могут быть:

– администрация предприятия;

– персонал;

– технические средства обеспечения производственной и трудовой деятельности.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

Каждая угроза влечет за собой определенный ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удается далеко не всегда.

С учетом этого угрозы конфиденциальной информации могут быть классифицированы следующим образом:

По величине принесенного ущерба:

– предельный, после которого фирма может стать банкротом;

– значительный, но не приводящий к банкротству;

– незначительный, который фирма за какое–то время может компенсировать и др.;

По вероятности возникновения:

– весьма вероятная угроза;

– вероятная угроза;

– маловероятная угроза;

По причинам появления:

– стихийные бедствия;

– преднамеренные действия;

По характеру нанесенного ущерба:

– материальный;

– моральный;

По характеру воздействия:

– активные;

– пассивные;

По отношению к объекту:

– внутренние;

– внешние.

По сфере воздействия на информационные ресурсы и системы источник угроз информационной безопасности можно разделить на внешние и внутренние с точки зрения их нахождения вне или внутри системы при ее проектировании и функционировании, а также места приложения возможных способов нарушения информационной безопасности [3].

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку – злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

– должно стать известно о средствах использования пробела в защите;

– должны быть выпущены соответствующие заплаты;

– заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий, поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать – вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и

все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

***Анализ потенциальных угроз конфиденциальной информации***

Конфиденциальная информация, в свою очередь, включает множество видов тайны, которые сводятся к шести основным видам:

1. Персональные данные.
2. Тайна следствия и судопроизводства.
3. Служебная тайна.
4. Профессиональная тайна.
5. Коммерческая тайна.
6. Тайна изобретения, полезной модели и промышленного образца.

Под угрозой, или опасностью, утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы дестабилизирующего воздействия любым (открытым и ограниченного доступа) информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам

проявляется повышенный интерес со стороны различного рода злоумышленников.

Под злоумышленником понимается лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленником, психически больных лиц и т. п.).

В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использования в своих целях.

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат – овладение информацией и противоправное ее использование или совершение иных дестабилизирующих действий.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники других организационных структур, работники коммунальных служб, экстремальной помощи, прохожие, посетители фирмы), а также сотрудники данной фирмы, не обладающие правом доступа в определенные помещения, к конкретному документу, информации, базе данных. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Целями и результатами несанкционированного доступа может быть не только овладение ценными сведениями и их использование, но и их видоизменение, модификация, уничтожение, фальсификация, подмена и т. п.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является интерес к ним со стороны конкурентов, определенных лиц,

служб и организаций. При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами, информацией и базами данных. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий злоумышленника, а из-за невнимательности и безответственности персонала. Следовательно, утрата информационных ресурсов ограниченного доступа может наступить при:

– наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

– возникновении риска угрозы, организованной злоумышленником, или при случайно сложившихся обстоятельствах;

– наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией.

Эти условия могут включать:

– отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

– неэффективную систему защиты информации или отсутствие этой системы, что образует высокую степень уязвимости информации;

– непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

– неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

– отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

– отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

– бесконтрольное посещение помещений фирмы посторонними лицами.

Задание возможных угроз информационной безопасности проводится с целью определения полного перечня требований к разрабатываемой системе защиты. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты автоматизированной системы (АС). Кроме выявления возможных угроз, должен быть проведен их анализ на основе классификационных признаков.

## 1.2. Существующие виды систем анализа информационных рисков

Анализ информационных рисков - это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск - это вероятный ущерб, который зависит от защищенности системы. Кроме того, анализ рисков также отличается по используемому подходу; обычно условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (обычно ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий).

О полном анализе информационных рисков мы поговорим подробно. Собственно, именно на нем скрещиваются копья большинства специалистов, так как с анализом рисков базового уровня больших вопросов обычно не возникает. Итак, основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируемой

информационной системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз.

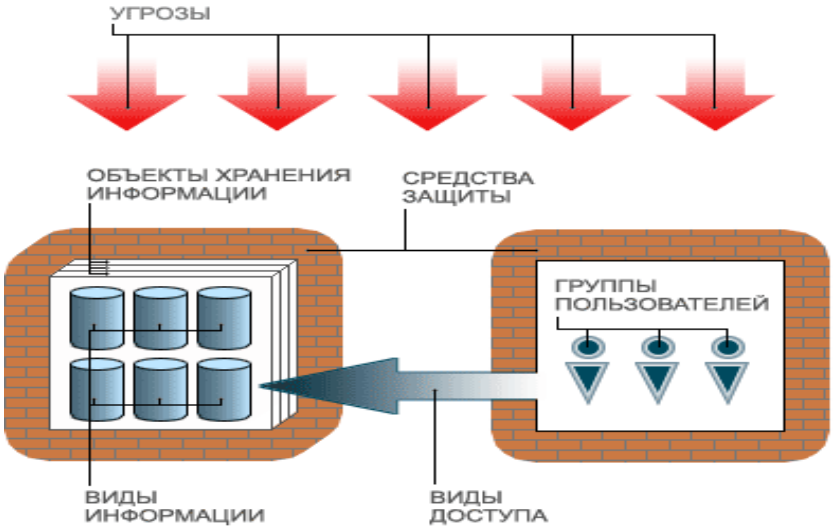


Рис.1.1 Системное моделирование представляющие алгоритмическую сложность для разработчиков

Далее после моделирования необходимо перейти к этапу анализа защищенности построенной полной модели информационной системы. И здесь мы попадаем в целый пласт теоретических и практических проблем, с которыми сталкиваются разработчики алгоритмов анализа риска полного уровня. Весь вышеуказанный комплекс проблем необходимо решать при создании алгоритма современного анализа рисков.

***Алгоритмический анализ технологических особенностей защищенности ИС***

Первая задача, решаемая алгоритмом ГРИФ: на основе построенной полной модели информационной системы оценить ее защищенность. При решении этой задачи активно применялся опыт экспертов. Отметим ряд некоторых особенностей алгоритма ГРИФ, основанных на практических аспектах анализа защищенности ИС. Одним из основных принципов, которые используются в алгоритме ГРИФ, являются: принцип передачи свойств объекта другим объектам данного множества; принцип выбора

уровня защищенности объектов одного множества по уровню наименее защищенного объекта множества; принцип оценки уровня защищенности взаимодействия между субъектом и объектом по наименее защищенному:

- при оценке уровня защищенности взаимодействия между субъектом (пользователем) и объектом (информация на объекте) выбирался наименее защищенный объект взаимодействия;
- при оценке защищенности видов информации (объекта взаимодействия), расположенных на одном из объектов информационной системы, итоговый уровень защищенности каждого вида информации выбирается по наименее защищенному;
- при оценке защищенности объектов взаимодействия, находящихся физически в одном сегменте, итоговый уровень защищенности выбирался по наименее защищенному объекту.

При этом на итоговую оценку защищенности информационной системы существенным образом влияют организационные аспекты: вопросы реализации требований политики безопасности согласно ISO 17799, что также учитывается алгоритмом ГРИФ.

***Оценка ущерба от угроз безопасности***

Одной из классических проблем алгоритмов анализа информационных рисков является выбор методики анализа и определения угроз безопасности информации [4].

Часть существующих алгоритмов (американский Risk Watch) использует следующий подход, когда пользователь указывает полный список угроз безопасности, специфичной для данной системы вместе с оценкой ущерба по каждому виду угроз. Данный подход является алгоритмически тупиковым путем, так как конечный элемент защиты - это информация и ущерб определяется именно по информации. Определение ущерба по конкретным, специфичным для данной системы угрозам приводит к тому, что данный ущерб будет в итоге выше, чем реальный ущерб по видам

информации, что не верно. Дело в том, что на один и тот же вид информации может быть реально направлено сразу несколько угроз, что и приведет к тому, что суммарный ущерб, подсчитанный по угрозам, будет неадекватен реальному, подсчитанному по информации. И с учетом того, что как конечным элементом защиты, так и конечным элементом оценки ущерба является информация, алгоритм анализа рисков должен отталкиваться не от частных угроз и ущербов по ним, а от информации и от ущерба по информации, учитывая при этом и сами угрозы.

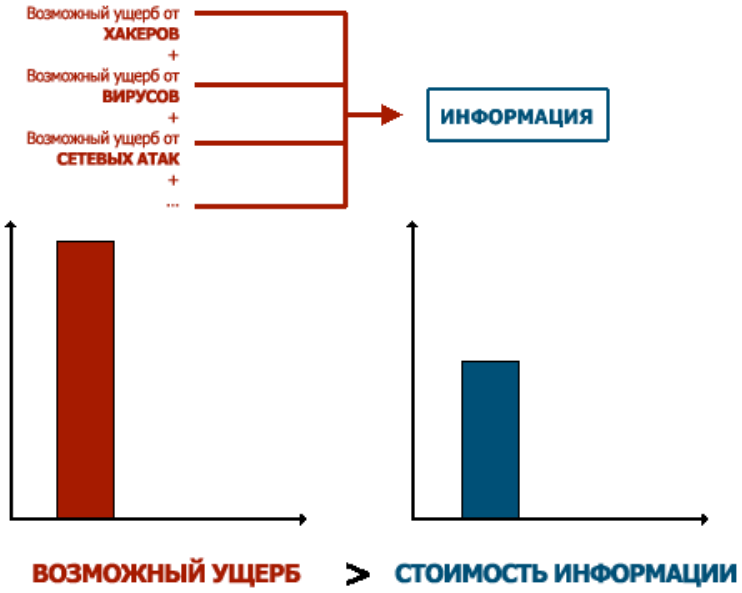


Рис.1.2 Алгоритмические противоречия в алгоритме ГРИФ

Для решения этого алгоритмического противоречия в алгоритме ГРИФ применяется новый метод классического непересекающегося поля угроз информации: угроз конфиденциальности, целостности и доступности. Алгоритм ГРИФ требует от пользователя внести ущерб по всем трем видам угроз по каждому виду ценной информации. Этот метод позволяет, во-первых, абстрагироваться на этапе моделирования системы от конкретных угроз безопасности (дело в том, что каждая конкретная угроза распадается на эти три классических непересекающихся вида угроз), во-вторых, избежать избыточного суммирования по ущербу, так как это поле непересекающихся угроз, и, в-третьих, это позволяет разбить процесс анализа защищенности

информационной системы на множество элементарных ситуаций, когда алгоритм анализирует возможность реализации данных классических угроз безопасности по каждому виду информации на каждом ресурсе и не привязывается на этапе анализа к конкретным реализациям угроз.

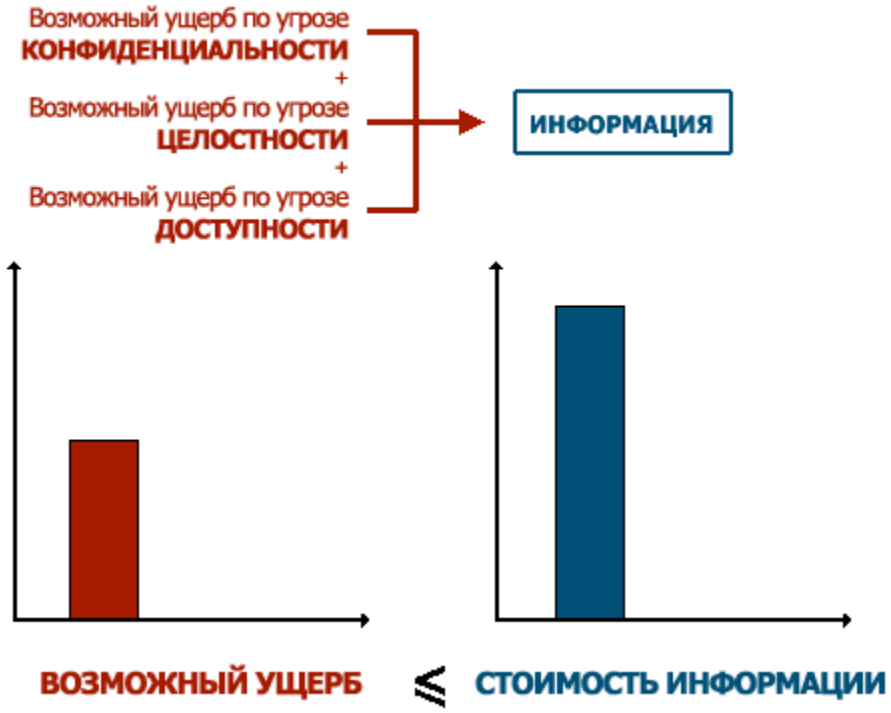


Рис.1.3 Угроз конфиденциальности, целостности и доступности

***Оценка вероятностей реализации обнаруженных угроз***

Фундаментальной проблемой любого алгоритма анализа рисков является определение вероятности реализации специфичной для данной системы угрозы. В случае применения подхода аналогичного Risk Watch (условно, подхода от частных угроз), пользователю на этапе моделирования необходимо или ввести вероятность реализации данной угрозы (что превращает сам "алгоритм" в простую формулу: Вероятность УЩЕРБ, тем самым, выхолащивая до нуля процесс анализа защищенности - его здесь просто нет) или оценить ее уровень. В алгоритме ГРИФ от пользователя не требуется вводить вероятности реализации угроз. В ГРИФ моделируются доступы всех групп пользователей ко всем видам информации и в зависимости от вида доступа и вида ресурса рассматриваются конечное

множество очевидных элементарных ситуаций, где начальную вероятность реализации угрозы можно определить достаточно просто и точно. А далее анализируется множество опять же элементарных факторов (идет анализ комплексной защищенности объекта), которые так или иначе влияют на защищенность, и, затем - делается вывод об итоговых рисках. То есть, в алгоритме ГРИФ применяется типовой алгоритмический подход, когда решение большой сложной задачи разбивается на множество небольших простых задач [5].

Итоговая оценка ГРИФ основывается на целом комплексе параметров, которые определяются, прежде всего, защищенностью анализируемого объекта: анализируются как технологические аспекты защищенности, так и вопросы комплексной безопасности согласно ISO 17799 (организация, управление, администрирование, физ. безопасность и т.д.). При этом подход ГРИФ обладает универсальностью, гибкостью и удобством для пользователя.

### 1.3. Вопросы анализа рисков и управления ими

***Идентификация рисков***

В любой методике необходимо идентифицировать риски, как вариант - их составляющие (угрозы и уязвимости). Естественным при этом является требование полноты списка. Сложность задачи составления списка и доказательства его полноты зависит от того, какие требования предъявляются к детализации списка. На базовом уровне безопасности (третий уровень зрелости организации) специальные требования к детализации классов, как правило, отсутствуют, так что достаточно воспользоваться каким-либо подходящим в данном случае стандартным списком классов рисков. Оценка величины рисков не рассматривается, что приемлемо для некоторых разновидностей методик базового уровня. Списки классов рисков содержатся в ряде руководств, в специализированном ПО

анализа рисков. Пример Германский стандарт BSI, в котором имеется каталог угроз применительно к различным элементам информационной технологии. Достоинством подобных списков является их полнота: классов, как правило, немного (десятки), они достаточно широкие и заведомо покрывают все существующее множество рисков. Недостаток - сложность оценки уровня риска и эффективности контрмер для широкого класса, поскольку подобные расчеты удобнее проводить по более узким (конкретным) классам рисов. К примеру, класс рисков «неисправность маршрутизатора» может быть разбит на множество подклассов, включающих возможные виды неисправности (уязвимости) ПО конкретного маршрутизатора и неисправности оборудования.

***Оценивание рисков***

При оценивании рисков рекомендуется рассматривать следующие аспекты:

- шкалы и критерии, по которым можно измерять риски;
- оценку вероятностей событий;
- технологии измерения рисков.

*Шкалы и критерии, по которым измеряются риски.* Для измерения какого-либо свойства необходимо выбрать шкалу. Шкалы могут быть прямыми (естественными) или косвенными (производными). Примерами прямых шкал являются шкалы для измерения физических величин, например шкалы для измерения объемов жидкости в литрах, шкалы для измерения длины в метрах. В ряде случаев прямых шкал не существует, приходится использовать либо прямые шкалы других свойств, связанных с интересующими нас, либо определять новые шкалы. Пример - шкала для измерения субъективного свойства «ценность информационного ресурса». Эта ценность может измеряться в единицах измерения производных шкал, таких как стоимость восстановления ресурса, время восстановления ресурса

и др. Другой вариант - определить шкалу для получения экспертной оценки, например имеющую три значения:

– малоценный информационный ресурс: от него не зависят критически важные задачи и он может быть восстановлен с небольшими затратами времени и денег;

– ресурс средней ценности: от него зависит ряд важных задач, но в случае утраты он может быть восстановлен за время, не превышающее критически допустимое, но стоимость восстановления - высокая;

– ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое либо стоимость чрезвычайно высока.

Для измерения рисков не существует естественной шкалы. Риски можно оценивать по объективным либо субъективным критериям. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например ПК, за определенный промежуток времени. Пример субъективного критерия - оценка владельцем информационного ресурса риска выхода из строя ПК. В последнем случае обычно разрабатывается качественная шкала с несколькими градациями, например: низкий, средний, высокий уровень. В методиках анализа рисков, как правило, используются субъективные критерии, измеряемые в качественных единицах, поскольку:

– оценка должна отражать субъективную точку зрения владельца информационных ресурсов;

– следует учитывать различные аспекты - не только технические, но и организационные, психологические и т.д.

Для получения субъективной оценки в рассматриваемом примере с оценкой риска выхода из строя ПК можно либо воспользоваться прямой экспертной оценкой, либо определить функцию, преобразующую объективные данные (вероятность) в субъективную шкалу рисков.

Субъективные шкалы бывают количественными и качественными, но на практике, как правило, применяются качественные шкалы с 3-7 градациями. С одной стороны, это просто и удобно, с другой - требует грамотного подхода к обработке данных.

***Объективные и субъективные вероятности***

Термин «вероятность» имеет несколько различных значений. Наиболее часто встречаются два толкования, которые обозначаются сочетанием «объективная вероятность» и «субъективная вероятность». Под объективной (иногда называемой физической) вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к общему количеству наблюдений. Это понятие применяется при анализе результатов большого числа наблюдений, имевших место в прошлом, а также полученных как следствия из моделей, описывающих некоторые процессы [6].

Под субъективной вероятностью имеется в виду мера уверенности некоторого человека или группы людей в том, что данное событие в действительности будет иметь место. Как мера уверенности в возможности наступления события субъективная вероятность может быть формально представлена различными способами: вероятностным распределением на множестве событий, бинарным отношением на множестве событий, не полностью заданным вероятностным распределением или бинарным отношением и другими способами. Наиболее часто субъективная вероятность представляет собой вероятностную меру, полученную экспертным путем. Именно в этом смысле мы и будем понимать субъективную вероятность в дальнейшем. Субъективная вероятность в современных работах в области системного анализа не просто позволяет определить меру уверенности на множестве событий, а увязывается с системой предпочтений лица, принимающего решения (ЛПР), и в конечном итоге с функцией полезности, отражающей его предпочтения из множества

альтернатив. Тесная связь между субъективной вероятностью и полезностью используется при построении некоторых методов получения субъективной вероятности.

***Получение оценок субъективной вероятности***

Процесс получения субъективной вероятности обычно разделяют на три этапа: подготовительный этап, получение оценок, этап анализа полученных оценок.

*Первый этап.* Во время этого этапа формируется объект исследования - множество событий, а также выполняется предварительный анализ свойств этого множества (устанавливается зависимость или независимость событий, дискретность или непрерывность случайной величины, порождающей данное множество событий). На основе такого анализа выбирается один из подходящих методов определения субъективной вероятности. На этом же этапе производится подготовка эксперта или группы экспертов, ознакомление их с методом и проверка понимания ими поставленной задачи.

*Второй этап.* Состоит в применении метода, выбранного на первом этапе. Результатом этого этапа является набор чисел, который отражает субъективный взгляд эксперта или группы экспертов на вероятность того или иного события, однако далеко не всегда может считаться окончательным распределением, поскольку нередко оказывается противоречивым.

*Третий этап.* На этом этапе исследуются результаты опроса. Если вероятности, представленные экспертами, не согласуются с аксиомами вероятности, то на это обращается внимание экспертов и ответы уточняются с целью приведения их в соответствие с выбранной системой аксиом.

Для некоторых методов получения субъективной вероятности третий этап исключается, поскольку сам метод состоит в выборе подчиняющегося аксиомам вероятности вероятного распределения, которое в том или ином смысле наиболее близко к оценкам экспертов. Особую важность третий этап приобретает при агрегировании оценок, предложенных группой экспертов.

***Оценка рисков по двум факторам***

В простейшем случае производится оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея может быть выражена формулой: РИСК = $п_{происшествия}$ × ЦЕНА ПОТЕРИ.

Если переменные являются количественными величинами, то риск - это оценка математического ожидания потерь [7].

Когда переменные - качественные величины, метрическая операция умножения не определена. Таким образом, в явном виде эту формулу применять не следует. Рассмотрено вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены шкалы.

Приведем пример субъективной шкалы вероятностей событий:

A - событие практически никогда не происходит;

B - событие случается редко;

C - вероятность события за рассматриваемый промежуток времени - около 0,5;

D - скорее всего, событие произойдет;

E - событие почти обязательно произойдет.

Кроме того, устанавливается субъективная шкала серьезности происшествий, скажем, в соответствии с:

– N (Negligible) - воздействием можно пренебречь;

– Mi (Minor) - незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;

– Mo (Moderate) - происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами, воздействие на

информационную технологию небольшое и не затрагивает критически важные задачи;

– S (Serious) - происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, влияет на выполнение критически важных задач;

– C (Critical) - происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков устанавливается шкала из трех значений:

– низкий риск;

– средний риск;

– высокий риск.

Риск, связанный с конкретным событием, зависит от двух факторов и может быть определен так, как в табл. 1.1.

Определение риска в зависимости от двух факторов Таблица 1.1

| Шкала | Negligible | Minor | Moderate | Serious | Critical |
|---|---|---|---|---|---|
| A | Низкий риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| B | Низкий риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| C | Низкий риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| D | Средний риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| E | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

Шкалы факторов риска и сама таблица могут быть построены иначе, иметь другое число градаций.

Подобный подход к оценке рисков достаточно распространен.

При разработке (использовании) методик оценивания рисков надо учитывать следующие особенности:

– значения шкал должны быть четко определены (необходимо их словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки;

– требуется обоснование выбранной таблицы. Следует убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков.

***Технология оценки угроз и уязвимостей***

Как правило, для оценки угроз и уязвимостей применяются различные методы, в основе которых могут лежать:

– экспертные оценки;

– статистические данные;

– учет факторов, влияющих на уровни угроз и уязвимостей.

Один из возможных подходов к разработке подобных методик - накопление статистических данных об имевших место происшествиях, анализ и классификация их причин, выявление факторов, от которых они зависят. Эта информация позволяет оценить угрозы и уязвимости в других информационных системах.

Однако при практической реализации такого подхода возникают следующие сложности.

Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.

Во-вторых, данный подход оправдан далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если же система сравнительно невелика и эксплуатирует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

Наиболее распространен в настоящее время подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Он позволяет абстрагироваться от малосущественных технических деталей, принять во внимание не только программно-технические, но и иные аспекты.

### 1.4. Многофакторный анализ рисков информационной безопасности

В классическом представлении оценка рисков включает в себя оценку угроз, уязвимостей и ущерба, наносимого при их реализации. Анализ риска заключается в моделировании картины наступления этих самых неблагоприятных условий посредством учета всех возможных факторов, определяющих риск как таковой. С математической точки зрения при анализе рисков такие факторы можно считать входными параметрами.

Перечислим эти параметры:

1) активы — ключевые компоненты инфраструктуры системы, вовлеченные в бизнес-процесс и имеющие определенную ценность;

2) угрозы, реализация которых возможна посредством эксплуатации уязвимости;

3) уязвимости — слабость в средствах защиты, вызванная ошибками или несовершенством в процедурах, проекте, реализации, которая может быть использована для проникновения в систему;

4) ущерб который оценивается с учетом затрат на восстановление системы в исходное состояния после возможного инцидента ИБ.

Итак, первым этапом при проведении многофакторного анализа рисков является идентификация и классификация анализируемых входных параметров. Далее необходимо провести градацию каждого параметра по уровням значимости (например: высокий, средний, низкий). Прежде всего, необходимо определить, что является ценным активом организации с точки зрения информационной безопасности. Стандарт ISO 17799, подробно

описывающий процедуры системы управления ИБ, выделяет следующие виды активов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.);
- программное обеспечение;
- материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.);
- сервисы (сервисы телекоммуникаций, системы обеспечения жизнедеятельности и др.);
- сотрудники компании, их квалификация и опыт;
- нематериальные ресурсы (репутация и имидж компании).

Следует определить, нарушение информационной безопасности, каких активов может нанести ущерб организации. В этом случае актив будет считаться ценным, и его необходимо будет учитывать при анализе информационных рисков. Инвентаризация заключается в составлении перечня ценных активов компании. Как правило, данный процесс выполняют владельцы активов. Понятие "владелец" определяет лиц или стороны, которые имеют утвержденные руководством компании обязанности по управлению созданием, разработкой, поддержанием, использованием и защитой активов.

***Категорирование активов организации***

В процессе категорирования активов необходимо оценить критичность активов для бизнес-процессов организации или, другими словами, определить, какой ущерб понесет организации в случае нарушения информационной безопасности активов. Данный процесс вызывает наибольшую сложность, т.к. ценность активов определяется на основе экспертных оценок их владельцев [8]. В процессе данного этапа часто проводятся обсуждения между консультантами по разработке системы

управления и владельцами активов. Это помогает владельцам активов понять, каким образом следует определять ценность активов с точки зрения информационной безопасности (как правило, процесс определения критичности активов является для владельца новым и нетривиальным). Кроме этого, для владельцев активов разрабатываются различные методики оценки. В частности, такие методики могут содержать конкретные критерии (актуальные для данной компании), которые следует учитывать при оценке критичности.

***Оценка критичности активов***

Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности. Т.е. следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов. Оценку критичности активов можно выполнять в денежных единицах и в уровнях. Однако, учитывая тот факт, что для анализа информационных рисков необходимы значения в денежных единицах, в случае оценки критичности активов в уровнях следует определить оценку каждого уровня в деньгах.

***Идентификация и категорирование угроз***

Согласно авторитетной классификации NIST, включенной в RISK MANAGEMENT GUIDE FOR THE INFORMATION TECHNOLOGY SYSTEMS, категорированию и оценке угроз предшествует непосредственная идентификация их источников. Так, согласно вышеупомянутой классификации, можно выделить основные источники угроз, среди которых:

- угрозы природного происхождения (землетрясения, наводнения и т.п.);
- угрозы, исходящие от человека (неавторизованный доступ, сетевые атаки, ошибки пользователей и т.п.);
- угрозы техногенного происхождения (аварии различного рода, отключение электроснабжения, химическое загрязнение и т.п.).

Вышеописанная классификация может быть далее категорирована более подробно.

Так, к самостоятельным категориям источников угроз, происходящих от человека, согласно упомянутой классификации NIST относятся:

- хакеры;
- криминальные структуры;
- террористы;
- организации, занимающиеся промышленным шпионажем;
- инсайдеры.

Каждая из перечисленных угроз, в свою очередь, должна быть детализирована и оценена по шкале значимости (например: низкий, средний, высокий).

***Идентификация и категорирование уязвимостей***

Очевидно, что анализ угроз должен рассматриваться в тесной связи с уязвимостями исследуемой нами системы. Задачей данного этапа управления рисками является составление перечня возможных уязвимостей системы и категорирование этих уязвимостей с учетом их "силы". Так, согласно общемировой практике, градацию уязвимостей можно разбить по уровням: критический, высокий, средний, низкий [9].

1. Критический уровень опасности. К этому уровню опасности относятся уязвимости, которые позволяют осуществить удаленную компрометацию системы без дополнительного воздействия целевого пользователя и активно эксплуатируются в настоящее время. Данный уровень опасности подразумевает, что эксплойт находится в публичном доступе.

2. Высокая степень опасности. К этому уровню опасности относятся уязвимости, которые позволяют осуществить удаленную компрометацию системы. Как правило, для подобных уязвимостей не существует эксплойта в публичном доступе.

3. Средняя степень опасности. К этому уровню опасности относятся уязвимости, которые позволяют провести удаленный отказ в обслуживании, неавторизованный доступ к данным или выполнение произвольного кода при непосредственном взаимодействии с пользователем (например, через подключение к злонамеренному серверу уязвимым приложением).

4. Низкий уровень опасности. К этому уровню относятся все уязвимости, эксплуатируемые локально, а также уязвимости, эксплуатация которых затруднена или которые имеют минимальное воздействие (например, XSS, отказ в обслуживании клиентского приложения).

Источником составления такого перечня/списка уязвимостей должны стать:

- общедоступные регулярно публикуемые списки уязвимостей (как пример: www.securitylab.ru);
- список уязвимостей публикуемых производителем ПО (как пример: www.apache.org);
- результаты тестов на проникновение (как пример: www.site-sec.com); анализ отчетов сканеров уязвимостей (проводится администратором безопасности внутри компании).

В общем случае уязвимости можно классифицировать следующим образом:

- уязвимости ОС и ПО (ошибки кода), обнаруженные производителем или независимыми экспертами (на момент написания статьи общее количество обнаруженных уязвимостей достигло отметки около ~1900 — сюда вошли уязвимости, опубликованные в "багтреках" на xakep.ru, securitylab, milw0rm.com и securityfocus.com);
- уязвимости системы, связанные с ошибками в администрировании (неадекватные окружению настройки web-сервера или PHP, не закрытые межсетевым экраном порты с уязвимыми сервисами и т.п.);

▪ уязвимости, источниками которых могут стать инциденты, не предусмотренные политикой безопасности, а также события стихийного характера. В качестве яркого примера распространенной уязвимости ОС и ПО можно привести переполнение буфера (buffer overflow). К слову будь сказано, абсолютное большинство из ныне существующих эксплойтов реализуют класс уязвимостей на переполнение буфера.

***Численные методы оценки рисков***

Простейшая оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей.

Классическая формула оценки рисков:

R=D*P(V), где R — информационный риск;

D — критичность актива (ущерб);

P(V) — вероятность реализации уязвимости.

Одним из примеров практической реализации вышеописанного подхода к определению уровней риска является матрица рисков, предложенная NIST.

Матрица рисков (согласно рекомендациям NIST "Risk Management Guide for Information Technology Systems") Таблица 1.2

| Threat Likelihood-угроза (ее вероятность) | Impact-ущерб | | |
|---|---|---|---|
| | Low (низкий) — 10 | Medium (средний) -50 | High (высокий) -100 |
| High (высокая) — 1 | Low (низкий) 10x1=10 | Medium (средний) 50x1=50 | High (высокий) 100x1=100 |
| Medium (средняя) — 0.5 | Low (низкий) 10x0.5=5 | Medium (средний) 50x0.5=25 | Medium (средний) 100x0.5=50 |
| Low (низкая) — 0.1 | Low (низкий) 10x0.1=1 | Low (низкий) 50x0.1=5 | Low (низкий) 100x0.1=10 |
| Уровень риска: Высокий (от 50 до 100); Средний (от 10 до 50); Низкий (от 1 до 10). | | | |

Каждый из возможных входных параметров (к примеру, уязвимость, угроза, актив и ущерб) описывается своей функцией принадлежности с учетом соответствующего коэффициента.

***Оценка рисков на основе нечеткой логики***

Механизмы оценки рисков на основе нечеткой логики включает в себя последовательность этапов, в каждом из которых используются результаты предыдущего этапа. Последовательность этих этапов обычно следующая:

- ввод правил программирования в виде продукционных правил ("ЕСЛИ,… ТО"), отражающих взаимосвязь уровня входных данных и уровня риска на выходе;
- задание функции принадлежности входных переменных (как пример — с помощью специализированных программ вроде "Fuzyy logic" — в данном примере мы использовали MatLab);
- получение первичного результата оценок входных переменных;
- фазификация оценок входных переменных (нахождение конкретных значений функций принадлежности);
- агрегирование (подразумевает проверку истинности условий путем преобразований функций принадлежности через нечеткую конъюнкцию и нечеткую дизъюнкцию);
- активизация заключений (нахождение весовых коэффициентов по каждому из правил и функций истинности);
- аккумуляция заключений (нахождение функции принадлежности для каждой из выходных переменных);
- дефазификация (нахождение четких значений выходных переменных).

# 2. ОСНОВНАЯ ЧАСТЬ. МЕТОДИКА РАЗРАБОТКИ АЛГОРИТМЫ ОЦЕНИВАНИЯ РИСКОВ НА ОСНОВЕ МОДЕЛИРОВАНИЯ УГРОЗ

## 2.1. Методология матричного подхода анализ рисков

Компьютерные сети и Интернет позволили увеличить производительность, как в государственных структурах, так и в частных организациях. Использование электронной почты и мгновенных сообщений выросло экспоненциально на протяжении нескольких лет и становится предпочтительным способом общения. Несмотря на взлеты и падения, Интернет продолжает вносит изменения в способы потребления в магазинах и в бизнес-модели компаний. Например, альтернативная модель распространения музыки через Интернет изменила музыкальную индустрию, а также способствовала развитию новых форматов, способов оцифровки и сжатия музыкальных файлов.

Несмотря на то, что влияние Интернет на электронную коммерцию, коммуникаций, и распространение информация очевидно, наибольший вклад компьютерные сети внесли в перестройку бизнес-процессов. Большинство рутинных корпоративных функций, в настоящее время выполняется с помощью автоматизированных процессов, связанных с базами данных. Сетевые информационные системы составляют основу предприятия и используются практически во всех сферах бизнеса, включая: выплату заработной платы, закупки, управление человеческими ресурсами, анализа и проектирования инженерных решений. Информационные системы значительно улучшили производительность предприятий. Тем не менее, полная зависимость информационных систем от критических операций сделала предприятий подверженными атакам из сети [10]. Поскольку зависимость экономики от информационных систем возрастает, финансовые потери от нарушения информационной безопасности также увеличиваются. Этот риск финансовых потерь в связи с нарушением информационной

безопасности является причиной для беспокойства и корпорации, и правительства. У большинства организаций не существует полной картины состояния своей информационной безопасности и рисков. Как правило, специальные решения относительно безопасности основаны на реализации руководящих принципов и документов, выданных государственными учреждениями или сторонними организациями. Информационные отделы могут поддерживать существующий уровень безопасности в проверке, но предприятию очень сложно иметь четкую картину состояния своей информационной безопасности без формального анализа рисков. Персонал информационных отделов может быть компетентными в методах реализации средств безопасности, но ему зачастую не хватает опыта в финансовом моделировании и анализе рисков. Методология формального анализа рисков хорошо изучена в некоторых областях науки (финансы, инженерия, авиация и д.р.). Тем не менее, в информационной безопасности эта дисциплина только зарождается. Одной из проблем, связанной с анализом рисков информационной безопасности, является отсутствие стандартизированных показателей и методов для оценки измерения воздействия угроз и оценки в интересах контроля и острой нехваткой статистических данных для оценки рисков. Еще одной проблемой является низкое качество данных о факторах риска и уязвимостях. Это вызвано тем, что организации опасаются разглашения инцидентов нарушения информационной безопасности, потому что это может привлечь новых хакеров. Наконец, процесс анализа информационных рисков очень слабо освещен в руководящих документах, является дорогостоящим и требует глубокого изучения внутренней структуры организации. Поэтому большинство организаций зачастую ограничивается внешней оценкой рисков и проводить такие оценки периодически (ежегодно или два раза в год), а не непрерывно. Кроме того, у организации нет возможности определить качество сделанной оценки, и они вынуждены полагаться на выводы, сделанные сторонними консультантами.

Анализ рисков информационный безопасности исследовался аудиторскими фирмами в течение долгого времени.

Данная методология связывает активы, уязвимости, угрозы и средства управления организацией и определяет важность различных средств управления, соответствующими активами организация Активы организации определены как вещи, имеющие значение. Активы могут быть материальными, такие как данные и сети и нематериальными, такие как репутация и доверие.

Методология использует три отдельных матрицы: матрицу уязвимостей, матрицу угроз и матрицу контроля, чтобы собрать данные, которые требуются для анализа риска.

Матрица уязвимости (таблица 2.1. содержит связь между активами и уязвимостями в организациях, матрица угроз (таблица 2.2) так же содержит отношения между уязвимостями и угрозами, а матрица контроля (таблица 2.3) содержат связи между угрозами и средствами управления. Значение в каждой ячейке показывает ценность отношения между элементом строки и столбца таблицы (например, активом и уязвимостью). Использует одна из трех оценок ценности: низкая, средняя или высокая.

При первоначальном анализе риска формируются списки активов, уязвимостей, угроз, и средств управления и добавляются к соответствующим таблицам.

Матрицы заполняются путем добавления данных о связи элемента столбца матрица с элементом строки. Наконец, данные из матрицы уязвимости преобразуются с помощью формулы (1), а затем заносятся в таблицу 2.2. Таким же образом данные из матрицы угроз преобразуются с помощью формулы (2) и заносятся в таблицу. В результате формируется матрица контроля, которая содержит относительную важность различных средств управления.

Матрица активов (связь между активами и уязвимостью) Таблица 2.1

| Шкала<br>0 - нет воздействия<br>1 - слабое воздействие<br>3 - умеренное воздействие<br>9 - сильное воздействие<br>**Уязвимость** | Активы затраты | Торговые секреты | Конфиденциальная информация | Репутация (доверие) | Потерянный доход | Затраты на восстановление | Информация | Аппаратные средства | Программное обеспечение | обслуживание | коммуникации |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Веб-сервер | | | | | | | | | | | |
| Вычислительный сервер | | | | | | | | | | | |
| Брандмауэр | | | | | | | | | | | |
| Маршрутизатор | | | | | | | | | | | |
| Клиентские узлы | | | | | | | | | | | |
| Базы данных | | | | | | | | | | | |

Пусть есть $m$ активов, относительная стоимость актива $\mathrm{a_j} \in \mathrm{C_j} (j = 1, n)$. Также пусть $\mathrm{c_{ij}}$ это воздействие уязвимости $\nu_\mathrm{i}$ на актив $\mathrm{a}_j$. Тогда совокупное воздействие уязвимости $\nu_\mathrm{i}$ на активы организации вычисляется по формуле:

$$V_i = \sum_{j=1}^{n} v_{ij} \cdot C_j \qquad (1)$$

Матрица активов (связь между угрозами и уязвимостями) Таблица 2.2

| Шкала<br>0- нет воздействия<br>1- слабое воздействие<br>3-умеренное воздействие<br>9 - сильное воздействие<br>**Средства контроля** | Угроза | Отказ в обслуживании (DoS) | Вредоносный код | Ошибки пользователя | Внутренние атаки | Спам | Физическое повреждение аппаратных |
|---|---|---|---|---|---|---|---|
| Вредоносный код | | | | | | | |
| Ошибки пользователя | | | | | | | |
| Внутренние атаки | | | | | | | |
| Спам | | | | | | | |
| Физическое повреждение аппаратных средств | | | | | | | |

Пусть имеется $p$ угроз, которые действуют на уязвимостей и $d_{ki}$ – потенциал повреждения от угрозы $t_k$ – уязвимости $v_{\text{i}}$. Тогда относительное совокупное воздействие угрозы $\text{T}_k$:

$$T_k = \sum_{i=1}^{m} d_{ki} \cdot V_i \qquad (2)$$

Матрица угроз (связь между средствами управления и угрозами) Таблица 2.3

| Шкала<br>0- нет воздействия<br>1- слабое воздействие<br>3 - умеренное воздействие<br>9 - сильное воздействие<br><br>**Средства контроля** | **Угроза** | Отказ в обслуживании (DoS) | Вредоносный код | Ошибки пользователя | Внутренние атаки | Спам | Физическое повреждение аппаратных |
|---|---|---|---|---|---|---|---|
| Брандмауэр | | | | | | | |
| Система обнаружения вторжений (IDS) | | | | | | | |
| Обучение персонала | | | | | | | |
| DMZ | | | | | | | |
| Политика безопасности | | | | | | | |
| Конфигурация архитектуры сети | | | | | | | |

Пусть есть $q$ средств управления, которые могут смягчить $p$ угроз, а $e_{lk} -$ воздействие средства контроля $z_0 -$ на угрозу $t_k$. Тогда относительное совокупное воздействие средств контроля $Z_o$

$$Z_0 = \sum_{l=1}^{p} e_{0l} \cdot T_l \qquad (3)$$

Представлена удобная методология для оценки рисков информационной безопасности, которую могут легко использовать организации. Методология обеспечивает удобные шаблоны, которые могут постепенно совершенствоваться с увеличением количества доступной информации. Методология обеспечивает прозрачность процесса анализа.

## 2.2. Алгоритм построения математической модели управления рисков от внешних угроз

Алгоритм управления рисков дает возможность повысить достоверность экспертных оценок по сравнению с моделями потенциальных нарушителей. При этом в анализе рисков участвуют только те ресурсы, которые интересуют этих противников, и которые в связи с этим можно оценить денежно.

***Условные обозначения:***

- *t* (*trespasser*) – конкретный противник организации, мотивированный на получение выгоды от реализации угрозы деструктивного воздействия на определенную информацию;
- *i* (*information*) – информация, интересующая противника;
- *r* (*resource*) – ресурс организации (физический, технический, персонал, в том числе носители информации);
- *d*(*i*), *d*(*r*) (*doing*) – действие противника по отношению к информации или ресурсу;
- $s(i_1 ... i_\alpha)$, $s(r_1 ... r_\beta)$ (*security facility*) – средство (мера) защиты (СЗ) по отношению к информации или ресурсам;

 *n*(*s*) – количество ресурсов, защищаемых СЗ;

- *M*(*i*, *t*) (*method*)– способ реализации угрозы (РУ) противником в отношении информации. Включает определенный способ доступа и способ использования информации (ИИ);

$$M\ (i,t) = (Ma\ (i,t); Mr\ (i,t));$$

 *Ma*(*i*, *t*) (*access*) – способ доступа противника к информации; доступ осуществляется через ресурсы *r* с помощью действий *d*(*r*).

 *Mr*(*i*, *t*) (*realization*) – способ использований информации противником; ИИ производится с помощью действия *d*(*i*):

- *o*(*M*) (*occurrence*) – инцидент в области ИБ;

$o(M) = (o(Ma); o(Mr))$, где $M = (Ma; Mr)$;

 $N(M) = N(o(M))$ (*number*) – количество инцидентов в области ИБ с использованием способа РУ, зафиксированных в статистических данных;

 $N(Ma)$, $N(Mr)$ – количество инцидентов в области ИБ с использованием способа доступа и способа ИИ:

$N(Ma) = Ns(Ma) + Nf(Ma)$, $N(Mr) = Ns(Mr) + Nf(Mr)$, где

- $Ns(Ma)$, $Ns(Mr)$ (*success*) – количество успешных атак в области ИБ с использованием способа доступа и способа ИИ;

- $Nf(Ma)$, $Nf(Mr)$ (*failure*) – количество предотвращенных атак в области ИБ с использованием способа доступа и способа ИИ;

- $G(M)$ (*gain*) – экспертная оценка выгоды, получаемой противником от РУ;

- $V(M)$ (*value*) – оценка стоимости для противника РУ: $V(M) = V(Ma) + V(Mr)$;

 $V(Ma)$ – оценка стоимости получения доступа способом *Ma*;

 $V(Mr)$ – оценка стоимости использования информации способом *Mr*;

Для расчета оценок стоимости используются следующие экспертные оценки:

- $Ve(s(i))$, $Ve(s(r))$ – экспертная оценка стоимости «взлома» средства защиты *s* на ресурсе *r* и для информации *i*.

- $Ve(r, d(r))$ – экспертная оценка затрат противника на осуществление действия *d* на ресурс *r*, не связанных со «взломом» средств защиты.

- $Ve(i, d(i))$ – экспертная оценка затрат противника на осуществление действия *d* над информацией *i* после получения доступа [11].

- $O(i, t)$ (*opposition*) – экспертная оценка возможных финансовых потерь противником *t*, получившим и реализующим информацию *i*, вследствие контрдействий владельца информации, применения им компрометирующей информации, данных службы безопасности, полученных методами агентурной и технической разведки;

- $P(M)$ (*probability*)– оценка вероятности РУ способом $M$. Оценка вероятности РУ рассчитывается на основании статистики инцидентов, анализа мотивации противника и психологической предрасположенности противника;

 $P^1(M)$ – компонента вероятности, рассчитанная на основании статистики инцидентов, рассчитывается как вероятность выполнения двух совместных событий: получения доступа и использование информации;

 $P^2(M)$ – компонента вероятности, рассчитанная на основании анализа мотивации противника; а именно оценок выгоды от РУ, затрат на РУ, потерь от контрдействий;

 $P^3(M)$ – компонента вероятности, оцениваемая экспертами и показывающая психологическую предрасположенность противника на РУ;

- $L(M)$ (*loss*) – оценка финансовых потерь владельца информации от РУ способом $M$:

$L(M)= L(Ma) + L(Mr)$, где

 $L(Ma)$ – оценка финансовых потерь за счет нарушения средств защиты, ресурсов в процессе получения доступа;

 $L(Mr)$ – оценка финансовых потерь за счет использования информации противником.

Для расчета оценок финансовых потерь используются следующие статистические данные:

- $L(o(Ma))$ (*occurrence loss*) – ущерб владельца от нарушения ресурсов в процессе успешного доступа в инциденте $o(M)$;

- $L(o(Mr))$ – ущерб владельца от успешного ИИ в инциденте $o(M)$ (судебные издержки, командировки, смена персонала и т.д.).

Для расчета оценок финансовых потерь организации от деструктивных действий противника используются следующие экспертные оценки:

- $Le(r, d(r))$ (*expert*) –оценка потерь от действия $d$ на ресурс $r$;

- *Le*(*i, d*(*i*)) – экспертная оценка финансовых потерь за счет использования информации противником.

- *R* (*risk*) – риск; *R*□ – не риск;

□ *R*(*M*) – оценка риска РУ способом *M*, является произведением вероятности РУ на ущерб от РУ;

□ *R*(*i*) – оценка риска для информации *i*, рассчитывается как максимальный риск РУ для данной информации;

□ *R*□(*M*) – оценка не риска РУ способом *M*, является произведением вероятности не реализации угрозы на ущерб от РУ;

□ *R*□(*i*) – оценка не риска для информации *i*, соответствует минимальному не риску РУ для данной информации.

- *C* (*cost*) – оценка суммарной стоимости средств (мер) защиты;

□ *C*(*s*) – оценка финансовых затрат на средство защиты *s*.

Для расчета оценок финансовых затрат используются следующие экспертные оценки:

- *Ci*(*s*) (*install*) – экспертная оценка стоимости покупки, установки и настройки СЗ (внедрения меры защиты) на один ресурс;

- *Cu*(*s*) (*use*) – экспертная оценка стоимости эксплуатации СЗ в год;

- *Cr*(*s*) (*removal*) – экспертная оценка стоимости вывода из эксплуатации СЗ;

- *I*(*s*) (*indirect gain*) – экспертная оценка косвенной выгоды от внедрения СЗ;

- *Profit* (*profitability*) – оценка рентабельности системы ИБ организации. Автором предлагается оценивать выгоду суммарными нерисками по информации, подвергающейся угрозам противников, в сумме с косвенной выгодой от внедрения средств защиты.

***Процедура анализа и управления рисками***

1. ***Выявление конкретных противников*** $t$, $t \in \{t_1,..., t_{nt}\}$. *Их характеристика.*

2. ***Описание структуры организации:***

2.1. описание значимых ресурсов $r$, $r \in \{r_1,..., r_{nr}\}$;

2.2. описание информации $i$, $i \in \{i_1,..., i_{ni}\}$;

2.3. описание действий противника над ресурсами $d(r)$, $d(r) \in \{d_1,..., d_{ndr}\}$ и над информацией $d(i)$, $d(i) \in \{d_1,..., d_{ndi}\}$;

2.4. описание используемых средств защиты $s(i_\alpha,\ldots,i_\beta)$, $s(r_\gamma,\ldots,r_\delta)$, $s \in \{s_1,..., s_{ns}\}$ для информации и ресурсов.

3. ***Получение экспертных оценок:***

3.1. $Ve(r, d(r))$, $Ve(i, d(i))$ - затраты противника на осуществление действий над ресурсами и информацией, не связанных со «взломом» СЗ:

$r \in \{r_1,..., r_{nr}\}$, $d(r) \in \{d_1,..., d_{ndr}\}$, $i \in \{i_1,..., i_{ni}\}$, $d(i) \in \{d_1,..., d_{ndi}\}$;

3.2. $Ve(s(r))$, $Ve(s(i))$ - затраты противника на «взлом» СЗ ресурса и информации соответственно; $s \in \{s_1,..., s_{ns}\}$;

3.3. $Ci(s)$, $Cu(s)$, $Cr(s)$ - затраты владельца информации на СЗ, $s \in \{s_1,..., s_{ns}\}$;

3.4. $I(s)$ - косвенная выгода от внедрения СЗ $s$, $s \in \{s_1,..., s_{ns}\}$;

3.5. $Le(r, d(r))$, $Le(i, d(i))$ – ущерб владельца от деструктивных действий противника по отношению к ресурсами и информации:

$r \in \{r_1,..., r_{nr}\}$, $d(r) \in \{d_1,..., d_{ndr}\}$, $i \in \{i_1,..., i_{ni}\}$, $d(i) \in \{d_1,..., d_{ndi}\}$.

4. ***Описание способов РУ.***

4.1. Выявление способов доступа. Доступ реализуется через некоторые ресурсы с помощью определенных действий:

$Ma(i,t) \in \{Ma_1,..., Ma_{nma}\}$; $Ma(i, t) = \{(r, d(r)) | r \in \{r_1,..., r_{nr}\}$, $d(r) \in \{d_1,..., d_{ndr}\}\}$;

4.2. Выявление способов использования информации.

$Mr\ (i,t) \in \{Mr_1,...,\ Mr_{nmr}\}$; $Mr(i,\ t) = (i;\ d(i))$, $i \in \{i_1,...,\ i_{ni}\}$, $d(i) \in \{d_1,...,\ d_{ndi}\}$.

4.3. Определение способов реализации угроз как комбинации способов доступа и способов использования информации.

$M\ (i,t) \in \{M_1,...,\ M_{nm}\}$;

$M\ (i,t) = \{(Ma\ (i,t); Mr\ (i,t)) \mid Ma\ (i,t) \in \{Ma_1,...,\ Ma_{nma}\},\ Mr\ (i,t) \in \{Mr_1,...,\ Mr_{nmr}\}\}$.

4.4. Экспертная оценка параметров, характеризующих способы РУ $M\ (i,t) \in \{M_1,...,\ M_{nm}\}$: $G(M)$, $P^3(M)$, $O(i,\ t)$, где $P^3(M) \in [0;1]$, и по умолчанию $O(i,\ t) = 0$.

5. ***Фиксация значений:***

5.1. фиксируется конкретная информация $i$, $i \in \{i_1,...,\ i_{ni}\}$;

5.2. фиксируется конкретный противник $t$, $t \in \{t_1,...,\ t_{nt}\}$;

5.3. фиксируется конкретный способ РУ, а именно - $M(i,\ t) = (Ma; Mr)$, $M \in \{M_1,...,\ M_{nm}\}$.

6. ***Анализ статистических данных об инцидентах в области ИБ.***

6.1. Описание инцидентов в области ИБ: $o(M)$, $o(M) \in \{o_1,...,\ o_{no}\}$, $o(M) = (o(Ma); o(Mr))$.

6.2. Указание ущерба владельца по каждому инциденту: $L(o(Ma))$, $L(o(Mr))$.

6.3. Подсчет количества успешных и предотвращенных атак по инцидентам: $Ns(Ma)$, $Nf(Ma)$, $Ns(Mr)$, $Nf(Mr)$.

Дальнейшие расчеты производятся при наличии достаточного объема статистических данных:

$Ns(Ma) + Nf(Ma) = N_a > 0$,

$Ns(Mr) + Nf(Mr) = N_r > 0$,

по умолчанию $N_a = N_r = 10$.

6.4. Расчет оценки компоненты вероятности РУ на основании статистики инцидентов:

$P^1(M) = P^1(Ma) \cdot P^1(Mr)$,

$$P^1(Ma) = \frac{Ns(Ma)}{Ns(Ma) + Nf(Ma)}, \quad P^1(Mr) = \frac{Ns(Mr)}{Ns(Mr) + Nf(Mr)}.$$

7. ***Анализ мотивации противника на реализацию угрозы.***

7.1. Расчет стоимости РУ для противника:

$V(M) = V(Ma) + V(Mr)$;

где $V(Ma)$ – оценка стоимости получения доступа, вычисляется как сумма экспертных оценок осуществления деструктивных действий и «взлома» средств защиты ресурсов, входящих в данный способ доступа, а также информации, к которой осуществляется доступ:

$$V(Ma) = \sum_r Ve(r, d(r)) + \sum_r \sum_s Ve(s(r)) + Ve(s(i));$$

$V(Mr)$ – оценка стоимости использования информации, равная экспертной оценке выполнения действия над информацией после получения доступа:

$$V(Mr) = Ve(i, r(i)).$$

7.2. Расчет оценки компоненты вероятности РУ на основании анализа мотивации противника:

$$P^2(M) = \frac{G(M) - V(M) - O(i,t)}{G(M)}.$$

Расчет производится только при наличии значений всех компонент формулы $P^2(M)$. При отсутствии оценок некоторых компонент $P^2(M)$ считается неоцененным, что учитывается при расчете общей оценки вероятности.

8. ***Вычисление общей оценки вероятности РУ.***

$$P(M) = \frac{\sum_{v} k_v \cdot P^v(M)}{\sum_{v} k_v}, \; v = 1,\ldots,3.$$

Коэффициенты: $k_1$ – статистический, $k_2$ – мотивационный, $k_3$ – психологический.

Коэффициенты рассчитываются следующим образом:

$k_v = 0$, если $P^v$ не оценено, $v = 1\ldots3$;

$k_1 = \log_N(N_a + N_r)$ при $N_a + N_r \leq N$;

$k_1 = 1$ при $N_a + N_r > N$;

$k_v = 1$, если $P^v$ рассчитано, $v = 2, 3$.

$N$ – граничное значение, задается экспертом, по умолчанию $N = 10$.

9. ***Расчет оценок риска и не риска для способа РУ.***

9.1. Расчет оценки ущерба от РУ для владельца информации:

$L(M) = L(Ma) + L(Mr)$;

где $L(Ma)$ - ущерб владельца от получения доступа, рассчитывается на основании статистики инцидентов (усредненные по статистике успешных инцидентов финансовые потери от получения доступа способом $Ma$) и на основании суммарных потерь от действий $d$ на ресурсы $r$, через которые осуществляется доступ:

$$L(Ma) = \frac{\frac{k_1}{Ns(Ma)} \cdot \sum_{o} L(o(Ma)) + \sum_{r} Le(r, d(r))}{k_1 + 1}, \; r \in Ma \; ;$$

$L(Mr)$ - ущерб владельца от ИИ, рассчитываются на основании статистики инцидентов (усредненные по статистике успешных инцидентов финансовые потери от ИИ способом $Mr$) и на основании экспертной оценки потерь за счет действия по использованию информации:

$$L(Mr) = \frac{\frac{k_1}{Ns(Mr)} \cdot \sum_{o} L(o(Mr)) + Le(i, d(i))}{k_1 + 1},$$

где $k_1$ – статистический коэффициент.

9.2. Расчет оценок риска и не риска для способа РУ:

$R(M) = L(M) \cdot P(M)$; $\tilde{R}(M) = L(M) \cdot [1 - P(M)]$.

10. ***Выбор следующих не рассмотренных значений.***

10.1. Переход к п. 5.3 и выбор следующего способа РУ $M(i, t)$. В случае рассмотрения всех значений переход к п. 10.2.

10.2. Переход к п. 5.2 и выбор следующего противника $t$. В случае рассмотрения всех значений переход к п. 11.

11. ***Нахождение риска и не риска для информации.***

Риск для информации – максимальный риск по всем способа РУ для этой информации:

$R(i) = \max_M R(M(i,t)) = R(M^{\max}(i))$, соответствует

способу РУ $M^{\max}(i)$, $M \in \{M_1, ..., M_{nm}\}$.

Не риск для информации (выгода от системы защиты) – величина не понесенного ущерба для способа РУ с максимальным риском для информации:

$\tilde{R}(i) = \tilde{R}(M^{\max}(i))$.

12. ***Переход к п. 5.1 и выбор не рассмотренной информации i. В случае рассмотрения всех значений переход к п. 13.***

13. ***Нахождение максимального и минимального риска для системы ИБ организации:***

$R^{\max} = \max_i R(i)$, что соответствует способу РУ $M^{\max}$;

$R^{\min} = \min_i R(i)$, что соответствует способу РУ $M^{\min}$; $i \in \{i_1, ..., i_{ni}\}$.

14. ***Вычисление оценки рентабельности системы ИБ:***

$$PRofit = \frac{K \cdot \sum_i \tilde{R}(i) + \sum_s I(s) - C}{C}, \text{ где}$$

$$C = \sum_s C(s) = \sum_s n(s) \cdot [Ci(s) + Cu(s)] \text{ , } s \in \{s_1, ..., s_{ns}\} \text{ , } i \in \{i_1, ..., i_{ni}\} .$$

$K$ – нормировочный коэффициент.

Коэффициент $K$ вводится для приведения значения суммарных не рисков в рамки максимально возможных потерь:

$$K = \frac{\max\limits_{M,i} L(M)}{\sum\limits_i L(M^{\max}(i))}$$, где

$\max\limits_{M,i} L(M)$ - максимально возможный ущерб от РУ для организации;

$\sum\limits_i L(M^{\max}(i))$ - максимальное значение для суммы не рисков $\sum\limits_i \tilde{R}(i)$.

15. ***Анализ результатов.***

15.1. Если получено, что *Profit* ≤ 0, затраты на систему защиты превышают выгоду от ее функционирования. Этот факт может инициировать уменьшение текущих затрат на поддержание ИБ организации. Выбирается средство защиты, соответствующее способу РУ с минимальным риском $R^{\min}$ ($M^{\min}$), процесс функционирования системы обеспечения ИБ организации без этого средства или снижение затрат на него (эксплуатационных расходов). Процедура повторяется с п. 5 до получения положительной рентабельности.

15.2. Если получено, что *Profit* > 0, можно попытаться повысить экономическую эффективность системы защиты. Для этого рассматривается способ РУ с максимальным риском $R^{\max}$ ($M^{\max}$) и моделируется введение нового средства защиты на его предотвращение. Процедура повторяется с п. 4.

Если значение рентабельности при этом увеличилось - затрата на использование этого средства принимается, если уменьшилось – отклоняется. Процедура повторяется до тех пор, пока суммарный (или

максимальный) риск не достигнет допустимого значения, установленного экспертом, а рентабельность при этом будет положительна. В случае использования показателя рентабельности как целевого критерия возможно проведение дальнейшего моделирования с целью повышения рентабельности при ограничении на риски.

Оценка параметров в п. 3, 4.4 процедуры проводится экспертом (группой экспертов) в денежных единицах. Для обработки экспертных оценок в работе использован метод групповой оценки объектов, описанный в литературе и адаптированный к специфике решаемой задачи. В рамках данного метода существует алгоритм вычисления коэффициентов компетентности экспертов.

1. В рамках метода осуществлен переход от абстрактных моделей потенциальных нарушителей к реальным выявленным противникам, что дает возможность оперативно реагировать и перестраивать систему защиты в зависимости от внешних условий.

2. В качестве исходных данных предложены параметры, которые могут быть оценены количественно, в денежных единицах. Их значения связаны с конкретными убытками и выгодой, которые несет сторона защиты и противник в случае атаки.

3. Защищаемая информация и противники, для которых параметры не могут быть оценены, не участвуют в рассмотрении. Это повышает достоверность исходных данных и, следовательно, результатов анализа.

4. Оценка вероятности реализации угрозы противником - рассчитываемый показатель. Исходными данными служат статистика инцидентов в области ИБ, оценка степени мотивировки противника на осуществление злонамеренных действий [12].

5. Введено понятие не риска как величины не понесенных потерь организации от действий противника за счет существующей системы ИБ. Показатель служит аналогом выгоды от системы ИБ.

6. В качестве оценки эффективности затрат на ИБ введен показатель рентабельности. Его значение чувствительно к изменению затрат и уровня рисков. Неотрицательное значение рентабельности говорит о «неубыточности» системы ИБ.

7. При использовании разработанного метода существует возможность повышения экономической эффективности системы защиты путем снижения определенных рисков за счет перераспределения затрат на ИБ адекватно текущей ситуации.

## 2.3. Алгоритмизация формирования автоматизированных средств анализа информационных рисков

Представлены результаты, позволяющие последовательно описать процесс формирования автоматизированных средств анализа информационных рисков с использованием опросных листов, средневзвешенных оценок и согласования мнений экспертов.

Рассмотрены следующие аспекты:

- формирование общей диаграммы потоков данных;
- алгоритм решения задачи в общем виде (блок-схема процесса);
- определение целей и порядка применения программного продукта;
- методика расчета рисков невыполнения требований;
- некоторые рекомендации по согласованию экспертных оценок.

*Диаграмма потоков данных*

В разработанной диаграмме потоков данных (Data flow diagram) обобщенная структура автоматизированного средства. Предлагаемая изображена на рис. 2.1.

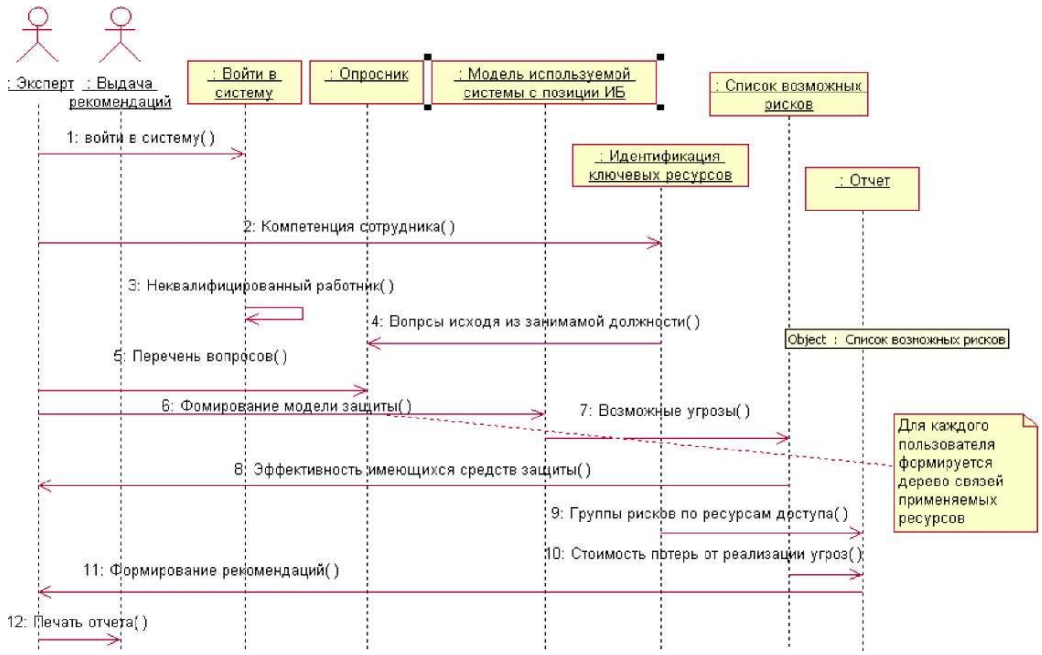


Рис. 2.1 Диаграмма последовательности этапов анализа информационных рисков

Первым этапом организации работ по формирования автоматизированного средства является подготовка и анализ руководящей документации, из которой формулируется требования к работе сотрудников и информационной системе и вытекающие рекомендации. На этом этапе формируются: опросное пространство, порядок перехода между вопросами, определение критичности признака для системы, составление квалификационных показателей [13].

Для подготовки данной информации были определены 11 ключевых элементов, которые имеют отношение к безопасности всей организации в различных условиях: политика безопасности, организация информационной безопасности, безопасность людских ресурсов, физическая безопасность и безопасность окружающей среды, управление коммуникациями и операциями, контроль доступа, приобретение, разработка и сопровождение информационной систем.

После формирования «опросников» проводится тестирование респондентов или сотрудников, работающих в анализируемой информационной системе.

Параллельно с процессом формирования «опросников» формируется шкала уровней риск. При этом решаются следующие вопросы: численное значение уровня риска, мероприятия необходимые для уменьшения величины значения риска.

Следующим этапом работы является определение организации и методики обработки данных опроса. На данном этапе необходимо определить процедуры и алгоритмы обработки полученных данных.

На этом этапе производится анализ результатов экспертного оценивания; составление отчета; представление итогов работы на утверждение; ознакомление с результатами должностных лиц.

*Определение целей использования*

На рис. 2.2 изображена UML - диаграмма, позволяющая наглядно представить возможные варианты использования разрабатываемого автоматизированного средства.

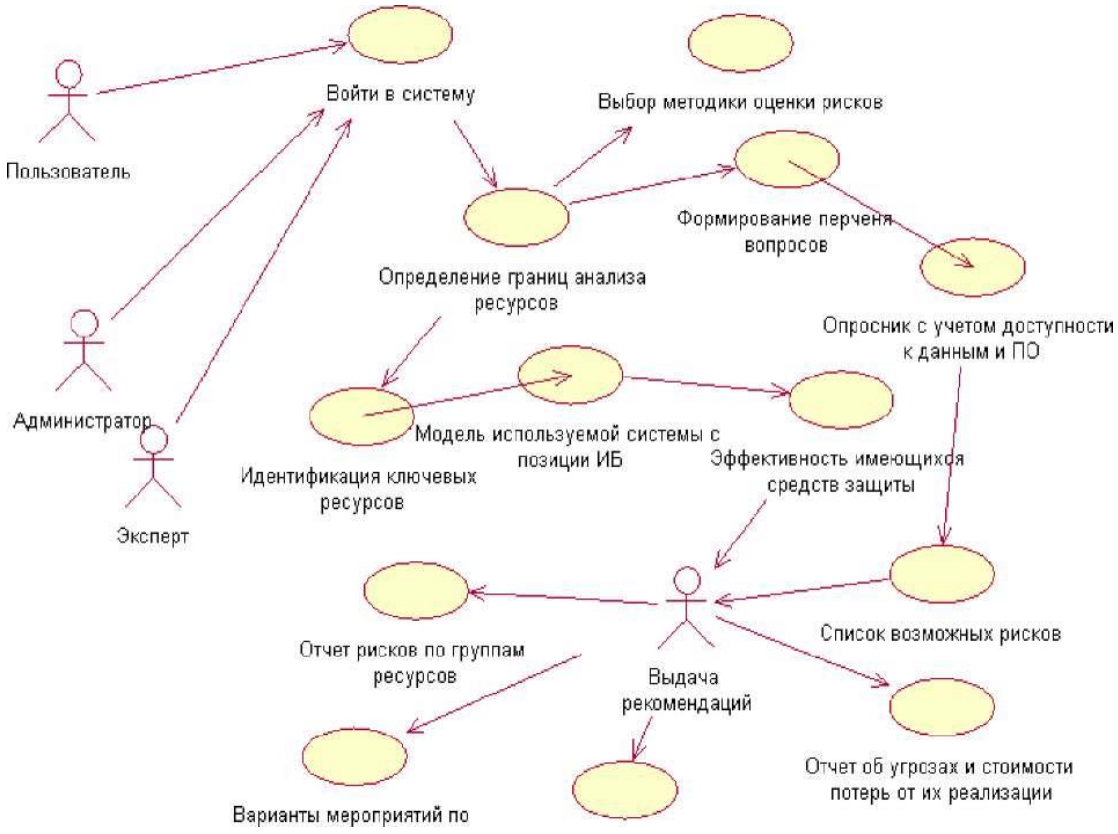


Рис.2.2 Диаграмма вариантов использования средства анализа информационных рисков

***Алгоритм решения задачи в общем виде***

Алгоритм решения задачи в общем виде представлен в виде блок-схемы рис.2.3.

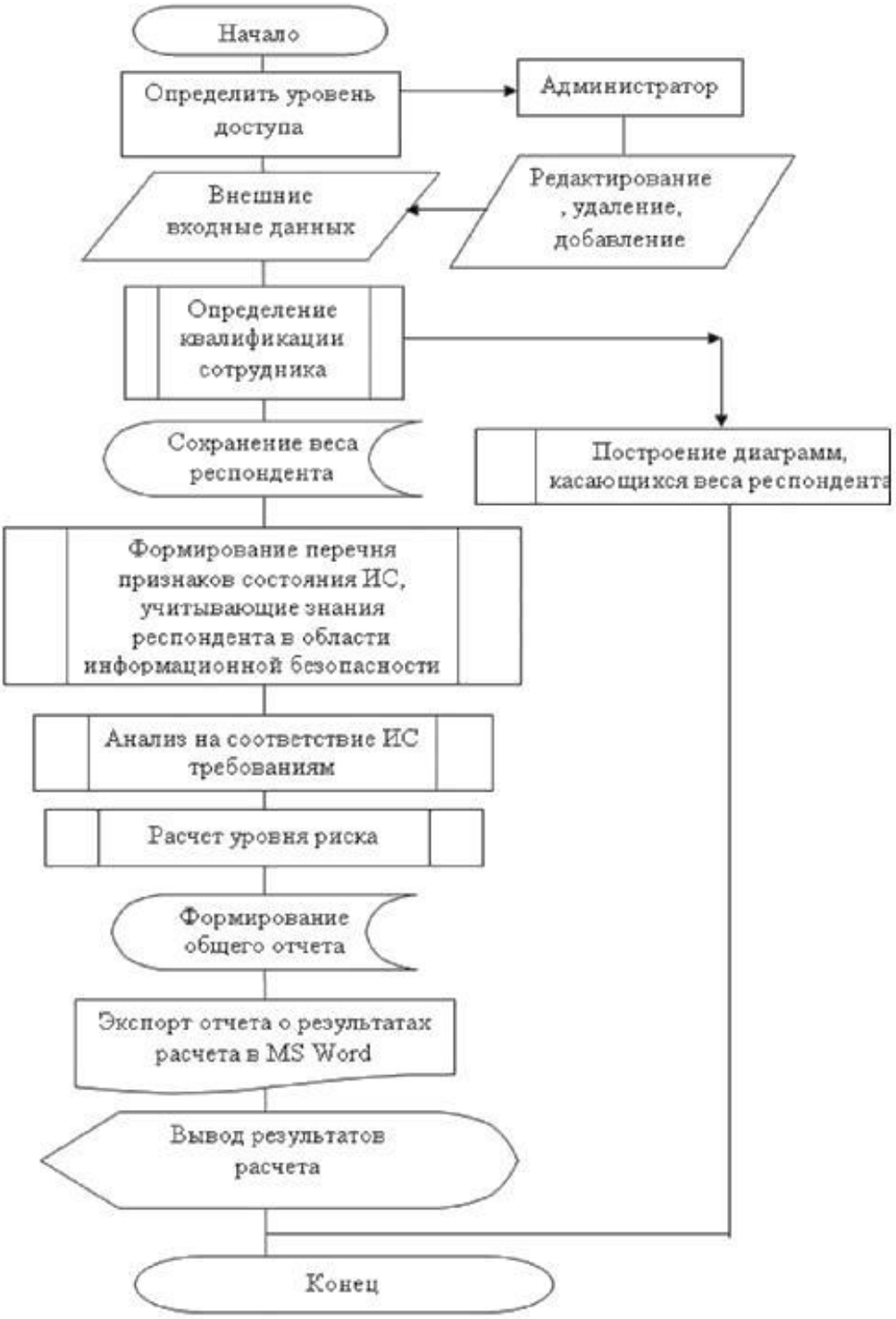


Рис. 2.3 Блок-схема решения задачи в общем виде

Предлагаемая блок-схема программного продукта «Автоматизированное средство базового экспертного анализа информационных рисков»:

- определяет слабые места в политике безопасности информационной системы;

- анализирует риск невыполнения каждого положения политики безопасности и ранжирует их по степени критичности;

- позволяет управлять рисками, возникающими в связи с невыполнением положений политики безопасности.

***Методика расчета рисков невыполнения требований***

Каждое требование стандартов имеет определенный вес.

Вес требования (Т) - степень влияния требования на защищенность информационной системы компании, указывается в значениях от 0 до 1. Вес требования, имеющий значение 1, показывает, что данное требование оказывает сильное влияние на обеспечение информационной безопасности компании [14].

Сумма весов всех требований $(T_{max}) -$ максимальный риск невыполнения требований стандартов, т.е. не выполнены все положения стандартов.

$$T_{max} = \sum_{i=1}^{n} T_i$$

где $T_{max} -$ сумма весов всех требований;

$T -$вес требования;

$n$ - всего требований;

Отношение суммы весов невыполненных в компании требований к сумме всех требований стандарта - риск невыполнения требований в компании (R).

$$R = \frac{\sum_{i=1}^{n} T_{\text{невып},i}}{T_{max}}$$

где $R$ −риск невыполнения требований $T_{\text{невып}}$ − вес невыполненного требования $n$ - количество невыполненных требований

Риск (R) невыполнения требований показывает, насколько значимы для информационной системы компании невыполненные требования. Риск зависит от количества невыполненных требований и их весов.

Для снижения риска несоответствия информационной системы стандартам советуется выполнить максимальное количество требований. Особенно важно выполнение требований, имеющих высокие веса, т.е. тех требований, чье влияние на уровень защищенности информационной системы компании значительно.

Задача определения ценностей требований по информационной безопасности, выделенных из стандартов, решилась путем применения сопоставления и ранжирования личностных и групповых мнений.

*Согласование экспертных оценок*

Поэтому для решения поставленной проблемы был использован алгоритм согласования экспертных оценок методом средневзвешенных коэффициентов (методом непосредственной оценки). Коротко применяемый алгоритм:

Пусть $m$ экспертов произвели оценку $n$ вопросов по $l$ требованиям. Результаты оценки представлены в виде величин $x_{ij}^{h}$, где $j$ - номер эксперта, $i$ - номер вопроса, $h$ – номер показателя (требования) сравнения, то величины $x_{ij}^{h}$ представляют собой числа из некоторого отрезка числовой оси, или баллы (доли).

Для получения групповой оценки объектов в этом случае можно (воспользоваться средним значением оценки для каждого объекта

$$X_i = \sum_{h=1}^{l} \sum_{j=1}^{m} q_h x_{ij}^{h} \, k_j (i = 1,2, \dots, n)$$

где $q_h$ – коэффициенты весов требований сравнения признаков, $k_j$ –коэффициенты компетентности экспертов. Коэффициенты весов требований и компетентности экспертов являются нормированными величинами

$$\sum_{h=1}^{l} q_h = 1; \sum_{j=1}^{m} k_i = 1$$

Коэффициенты весов показателей могут быть определены экспертным путем. Если $q_{hi}$ – коэффициент веса $h$ –го требования, даваемый $j$ –м экспертом, то средний коэффициент веса $h$ –го показателя по всем экспертам равен:

$$q_h = \sum_{j=1}^{m} q_{hj} k_j (h = 1,2, \dots, l)$$

Получение групповой экспертной оценки путем суммирования индивидуальных оценок с весами компетентности и важности показателей при измерении свойств объектов в кардинальных шкалах основывается на предположении о выполнении аксиом теории полезности фон Неймана-Моргенштерна как для индивидуальных, так и для групповой оценки и условий неразличимости объектов в групповом отношении, если они неразличимы во всех индивидуальных оценках (частичный принцип Парето). В реальных задачах эти условия, как правило, выполняются, поэтому получение групповой оценки объектов путем суммирования с весами индивидуальных оценок экспертов широко применяется на практике.

Коэффициенты компетентности экспертов можно вычислить по апостериорным данным, т. е. по результатам оценки требований. Основной идеей этого вычисления является предположение о том, что компетентность экспертов должна оцениваться по степени согласованности их оценок с групповой оценкой объектов.

Результатом является обобщенный алгоритм процесса проектирования программного средства или частично автоматизированной методики,

предназначенных для анализа информационных рисков с учетом требований нормативных документов.

## 2.4. Методика разработки оценивания рисков при обеспечении информационной безопасности

В настоящее время любая современная компания активно использует информационные технологии, а информация стала важнейшим объектом деловых отношений. В связи с этим не так давно возник новый класс рисков, присущих деятельности организаций и отличных от уже существовавших, — риски, связанные с угрозой нарушения информационной безопасности.

В основу современных стандартов в обеспечении целостности информации заложен подход, при котором производится управление рисками при их наличии. А чтобы управлять этими рисками, предприятию необходимо для начала выбрать методику, по которой рассчитывалась бы оценка рисков. И этот шаг, как правило, представляет сложность по тем или иным причинам. С одной стороны, не существует программного комплекса, который бы удовлетворял по всем параметрам, с другой — руководство организации зачастую не желает выделять на это достаточное количество времени и денег, так как не видит в этом практической пользы, а если и выделяет, то на выходе может получить нечто неприменимое к действительности.

Информационные технологии не стоят на месте, совершенствуются с каждым днём, из-за чего приходится повышать и качество управления рисками. Неизбежно устаревают одни методики, другие — возникают и совершенствуются, в связи с чем очень важно работать по максимально актуальной на данный момент. В результате на рынке программ оценивания рисков формируется лишь несколько лидеров, заслоняя собой редко обновляющиеся или неэффективные аналоги, а у самих методик появляются

отличия, на которых и основаны все достоинства и недостатки программных комплексов.

Так как вычислительная сеть используется на большом количестве предприятий, актуальность проблемы информационной безопасности велика. Рассмотрено и сравнено основные системы анализа информационных рисков.

OCTAVE. Название расшифровывается как «Operationally Critical Threat, Asset, and Vulnerability Evaluation», то есть «Оценка критичных угроз, активов и уязвимостей».

При работе с этой системой происходит активное участие владельцев информации в процессе определения наиболее незащищённых информационных массивов и наиболее вероятных рисков. Методология основана на последовательности специально организованных внутренних семинаров, а оценка рисков производится в три этапа, перед которыми предлагается согласовать график семинаров, распланировать действия участников и назначить им роли.

Первый этап заключается в разработке профилей угроз, соответствующих сети данной организации, а также законодательной базе. На втором этапе происходит анализ уязвимостей систем предприятия по отношению к угрозам, профили которых были составлены на первом этапе. И, наконец, третий этап включает в себя оценивание рисков информационной безопасности, заключающееся в установлении вероятности или степени причинения ущерба в случае осуществления угроз при действующих уязвимостях. По окончании производится принятие решений по обработке рисков.

Oracle Crystal Ball. Это приложение к Microsoft Excel для моделирования бизнес-процессов, установления рисков, прогнозирования неопределённых данных и оптимизации результатов. Методика позволяет использовать исторические данные по продажам, на основании чего может быть составлен прогноз. Использование моделирования по методу Монте

Карло даёт дополнительные возможности по оптимизации. Crystal Ball обеспечивает возможность моделирования и имитации для осуществления «What-If» анализа. Немаловажным преимуществом является простота в использовании и наглядность выходных данных.

CRAMM. Был разработан в 1985 году в Великобритании Центральным агентством по компьютерам и телекоммуникациям (CCTA) и является одной из первых методик оценки рисков в рамках информационный безопасности. Название расшифровывается как CCTA Risk Analysis & Management Method.

Программное обеспечение является настраиваемым для различных сфер деятельности с использованием встроенных профилей: коммерческий, гражданское государственное учреждение, финансовый сектор и прочее. При анализе рисков происходит идентификация и вычисление уровней рисков на основе оценок, которые были присвоены элементам модели угроз. На выходе получается профиль контрмер, благодаря которому производится контроль рисков [15].

Исследование безопасности информации проводится в четыре этапа: идентификация и оценка ресурсов, оценивание угроз и уязвимостей, анализ рисков и управление рисками.


Рис.2.4 Управление рисками в методике CRAMM осуществляется в несколько этапов

CORAS. Разработано в рамках программы Information Society Technologies. Основывается на адаптации, уточнении и комбинировании следующих методов анализа рисков: цепи Маркова, FMECA, Event-Tree-Analysis и HazOp. В системе используется технология UML, а базируется она

на австралийском/новозеландском стандарте AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799–1: 2000 Code of Practice for Information Security Management.

В данной методологии информационные системы представлены как сложный комплекс с учётом человеческого фактора, а не только на основе используемых технологий. Правила методологии реализованы в виде Java- и Windows-приложений.

Risk Watch. Разрабатывается одноимённой американской компанией и включает средства, как для информационной безопасности, так и для физических методов защиты. В качестве критериев оценки используются оценка возврата от инвестиций и предсказание годовых потерь.

Методика состоит из четырёх этапов. На первом определяют предмет исследования, то есть состав системы в общих чертах, элементы можно выбрать уже из заготовленного списка. На втором этапе вводят данные, подробно описывают ресурсы сети, отвечают на вопросы для выявления уязвимостей. На третьем этапе рассчитывается профиль рисков, выбираются меры по обеспечению безопасности, для чего устанавливают связи между ресурсами, вводят количественную оценку. На четвёртом этапе генерируется отчёт.

ГРИФ. Анализируется уровень защиты всех ресурсов организации, оценивается возможный ущерб, предоставляется возможность выбора контрмер для обеспечения эффективного управления рисками. Проведение полного анализа происходит в несколько этапов, на которых менеджеру предлагается ввести список ресурсов компании, виды информации, ущерб по каждой группе информации, доступ пользователей к ресурсам, средства защиты и ответить на ряд вопросов, предложенных системой. Несмотря на сложность внутренних алгоритмов, программа проста в использовании, и на выходе предлагается наглядный и полный отчёт.

Рассмотренные лидирующие методологии позволяют достаточно ёмко оценить весь ассортимент предлагаемых средств оценки рисков в информационном поле по причине их повсеместного использования. Все они хорошо справляются с оценкой и управлением рисков, но имеют свои недостатки, связанные с мониторингом. Ни в одной системе не предполагается расчёт оптимального баланса способов управления, не производится обработка остаточных рисков, не даётся указаний по дальнейшим анализам рисков в сети, не учитывается непостоянство факторов риска.

Критерию «Простота использования» не соответствуют лишь CRAMM и Risk Watch, для успешной и продуктивной работы с которыми необходимо обучение либо привлечение экспертов. К тому же CRAMM предполагает большие сроки для анализа. Остальные рассмотренные комплексы данных проблем не проявляют, а Crystal Ball даже слишком прост в использовании.

Методология OCTAVE является гибкой, организации могут использовать ряд критериев для «заточки» программы под свои нужды. Также данный комплекс может нести информативную функцию благодаря встроенной программе повышения квалификации сотрудников. OCTAVE не использует количественную оценку рисков, но качественная оценка довольно легко описывает количественное отношение.

Очень важным должно являться наличие «What-If» анализа, то есть оценки ситуации при использовании профиля защиты. Это позволяет предприятию заглянуть вперёд и оценить возможные выгоды при использовании специальных средств и действий по защите информации. Такую оценку дают лишь Crystal Ball и Risk Watch.

В методологии CRAMM отсутствуют: интеграция способов управления и описания назначения этих способов; перерасчёт максимально допустимых величин рисков; реагирование на инциденты. При работе с рисками CRAMM

использует только методы их снижения, а такие способы управления рисками, как «обход» или «принятие», не затрагиваются [16].

Одним из преимуществ для предприятий с ограниченными финансовыми возможностями является бесплатность использования. Таким могут похвастаться CORAS и OCTAVE, первый из которых не требует значительных ресурсов при применении.

В отличие от CRAMM программа Risk Watch более ориентирована на количественную оценку. С недавних пор она имеет русскую локализацию, что является несомненным плюсом на российском рынке. Risk Watch позволяет производить анализ только на программно-техническом уровне, но не учитывает административных факторов, а значит, получаемая оценка не является полной и не учитывает комплексный подход к безопасности.

Программный комплекс ГРИФ является сильной отечественной разработкой, что выглядит преимуществом для русскоязычных компаний. Но в этой методологии отсутствует возможность сравнения отчётов на различных стадиях внедрения мер по обеспечению защищённости.

Если требуется оценить риски одноразово, то уместно применить методологию CORAS, а в случае периодического использования целесообразнее система CRAMM. OCTAVE будет актуальной в крупных организациях, где постоянная оценка рисков является неотъемлемой частью работы. По целому ряду критериев невозможно установить превосходство того или иного средства оценки рисков, но каждое предприятие определяет для себя приоритетные направления, по которым и выбирает методику. В идеале необходимо получить не только удовлетворительные результаты оценивания, но и удобный в использовании программный комплекс, который бы являлся инструментом при таком оценивании. Естественно желание получить ясные результаты исследования, а также рекомендации по снижению рисков. Инструмент обязан проследить связь между рисками и

причинами, приводящими к этим рискам. Именно этим требованиям наиболее удовлетворяет OCTAVE.

Описанные программы достаточно популярны среди организаций, причиной чего может быть назван целый ряд достоинств каждой методологии, но даже несмотря на это, невозможно выделить какую-то одну из них. Это можно объяснить тем, что достоинства каждой программы выделяются по совершенно разным критериям, и каждая организация выбирает средство под свои нужды. Но это же говорит и о том, что у каждого комплекса есть и свои недостатки. Поэтому проблема актуальна до сих пор: нет универсальной методологии, которая бы решила все нужды. А наличие таковой важно, так как до сих пор некоторые руководители не понимают важность работ по оценке рисков в их сетях, в том числе и по причине неполного совершенства фигурируем на рынке программ.

Сравнительные характеристики основных систем анализа рисков Таблица 2.4

| Критерий | OCTAVE | Oracle Crystal Ball | CRAMM | CORAS | Risk Watch | ГРИФ |
|---|---|---|---|---|---|---|
| Общие характеристики | | | | | | |
| Рассчитанность на организации разного размера и область деятельности | + | + | + | + | + | + |
| Автоматизация «What-if» | - | + | - | ? | + | ? |
| Удобство восприятия графиков и отчетов | + | + | - | + | - | + |
| Простота использования | + | + | - | + | - | + |
| Бесплатное использование | + | - | - | + | - | - |
| Поддержка | + | + | + | + | + | + |
| Количественная оценка | - | ? | + | + | + | + |
| Качественная оценка | + | ? | + | + | - | + |

| | | | | | | |
|---|---|---|---|---|---|---|
| Русская локализация | ? | - | - | ? | + | + |
| Повышение информированности сотрудников | + | ? | - | - | - | ? |
| Пригодность к регулярному использованию | + | ? | + | - | ? | ? |
| Использование независимой оценки | - | ? | + | + | ? | + |
| Входные данные | | | | | | |
| Ресурсы | + | + | + | + | + | + |
| Тип информационной системы | + | - | + | ? | + | - |
| Ценность ресурсов | + | ? | + | + | + | + |
| Угрозы | + | + | + | + | + | + |
| Уязвимости системы | + | + | + | + | + | + |
| Выбор контрмер | - | - | + | ? | + | + |
| Базовые требования в области безопасности | - | - | - | ? | + | - |
| Потери | - | - | - | ? | + | - |
| Меры защиты | + | - | + | - | + | - |
| Частота возникновения угроз | - | - | - | ? | + | - |
| Сетевое оборудование | + | - | - | ? | - | + |
| Виды информации | ? | - | - | ? | - | + |
| Группы пользователей | - | - | - | ? | - | + |
| Средства защиты | + | - | - | ? | - | + |

А также рассмотрен исходный состав системы защиты ИВС от спама и вирусов, а также 6 его комбинаций. Результаты представлены в таблице 2.5. Числовые значения параметров (кроме рентабельности) даны в руб. из расчета на месяц.

Результаты анализа рисков по спаму и вирусам. Таблица 2.5.

| Вариант | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Угроза | Параметры | Spam-Assassin Sophos Symantec | Spam-Assassin Sophos | Spam-Assassin Symantec | Spam-Assassin | Sophos Symantec | Sophos | Symantec |
| Спам с пометкой | $P(M_1)$ | 6,13 % | 6,13 % | 6,13 % | 6,13 % | 0 % | 0 % | 0 % |
| | $L(M_1)$ | 25000 | 25000 | 25000 | 25000 | 25000 | 25000 | 25000 |
| | $R(M_1)$ | 1533 | 1533 | 1533 | 1533 | 0 | 0 | 0 |
| | $R□(M_1)$ | 23466 | 23466 | 23466 | 23466 | 25000 | 25000 | 25000 |
| Спам без пометки | $P(M_2)$ | 5,73 % | 5,73 % | 5,73 % | 5,73 % | 100 % | 100 % | 100 % |
| | $L(M_2)$ | 25000 | 25000 | 25000 | 25000 | 25000 | 25000 | 25000 |
| | $R(M_2)$ | 1434 | 1434 | 1434 | 1434 | 25000 | 25000 | 25000 |
| | $R□(M_2)$ | 23565 | 23565 | 23565 | 23565 | 0 | 0 | 0 |
| Вирус | $P(M_3)$ | 2,55 % | 10,5 % | 44,5 % | 53 % | 2,55 % | 10,5 % | 44,5 % |
| | $L(M_3)$ | 1590 | 1590 | 1590 | 1590 | 1590 | 1590 | 1590 |
| | $R(M_3)$ | 40,5 | 167,1 | 708 | 843 | 40,5 | 167,1 | 708 |
| | $R□(M_3)$ | 1551 | 1422 | 882 | 747 | 1551 | 1422 | 882 |
| Стоимость ср-в защиты $C$ | | 1473 | 1148 | 375,3 | 52,2 | 1419 | 1096 | 323,1 |
| Рентабельность *Profit* | | 0,052 | 0,24 | 1,35 | 13,3 | -1 | -1 | -1 |

Получено, что исследуемый вариант системы защиты имеет минимальные риски и вероятность реализации угрозы по двум угрозам, минимальные суммарные риски, максимальная стоимость системы ИБ. При этом рентабельность положительна. Это говорит о том, что затраты на защиту оправданы. Другие варианты отличаются большими рисками, что недопустимо, а также отрицательной рентабельностью [17].

Надежность защиты (уменьшение вероятностей и суммарных рисков) может быть повышена путем усиления антивирусной защиты и добавления дополнительных элементов для фильтрации спама. При планировании ввода дополнительных средств защиты нельзя забывать об экономической эффективности таких денежных вложений. Следует изначально спроектировать изменения, описать их с использованием разработанной инструментальной системы, просчитать для предполагаемой конфигурации оценки вероятностей реализации угроз, рисков, рентабельности, и после этого обоснованно принимать решения по управлению конфигурацией системой безопасности.

Оценки уровня защищенности, а также рекомендации по усилению защиты ИВС, полученные по результатам анализа с использованием разработанного метода анализа и управления рисками, согласуются с экспертными оценками специалистов ИВС.

Для иллюстрации работы метода при анализе рисков по конкретным противникам было проведено их моделирование для МЭИ как организации. Были описаны противники: хакерская группа «Мошенники», целью которой является фальсификация электронных платежей института, и фирма «Разработка», заинтересованная в краже коммерческих разработок МЭИ. Пример полной характеристики противника по угрозам представлен в таблице 2.6.

Характеристика противника «Мошенники» Таблица 2.6.

| **Характеристика** | **Описание** | **Обозначение** |
|---|---|---|
| Название | Хакерская группа «Мошенники» | $t_3$ |
| Информация | Электронные счета, электронные переводы | $i_2$ |
| Требования | Целостность, доступности информации | |

| | | |
|---|---|---|
| Носители информации, ресурсы: | 1. *Персонал*:<br>1) Администратор бухгалтерии<br>2) Сотрудники бухгалтерии (4 человека)<br>3) Субъект защиты<br>2. *Технические средства:*<br>1) Сервер 1 бухгалтерии<br>2) Рабочие станции сотрудников<br>3) Линии связи локальной ВС бухгалтерии<br>4) Открытый канал связи «МЭИ– банк». | <br>$r_3$<br>$r_4$<br>$r_5$<br><br>$r_6$<br>$r_7$<br>$r_8$<br>$r_9$ |
| Способы получения доступа противника к информации | 1 *Персонал.*<br>1.1 Посредством неформальных контактов с персоналом ($r_3$, $r_4$, $r_5$) – действие $d_6$.<br>1.2 Подкуп персонала ($r_3$, $r_4$, $r_5$) – действие $d_7$.<br>2 *Технические средства.*<br>2.1 НСД к инф-ии в ЛВС из Internet с целью несанкционированной модификации или уничтожения ($r_6$, $r_7$) – действие $d_8$.<br>2.2 Перехват инф-ии, передаваемой по открытым каналам связи с целью модификации, уничтожения, фальсификация в каналах связи ($r_8$, $r_9$) - действие $d_9$.<br>2.3 Использование штатных средств ЛВС для модификации, уничтожения, фальсификация инф-ии (незаблокированных станций, визуально, при помощи подбора паролей и др.) ($r_6$, $r_7$) - действие $d_{10}$. | <br>$Ma(r_3, d_6)$<br>$Ma(r_4, d_6)$<br>$Ma(r_5, d_6)$<br>$Ma(r_3, d_7)$<br>$Ma(r_4, d_7)$<br>$Ma(r_5, d_7)$<br>$Ma(r_6, d_8)$<br>$Ma(r_7, d_8)$<br>$Ma(r_8, d_9)$<br>$Ma(r_9, d_9)$<br>$Ma(r_6,d_{10})$<br>$Ma(r_7,d_{10})$ |
| Способы ИИ | Перевод денег на собственные счета - действие $d_{11}$. | $Mr(i_2, d_{11})$ |

# 3. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

## 3.1. Искусственное освещение производственных помещений

Свет является одним из важнейших условий существования человека. Он влияет на состояние организма человека, правильно организованное освещение стимулирует протекание процессов высшей нервной деятельности и повышает работоспособность. При недостаточном освещении человек работает менее продуктивно, быстро устаёт, растёт вероятность ошибочных действий, что может привести к травматизму. 5% травм может быть причиной профессионального заболевания - рабочая миопия (близорукость). В зависимости от длины волны свет оказывает возбуждающее (оранжево-красный) или успокаивающее (жёлто-зелёный) действие. Спектральный состав света влияет на производительность труда. Если при естественном освещении принять за 100%, то при красном и оранжевом освещении она составляет 76%. При полностью или частичном лишении естественного света - световое голодание.

Освещение рабочих помещений должно удовлетворять следующим условиям:

Уровень освещённости рабочих поверхностей должен соответствовать гигиеническим нормам для данного вида работы.

Равномерность и устойчивость уровня освещённости в помещении, отсутствие резких контрастов.

Не должно создаваться источниками света блеска в поле зрения.

Искусственный свет по спектральному составу должен приближаться к естественному.

*Искусственное освещение*

На предприятиях связи для освещения производственных помещений применяются две системы искусственного освещения:

- общее освещение с равномерным (симметричным) или локализованным размещением светильников;

-комбинированное освещение, представляющее одновременное использование общего и местного освещения.

Местное освещение может быть стационарным и переносным. Применение одного местного освещения в условиях производства не допускается, т.к. освещённости рабочего места и окружающего пространства сильно различаются [18]. В результате создаются неблагоприятные условия для работы, увеличивается опасность производственного травматизма, снижается производительность труда. Применение одного местного освещения разрешается только для периодических работ с переносными лампами.

Общее освещение используется при небольших уровнях нормированной освещённости (50 лк и ниже) там, где по условиям работы не требуется повышенной освещённости рабочих мест, а также, где местное освещение невозможно по условиям производства (механические сотрясения).

Для создания высокой освещённости рабочих мест без использования местного освещения применяется освещение с локализованным размещением светильников. Такая система позволяет направлять больше света на рабочие места и экономично освещать большие пространства производственных помещений.

Комбинированное освещение применяется в тех случаях, когда необходимо создать на рабочих местах высокие уровни освещённости. Применение местного освещения наряду с общим освещением даёт возможность работнику направлять световой поток от местного светильника в пустом направлении. При необходимости местное освещение отключается. Система комбинированного освещения получила широкое распространение.

По назначению электрическое освещение разделяют на рабочее, аварийное, ремонтное, охранное. Санитарными нормами нормируются только рабочее и аварийное освещение.

Искусственное освещение осуществляется электрическими источниками света, которые основаны на применении теплового излучения - электрические лампы накаливания, или на принципе люминесцентного излучения - ртутные, натриевые и люминесцентные лампы. В лампах накаливания энергия расходуется в основном на излучение тепла (80%) и лишь 10% на излучение в видимой части спектра. Основные характеристики ламп накаливания: номинальное напряжение, мощность, световой поток, световая отдача и срок службы. Источником света является нить из вольфрама. Лампы накаливания малой мощности (до 60 Вт) изготавливают вакуумными, большой мощности - газо-полными. Колба лампы наполняется нейтральным газом аргоном, либо азотом; в новых типах ламп криптоном или ксеноном, нить накала двойная или зигзагообразная, либо двойная спираль. Средняя продолжительность горения нормальных ламп накаливания по действующему стандарту до 1000 часов. Световая отдача лампы не превышает 20 лм/Вт электроды в виде вольфрамовых биспиралей. Внутри лампы смесь паров ртути и аргона.

Прохождение электрического тока через смесь сопровождается испусканием ультрафиолетовых невидимых глазом лучей, вызывающих свечение люминофора. Таким образом, энергия сначала превращается в ультрафиолетовые лучи, затем с помощью люминофора в видимый свет. Применяя различные люминофоры (вольфро-маты магния и кальция, силикат цинка, борат кадмия и др. материалы) можно придавать лампам различную цветность. Трубчатые люминесцентные лампы - это ртутные лампы низкого давления.

Преимущество люминесцентных ламп: большая световая отдача (750 лм/Вт), продолжительный срок службы (10000 часов), более экономичны по

расходу электроэнергии, обладают небольшой яркостью и поэтому не оказывают слепящего действия на глаза, лучший спектральный состав.

Недостатки трубчатых люминесцентных ламп: для зажигания и стабилизации режима горения необходима специальная пускорегулирующая аппаратура, что усложняет их эксплуатацию и снижает КПД. Освещение от люминесцентной лампы может вызывать стробоскопический эффект, заключающийся в том, что из-за отсутствия тепловой инерции освещенные лампой вращающиеся части машин могут казаться неподвижными или множественными. Этот эффект можно снизить включением соседних ламп в различные фазы сети переменного тока.

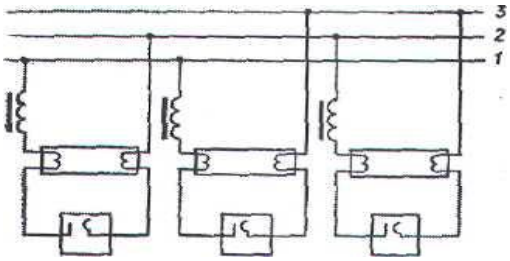


Рис 3.1 Схемы включения люминесцентных ламп в сеть трехфазного тока.

На рис.3.1 приведена схема включения люминесцентных ламп в сеть переменного тока с f = 50 Гц. Как и все лампы газового разряда, люминесцентные лампы включаются в сеть только последовательно со специальным дросселем.

Основным недостатком трубчатых люминесцентных ламп является большая чувствительность к изменению температуры окружающей среды.

Световым прибором принято называть устройство, состоящие из источника света (лампы) и осветительной арматуры. Различают две группы осветительных приборов: ближнего действия - светильники и дальнего действия - прожекторы.

Светильники, в зависимости от светораспределения, разделяют на три класса:

- прямого света - не менее 90% всего светлого потока излучается в нижнюю полусферу;

- отражённого света - не менее 90% всего светового потока излучается в верхнюю полусферу;

- рассеянного света - световой поток распределён по обеим полусферам так, что в одну из них излучается более 10%, в другую не менее 90%.

$$\eta = \frac{F_{СВ}}{F_{л}}$$

КПД светильников лучших образцов составляет свыше 0,8. Защитный угол светильника определяет степень защиты глаза от воздействия ярких частей лампы.

Величина защитного угла определяется по формуле

$$tg\,\gamma = \frac{h}{R + r}$$

где:

h - расстояние от тела накала лампы до уровня выходного отверстия светильника, мм;

г - радиус выходного тела накала, мм;

R - радиус выходного отверстия светильника, мм;

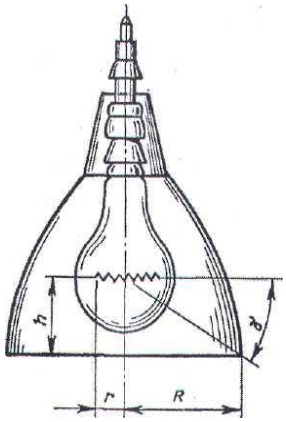


Рис. 3.2 Защитный угол светильника

В зависимости от величины защитного угла нормируют высоту подвеса светильника, исходя из требований ограничения слепящего действия. Чем больше защитный угол, тем меньше слепящее действие светильника.

Оптимальным является защитный угол от 10 до 30°. Светильники с лампами мощностью более 200 вт должны подвешиваться на высоте не менее 3 м от уровня пола. При защитном угле меньше 10° высота подвеса должна быть соответственно не менее 4 м.

Расположение светильников общего освещения должно быть, более равномерным. При высоте подвеса светильника над рабочей поверхностью $H_P$ рекомендуется выбирать расстояние между двумя последовательно расположенными светильниками, равное (1,5-2) Н.

Аварийное освещение должно быть предусмотрено в помещениях и на открытых пространствах в тех случаях, когда оно необходимо для продолжения работы или для эвакуации людей при внезапном отключении рабочего освещения. Аварийное освещение для продолжения работы должно обеспечивать на рабочих поверхностях, требующих обслуживания при аварийном режиме, освещённость не менее 20% от норм, установленных для рабочего освещения этих поверхностей при системе одного общего освещения лампами накаливания.

Аварийное освещение включается автоматически и функционирует одновременно с рабочим освещением от сети переменного тока, а при аварии внешней сети автоматически переключается на питание от аккумуляторной батареи или резервных электростанций предприятий связи.

Аварийное освещение для эвакуации людей разрешается включать вручную. Освещённость по линиям основных проходов на уровне пола и на ступеньках лестниц должна быть не менее 0,3 лк, а на открытых пространствах - не менее 0,2 лк. Выходные двери помещений общественного назначения, где могут находиться одновременно более 50 человек, должны иметь световые указатели «Выход».

Для аварийного освещения применяются светильники, отличающиеся от светильников рабочего освещения типом или размером или же тем, что на них нанесены специальные знаки. Освещение антенных полей и сигнальное

освещение радиомачт (СОМ) выполняется в соответствии с требованиями специальной инструкции.

### 3.2. Пожарная безопасность

Степень огнестойкости зданий принимается в зависимости от их назначения, категории по взрывопожарной и пожарной опасности, этажности, площади этажа в пределах пожарного отсека.

Здание, в котором находится лаборатория по пожарной опасности строительных конструкций относится к категории К1 (малопожароопасное), поскольку здесь присутствуют горючие (книги, документы, мебель, оргтехника и т.д.) и трудносгораемые вещества (сейфы, различное оборудование и т.д.), которые при взаимодействии с огнем могут гореть без взрыва.

По конструктивным характеристикам здание можно отнести к зданиям с несущими и ограждающими конструкциями из естественных или искусственных каменных материалов, бетона или железобетона, где для перекрытий допускается использование деревянных конструкций, защищенных штукатуркой или трудногорючими листовыми, а также плитными материалами.

Следовательно, степень огнестойкости здания можно определить как третью (III).

Помещение лаборатории по функциональной пожарной опасности относится к классу Ф 4.2 – высшие учебные заведения, учреждения повышения квалификации.

*Причины возникновения пожара*

Пожар в лаборатории, может привести к очень неблагоприятным последствиям (потеря ценной информации, порча имущества, гибель людей и т.д.), поэтому необходимо: выявить и устранить все причины возникновения пожара; разработать план мер по ликвидации пожара в здании; план эвакуации людей из здания.

Причинами возникновения пожара могут быть:

неисправности электропроводки, розеток и выключателей которые могут привести к короткому замыканию или пробою изоляции;

использование поврежденных (неисправных) электроприборов;

использование в помещении электронагревательных приборов с открытыми нагревательными элементами;

возникновение пожара вследствие попадания молнии в здание;

возгорание здания вследствие внешних воздействий;

неаккуратное обращение с огнем и несоблюдение мер пожарной безопасности.

*Профилактика пожара*

Пожарная профилактика представляет собой комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, на предотвращении пожара, ограничение его распространения, а также создание условий для успешного тушения пожара. Для профилактики пожара чрезвычайно важна правильная оценка пожаро опасности здания, определение опасных факторов и обоснование способов и средств пожаро предупреждения и защиты [19].

Одно из условий обеспечения пожаробезопасности - ликвидация возможных источников воспламенения.

В лаборатории источниками воспламенения могут быть:

1. неисправное электрооборудование, неисправности в электропроводке, электрических розетках и выключателях. Для исключения возникновения пожара по этим причинам необходимо вовремя выявлять и устранять неисправности, проводить плановый осмотр и своевременно устранять все неисправности;
2. неисправные электроприборы. Необходимые меры для исключения пожара включают в себя своевременный ремонт электроприборов,

качественное исправление поломок, не использование неисправных электроприборов;

3. обогревание помещения электронагревательными приборами с открытыми нагревательными элементами. Открытые нагревательные поверхности могут привести к пожару, так как в помещении находятся бумажные документы и справочная литература в виде книг, пособий, а бумага – легковоспламеняющийся предмет. В целях профилактики пожара предлагаю не использовать открытые обогревательные приборы в помещении лаборатории;

4. попадание в здание молнии. В летний период во время грозы возможно попадание молнии вследствие чего возможен пожар. Во избежание этого я рекомендую установить на крыше здания молниеотвод;

5. несоблюдение мер пожарной безопасности и курение в помещении также может привести к пожару. Для устранения возгорания в результате курения в помещении лаборатории предлагаю категорически запретить курение, а разрешить только в строго отведенном для этого месте.

В целях предотвращения пожара предлагаю проводить с инженерами, работающими в лаборатории, противопожарный инструктаж, на котором ознакомить работников с правилами противопожарной безопасности, а также обучить использованию первичных средств пожаротушения.

В случае возникновения пожара необходимо отключить электропитание, вызвать по телефону пожарную команду, эвакуировать людей из помещения согласно плану эвакуации. При наличии небольшого очага пламени можно воспользоваться подручными средствами с целью прекращения доступа воздуха к объекту возгорания.

## Заключение

Основные результаты выпускной квалификационной работы могут быть сформулированы в следующем виде:

1. Приведены классификации и анализа угроз конфиденциальной информации.
2. Описаны виды систем анализа информационных рисков в системе защиты информации.
3. Проанализированы вопросы анализа рисков и управления ими.
4. Введен многофакторный анализ рисков информационной безопасности.
5. Исследована методология матричного подхода анализ рисков.
6. Построены алгоритмы математической модели управления рисков от внешних угроз и алгоритмизация формирования автоматизированных средств анализа информационных рисков.
7. Анализирована алгоритмизация формирования автоматизированных средств анализа информационных рисков.
8. Описаны методика разработки оценивания рисков, обеспечивающего безопасности информации в четыре этапа: идентификация и оценка ресурсов, оценивание угроз и уязвимостей, анализ рисков и управление рисками.

## Использованные литературы


1. Постановление Президента Республики Узбекистан "О дополнительных мерах по дальнейшему развитию информационно-коммуникационных технологий". от 21 марта 2012 года, ПП – 1730.

2. Петренко С. А., Симонов С. В. Управление информационными рисками [Текст]. // Экономически оправданная безопасность. — М.: Компания АйТи; ДМК Пресс, 2011. — 384 с.

3.Степанов, Е. А. Информационная безопасность и защита информации [Текст] : учебное пособие / Е. А. Степанов, И. К. Корнеев. – М. : Инфра-М, 2001. – 304 с.: – ил. – 2010 экз. – ISBN: 5-16-000491-2.

4. Глущенко В.В. «Управление рисками. Страхование» -М.,1999 г.

5. Ярочкин, В. И. Информационная безопасность [Текст] : учебник для студентов вузов / В. И. Ярочник. – М. : Академический проект, 2004. – 544 с.: – ил. – 3000 экз. – ISBN: 5-8291-0408-3.

6. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования : автореф. дис. канд. техн. наук. – Уфа, 2008. – 17 с.

7. Кустов Г.А. Управление информационными рисками организации на основе логико-вероятностного метода: автореф. дис. ... канд. тех. наук. – Уфа, 2008. – 18 с.

8. Васильева Т. Н., Львова А. В., Хорьков С. Н. Применение оценок рисков при защите от реальный угроз информационной безопасности. // Современные технологии в задачах управления, автоматики и обработки информации: труды XVII Международного научно-технического семинара. Алушта, сентябрь 2008 г. - СПб.: ГУАП, 2008.

9. Бородюк В. П., Львова А. В. Методика определения оптимального уровня защиты информационной системы по критерию рентабельности // Труды XIV Международной конференции «Информационные средства и технологии». М.: МЭИ, 2009.

10. Терновая Н. Информация под защитой. // Финанс., №44, 2010.

11. Пастоев. А. Методологии управления ИТ-рисками [Электронный ресурс]. — Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami, свободный. — Язык русский.

12. Максимов, Ю. Н. Технические методы и средства защиты информации [Текст] : учебное пособие / Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров. – СПб : Полигон, 2000. – 314 с.: – ил. – 2000 экз. – ISBN: 5-89173-096-0.

13. Мельников В. В. Безопасность информации в автоматизированных системах [Текст] : учебное пособие / В. В. Мельников. – М. : Финансы и статистика, 2009. – 368 с.: – ил. – 4000 экз. – ISBN: 5-279-02560-7.

14. Мельников В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – М. : Академия, 2010. – 336 с.: – ил. – 2500 экз. – ISBN: 978-5-7695-4884-0.

15. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] : учебное пособие / Ю. В. Романец, П. А. Тимофеев, В. Ф Шаньгин. – М. : Радио и связь, 2001. – 304 с.: – ил. – 3000 экз. – ISBN: 5-256-01518-4.

16. www.bdm.ru материалы WEB-сайта.

17. www.citforum.ru материалы WEB-сайта.

18. ВишняковЯ.Д., Вагин В.И., Овчинников В.В., Стародубец А.Н. Безопасность жизнедеятельности. Защита населения и территорий в чрезвычайных ситуациях. Уч. Пособие. Москва. 2007.

19.Безопасность жизнедеятельности. Учебник для ВУЗов. С.В. Белов, А.В. Ипьницкая, А.Ф. Козьяков и др. Под общей ред. С.В. Белова. М. Высшая школа. 1999 г.