ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

А.А. ВАРФОЛОМЕЕВ

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Учебное пособие

Москва
2008

Инновационная образовательная программа
Российского университета дружбы народов

«Создание комплекса инновационных образовательных программ и формирование инновационной образовательной среды, позволяющих эффективно реализовывать государственные интересы РФ через систему экспорта образовательных услуг»

Экспертное заключение –

кандидат технических наук, доцент МИФИ *С.В. Запечников*

Варфоломеев А.А.

Управление информационными рисками: Учеб. пособие. – М.: РУДН, 2008. – 158 с.: ил.

В пособии рассматриваются основные понятия и методы управления информационными рисками. При этом основу составляют положения современных принятых и разрабатываемых стандартов, в частности, в области информационной безопасности. Большое внимание уделено технологии управления информационными рисками.

Данная книга существенно дополняет материал пособия и курса «Основы информационной безопасности».

Учебное пособие выполнено в рамках инновационной образовательной программы Российского университета дружбы народов, направление «Комплекс экспортоориентированных инновационных образовательных программ по приоритетным направлениям науки и технологий», и входит в состав учебно-методического комплекса, включающего описание курса, программу и электронный учебник.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Требования по управлению информационными рисками содержатся во многих международных и отечественных регламентирующих документах и обоснованы существующей практикой развития информационных технологий. Поэтому изучение проблем управления рисками и методов их решения является актуальным и востребованным в современном информационном обществе.

К настоящему времени накоплен достаточный опыт и знания по анализу рисков, в том числе и информационных, для того, чтобы отразить их в отдельном курсе. Конечно, некоторые общие подходы к этой проблематике должны излагаться при изучении основ информационной безопасности, но освоить весь материал, с учетом разнообразия существующих информационных систем, при этом не представляется возможным. Для этого необходимо дополнительное изучение.

Рассматриваемая проблематика изучения информационных рисков достаточно новая по сравнению с финансовыми, банковскими и другими рисками. Но значимость ее повышается по мере возрастания зависимости общества от информационных технологий.

На слуху у всех, кто работает с информационными технологиями, находятся понятия «информационного риска», «ИТ-риска», «операционного риска», «риска информационной безопасности» и др. Необходимо разобраться в этих понятиях, в их отличиях друг от друга, общих чертах, для последующего использования в своей практике.

Представлен достаточно внушительный список литературы по данной теме. Многие источники доступны в электронном виде в Интернете, что облегчит получение дополнительного материала, даст возможность углубить свои знания.

Раздел 1

Основные понятия и определения управления информационными рисками

Управление рисками и управление информационной безопасностью

Все чаще в отечественных публикациях по вопросам управления само слово «управление» заменяется на слово «менеджмент», кальку с английского слова «management», означающего «управление, руководство». Например, в стандарте Банка России СТО БР ИББС 1.0-2006 стало употребляться понятие **«система менеджмента информационной безопасности» (СМИБ)**, вместо «системы управления информационной безопасностью» (СУИБ). В других документах и статьях употребляются оба этих понятия. Путаницы, как правило, это не вызывает.

Следует также заметить, что термин «менеджмент (management)» иногда относится к людям, т.е. к лицу или группе работников, наделенных полномочиями и ответственностью для руководства организацией. Когда «менеджмент (management)» используется в этом смысле, его рекомендуется применять с определяющими словами. Например, не одобряется выражение «руководство должно...», в то время как «высшее руководство должно…» – приемлемо.

Больше сложности возникает при переводе таких терминов, как «Risk assessment», «Risk estimation», «Risk evaluation»; вторые слова в этих сочетаниях имеют при переводе одинаковое значение – «оценка». Чтобы разделить эти понятия, будем в русском переводе представлять их как:

Risk assessment – оценка рисков,

Risk evaluation – оценивание рисков, сопоставление рисков.

Risk estimation – количественная оценка рисков, предварительная оценка рисков. Это понятие присутствует в проекте ISO 27005, но отсутствует в ISO 31000, BS 7799-3:2006, AS/NZS 4360:2004.

В курсе «Основы информационной безопасности» приводятся и обсуждаются основные понятия: риск, информационный риск, риск информационной безопасности (см. Приложение). Существенную часть информационных и других рисков составляют риски информационной безопасности. Поэтому им будет уделено особое внимание в данном учебном пособии.

Менеджмент информационной безопасности, согласно стандарту ИСО/МЭК 27001, состоит из всех мероприятий, направленных на достижение и поддержку соответствующих уровней конфиденциальности, целостности и доступности. К этому должны быть добавлены и рассмотрены неотказуемость, учетность, подлинность и надежность.

Менеджмент информационной безопасности включает:

- планирование, реализацию и мониторинг обеспечения безопасности;
- обеспечение того, чтобы меры безопасности учитывали требования;
- обеспечение того, чтобы кадровая, физическая и информационная безопасность соответствовали целям;
- обеспечение того, чтобы вопрос инцидентов разрешался в соответствии со структурой менеджмента;
- обеспечение того, чтобы персонал был образованным, обученным и сознавал свои обязанности и роли в отношении обеспечения безопасности;
- обеспечение соответствия политикам, стандартам и процедурам;
- аудит и проверку соответствия механизмов и целей безопасности.

В стандарте Банка России СТО БР ИББС 1.0-2006 понятие «**менеджмент риска**» трактуется как «скоординированные действия по

руководству и управлению в отношении риска с целью его минимизации». Если напомнить, что в стандарте риск – «неопределенность, предполагающая возможность потерь (ущерба)», то получается, что цель этого процесса в уменьшении указанной неопределенности.

Помимо просто риска, в стандарте выделяется **риск нарушения информационной безопасности организации банковской системы Российской Федерации,** который определяется как «неопределенность, предполагающая возможность ущерба состояния защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз в информационной сфере».

Отмечается, что обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска. Но далее мы рассмотрим несколько другой состав менеджмента риска, следующий из международных стандартов и их проектов.

Менеджмент риска информационной безопасности идентифицирует контекст, производит оценку рисков, обрабатывает риск и предлагает план по обеспечению безопасности для реализации рекомендаций и решений. **Менеджмент риска** тщательно анализирует, что может произойти и каким может быть ущерб, прежде чем определять, что должно быть сделано и когда для снижения ущерба до приемлемого уровня. Реализация, выполнение и мониторинг этих решений являются частью менеджмента риска.

Процесс **менеджмента риска** (risk management) информационной безопасности состоит из двух основных элементов: **оценки риска** (risk assessment) и **обработки риска** (risk treatment). Процесс **оценки риска** информационной безопасности состоит из **анализа риска** и

оценивания риска, а **анализ риска** к тому же состоит из **идентификации риска** и **количественной оценки риска**.

В обязанность каждой организации входит определение **методологии оценки риска**, которая наилучшим образом соответствует конкретной организации.

За этим должно следовать рассмотрение **угроз и уязвимостей** с целью содействия выбору **средств контроля (защитных мер)**, соразмерных оцененным рискам. Уровень детальности этого рассмотрения может различаться в зависимости от рассматриваемых информационных активов, процесса или системы и от определения наиболее подходящего подхода к оценке риска.

Вслед за **оценкой риска** должны быть приняты решения по **обработке риска**: следует ли **предотвращать, переносить, принимать или снижать** идентифицированные риски. В тех случаях, когда решением, вытекающим из оценки риска, является снижение риска, должны быть определены соответствующие средства контроля (защиты) для снижения рисков до приемлемого уровня.

Кроме того, менеджмент риска включает **коммуникацию риска**, в цели которой входит сбор информации для обнаружения и идентификации рисков, предотвращение нарушений безопасности, обусловленных разногласиями среди **причастных сторон**, снижение уровня последствий, а также **мониторинг и пересмотр риска** для обеспечения того, чтобы процесс оставался адекватным и поддерживаемым.

Менеджмент риска является постоянной деятельностью. Для новых информационных процессов и систем, а также систем обработки информации, находящихся на стадии планирования, менеджмент риска должен быть частью проектирования и разработки. Для существующих информационных процессов и систем менеджмент риска должен быть

введен в любой соответствующий момент. Когда планируются существенные изменения информационных процессов и систем, менеджмент риска должен быть частью этого процесса планирования. Он должен принимать в расчет все информационные активы, процессы и системы в организации, а не применяться к любому из них изолированно.

В настоящее время разрабатывается и разработано несколько стандартов по управлению рисками, рисками ИБ и другими. Например, ISO 31000 CD «Risk management – Guidelines on principles and implementation of risk management» Doc/ISO/TMB/RMWG № 47 2007-06-15, рассматривает риски вообще. Но раньше был создан стандарт BS 7799-3:2006, который посвящен специально управлению рисками ИБ.

Для удобства и простоты понимания будем опираться в изложении на схему процесса управления рисками из ISO 27005 или [Цирлов, Марков].

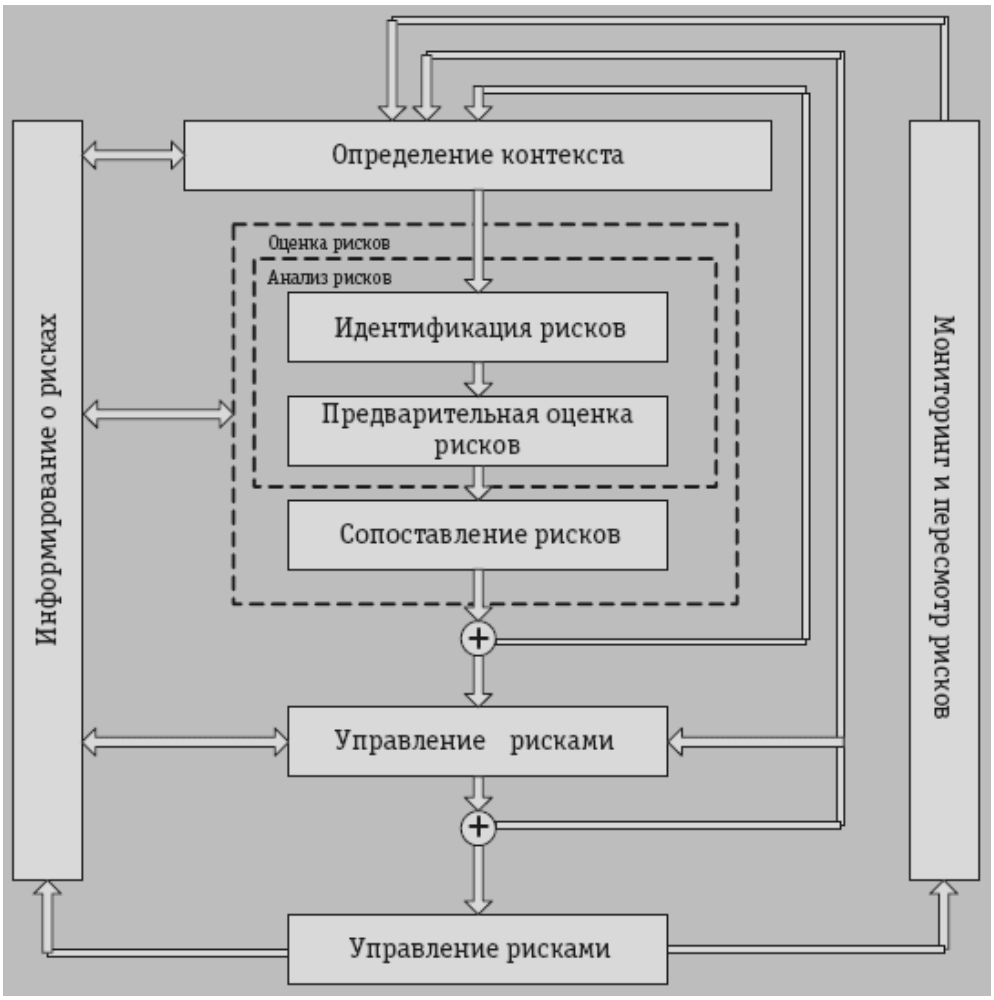

Рис.1. Процесс менеджмента риска информационной безопасности

Как показывает рисунок, процесс менеджмента риска **итеративный**.

Первая итерация оценки рисков состоит из задач по **определению контекста**, **идентификации угроз и уязвимостей**, а также по выполнению **количественной оценки рисков** и **оцениванию (сопоставлению) рисков**. Результат первой итерации оценки рисков может быть удовлетворительным для поддержки процесса **обработки риска**. Если это не так, например, вследствие того, что было доступно недостаточное количество информации, должна быть проведена еще одна итерация оценки рисков, которая будет, например, включать сбор дополнительной информации, уточнение сферы и определение контекста, дальнейшее рассмотрение внешних влияний и ограничений, дальнейшее исследование уязвимостей и угроз.

Цель следующего за этим процесса **обработки риска** состоит в достижении приемлемого уровня рисков, например, путем применения соответствующих **средств контроля (контрмер)**. Эти средства контроля обычно включают средства контроля, относящиеся к лучшим практическим приемам (например, из ИСО/МЭК 17799), но часто также необходимы более специфические средства контроля.

Успех процесса обработки риска зависит от результатов оценки риска. Ситуация, в которой процесс обработки риска немедленно не приводит к приемлемому остаточному риску, весьма вероятна. В такой ситуации происходит еще одна итерация оценки риска с последующей обработкой риска.

Следующий за этим процесс **принятия риска** должен обеспечить ясное принятие **оставшихся рисков** руководством организации. Это особенно важно в ситуации, когда внедрение средств контроля не выполняется или откладывается, например, из-за стоимости.

Важно, чтобы во время всего процесса менеджмента риска осуществлялась **коммуникация риска** соответствующим сторонам, например руководству и операционному персоналу.

Менеджмент риска является постоянным процессом. **Контекст**, а также **активы**, **угрозы и уязвимости** меняются с течением времени, и это делает необходимым осуществление постоянного **мониторинга и пересмотра рисков**.

Определение контекста (establishing the context) состоит из установления **основных параметров** для осуществления менеджмента рисков ИБ, определения **сферы и границ,** а также соответствующей организации процесса менеджмента риска ИБ и, наконец, подготовки **детальной структуры** для запуска процесса.

К **основным параметрам**, которые должны быть установлены, относятся:

- выбор соответствующего подхода оценки риска;
- установление критериев оценивания риска;
- установление критериев влияния;
- установление критериев принятия риска;
- определение потенциально доступных ресурсов.

Критериями оценивания рисков информационной безопасности обычно являются (но не ограничиваются ими) финансовые и иные последствия, связанные с:

- правовыми и регулятивными требованиями и договорными обязательствами;

- операционными и деловыми последствиями недоступности;

- операционными и деловыми последствиями утраты конфиденциальности;

- операционными и деловыми последствиями утраты целостности;

- восприятием клиентов и неблагоприятным влиянием на репутацию.

Организация должна определить собственные **границы для последствий**, таких как «низкие» или «высокие». Например, финансовый ущерб, который может быть катастрофическим для маленькой организации, может быть низким или даже незначительным для очень большой организации.

Определение **сферы и границ** процесса менеджмента риска, включает:

- стратегические бизнес-цели, задачи, процессы и стратегии организации;
- политику информационной безопасности организации;
- правовые и регулятивные требованиям;
- область применения, например, путем определения системы или географических границ;
- обоснование исключения из сферы каких-то вопросов.

Перед сбором входных данных для идентификации и определения **ценности активов** должна быть определена **сфера рассмотрения**. Тщательное определение границ для содействия определению контекста на этой стадии избавляет от ненужной работы и улучшает качество оценки риска. **Определение границ** должно четко обозначить, что из ниже перечисленного должно учитываться при выполнении рассмотрения оценки риска для рассматриваемой информационной системы:

- бизнес-цели и политики;
- информационные активы и активы информационно-коммуникационных технологий (ИКТ) (например, аппаратные средства, программное обеспечение, элементы системы связи);
- люди (например, персонал, подрядчики, другой внешний персонал);

- физическая среда (например, здания, сооружения);
- социокультурная среда;
- экономическая, законодательная и регулятивная среда;
- деловые процессы и деятельность (операции).

Контекст касается взаимосвязи рисков ИБ с общими **деловыми рисками,** с которыми сталкивается организациям. Организация должна стремиться идентифицировать те элементы **общего плана обработки риска**, где требуется поддержка ИБ или информационно-коммуникационных технологий для других механизмов безопасности, чтобы соответствовать общей стратегии уменьшения риска.

Подготовка процесса менеджмента риска ИБ включает:

- идентификацию и анализ причастных сторон (управление);
- определение ролей и обязанностей всех сторон в рамках организации;
- установление необходимых взаимосвязей в задействованных частях организации, а также с другими уместными проектами или мероприятиями.

Определение детальной структуры для выполнения процесса менеджмента риска включает:

- идентификацию необходимой информации, включая ее доступность и потенциальную стоимость сбора;
- определение и соответствующее распределение мероприятий и задач процесса;
- управление ресурсами;
- определение путей эскалации решений.

Процесс **оценки риска** информационной безопасности состоит из **анализа риска** и **оценивания риска**, а **анализ риска** к тому же состоит из **идентификации риска** и **количественной оценки риска**.

Идентификация рисков включает **идентификацию активов**, **угроз, уязвимостей, вероятностей и последствий (ущерба)**. Идентификация должна включать все риски независимо от того, подпадают они под контроль организации или нет.

Существует **много методологий идентификации риска**, таких как перечни контрольных вопросов, аудиты, инспекция на местах, решения, основанные на опыте и записях, блок-схемы, «мозговая атака», собеседование, анализ систем, анализ сценариев и методы проектирования систем. Они должны выбираться в соответствии с потребностями организации.

Идентификация активов. Активы в рамках установленных границ рассмотрения должны быть идентифицированы с достаточным уровнем детальности по отношению к сфере и уровню проводимой оценки. И наоборот, любые активы, исключенные из сферы рассмотрения по любым причинам, должны быть приписаны к другому рассмотрению, чтобы гарантировать, что они не забыты или не упущены из виду. Также для целей менеджмента риска важно вести запись активов, деловых процессов, которые они поддерживают, и их соответственной значимости для организации в инвентарном списке активов.

Определение ценности активов и оценка влияния. После выполнения задачи идентификации активов должна быть определена ценность этих активов. Она представляет собой важность этих активов для организации. Определение ценности активов начинается с классификации активов в соответствии с их приоритетом, с точки зрения важности активов для выполнения деловых целей организации.

Затем определяется ценность, используя две меры: во-первых, восстановительную стоимость актива – стоимость его замены, и, во вторых, деловые последствия от потери или компрометации актива, такие как потенциальные неблагоприятные деловые последствия из-за раскрытия,

модификации, недоступности и/или разрушения информации и других активов информационной системы. (Это может быть определено из анализа делового влияния.) Ценность, определяемая последствиями для бизнеса, обычно значительно выше просто восстановительной стоимости и зависит от важности актива для организации при выполнении ее деловых целей. Определение ценности активов является ключевым фактором в оценке влияния инцидента безопасности, потому что инцидент может затрагивать более чем один актив или только часть актива. В приложении А к ISO 27005 приводится больше информации об определении ценности активов и оценке влияния.

Примером идентификации (описания) активов может служить проект рекомендаций Банка России **РС БР ИББС – 2.2 «Методика классификации активов».**

Идентификация угроз. Угроза обладает потенциалом причинения вреда активам. Угрозы могут быть природного или человеческого происхождения, они могут быть случайными или умышленными. Должны быть идентифицированы и случайные и умышленные **источники угроз** и оценена **вероятность** их возникновения. Важно, чтобы ни одна угроза не была упущена.

Входные данные для оценки угроз должны быть получены от владельцев или пользователей активов, персонала отдела кадров, руководства учреждения и специалистов в сфере информационно-коммуникационных технологий, а также от лиц, отвечающих за обеспечение безопасности организации.

Возможно использование статистики угроз из других организаций, таких как юридические организации и правительственные учреждения. При использовании **реестров угроз** и **статистики угроз** или результатов проводившихся ранее оценок угроз нужно сознавать, что угрозы постоянно

меняются, особенно если меняется деловая среда или информационно-коммуникационные технологии.

После идентификации **источника угрозы** (кто и что вызывает угрозу) и **объекта угрозы** (т.е. какие элементы системы могут быть затронуты угрозой) необходимо оценить **вероятность угроз**. При этом следует принимать в расчет:

- частоту угрозы (насколько часто она может происходить в соответствии с опытом, применимой статистикой и т.д.);

- для умышленных источников угрозы: мотивацию возможных нарушителей, их возможности, доступные им ресурсы, восприятие привлекательности и уязвимости активов информационной системы;

- для случайных источников угрозы: географические факторы, такие как близость к химическим или нефтяным заводам, возможность экстремальных погодных условий и факторы, которые могут влиять на человеческие ошибки и неправильное функционирование оборудования.

В зависимости от потребности в точности, может возникнуть необходимость **разбиения активов на компоненты** и определения связи угроз с компонентами.

По завершении оценки угроз будет составлен список идентифицированных угроз, затрагиваемых ими активов или групп активов и меры вероятности того, что угроза произойдет, например, по **шкале,** такой как **высокая, средняя или низкая**.

Идентификация уязвимостей. Идентификация уязвимостей включает идентификацию слабых мест, которые могут быть использованы источником угрозы для причинения вреда активам. Слабые места могут возникать в любом из следующего: организация; процессы и процедуры; менеджмент; персонал; физическая среда; конфигурация системы

информационно-коммуникационных технологий; аппаратные средства, программное обеспечение или аппаратура связи.

Наличие уязвимости не причиняет вреда само по себе, так как должна присутствовать угроза, которая воспользуется ей. Уязвимость, не имеющая соответственной угрозы, может не требовать внедрения средства контроля, но должна осознаваться и подвергаться мониторингу на предмет измерений. Следует отметить, что неверно реализованное или неправильно функционирующее средство контроля или средство контроля, которое неправильно используется, само может быть уязвимостью. И наоборот, угроза, не имеющая соответственной уязвимости, может не приводить к ущербу.

Важно оценивать, насколько серьезными являются уязвимости, другими словами, насколько просто их можно использовать. Уязвимость следует оценивать, рассматривая все угрозы, которые могут использовать ее в конкретной ситуации. Например, у информационной системы может быть уязвимость к угрозам имитации личности пользователя и злоупотребления ресурсами. Уязвимость к имитации личности пользователя может быть высокой из-за отсутствия аутентификации пользователей. С другой стороны, уязвимость к злоупотреблению ресурсами может быть низкой, потому что даже при отсутствии аутентификации пользователей средства, с помощью которых может происходить злоупотребление ресурсами, ограничены. Организации должны принимать в расчет существующие средства контроля и оценивать, насколько они снижают уязвимости.

Результатом данного шага должен быть список уязвимостей, идентификация угроз, относящихся к каждой уязвимости, и оценка простоты использования уязвимости, например **по шкале**, такой как **высокая, средняя или низкая**.

Примеры уязвимостей и методы оценки уязвимостей можно найти в немецком стандарте BSI IT Grundshuts.

Идентификация влияния (воздействия). Когда происходит **инцидент**, он вызывает **ущерб**. Этот ущерб непосредственно связан с затронутым активом (активами) или частью актива, так как активы имеют ценность.

Организации должны идентифицировать, какие операционные последствия происходят, когда активам причиняется ущерб, в терминах:

- времени на расследование и ремонт;
- потерянного (рабочего) времени;
- упущенных возможностей;
- финансов, необходимых для восстановления ущерба.

Последствия могут быть определены путем моделирования исходов события или совокупности событий или экстраполяции экспериментальных исследований или прошлых данных. Последствия могут быть выражены на языке критериев денежного и технического влияния, влияния на людей или на языке любых других уместных критериев. В некоторых случаях требуется более чем одно цифровое значение для определения последствий для различных периодов времени, мест, групп или ситуаций.

Способ выражения последствий и вероятности и способы их комбинирования для предоставления уровня риска различаются в соответствии с видом риска и целью, для которой должны использоваться результаты оценки риска. Неопределенность и изменчивость последствий и вероятности должны учитываться в анализе.

Влияние по времени и финансам должно оцениваться с помощью того же подхода, который использовался для вероятности угроз и уязвимостей.

Оценка влияния помогает определить полную картину риска.

Идентификация существующих и планируемых средств контроля (контрмер, средств защиты)

Важно, чтобы существующие и планируемые средства контроля были идентифицированы, во избежание излишней работы или расходов, например, при дублировании средств контроля. Может быть также определено, что существующих или планируемых средств контроля либо недостаточно, либо они не оправданы. В данном случае следует проверить, стоит ли убрать данное средство контроля, заменить другим, более подходящим, или стоит оставить средство контроля на месте (например, по стоимостным причинам).

Следует также провести проверку, чтобы удостовериться, что средства контроля работают правильно. Если работают не правильно, то это будет создавать уязвимости. Следует обратить внимание на ситуацию, когда выбранное средство контроля не достигает успеха и поэтому требуются дополнительные средства контроля.

Для определения существующих или планируемых средств контроля могут быть полезны следующие **мероприятия**.

- Просмотр документов, содержащих информацию о средствах контроля; если процесс обеспечения безопасности хорошо задокументирован, все существующие или планируемые средства контроля и состояние их реализации должны быть перечислены там.

- Проверка вместе с лицами, отвечающими за ИБ, и пользователями, какие средства контроля действительно реализованы для рассматриваемого информационного процесса или системы ИКТ.

- Обход здания, осматривая существующие физические средства контроля, сравнение реализованных средств контроля со списком средств контроля, которые должны быть, и проверка реализованных средств контроля на предмет правильной и эффективной работы.

Существующие и планируемые средства контроля должны быть вновь изучены с точки зрения стоимостного сравнения, включая поддержку, с намерением удаления (или не реализации; или совершенствования их, если они недостаточно эффективны). Здесь следует отметить, что иногда дороже удалить несоответствующее средство контроля, чем оставить его на месте и, возможно, добавить еще одно средство контроля.

Результатом данного шага является список всех существующих и планируемых средств контроля с состоянием их реализации и использования.

На **выбор средств контроля** могут оказывать влияние существующие ограничения. Далее перечислим типичные ограничения.

1. Временные ограничения. 2. Финансовые ограничения. 3. Технические ограничения. 4. Культурные ограничения. 5. Этические ограничения. 6. Ограничения, связанные с окружающей средой. 7. Юридические ограничения. 8. Простота использования. 9. Кадровые ограничения. 10. Ограничения, касающиеся интеграции новых и существующих средств контроля.

Качественная, полуколичественная и количественная оценка риска (Предварительная оценка риска)

Заключительным этапом анализа риска является количественная оценка уровня рисков (Risk Estimation). Количественную оценку риска организация должна осуществлять на основе результатов идентификации риска. Для получения количественной оценки риска должны быть скомпонованы все составляющие риска: последствия и вероятности.

Последствия должны оцениваться в терминах ущерба, который может быть причинен нарушением **конфиденциальности, целостности, доступности, неотказуемости, учетности, подлинности и надежности**. (См. *ИСО/МЭК13335-1)*.

Может быть проведен **предварительный анализ**, чтобы риски, последствия которых считаются низкими, были исключены из подробного изучения. Исключенные риски должны быть внесены в список, чтобы продемонстрировать полноту оценки риска.

На практике часто используется первой **качественная оценка** для получения общего указания на уровень риска и обнаружения основных рисков. Позднее может быть необходимо осуществить более конкретный или количественный анализ основных рисков. Форма анализа должна согласовываться с критериями оценивания риска, разработанными как часть установки контекста.

Качественная оценка использует слова для описания величины потенциальных последствий и вероятности возникновения этих последствий. Эти шкалы могут быть приспособлены или отрегулированы для соответствия обстоятельствам, и для различных рисков могут использоваться разные описания. Качественная оценка может использоваться:

- как первоначальное мероприятие отбора для идентификации рисков, требующих более детального анализа;

- в тех случаях, когда данный вид анализа подходит для решений;

- в тех случаях, когда числовые данные или ресурсы неадекватны для выполнения количественной оценки.

Более сложно и дорого провести так называемую «полуколичественную» оценку.

В **полуколичественной оценке** качественным шкалам даны значения. Цель состоит в том, чтобы создать более расширенную ранжированную шкалу, чем та, что обычно достижима при качественной оценке, а не в том, чтобы предложить реалистические значения риска, такие как при действительно количественной оценке. Однако, поскольку значения, присвоенные каждому описанию, могут не нести на себе точную

взаимосвязь с реальной величиной последствий или вероятности, числа должны комбинироваться, только используя формулу, признающую ограничения таких используемых шкал.

Следует проявлять осторожность при использовании полуколичественной оценки, потому что выбранные цифры могут не отражать реальность должным образом, и это может приводить к несогласованным, неправильным или несоответствующим результатам.

Самая сложная и дорогая – это количественная оценка. **Количественная оценка** использует числовые значения для последствий и вероятностей, а не описательные шкалы, которые используются в качественной и полуколичественной оценке. При этом применяются данные из различных источников, в том числе и данные собственной статистики организации об инцидентах за прошлый период. Качество анализа зависит от точности и полноты числовых значений и от корректности используемых моделей.

Здесь мы рассматриваем так называемый **«полный анализ рисков (Full Risk Analysis)».** Но возможен на практике и так называемый **«базовый анализ рисков (Baseline Risk Analysis)»,** который применяется в случаях, когда не предъявляются повышенные требования в области ИБ, а базовые требования в соответствии с **базовым уровнем безопасности (Baseline Security)**. В ряде стран и организаций этот минимальный базовый уровень защищенности определен и зафиксирован документально.

При базовом анализе рисков рассматривается стандартный набор наиболее распространенных угроз безопасности без оценки их вероятности (вирусы, сбои оборудования, не санкционируемый доступ и т.д.). В соответствии с этими угрозами и должны быть приняты меры защиты.

Оценивание риска информационной безопасности

Оценивание риска (Risk Evaluation) информационной безопасности (или Сопоставление риска) следует после анализа риска и завершает этап оценки рисков.

Для оценивания рисков необходимо сравнивать получившие количественную оценку риски, используя выбранную методологию, с критериями риска, определенными во время оценки контекста. Критерии, используемые для принятия решений, должны согласовываться с определенным внешним и внутренним контекстом и контекстом менеджмента риска и принимать в расчет цели организации, мнения причастных сторон и т.д. Решения могут основываться на уровне риска, но должны также учитываться последствия, вероятность, совокупный эффект множественных рисков, степень уверенности в идентификации и анализе риска.

Соображения должны включать:

- критерии безопасности: если один критерий не уместен для организации (например, конфиденциальность), то все риски, влияющие на этот критерий, могут быть неуместными;

- значимость бизнес-процесса или деятельности, поддерживаемых конкретным активом или совокупностью активов: если процесс определен как имеющий низкую значимость, связанные с ним риски должны более слабо учитываться, чем риски, влияющие на более важные процессы или деятельность.

Оценивание риска использует понимание риска, полученное посредством анализа риска, для принятия решений о будущих действиях.

Обработка риска информационной безопасности

Для обработки риска (Risk Treatment) возможны четыре варианта: предотвращение, перенос, снижение и принятие риска.

1. **Предотвращение риска**: рассмотрение способов устранения угрозы или уязвимости или изменения процесса или деятельности таким образом, чтобы угроза к ним больше не была применима. Когда идентифицированные риски считаются слишком высокими, может быть принято решение о полном прекращении или отказе от планируемой или существующей деятельности.

2. **Перенос риска**: перенос риска на третью сторону, которая может взять на себя риск, как, например, страховые компании, или через передачу функций поставщикам сетевых решений или службам управления безопасностью, аутсорсинг. Перенос риска может создавать новые риски или модифицировать существующие идентифицированные риски, поэтому может быть необходима дополнительная обработка риска.

3. **Снижение риска**: применение соответствующих средств контроля для снижения риска (в терминах снижения уязвимостей или возможных последствий). В целом каждое средство контроля может обеспечивать один или несколько из следующих видов защиты: предупреждение, сдерживание, обнаружение, снижение, восстановление, исправление, мониторинг и информированность.

4. **Принятие риска**: принятие решения в отношении всего оставшегося риска. Организация должна прийти к решению о принятии риска на основе **критериев принятия**. Это решение проистекает из двух причин. Первой причиной является успешное снижение риска, т.е. **остаточный риск** после реализации средств контроля не превышает критериев для принятия риска. Второй причиной является сохранение риска, т.е., даже если первоначальный или остаточный риск превышает критерии, руководство выносит решение о принятии риска, принимая в расчет различные условия, такие как бюджет, временные ограничения и т.д.

Когда новые или изменившиеся риски в производственной среде оцениваются как неприемлемые, на выполнение обработки риска может потребоваться определенное время. В таких случаях руководство должно понимать, что такие риски принимаются на период времени, который потребуется для выполнения обработки риска. Может быть уместно наложить ограничения на операции на этот период.

Варианты обработки риска должны быть оценены на основе степени снижения риска и степени любых создаваемых дополнительных выгод или возможностей, принимая в расчет разработанные ранее критерии. Некоторые незамедлительные варианты могут быть технически неосуществимыми или требовать значительных инвестиций в поддержку. Должен быть рассмотрен ряд вариантов и применен либо индивидуально, либо в комбинации.

Выбор наиболее соответствующего варианта включает сопоставление стоимости реализации каждого варианта с выгодами, получаемыми от него. В общем, стоимость менеджмента рисков должна быть соразмерна получаемым выгодам.

Решения должны учитывать потребность тщательного рассмотрения редких, но серьезных рисков, которые могут служить основанием для мер снижения риска, не являющихся оправданными на строго экономической основе. В общем, неблагоприятные последствия рисков должны быть сделаны настолько низкими, насколько это разумно осуществимо, независимо от любых абсолютных критериев.

Во многих случаях маловероятно, чтобы один вариант обработки риска был полным решением конкретной проблемы. Часто организация извлекает значительную пользу путем комбинирования таких вариантов, как снижение вероятности рисков, уменьшение их последствий и перенос или сохранение любых остаточных рисков.

Некоторые варианты обработки риска могут эффективно решать вопрос более чем одного риска (например, обучение и повышение осознания безопасности).

В тех случаях, когда совокупная стоимость реализации всех вариантов обработки риска превышает доступный бюджет, **план обработки риска** должен четко идентифицировать упорядочение по приоритетам, в котором будут реализовываться индивидуальные варианты обработки риска. Упорядочение по приоритетам может быть установлено с использованием различных методов, включая ранжирование риска и анализ затрат и выгод.

Коммуникация риска информационной безопасности

Организация должна установить процедуры коммуникации риска между принимающими решения лицами и причастными сторонами, чтобы: обеспечивать доверие к менеджменту риска организации; собирать информацию о рисках; избегать нарушений безопасности из-за отсутствия взаимопонимания между принимающими решения лицами и причастными сторонами.

Организация должна разработать **планы коммуникации** для обычных деловых ситуаций и для чрезвычайных ситуаций.

Эффективная внутренняя и внешняя коммуникация со всеми причастными сторонами имеет важное значение, так как она может оказывать существенное влияние на принятие решений. Коммуникация будет гарантировать, что лица, отвечающие за осуществление менеджмента риска, и лица, относящиеся к заинтересованным кругам, понимают основу, на которой принимаются решения, и причины необходимости определенных действий.

Восприятие риска может отличаться из-за различий в предположениях, понятиях и потребностях, проблемах и беспокойствах.

Причастные стороны выносят суждения о приемлемости рисков на основе своего восприятия риска. Поэтому очень важно обеспечить, чтобы восприятие риска причастными сторонами, а также восприятие ими выгод могло быть идентифицировано и задокументировано, а лежащие в основе причины были четко поняты и учтены.

Мониторинг и пересмотр риска информационной безопасности

Следует помнить, что лишь немногие риски остаются статичными. Постоянный мониторинг и пересмотр необходимы, чтобы гарантировать, что контекст, результат оценки риска и обработки риска, а также планы менеджмента остаются уместными и соответствующими обстоятельствам. Факторы, которые могут оказывать влияние на вероятность и последствия происходящих угроз, могут меняться, как и факторы, влияющие на приемлемость или стоимость различных вариантов обработки риска. Поэтому необходимо регулярно повторять процесс оценки риска.

Важные изменения, влияющие на организацию, должны быть основанием для более конкретного пересмотра. Результаты мероприятий мониторинга и пересмотра должны возвращаться по обратной связи, в процесс оценки риска. Новые угрозы, уязвимости или изменения вероятности или влияния могут увеличивать ранее оцененные низкие риски или влияния. Процесс пересмотра низких и принятых рисков должен рассматривать каждый риск отдельно, а также все эти риски как совокупное целое, чтобы оценивать их потенциальное суммарное влияние. Если риски не попадают в категорию низких или приемлемых рисков, они должны обрабатываться. Выбранные варианты обработки риска должны периодически пересматриваться.

Организации должны обеспечивать постоянный пересмотр следующих элементов:

- новых угроз, которые могут быть активными вне и внутри организации и которые еще не оценивались;

- надлежащей оценки вероятности возникновения;

- вероятности того, что новые или увеличившиеся уязвимости могут позволить угрозам использовать эти новые или изменившиеся уязвимости;

- увеличившегося влияния или последствий оцененных угроз, уязвимостей и рисков, в совокупности приводящих к неприемлемому уровню риска.

Должен подвергаться мониторингу и пересмотру и процесс менеджмента риска. Организация должна убеждаться в том, что соответствующие процедуры соблюдаются, с тем чтобы руководство имело гарантии, что никакой риск или элемент риска не упущен из виду или недооценен и что для обеспечения реалистического понимания риска и способности реагирования предпринимаются необходимые действия и принимаются решения.

Кроме того, организация должна регулярно проверять, что критерии и пороговые значения, используемые для оценки риска и его элементов, по-прежнему остаются действительными и согласующимися с деловыми целями, стратегиями и политиками и что изменения делового контекста принимаются во внимание на адекватном уровне во время процесса менеджмента риска.

Мониторинг и пересмотр должны уделять внимание: правовому контексту и контексту окружающей среды; контексту конкуренции; критериям оценивания риска; ценности и категориям активов; пороговым значениям рассмотрения элементов риска; пороговым значениям решений об обработке риска; значениям стоимости средств контроля и другому.

Существует тенденция к ухудшению со временем производительности или состояния служб или мер обеспечения

безопасности. Мониторинг нужен для выявления этих ухудшений и инициирования корректирующих действий.

Раздел 2
Технологии (методики) управления информационными рисками

Материал раздела подготовлен на основе книг [24, 14].

Каждая компания или организация имеет свои особенности, связанные со спецификой ее деятельности, уровнем развития и другими факторами. Поэтому невозможно предложить какую-либо единую, универсальную технологию управления рисками. Все опубликованные документы различных организаций, содержащие рекомендации и стандарты по этим вопросам, не содержат ряда важных деталей, которые надо обязательно конкретизировать при разработке на практике методик для конкретной организации.

Рассмотрим типичные вопросы и проблемы, возникающие при разработке таких методик, возможные подходы к решению этих проблем.

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 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 IT-Grundschutz [28], в котором имеется каталог угроз и уязвимостей 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). 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, и 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, иногда математической) **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.

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, 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 оценок 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.

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.

Иногда удобно использовать качественное описание при определении балльной оценки вероятностей.

Таблица 1

Значение шкалы (балл)	**Название**	**Качественное описание**
0	Очень низкая	Частота возникновения угрозы в среднем 1 раз в 3 года (Вероятность возникновения 0,2-0,4)
1	Низкая	Частота возникновения угрозы в среднем 1 раз в год (Вероятность возникновения 0,4-0,6)
2	Средняя	Частота возникновения угрозы в среднем 1 раз в 4 месяца (Вероятность возникновения 0,6-0,8)
3	Высокая	Частота возникновения угрозы в среднем 1 раз в месяц (Вероятность возникновения более 0,8)
4	Очень высокая	Частота возникновения угрозы в среднем 1 раз в неделю (Вероятность возникновения более 0,9)

В случае, если применение данной шкалы вызывает затруднения, может использоваться трехбалльная шкала следующего вида.

Таблица 2

Значение шкалы (балл)	**Название**	**Качественное описание**
1	Низкая	Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали на то, что это может произойти.
2	Средняя	Возможно, что эта угроза осуществится. В прошлом происходили инциденты, или существует статистика, или другая информация указывает на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий.
3	Высокая	Эта угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия.

Оценка ущерба

Оценку возможного ущерба может сделать только собственник или владелец актива. Часто бывает удобнее и проще это сделать с использованием качественного описания.

Таблица 3

Значение шкалы (балл)	**Название**	**Качественное описание**
0	Нулевой	Ущерб отсутствует.
1	Очень низкий	Может привести к незначительному материальному ущербу.
2	Низкий	Информация может быть интересна конкурентам, но не имеет коммерческой ценности. Может привести к осуществлению неэффективной деятельности одного подразделения организации И/ИЛИ невозможности оперативно выполнять распоряжения руководства организации.
3	Средний	Может привести к нарушению обязательств организации, в том числе к нарушению надлежащих обязательств сохранять конфиденциальность информации, принадлежащей третьей стороне, в результате чего возможно предъявление гражданского или уголовного иска против организации в результате причинения ущерба И/ИЛИ может привести к потере конкурентного преимущества или содействию несанкционированным целям и преимуществу других лиц или организаций И/ИЛИ информация имеет ценность для конкурентов ввиду того, что имеет коммерческую ценность

Окончание табл. 3

Значение шкалы (балл)	**Название**	**Качественное описание**
		И/ИЛИ может привести к нарушению надлежащего управления организацией или ее деятельностью (например, может быть затронута деятельность ряда подразделений организации) И/ИЛИ возможно искажение оперативной отчетности.
4	Высокий	Может привести к частичной остановке или иному нарушению основных операций в организации.
5	Очень высокий	Может привести к остановке или иному существенному нарушению основных операций в организации.

Измерение рисков

Сегодня существует ряд подходов к измерению рисков. Обсудим наиболее распространенные из них, а именно – **оценку рисков по двум и по трем факторам.**

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:

$$\text{РИСК} = \text{Р}_{\text{происшествия}} * \text{ЦЕНА ПОТЕРИ}.$$

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

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

Сначала должны быть определены шкалы.

Приведем пример субъективной шкалы вероятностей событий [NIST SP 800-30]:

A – событие практически никогда не происходит;

B – событие случается редко;

C – вероятность события за рассматриваемый промежуток времени – 0, 5;

D – скорее всего, событие произойдет;

E – событие почти обязательно произойдет.

Кроме того, устанавливается субъективная шкала серьезности происшествий, скажем, в соответствии с [NIST SP 800-30]:

• 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. (Возможно, например, разделение рисков на приемлемые (допустимые) и неприемлемые.)

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

Таблица 4. Определение риска в зависимости от двух факторов

	Negligible	**Minor**	**Moderate**	**Serious**	**Critical**
A	Низкий	Низкий	Низкий	Средний	Средний
B	Низкий	Низкий	Средний	Средний	Высокий
C	Низкий	Средний	Средний	Средний	Высокий
D	Средний	Средний	Средний	Средний	Высокий
E	Средний	Высокий	Высокий	Высокий	Высокий

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.

Оценка рисков по трем факторам

В зарубежных методиках, рассчитанных на более высокие требования, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. В этих методиках под понятиями «угроза» и «уязвимость» понимается следующее.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$$Р_{происшествия} = Р_{угрозы} * Р_{уязвимости}$$

Соответственно, риск рассчитывается следующим образом:

$$РИСК = Р_{происшествия} * ЦЕНА\ ПОТЕРИ =$$

$$Р_{угрозы} * Р_{уязвимости} * ЦЕНА\ ПОТЕРИ.$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал – качественная. В последнем случае применяются различного рода табличные методы для расчета риска в зависимости от трех факторов.

Интерпретация трехбалльной шкалы оценивания уязвимостей следующая.

Таблица 5

Значение шкалы (балл)	**Название**	**Качественное описание**
1	Маловероятно	Уязвимость сложно использовать, и существует хорошая защита.
2	Возможно	Уязвимость может быть использована, но существует определенная защита.
3	Очень вероятно или вероятно	Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует.

Например, **показатель риска** измеряется по 8-балльной шкале следующим образом:

1 – риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик;

2 – риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики;

……

8 – риск очень велик. Событие, скорее всего, наступит, и последствия будут чрезвычайно тяжелыми.

Матрица может быть построена так, как в табл.

Таблица 6. Определение риска в зависимости от трех факторов

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	низкий			средний			высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

В данной таблице уровни уязвимости Н, С, В означают, соответственно, низкий, средний и высокий.

Такие таблицы используются как в «бумажных» вариантах методик оценки рисков, так и в различного рода инструментальных средствах.

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.

В книге [24] рассмотрен пример реализации подобного подхода, используемого в методе CRAMM 4. 0 для одного из классов рисков

(**Оценка факторов риска использования чужого идентификатора сотрудниками организации («маскарад»)**).

Возможности и ограничения данного подхода

Несомненным достоинством данного подхода является возможность учета многих косвенных факторов (не только технических). Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить оценки.

К недостаткам относится то, что косвенные факторы и их вес зависят от сферы деятельности организации, а также от ряда иных обстоятельств. Таким образом, методика всегда требует подстройки под конкретный объект. При этом доказательство полноты выбранных косвенных факторов и правильности их весовых коэффициентов – задача мало формализованная и сложная, которая на практике решается экспертными методами (проверка соответствия полученных по методике результатов ожидаемым для тестовых ситуаций).

Подобные методики, как правило, разрабатываются для организаций определенного профиля (ведомств), апробируются и затем используются в качестве ведомственного стандарта. По такому пути пошли и создатели CRAMM, выпустив около десятка версий метода для разных ведомств (министерство иностранных дел, вооруженные силы и т. д.).

Оценки рисков и уязвимостей в рассмотренном примере являются качественными величинами. Однако подобными методами могут быть получены и количественные оценки, необходимые при расчете остаточных рисков и решении оптимизационных задач. Для этого применяется ряд методов, позволяющих установить на упорядоченном множестве оценок систему расстояний.

Выбор допустимого уровня риска

Выбор допустимого уровня риска связан с затратами на реализацию подсистемы информационной безопасности. Как минимум существует два подхода к выбору допустимого уровня рисков.

Первый подход типичен для базового уровня безопасности. Уровень остаточных рисков не принимается во внимание. Затраты на программно-технические средства защиты и организационные мероприятия, необходимые для соответствия информационной системы спецификациям базового уровня (антивирусное ПО, МЭ, системы резервного копирования, системы контроля доступа), являются обязательными, их целесообразность не обсуждается.

Дополнительные затраты (если такой вопрос будет поставлен по результатам проведения аудита ИБ либо по инициативе службы безопасности) должны находиться в разумных пределах и не превышать 5–15% средств, которые тратятся на поддержание работы информационной системы.

Второй подход применяется при обеспечении повышенного уровня безопасности. Собственник информационных ресурсов должен сам выбирать допустимый уровень остаточных рисков и нести ответственность за свой выбор.

В зависимости от уровня зрелости организации и характера основной деятельности обоснование выбора допустимого уровня риска может проводиться разными способами. Наиболее распространенным является анализ по критерию «стоимость – эффективность» различных вариантов защиты. Приведем примеры постановки задач:

1**.** Стоимость подсистемы безопасности должна составлять не более 20% от стоимости информационной системы. Найти вариант контрмер, максимально снижающих уровень интегральных рисков.

2. Риски по всем классам не должны превышать очень низкий уровень. Найти вариант контрмер с минимальной стоимостью.

Если ставятся оптимизационные задачи, важно правильно выбрать комплекс контрмер (перечислить возможные варианты) и оценить его эффективность.

Выбор контрмер и оценка их эффективности

Система защиты строится комплексно, включает контрмеры разных уровней (нормативно-правовые, организационные, программно-технические). Для облегчения выбора комплекса контрмер в различных методиках используются таблицы, в которых классам угроз ставятся в соответствие возможные контрмеры. Пример классификатора контрмер CRAMM 4 см. в [24]

Подобные классификаторы позволяют автоматически выбирать и предлагать конкретные варианты контрмер, возможных для рассматриваемой информационной системы. Владельцу информационных ресурсов остается отобрать из них приемлемые.

Следующий шаг – оценка эффективности контрмер. Задача оценки эффективности контрмер не проще, чем оценка рисков. Это объясняется тем, что оценка эффективности комплексной подсистемы безопасности, включающей контрмеры разных уровней (административные, организационные, программно-технические), в конкретной информационной системе – методологически чрезвычайно сложная задача. По этой причине обычно ограничиваются упрощенными, качественными оценками эффективности контрмер.

Примером является таблица (см. табл.) типичных значений эффективности контрмер, используемых в методе анализа рисков RiskWatch,

Таблица 7. Ориентировочная эффективность мероприятий в области защиты информации

Мероприятия	**Степень эффективности**
Разработка и внедрение политики информационной безопасности	2
Работа с персоналом (наведение справок, контроль поведения и т. п.)	3
Совершенствование организационной структуры	4
Анализ рисков	5
Управление жизненным циклом (управление рисками)	5
Совершенствование должностных инструкций и условий контрактов	5
Меры контроля за посетителями	6
Управление имуществом компании	7
Обучение персонала и контроль соблюдения режима ИБ	9
Меры контроля за работой приложений	10

Указанные в таблице значения представляют собой ориентировочные оценки эффективности вложений в различные классы мероприятий в области защиты информации.

В ряде случаев применяются более сложные таблицы, в которых отражена зависимость эффективности от ряда факторов.

На основе подобных таблиц делаются качественные оценки эффективности контрмер.

Раздел 3

Управление информационными рисками, стандарты, нормативные документы, рекомендации

В разных технологически развитых странах разработано и разрабатывается большое число стандартов информационной безопасности. Это прежде всего международные и национальные стандарты оценки информационной безопасности и управления ею – ISO 15408, ISO 17799 (BS7799), ISO 27001, BSI; стандарты аудита, отражающие вопросы информационной безопасности, – COBIT, SAC, COSO, SAS 55/78 и некоторые другие.

В 2006 г. принята серия стандартов и рекомендаций Банка России в области информационной безопасности. Они вобрали в себя лучшие практики по управлению ИБ. Следует отметить, что положения этих документов подходят и могут быть использованы различными организациями, а не только организациями банковской системы.

Рекомендации готовящегося в настоящее время проекта **РС БР ИББС 2.2-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»** являются обязательными только для самого Банка России, а для остальных организаций нет.

Некоторые из документов по управлению рисками (операционными, банковскими) являются обязательными для выполнения организациями кредитно-финансовой сферы. Это:

76-Т «Об организации управления операционным риском в кредитных организациях» (2005).

26-Т «О Методических рекомендациях по проведению проверки системы управления банковскими рисками в кредитной организации (ее филиале) (от 23.03.2007).

В 2007 г. в России были приняты стандарты ГОСТ ИСО/МЭК 17799 и ГОСТ ИСО/МЭК 27001, являющиеся гармонизированными переводами версий международных стандартов серии ISO 27000, в основе которых лежит авторитетный британский стандарт BS 7799, включающий в себя три составные части:

- BS 7799-1:2005. Information security management. Code of practice for information security management (Практические правила управления информационной безопасностью);
- BS 7799-2:2005. Information security management. Specification for information security management systems (Требования к системам управления информационной безопасностью);
- BS 7799-3:2006. Information security management systems. Guidelines for information security risk management (Руководство по управлению рисками информационной безопасности).

Первые две части получили международное признание и представляют собой практические рекомендации по построению системы ИБ и оценочные требования (главным образом сертификационные) к системам менеджмента ИБ (СМИБ).

Третья часть британского стандарта BS 7799-3 еще ожидает получения международного статуса и пока существует в виде проекта стандарта ISO 27005. Помимо проекта ISO 27005, существует проект и другого более общего международного стандарта ISO 31000 «Risk management». Надо сказать, что национальные стандарты опережают международные. Например, BS 31100 Code of Practice for risk management,

2007, Draft, опережает указанный ISO 31000. Оба стандарта относятся к рискам вообще, а не только к информационным рискам.

Острая необходимость в стандарте, регламентирующем вопросы оценки и управления рисками ИБ, прямо вытекает из введенного с 2007 г. в нашей стране ГОСТа ИСО/МЭК 27001-2005. Согласно российскому стандарту, СМИБ трактуется как часть общей системы управления, основанной на оценке бизнес-рисков и предназначенной для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

Внедрение стандартов ГОСТ 17799 и ГОСТ 27001 в практику подразумевает наличие в организации как минимум двух документов: политики ИБ и методологии оценки рисков ИБ, однако для последнего документа в российской нормативной базе не отражены вопросы разработки, форма и содержание.

Стандарт BS 7799-3

Стандарт BS 7799-3:2006 гармонизирован с ISO 17799:2005 (ныне ISO 27002:2007) относительно примеров по компонентам системы защиты и с ISO серии 9000 по требованиям к документам. Стандарт допускает использование любых стратегий организации оценки рисков, в частности изложенных в ISO 13335-3 (Методы менеджмента безопасности информационных технологий). Сравнительный анализ BS 7799-3 с популярным американским стандартом NIST SP 800-30:2002 (Руководство по управлению рисками в системах информационных технологий) показал идентичность по сути изложенных в них подходов к анализу, оценке и управлению рисками.

Недостаток отечественной нормативной базы ИБ состоит в отсутствии российского ГОСТа по рискам.

По линии международного комитета ПК 27 СТК 1 ИСО/МЭК идет активное обсуждение организационных стандартов ИБ в рамках серии ISO/IEC 27000 ISMS и уже ратифицированы три стандарта.

Стандарт BS 7799-3 содержит вводную часть, разделы по оценке рисков, обработке рисков, непрерывным действиям по управлению рисками, а также имеет приложение с примерами активов, угроз, уязвимостей, методов оценки рисков. Стандарт придерживается самого общего понятия **риска** [ISO Guide 73, 2002], под которым понимают комбинацию вероятности события и его последствий. **Управление риском** (risk management) сформулировано как скоординированные непрерывные действия по управлению и контролю организации в отношении риска.

В соответствии с подходом, принятым в серии 27000, непрерывный процесс управления спроецирован на четыре фазы менеджмента: «планирование – реализация – проверка – совершенствование». В контексте стандарта эти четыре фазы (рис. 2) выглядят следующим образом:

- оценка рисков, включающая анализ и вычисление рисков;

- обработка риска – выбор и реализация мер и средств безопасности;

- контроль рисков путем мониторинга, тестирования, анализа механизмов безопасности, а также аудита системы;

- оптимизация рисков путем модификации и обновления правил, мер и средств безопасности.

Оценка рисков (risk assessment) – первый этап в управлении системы информационной безопасности, предназначенный для идентификации источников рисков и определения его уровня значимости. Оценку разбивают на анализ рисков и оценивание рисков.

В рамках анализа проводится инвентаризация и категоризация защищаемых ресурсов, выясняются нормативные, технические, договорные требования к ресурсам в сфере ИБ, а затем с учетом этих

требований определяется стоимость ресурсов. В стоимость входят все потенциальные затраты, связанные с возможной компрометацией защищаемых ресурсов. Следующим этапом анализа рисков является составление перечня значимых угроз и уязвимостей для каждого ресурса, а затем вычисляется вероятность их реализации.

Стандарт допускает двоякое толкование **понятия угрозы ИБ**: как условие реализации уязвимости ресурса (в этом случае уязвимости и угрозы идентифицируются отдельно) и как общее потенциальное событие, способное привести к компрометации ресурса (когда наличие возможности реализации уязвимости и есть угроза). Не возбраняется разделение угроз ИБ на угрозы целостности, доступности и конфиденциальности.

Оценивание риска проводится путем его вычисления и сопоставления с заданной шкалой. Вычисление риска состоит в умножении вероятности компрометации ресурса на значение величины ущерба, связанного с его компрометацией. **Сопоставление риска** выполняется с целью упрощения процесса использования на практике точечных значений риска.

BS 7799-3 допускает использование как количественных, так и качественных методов оценки рисков, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ. Приложение к стандарту содержит единственный пример, который условно можно отнести к качественному методу оценки. Данный пример использует трех- и пятибалльные оценочные шкалы.

Оцениваются уровни стоимости идентифицированного ресурса по пятибалльной шкале: «незначительный», «низкий», «средний», «высокий», «очень высокий». Оцениваются уровни вероятности угрозы по трехбалльной шкале: «низкий», «средний», «высокий». Оцениваются уровни вероятности уязвимости: «низкий», «средний», «высокий». По

заданной таблице рассчитываются уровни риска. Проводится ранжирование.

Обработка риска. После того как риск оценен, должно быть принято решение относительно его обработки (risk treatment). Помимо оцененного уровня риска, при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др. Предлагается одна из четырех мер обработки риска:

Уменьшение риска. Риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие меры и средства безопасности.

Передача риска. Риск считается неприемлемым и на определённых условиях (например, в рамках страхования, поставки или аутсорсинга) переадресуется сторонней организации.

Принятие риска. Риск в конкретном случае считается осознанно допустимым – организация должна смириться с возможными последствиями. Обычно это означает, что стоимость контрмер значительно превосходит финансовые потери в случае реализации угрозы либо организация не может найти подходящие меры и средства безопасности.

Отказ от риска. Отказ от бизнес-процессов организации, являющихся причиной риска. Например, отказ от электронных платежей.

В результате обработки риска остается так называемый **остаточный риск**, относительно которого принимается решение о завершении этапа отработки риска. В стандарте BS7799:3 ничего не сказано об эффективности мер, средств и сервисов, которые могут быть использованы при обработке риска.

Управление рисками. Раздел 7 BS 7799-3 «Непрерывная деятельность по управлению рисками» затрагивает следующие две фазы менеджмента системы**: контроль риска и оптимизация риска**.

Для контроля риска рекомендуются технические меры (мониторинг, анализ системных журналов и выполнения проверок), анализ со стороны руководства, независимые внутренние аудиты ИБ.

Фаза оптимизации риска содержит переоценку риска и, соответственно, пересмотр политик, руководств по управлению рисками, корректировку и обновление механизмов безопасности.

Процедуры контроля рисков и оптимизации, включая использование политик, мер и средств безопасности, идентификацию ресурсов, угроз и уязвимостей, документирование, гармонизированы с ISO 27001 и 27002.

Принцип осведомленности. Отличительной чертой стандарта является принцип осведомленности о процессах оценки, отработки, контроля и оптимизации рисков в организации. На каждом этапе управления рисками предусмотрено информирование всех участников процесса управления безопасностью, а также фиксирование событий СМИБ.

Наряду с **планом обеспечения непрерывности бизнеса**, к основным документам по управлению рисками в британском стандарте отнесены:

- описание методологии оценки рисков,
- отчет об оценке рисков,
- план обработки рисков.

Кроме того, в непрерывном цикле управления рисками задействовано огромное множество рабочей документации: реестры ресурсов, реестры рисков, декларации применимости, списки проверок, протоколы процедур и тестов, журналы безопасности, аудиторские отчеты, планы коммуникаций, инструкции, регламенты и др.

Стандарт перечисляет обязанности и задает требования к категории лиц, непосредственно участвующих при управлении рисками, а именно: экспертам по оценке рисков, менеджерам по безопасности, менеджерам

рисков безопасности, а также владельцам ресурсов и даже руководству организации.

Модель управления рисками, предложенная в проекте ISO 27005, по сути, почти соответствует концепции BS 7799-3, а также NIST SP 800-30:2002. В целом, и BS 7799-3 и проект 27005 имеют описательный характер и не содержат конкретных требований к способам управления рисками. Стандарты позволяют самостоятельно учесть различные аспекты СМИБ, идентифицировать уровни риска, определить критерии для принятия риска, идентифицировать приемлемые уровни риска и т.д. Стандарты придерживаются непрерывного 4-процессного подхода к менеджменту систем качества, включают аналогичные этапы анализа, оценки и управления, правила и рекомендации, носят итеративный характер, не предъявляют конкретных требований к методам, содержат требования по информативности каждого этапа.

Все современные стандарты в области безопасности – NIST SP 800-30, BS 7799-3 и проект ISO 27005 отражают сложившийся в международной практике общий **процессный подход** к организации управления рисками. При этом управление рисками представляется как базовая часть **системы менеджмента качества организации**. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, отработки и управления рисками. С другой стороны, стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также по синтезу мер, средств и сервисов безопасности, используемых для минимизации рисков.

Потребность в соответствующем национальном стандарте по управлению рисками определяется не только популяризацией экономически оправданных подходов к ИБ, но и требованиями и рекомендациями, заданными ГОСТ 27001:2005 и ГОСТ 17799:2005, а также

вытекает из требований к организации бизнес-процессов, определенных в актуальных стандартах серии 9000.

Германский стандарт BSI и BSI-Standards 100-3

В Германии в 1998 г. вышло «Руководство по защите информационных технологий для базового уровня защищенности» [IT Baseline Protection Manual]. Оно представляет собой гипертекстовый справочник объемом около 4 Мб (в формате HTML).

Можно выделить следующие блоки этого документа:

• методология управления ИБ (организация менеджмента в области ИБ, методология использования руководства);

• компоненты информационных технологий:

- основные компоненты (организационный уровень ИБ, процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях);

- инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа);

- клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы);

- сети различных типов (соединения «точка-точка», сети Novell NetWare, сети с ОС UNIX и Windows, разнородные сети);

- элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т. д.);

- телекоммуникации (факсы, автоответчики, интегрированные системы на базе ISDN, прочие телекоммуникационные системы);

- стандартное ПО;

- базы данных;

- каталоги угроз безопасности и контрмер (около 600 наименований в каждом каталоге).

При этом все каталоги структурированы следующим образом. Угрозы по классам: форс-мажорные обстоятельства; недостатки организационных мер; ошибки человека; технические неисправности; преднамеренные действия.

Контрмеры по классам: улучшение инфраструктуры; административные контрмеры; процедурные контрмеры; программно-технические контрмеры; уменьшение уязвимости коммуникаций; планирование действий в чрезвычайных ситуациях.

Все компоненты рассматриваются по такому плану: общее описание, возможные сценарии угроз безопасности (перечисляются применимые к данному компоненту угрозы из каталога угроз безопасности), возможные контрмеры (перечисляются возможные контрмеры из каталога контрмер). Фактически сделана попытка описать с точки зрения ИБ наиболее распространенные компоненты информационных технологий и максимально учесть их специфику. Предполагается оперативное пополнение и обновление стандарта по мере появления новых компонентов. Версии стандарта на немецком и английском языках имеются на сайте BSI.

Каталоги угроз безопасности и контрмер германского стандарта, содержащие более 600 позиций, являются наиболее подробными из общедоступных. Ими можно пользоваться самостоятельно – при разработке методик анализа рисков, управления рисками и при аудите информационной безопасности.

Большее внимание в связи с рассматриваемым вопросом вызывает стандарт «BSI-Standards 100-3, Risk Analysis based on IT-Grundschutz (Анализ рисков на основе « Руководства по защите ИТ для базового уровня защищенности»), ver. 2.0, 2005. – 19р.».

Стандарт США NIST 800-30

Данный стандарт подробно рассматривает вопросы управления информационными рисками. Считается, что система управления рисками организации должна минимизировать возможные негативные последствия, связанные с использованием информационных технологий, и обеспечить выполнение основных бизнес-целей предприятия.

Таблица 8. Управление рисками на различных стадиях жизненного цикла информационной технологии

Фаза жизненного цикла информационной технологии	**Соответствие фазе управления рисками**
1. Предпроектная стадия (концепция данной ИС: определение целей и задач и их документирование)	Выявление основных классов рисков для данной ИС, вытекающих из целей и задач, концепция обеспечения ИБ
2. Проектирование ИС	Выявление рисков, специфичных для данной ИС (вытекающих из особенностей архитектуры ИС)
3. Создание ИС: поставка элементов, монтаж, настройка и конфигурирование	До начала функционирования ИС должны быть идентифицированы и приняты во внимание все классы рисков
4. Функционирование ИС	Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС
5. Прекращение функционирования ИС (информационные и вычислительные ресурсы более не используются по назначению и утилизируются)	Соблюдение требований информационной безопасности по отношению к выводимым информационным ресурсам

Обсудим стадии технологии управления информационными рисками подробнее.

Алгоритм описания информационной системы

На данном шаге описываются цели создания информационной системы, ее границы, информационные ресурсы, требования в области ИБ и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом: аппаратные средства ИС, их конфигурация; используемое ПО; интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии; типы данных и информации; персонал, работающий в данной ИС (обязанности); миссия данной ИС (основные цели); критичные типы данных и информационные процессы; функциональные требования к ИС; категории пользователей системы и обслуживающего персонала; формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т. д.); архитектура подсистемы ИБ; топология локальной сети; программно-технические средства обеспечения ИБ; входные и выходные потоки данных; система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ); существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т. д.); организация физической безопасности; управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т. д.).

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Технология описания системы

Для получения информации по перечисленным пунктам на практике рекомендуется использовать:

• разнообразные вопросники (check-листы), которые могут быть адресованы к различным группам управленческого и обслуживающего персонала;

• интервью аналитиков (внешних), которые проводят неформальные беседы с персоналом и затем готовят формализованное описание;

• анализ формальных документов и документации предприятия;

• специализированный инструментарий (ПО). Существует разнообразное ПО, благодаря которому удается частично автоматизировать процесс описания. К нему относятся разнообразные сканеры, дающие возможность составить схему информационной системы, программы для структурированного описания информационных систем, позволяющие создать необходимые отчетные формы.

Идентификация угроз и уязвимостей

Основные применяющиеся при этом понятия:

• источник угрозы – событие либо ситуация и способ, который может привести к реализации угрозы (в результате использования потенциальной уязвимости);

• угроза – потенциал (или мера) возможности реализации источника угрозы;

• уязвимость – слабость в защите.

Одним из способов идентификации угроз является построение модели нарушителя (см. табл.).

Таблица 9. Пример модели нарушителя

Источник угрозы	**Мотивация**	**Результат реализации угрозы (сценарий)**
Хакер	Хулиганство, самоутверждение	Неавторизованный доступ к ИС с использованием известных уязвимостей ОС (описание сценария)
Криминальные структуры	Получение финансовой информации	Проникновение в ИС с целью получить конфиденциальные данные (описание сценария)

При составлении перечня угроз и оценке их уровня обращаются к спискам классов угроз различных организаций и информации об их рейтингах либо к средним значениям вероятности реализации данной угрозы. Подобные списки составляются и поддерживаются в актуальном состоянии несколькими организациями: The Federal Computer Incident Response Center (FedCIRC), Federal Bureau of Investigation's National Infrastructure Protection Center, SecurityFocus и др.

Идентификация уязвимостей

В результате выполнения данного шага составляется список потенциальных уязвимостей ИС и возможные результаты их реализации. Одним из способов является представление в виде таблицы (см. табл.).

Таблица 10. Идентификация уязвимостей

Уязвимости	**Источник угрозы**	**Результат реализации угрозы (сценарий)**
МЭ допускает доступ из публичной сети к серверу А по протоколу Telnet, в том числе в гостевом режиме (ID= guest).	Неавторизованные пользователи извне.	При использовании уязвимости протокола возможен доступ к файловой системе сервера А (описание сценария).
Учетные записи сотрудников, покидающих компанию, удаляются из ИС системы с запаздыванием в 1-2 дня.	Внутренние нарушители, возможно, в сговоре с увольняющимися сотрудниками.	Незаконные финансовые операции (описание сценария).

Для существующей ИС при составлении списков прибегают к ряду источников: сетевые сканеры уязвимостей, каталоги уязвимостей разных организаций (например, база данных по уязвимостям института стандартов США (NIST) [--]). При оценке уровня уязвимости принимаются во внимание существующие процедуры и методы обеспечения режима информационной безопасности, данные внутреннего аудита и результаты анализа имевших место инцидентов.

Если ИС находится в стадии проектирования, учитываются планируемые процедуры обеспечения ИБ, статистика по уязвимостям, данные производителей средств защиты информации.

Организация защиты информации. Формирование списка управляющих воздействий организации

Составляется список управляющих воздействий, структурированный по уровням или областям ответственности, в соответствии с принятой моделью комплексного обеспечения режима информационной безопасности (см. табл.).

Таблица 11. Управление ИБ

Уровень	**Классы управляющих воздействий и критерии безопасности**
Организационный уровень	- разграничение ответственности; - периодический пересмотр системы управления в области ИБ; - протоколирование и разбор инцидентов в области ИБ; - оценка рисков; - обучение в области ИБ; - процедура авторизации в ИС и удаления учетных записей; - поддержание в актуальном состоянии плана обеспечения ИБ.
Процедурный уровень	Обеспечение правил поддержания режима ИБ, в частности: - доступ к носителям информации; - контроль за работой сотрудников в ИС; - обеспечение должного качества работы силовой сети, климатических установок; - контроль за поступающими в ИС данными.

Окончание табл. 11

Уровень	**Классы управляющих воздействий и критерии безопасности**
Программно-технический уровень	Комплекс мер защиты программно-технического уровня: - активный аудит и система реагирования; - идентификация и аутентификация; - криптографическая защита; - реализация ролевой модели доступа; - контроль за режимом работы сетевого оборудования.

Подробно эти и некоторые другие средства управления описываются в различных руководствах, например в NIST SP 800-26.

Анализ системы управления ИС

Параметры угроз, определяемых на следующем шаге, зависят от организации системы управления ИС. На данном шаге анализируется система управления с позиции возможного воздействия на выявленные угрозы и уязвимости.

Обычно рассматриваются две категории методов управления: **технического** и **нетехнического** уровня.

Методы технического уровня, в свою очередь, подразделяются на:

• обеспечение требований базового уровня (идентификация, управление системой распределения ключей, администрирование, способы защиты элементов системы и ПО);

• упреждающие меры (аутентификация, авторизация, обеспечение безотказности, контроль доступа, сохранение конфиденциальности транзакций);

• обнаружение нарушений в области ИБ и процедуры восстановления (аудит, выявление вторжений, антивирусная защита, проверка целостности ПО и данных).

Методы нетехнического уровня – множество методов управления организационного и процедурного характера.

Выбор шкалы для оценки параметров рисков

Под оценкой параметров рисков понимается определение вероятности реализации потенциальной уязвимости, которая приведет к инциденту.

Типичной (наиболее распространенной) шкалой является качественная (балльная) шкала с несколькими градациями, например: низкий средний и высокий уровень. Оценка производится экспертом с учетом ряда объективных факторов. Уровни рисков устанавливаются, например, как в табл.

Таблица 12. Пример качественной шкалы для оценки риска

Уровень риска	**Определение**
Высокий	Источник угрозы (нарушитель) имеет очень высокий уровень мотивации, существующие методы уменьшения уязвимости малоэффективны.
Средний	Источник угрозы (нарушитель) имеет высокий уровень мотивации, однако используются эффективные методы уменьшения уязвимости.
Низкий	Источник угрозы (нарушитель) имеет низкий уровень мотивации, либо существуют чрезвычайно эффективные методы уменьшения уязвимости.

Анализ возможных последствий нарушения режима ИБ

Определяется цена нарушения режима ИБ. Последствия нарушения режима ИБ могут быть разноплановыми, например: прямые финансовые убытки, потеря репутации, неприятности со стороны официальных структур и т. д. На данном шаге выбирается система критериев для оценки последствий нарушения режима ИБ и принимается интегрированная шкала для оценки тяжести последствий.

Оценка рисков

На этом шаге измеряется **уровень рисков** нарушения конфиденциальности, целостности и доступности информационных ресурсов. Уровень риска зависит от уровней угроз, уязвимостей и цены возможных последствий.

Таблица 13. Оценка тяжести последствий нарушения режима ИБ

Уровень тяжести последствий нарушения ИБ	**Определение**
Высокий	Происшествие оказывает сильное (катастрофичное) воздействие на деятельность организации, что выражается в одном или нескольких проявлениях: - большая сумма (должна быть конкретизирована) прямых финансовых потерь; - существенный ущерб здоровью персонала (гибель, инвалидность или необходимость длительного лечения сотрудника); - потеря репутации, приведшая к существенному снижению деловой активности организации; - дезорганизация деятельности на длительный (конкретизируется) период времени.

Окончание табл. 13

Уровень тяжести последствий нарушения ИБ	**Определение**
Средний	Происшествие приводит к заметным негативным результатам, выражающимся в одном или нескольких проявлениях: - заметная сумма (должна быть конкретизирована) прямых финансовых потерь; - потеря репутации, которая может вызвать уменьшение потока заказов и негативную реакцию деловых партнеров; - неприятности со стороны государственных органов, в результате чего снизилась деловая активность компании.
Низкий	Происшествие сопровождается небольшими негативными последствиями, выражающимися в одном или нескольких проявлениях: - небольшая сумма (должна быть конкретизирована) прямых финансовых потерь; - задержки в работе некоторых служб либо дезорганизация деятельности на непродолжительный период времени; - необходимость восстановления ресурсов.

Существуют различные методики измерения рисков. Чаще всего используются табличные методы.

Риски могут быть оценены с помощью количественных шкал. Это даст возможность упростить анализ по критерию «стоимость – эффективность» предлагаемых контрмер. Однако в этом случае

предъявляются более высокие требования к шкалам измерения исходных данных и проверке адекватности принятой модели.

Выработка рекомендаций по управлению рисками

Рекомендации по уменьшению рисков до допустимого уровня являются необходимыми. Они должны быть комплексными и учитывать возможные меры различных уровней, например: внесение изменений в политику ИБ; изменения в регламентах обслуживания и должностных инструкциях; дополнительные программно-технические средства.

Разработка итоговых отчетных документов

Существуют определенные требования к содержанию отчетных документов. Обязательно наличие следующих разделов: цели работы; принятая методология; описание ИС с позиции ИБ; угрозы; уязвимости; риски; предлагаемые контрмеры.

Раздел 4

Программные средства, используемые для анализа и управления рисками

Данный раздел подготовлен на основе материалов из книги [24], а также материалов самих фирм разработчиков данного ПО. Инструментальные средства анализа рисков позволяют автоматизировать работу специалистов в области защиты информации.

Предлагаемое на рынке ПО ориентировано в основном на уровень информационной безопасности, несколько превышающий базовый уровень защищенности.

На момент начала 2008 г. международный стандарт ISO 2005 по менеджменту риска информационной безопасности еще существует только в проекте. Поэтому большинство инструментальных средств (ПО анализа риска) было создано так, чтобы соответствовать требованиям стандарта ISO 17799, или британского стандарта BS 7799-3. Рассмотрим специализированное ПО, условно разделив его на две группы: ПО базового уровня и ПО полного анализа рисков.

4. 1. Инструментарий базового уровня

4.1.2. COBRA

Программный продукт для анализа и управления рисками COBRA [www.pcorp.u-net.com/risk.htm], производитель – C & A Systems Security Ltd., позволяет формализовать и ускорить процесс проверки на соответствие режима информационной безопасности требованиям Британского стандарта BS 7799 (ISO 17799) и провести простейший анализ рисков. Имеется несколько баз знаний: общие требования BS 7799 (ISO 17799) и специализированные базы, ориентированные на различные области применения. Доступна демонстрационная версия этого ПО.

COBRA позволяет представить требования стандарта в виде тематических «вопросников» по отдельным аспектам деятельности организации.

Анализ рисков, выполняемый данным методом, отвечает базовому уровню безопасности, то есть уровни рисков не определяются. Достоинство методики – в ее простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

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

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

4.1.3. RA Software Tool

Еще одно средство, условно относящееся к базовому уровню, – RA Software Tool [www.aexis.de/RA%20ToolPage.htm] – базируется на:

- британском стандарте BS 7799, части 1 и 2;

- на методических материалах Британского института стандартов: (BSI) PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты), а также на стандарте ISO 13335, части 3 и 4 (Руководство по управлению режимом информационной безопасности, технологии управления безопасностью и выбор средств защиты).

Демонстрационная версия данного метода, доступная на сайте, отличается от полной небольшими купюрами.

4. 2. Средства полного анализа рисков

Четко провести границу между методами базового и полного анализа рисков сложно. Например, метод **RA Software Tool** имеет ряд простейших средств, которые дают возможность формально отнести его к средствам полного анализа рисков.

Ниже рассматривается инструментарий с более развитыми средствами анализа рисков и управления ими.

Программные средства, позволяющие провести полный анализ рисков, создаются с использованием структурных **методов системного анализа** и **проектирования** (SSADM - Structured Systems Analysis and Design) и относятся к категории **средств автоматизации разработки** или **CASE-средств (Computer Aided System Engineering**).

4. 2. 1. Метод CRAMM

В 1985 г. Центральное агентство по компьютерам и телекоммуникациям (CCTA) Великобритании начало исследования существующих методов анализа ИБ, чтобы рекомендовать методы, пригодные для использования в правительственных учреждениях, занятых обработкой несекретной, но критичной информации. Ни один из рассмотренных методов не подошел. Поэтому был разработан новый метод, соответствующий требованиям CCTA. Он получил название CRAMM - метод CCTA анализа и контроля рисков. Затем появилось несколько версий метода, ориентированных на требования Министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций. Одна из версий, «коммерческий профиль», представляет собой коммерческий продукт.

CRAMM, судя по числу ссылок в Internet, – самый распространенный метод анализа рисков и управления ими. В настоящее время продается

версия CRAMM 5 [www.insight.co.uk/cram/index.htm], соответствующая стандарту BS 7799 (ISO 17799).

Анализ рисков включает идентификацию и вычисление уровней рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов. Контроль рисков состоит в идентификации и выборе контрмер, благодаря которым удается снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, позволяет убедиться, что защита охватывает всю систему и существует уверенность в том, что: все возможные риски идентифицированы; уязвимости ресурсов идентифицированы и их уровни оценены; угрозы идентифицированы и их уровни оценены; контрмеры эффективны; расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в несколько этапов. На первом этапе, Initiation, производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании.

На этапе идентификации и оценки ресурсов, Identification and Valuation of Assets, описывается и анализируется все, что касается идентификации и определения ценности ресурсов системы. В конце этой стадии заказчик исследования будет знать, удовлетворит ли его существующая традиционная практика или он нуждается в проведении полного анализа рисков. В последнем случае будет построена модель информационной системы с позиции информационной безопасности.

Этап оценивания угроз и уязвимостей, Threat and Vulnerability Assessment, не является обязательным, если заказчика удовлетворит **базовый уровень информационной безопасности**. Эта стадия выполняется при проведении **полного анализа рисков**. Принимается во внимание все, что относится к идентификации и оценке уровней угроз для

групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни угроз и уязвимостей для своей системы.

Этап анализа рисков, Risk Analysis, позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей при проведении полного анализа рисков, либо путем использования упрощенных методик для базового уровня безопасности.

На этапе управления рисками, Risk Management, производится поиск адекватных контрмер. По существу речь идет о нахождении варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

Каждый этап объявляется законченным после детального обсуждения и согласования результатов с заказчиком.

4. 2. 2. Пример использования метода CRAMM

Возможности метода лучше всего продемонстрировать на небольшом примере. Рассмотрим информационную систему поддержки принятия решений аварийно-спасательной службы. Система состоит из следующих элементов: рабочие места, с которых операторы вводят информацию, поступающую по телефонам, радиоканалам и др.; почтовый сервер, куда информация приходит с удаленных узлов ведомственной сети и через Internet; сервер обработки, на котором установлена СУБД и производится автоматизированный анализ текущей ситуации; сервер резервного копирования; рабочие места группы оперативного реагирования; рабочее место администратора безопасности; рабочее место администратора БД.

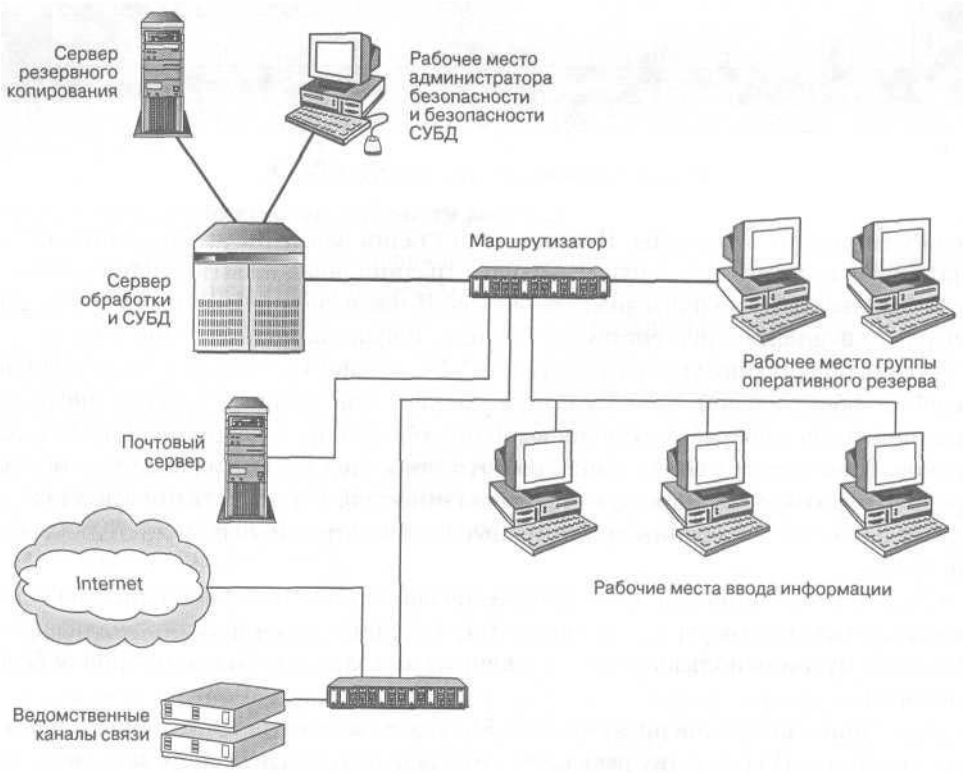

Рис. 2. Информационная система поддержки принятия решений

Система функционирует следующим образом. Информация, введенная с рабочих мест и поступившая на почтовый сервер, направляется на сервер обработки. Затем она приходит на рабочие места группы оперативного реагирования, которая принимает решения.

Постановка задачи. Требуется провести анализ рисков системы и предложить контрмеры для обеспечения должного уровня ИБ.

Этап идентификации и оценки ресурсов. Основные шаги: определение границ исследования (границы системы); идентификация ресурсов (оборудование, данные, программное обеспечение); построение модели с точки зрения ИБ; определение ценности ресурсов; составление отчета и обсуждение его с заказчиком.

Определение границ исследования

Этап начинается с решения задачи определения границ исследуемой системы. Для этого собирается такая информация: ответственные за физические и программные ресурсы; кто является пользователем и как

пользователи применяют или будут применять систему; конфигурация системы. Первичная информация добывается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

Идентификация ресурсов и построение модели системы с точки зрения ИБ

Проводится идентификация следующих ресурсов: физических, программных и информационных, содержащихся внутри границ системы. Каждый ресурс необходимо отнести к одному из предопределенных классов.

Классификация физических ресурсов представлена в приложении 5 книги [24].

Затем строится модель информационной системы с позиции ИБ. Для каждого информационного процесса, имеющего самостоятельное значение с точки зрения пользователя и называемого **пользовательским сервисом (End-User-Service**), формируется дерево связей применяемых ресурсов. В рассматриваемом примере будет единственный подобный сервис. Построенная модель позволяет выделить критичные элементы.

Ценность ресурсов

Метод позволяет установить ценность ресурсов. Этот шаг является обязательным в полном варианте анализа рисков. Ценность физических ресурсов в данном методе зависит от цены их восстановления в случае разрушения. Ценность данных и программного обеспечения определяется в следующих ситуациях: недоступность ресурса в течение определенного периода времени; разрушение ресурса – потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение; нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц; модификация данных – рассматривается для случаев мелких ошибок персонала (ошибки ввода),

программных ошибок, преднамеренных ошибок; наличие ошибок, связанных с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба рекомендуется воспользоваться некоторыми из перечисленных критериев: ущерб репутации организации; нарушение действующего законодательства; ущерб для здоровья персонала; ущерб, связанный с разглашением персональных данных отдельных лиц; финансовые потери от разглашения информации; финансовые потери, связанные с восстановлением ресурсов; потери, связанные с невозможностью выполнения обязательств; дезорганизация деятельности.

Приведенная совокупность критериев характерна для коммерческого варианта метода (профиль Standard). В других версиях совокупность будет иной. Так, в версии, применяемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к исследуемой ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

Далее следует выбор существенных параметров и разработка шкал. В обсуждаемом примере анализ, проведенный экспертом совместно с руководством организации, показал, что для данной информационной технологии будут приниматься во внимание такие параметры: ущерб для здоровья персонала; ущерб репутации организации; финансовые потери, связанные с восстановлением ресурсов; дезорганизация деятельности в связи с недоступностью данных.

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

Ущерб репутации организации:

• 2 – негативная реакция отдельных чиновников, общественных деятелей;

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

• 6 – негативная реакция отдельных депутатов Государственной Думы, Совета Федерации;

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

• 10 – негативная реакция на уровне президента и правительства.

Ущерб для здоровья персонала:

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

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

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

• 10 – гибель людей.

Финансовые потери, связанные с восстановлением ресурсов:

• 2 – менее 1000 долл.; • 6 – от 1000 до 10 000 долл.; • 8 – от 10 000 до 100 000 долл.; • 10 – свыше 100 000 долл.

Дезорганизация деятельности в связи с недоступностью данных – отсутствие доступа к информации:

• 2 – до 15 минут; • 4 – до 1 часа; • 6 – до 3 часов; • 8 – от 12 часов; • 10 – более суток.

Далее рассматриваются основные сценарии, приводящие к различным негативным последствиям, описываемым в терминах выбранных параметров.

На данной стадии может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов). Если ценности ресурсов низкие, допускается ограничиться базовым вариантом защиты. В таком случае исследователь может перейти от этой стадии сразу к анализу рисков. Однако для адекватного учета потенциального воздействия какой-либо угрозы, уязвимости или комбинации угроз и уязвимостей, которые имеют высокие уровни, следует обратиться к сокращенной версии стадии оценки угроз и уязвимостей. Это позволит разработать более эффективную схему защиты.

На этапе оценивания угроз и уязвимостей:

• оценивается зависимость пользовательских сервисов от определенных групп ресурсов;

• оценивается существующий уровень угроз и уязвимостей;

• анализируются результаты.

Зависимость системы от групп ресурсов

Ресурсы группируются в соответствии с угрозами и уязвимостями. Например, в случае существования угрозы пожара или кражи в качестве группы ресурсов разумно объединить все ресурсы, находящиеся в одном месте (серверный зал, комната средств связи и т.д.).

Оценка уровней угроз и уязвимостей

Для уровней угроз и уязвимостей возможна оценка, выполненная по результатам исследования косвенных факторов, либо прямая оценка экспертов (упрощенным способом). В первом случае программное обеспечение CRAMM для каждой группы ресурсов и каждого отдельного ресурса генерирует список вопросов, допускающих однозначный ответ.

Методика оценки рисков и уязвимостей на основе косвенных факторов для данного метода рассматривалась в главе 3 книги [Петренко-Симонов].

Уровень угроз оценивается в зависимости от ответов, как: очень высокий; высокий; средний; низкий; очень низкий.

Уровень уязвимости оценивается, в зависимости от ответов, как: высокий; средний; низкий; отсутствует.

Возможно проведение коррекции результатов или использование других методов оценки. На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7 (этап анализа рисков).

Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительному этапу метода.

Управление рисками

На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиты на группы (см. приложение 5 из [Петренко-Симонов]). Условно их можно разделить на пять категорий:

1 – рекомендации общего плана, относящиеся к технологии в целом;

2 – обеспечение безопасности на сетевом уровне;

3 – обеспечение физической безопасности;

4 – обеспечение безопасности поддерживающей инфраструктуры;

5 – меры безопасности на уровне системного администратора.

В результате выполнения данного этапа формируются несколько видов отчетов.

Особенно полезным представляется обращение к инструментальным средствам типа метода CRAMM при проведении анализа рисков информационных систем с повышенными требованиями в области ИБ. Это позволяет получать обоснованные оценки существующих и допустимых уровней угроз, уязвимостей, а также эффективности защиты.

CRAMM как инструментарий аудитора

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

- политика информационной безопасности;
- система управления информационной безопасностью;
- план обеспечения бесперебойной работы;
- ведомость соответствия.

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

4. 2. 3. Средства компании MethodWare

Компания MethodWare [www.methodware.com] выпускает ряд продуктов, которые могут быть полезными для аналитиков в области информационной безопасности при проведении анализа рисков, управлении рисками, аудите информационной безопасности. Речь идет о:

• ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методология отвечает австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360: 1999). Имеется версия, соответствующая ISO 17799;

• ПО управления жизненным циклом информационной технологии в соответствии с открытым стандартом в области информационных технологий CobiT Advisor 3rd Edition (Audit) и CobiT 3rd Edition Management Advisor. В руководствах CobiT существенное место уделяется анализу и управлению рисками;

• ПО для автоматизации построения разнообразных опросных листов Questionnaire Builder.

Демонстрационную версию этого ПО можно загрузить с сайта компании Methodware.

Рассмотрим ПО Risk Advisor. Оно позиционируется как инструментарий аналитика или менеджера в области информационной безопасности. Реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. Основные этапы работы: описание контекста; описание рисков; описание угроз; оценка потерь; анализ управляющих воздействий; предложение контрмер и плана действий.

Описание контекста. На этом этапе рассматривается несколько аспектов модели взаимодействия организации с внешним миром: стратегический, организационный, бизнес-цели, управление рисками, а также критерии оценивания рисков. В стратегическом аспекте анализируются сильные и слабые стороны организации с внешних позиций, варианты развития, классы угроз и отношения с партнерами. Организационный контекст отражает отношения внутри организации: стратегию, цели на организационном уровне, внутреннюю политику. Контекст управления рисками представляет собой концепцию информационной безопасности.

Контекст бизнес-целей – основные бизнес-цели. Критерии оценивания рисков – имеются в виду критерии, принятые при управлении рисками.

Описание рисков. Задается матрица рисков, поэтому риски описываются в соответствии с определенным шаблоном и устанавливаются связи этих рисков с другими элементами модели. Риски оцениваются по качественной шкале и разделяются на приемлемые и неприемлемые на основе простейшей модели. Затем выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев,

эффективности контрмер и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах.

Описание угроз. Прежде всего формируется список угроз. Угрозы определенным образом классифицируются, затем рассматривается связь между рисками и угрозами. Описание также делается на качественном уровне и позволяет зафиксировать эти взаимосвязи.

Описание потерь. Перечисляются события (последствия), связанные с нарушением режима информационной безопасности. Потери оцениваются в выбранной системе критериев.

Анализ результатов. В результате построения модели можно сформировать подробный отчет (около 100 разделов), посмотреть на экране агрегированные описания в виде графика рисков.

Оценка возможностей метода Risk Advisor

Данный инструмент позволяет документировать всевозможные аспекты, связанные с управлением риском, на верхних уровнях – административном и организационном. А программно-технические аспекты фиксировать в этой модели не очень удобно. Оценки даются в качественных шкалах, подробного анализа факторов рисков не предусмотрено.

Сильной стороной данного метода является возможность представления разноплановых взаимосвязей, адекватного учета многих факторов риска.

4. 2. 4. Экспертная система «АванГард»

В настоящее время на российском рынке продается отечественное ПО «АванГард» – разработка Института системного анализа РАН, подробное описание которого можно найти в [Кононов А.А. Connect № 12, 2001].

«АванГард» позиционируется как экспертная система управления информационной безопасностью. Типовой пакет программных средств «АванГард» включает два программных комплекса – «АванГард-Анализ» и «АванГард-Контроль». Каждый из этих комплексов базируется на своей методике оценки рисков.

4. 2. 5. RiskWatch

Компания RiskWatch [www.riskwatch.com] предлагает два продукта: один относится к информационной, второй – к физической безопасности. ПО предназначено для идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в области компьютерной и физической безопасности предприятия.

В продукте, предназначенном для управления рисками в информационных системах, учитываются требования стандартов США (можно выбирать требуемый уровень защищенности). Кроме того, выпущена версия продукта RiskWatch RW17799®, соответствующая стандарту ISO 17799.

RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика состоит из четырех этапов.

Первый этап – определение предмета исследования. На данном этапе описываются параметры организации: ее тип, состав исследуемой системы, базовые требования в области безопасности. Описание формализуется в ряде подпунктов, которые можно отметить для подробной детализации или пропустить.

Далее каждый из указанных пунктов описывается подробно.

Для облегчения работы аналитика в шаблонах даются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер

защиты. Из них нужно отобрать те, которые реально присутствуют в организации.

Допускается модификация названий и описаний, а также добавление новых категорий, что позволяет достаточно просто русифицировать данный метод.

Второй этап – внесение данных, касающихся конкретных характеристик системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе:

• подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов;

• с помощью опросника, база которого содержит более 600 вопросов, выявляются возможные уязвимости. Вопросы связаны с категориями ресурсов. Допускается корректировка и исключение вопросов или добавление новых;

• задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов.

Все это служит в дальнейшем для расчета эффективности внедрения средств защиты.

Третий этап – оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах.

Для рисков рассчитываются математические ожидания потерь за год по формуле:

$m = p * v,$

где p – частота возникновения угрозы в течение года,

v – стоимость ресурса, который подвергается угрозе.

Например, если стоимость сервера составляет 150 000 долл., а вероятность его уничтожения пожаром в течение года – 0,01, то ожидаемые потери будут равны 1500 долл.

Дополнительно рассматриваются сценарии «что если...», которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при наличии защитных мер и без них, можно оценить эффект от таких мероприятий.

Четвертый этап – генерация отчетов.

Типы отчетов:

- краткие итоги;
- полные и краткие отчеты об элементах, описанных на стадиях 1 и 2;
- отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз;
- отчет об угрозах и мерах противодействия;
- отчет о результатах аудита безопасности.

Возможности RiskWatch

В RiskWatch используется упрощенный подход как к описанию модели информационной системы, так и к оценке рисков.

Данный метод удобен, если требуется провести анализ рисков на программно-техническом уровне защиты без учета организационных и административных факторов.

Существенным достоинством RiskWatch с точки зрения отечественного потребителя является его сравнительная простота, малая трудоемкость русификации и большая гибкость метода, обеспечиваемая возможностью введения новых категорий, описаний, вопросов и т.д. На основе этого метода отечественные разработчики могут создавать свои профили, отражающие отечественные требования в области безопасности, разрабатывать ведомственные методики анализа и управления рисками.

Digilal Security Office

Digital Security Office 2006 разработан и поставляется компанией Digital Security (http://www.dsec.ru/products/dsoffice/).

Digital Security Office 2006 – комплексное решение для управления информационной безопасностью, позволяющее построить систему управления информационной безопасностью в соответствии со стандартами ISO 17799:2005 и ISO 27001, а также самостоятельно проводить регулярный анализ рисков и управлять полученными результатами.

Digital Security Office 2006 – законченное решение для комплексного управления информационной безопасностью, которое включает в себя систему анализа и управления информационными рисками **ГРИФ** и систему разработки и управления политикой безопасности информационной системы **КОНДОР.** Раньше ГРИФ и КОНДОР были отдельными продуктами. Все данные, которые заносятся для анализа политики безопасности, используются и при анализе рисков и наоборот.

ГРИФ 2006 – комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2006 дает полную картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты информации.

Система ГРИФ

- анализирует уровень защищенности всех ценных ресурсов;

- оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности;

- позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество.

Система ГРИФ 2006 предоставляет возможность проводить анализ рисков информационной системы при помощи анализа модели информационных потоков, а также, анализируя модель угроз и уязвимостей

– в зависимости от того, какие исходные данные есть в вашем распоряжении, а также от того, какие данные вас интересуют на выходе.

При работе с моделью информационных потоков в систему вносится полная информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы.

Работа с моделью анализа угроз и уязвимостей подразумевает определение уязвимостей каждого ресурса с ценной информацией и подключение соответствующих угроз, которые могут быть реализованы через данные уязвимости. В результате получается полная картина того, какие слабые места есть в информационной системе и тот ущерб, который может быть нанесен. Система ГРИФ 2006 содержит обширные встроенные базы угроз и уязвимостей, которые можно использовать при проведении анализа рисков. Для достижения максимальной полноты и универсальности данных баз экспертами Digital Security была разработана специальная классификация угроз, в которой реализован многолетний практический опыт в области информационной безопасности.

Алгоритм системы ГРИФ 2006 анализирует построенную модель и генерирует отчет, который содержит значения риска для каждого ресурса. Конфигурация отчета может быть практически любой, таким образом, позволяя создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами.

Система ГРИФ 2006 содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Таким образом, зная причины, вы будете обладать всеми данными, необходимыми

для реализации контрмер и, соответственно, снижения уровня риска. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска, вы сможете выбрать наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

В результате работы с системой ГРИФ получается подробный отчет об уровне риска каждого ценного ресурса информационной системы, все причины риска с подробным анализом уязвимостей и оценкой экономической эффективности всех возможных контрмер.

Описание алгоритма ГРИФ

Модель информационных потоков

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

В результате работы алгоритма программа представляет следующие данные: инвентаризация; значения риска для каждого ценного ресурса организации; перечень всех уязвимостей, которые стали причиной полученного значения риска; значения риска для ресурсов после задания контрмер (остаточный риск); эффективность контрмер; рекомендации экспертов.

Введение в модель

Для того чтобы оценить риск информации, необходимо проанализировать защищенность и архитектуру построения информационной системы.

Владельцу информационной системы требуется сначала описать архитектуру своей сети: все ресурсы, на которых хранится ценная

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

Исходя из введенных данных, можно построить полную модель информационной системы, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Модель анализа угроз и уязвимостей

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

Даная модель основана на построении модели угроз и уязвимостей.

Для того чтобы оценить риск информации, необходимо проанализировать все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз.

Исходя из введенных владельцем информационной системы данных, можно построить модель угроз и уязвимостей, актуальных для информационной системы компании. На основе полученной модели будет проведен анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитаны риски.

Модуль управления рисками

Для эффективного управления информационными рисками в системе ГРИФ существует специальный модуль «Управление рисками».

Функции модуля:

Определяет все уязвимости, которые необходимо закрыть. Предоставляет все данные для принятия решения о целесообразности внедрения контрмеры:

риск до задания контрмер;

риск после задания контрмер;

эффективность комплекса контрмер;

ROSI (возврат инвестиций на информационную безопасность). При этом вы сами задаете значение остаточного риска, который приемлем для вашей компании после внедрения контрмер.

Удобство работы с модулем управления рисками заключается в том, что алгоритм просчитывает все возможные варианты контрмер, не занося их в проект. Таким образом, только после того, как выбранные контрмеры были внедрены в реальную информационную систему, они отображаются в проекте, сохраняя полное соответствие рабочего проекта и информационной системы.

RA2 art of risk

Разработанный **AEXIS Security Consultants** (www.aexis.de)и **XiSEC Consultants Ltd** инструментарий RA2 art of risk предоставляет программные средства для проектирования и внедрения системы управления информационной безопасностью (СУИБ) в соответствии с требованиями стандартов BS 7799-2 и BS ISO/IEC 17799, включающие в себя:

определение области действия и бизнес требований, политики и целей СУИБ; разработка реестра ресурсов СУИБ; оценка рисков СУИБ;

принятие решения по обработке рисков путем рассмотрения подходящих контрмер; процесс выбора системы механизмов контроля; средства оценки безопасности предприятия, средства анализа расхождений с ISO 17799; средства документирования для разработки, например, Декларации о применимости и других документов СУИБ.

В **RA2 art of risk** реализован простой для понимания процессный подход. Процесс управления рисками может настраиваться под потребности конкретной организации.

Можно скачать демонстрационную версию [http://www.iso27000.ru/freeware/sredstva-dlya-ocenki-riskov/RA2_art_of_risk_%20Demo.zip/view].

vsRisk

Программное обеспечение для оценки рисков информационной безопасности в соответствии с требованиями стандартов ISO 27001 и BS 7799-3. vsRisk Risk Assessment Tool – это совершенно новый и уникальный в своем роде инструмент для оценки рисков:

- Позволяет оценивать риски нарушения конфиденциальности, целостности и доступности информации для бизнеса, а также с точки зрения соблюдения законодательства и контрактных обязательств.
- Поддерживает ISO/IEC 17799.
- Соответствует BS7799-3:2006.
- Поддерживает ISO/IEC TR 13335-3:1998.
- Соответствует NIST SP 800-30.
- Содержит интегрированную, регулярно обновляемую базу данных угроз и уязвимостей, соответствующую требованиям BS7799-3.
- Интергируется с инструментальным комплектом: ISMS Documentation Toolkit.

Callio Secura 17799

Callio Secura 17799 (Callio Technologies. http://www.callio.com)является web-приложением, которое включает все необходимое для менеджера при разработке, внедрении, управлении и сертификации Information Security Management System (ISMS – Системы Управления Информационной Безопасностью), основанной на стандарте ISO 17799 / BS7799. С помощью Callio Secura 17799 вы примените практический метод разработки, внедрения, управления и сертификации Information Security Management System.

Сравнительный анализ некоторых приведенных выше ПО, выполненный сотрудницей российской фирмы Digital Security Н. Кукановой, приведен на сайте (http://dsec.ru/about/articles/ar_compare/)

Относительно недавно появились следующие продукты:

Decisioneering Crystal Ball и Microsoft Risk Modeling Tool .

Раздел 5

Аудит безопасности и анализ информационных рисков

Под **аудитом информационной безопасности корпоративной системы** обычно понимается системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ организации в соответствии с определенными критериями и показателями безопасности.

Аудит дает возможность анализировать текущую безопасность функционирования корпоративной информационной системы, оценивать и прогнозировать риски, управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу поддержания безопасности ее активов. Грамотно проведенный аудит безопасности корпоративной информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание систем безопасности.

Современные методики анализа рисков информационной безопасности, проектирования и сопровождения систем безопасности дают возможность:

- количественно оценить текущий уровень безопасности, обосновать допустимые уровни рисков, разработать план мероприятий по поддержанию требуемого уровня безопасности на организационно-управленческом, технологическом и техническом уровнях;
- рассчитать и экономически обосновать размер необходимых вложений в систему безопасности, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередные мероприятия для уменьшения наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;

• определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц, ответственных за информационную безопасность организации, создать или модифицировать необходимый пакет организационно-распорядительной документации;

• разработать и согласовать со службами организации и надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;

• организовать поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Основные понятия и определения

Все понятия и определения в области аудита и сертификации и аттестации можно найти в современных зарубежных стандартах и в российских руководящих документах. В последнее время все активнее идет процесс принятия международных стандартов в качестве российских ГОСТов.

Долгое время российские термины, относящиеся к сертификации и аттестации по требованиям ИБ (определения ФСТЭК (Гостехкомиссии)), и аналогичные термины зарубежных стандартов трактовались и трактуются по-разному. Проведем сравнение определений и терминов следующих российских и зарубежных стандартов и руководств в области защиты информации:

• РД Гостехкомиссии (ныне – ФСТЭК) при Президенте РФ 1992–1998 гг.;

• Практические рекомендации по управлению информационной безопасностью – стандарт BS 7799 (Великобритания);

• Управление в информационных технологиях – CobiT (Международная ассоциации аудита и управления информационными системами);
• стандарты NIST (США) по обеспечению ИБ NIST 800-16, 800-18, 800-30.

В российской нормативно-методической базе основными терминами являлись: **сертификация средств защиты информации** и **аттестация объектов информатизации**.

Под **сертификацией средств защиты информации** по требованиям безопасности информации понимается деятельность, позволяющая убедиться в их соответствии требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Гостехкомиссией РФ.

Под **аттестацией объектов информатизации** подразумевается комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией РФ.

Отметим, что для банковской системы РФ требования по информационной безопасности сформулированы в стандарте Банка России СТО БР ИББС 1.0-2006. Работа по проверке выполнения этих требований получила название не сертификация, а **оценка соответствия** ИБ организации банковской системы требованиям стандарта Банка России. Кроме того, документами Банка России предполагается и проведение самооценки соответствия ИБ организации требованиям стандарта СТО БР ИББС 1.0-2006.

В стандартах NIST аналогичные термины определяются следующим образом.

Сертификация (Certification) – подтверждение соответствия заявленных и фактических технических характеристик в области ИБ для приложений, компьютерных систем, инфраструктуры.

Аккредитация (Accreditation) – разрешение использования информационной системы общего применения или специализированных приложений (имеющих специальные требования к ИБ) для обработки информации. Основанием для выдачи разрешения служит сертификация выбранных решений на соответствие заданным требованиям по ИБ.

Ответственный за выдачу разрешения (Designated Approving Authority) – лицо, уполномоченное принять решение о допустимости определенного уровня рисков для рассматриваемой информационной системы или технологии обработки информации.

Сравнение приведенных определений показывает, что:

• термин сертификация понимается одинаково;

• приблизительным аналогом российского термина «аттестация объектов информатизации» является термин «аккредитация» – с одним существенным отличием: в американском варианте явно указано, что аккредитация производится специалистами, уполномоченными принять решение о допустимости определенного уровня рисков для рассматриваемой информационной системы или технологии.

Для банковской системы РФ к понятию «оценка соответствия» ближе понятие «аттестации объектов информатизации».

При этом в российской нормативно-методической базе аспект рисков, допустимый уровень остаточных рисков, ответственность за принятие определенного уровня рисков присутствуют только в стандарте Банка России.

После аккредитации информационной системы возможно проведение независимой экспертизы существующего режима ИБ – аудит ИБ в информационной системе. Этот термин также встречается в англоязычной литературе и трактуется следующим образом.

Аудит ИБ в информационной системе – процесс сбора сведений, позволяющих установить, поддерживается ли безопасность ресурсов

организации (включая данные); обеспечиваются ли необходимые параметры целостности и доступности данных; достигаются ли цели организации в части эффективности информационных технологий.

В российских РД не предусматривается возможность проведения аудита ИБ, вместо этого допускается повторная аттестация (возможно, другим органом по аттестации). Российские РД и рассматриваемые зарубежные стандарты относятся фактически к различным классам, их системы понятий различаются. Существенными отличиями зарубежных стандартов являются:

• большое внимание к выбору и формальному описанию целей, которые ставятся в области ИБ для конкретной информационной системы. Используются механизмы оценки соответствия декларированных целей существующим показателям ИБ;

• учет аспектов, связанных с рисками, что позволяет оптимизировать построение подсистемы безопасности по критериям «цена – эффективность».

• лучший учет таких составляющих ИБ, как целостность и доступность. Российские РД в основном ориентированы на обеспечение конфиденциальности;

• большая степень формализации требований к подсистеме ИБ. В современных стандартах и руководствах формальные требования и рекомендации излагаются в нескольких сотнях подразделов. Соответственно методики построения подсистем ИБ более конкретны, процедуры проведения аудита ИБ достаточно формализованы.

В настоящее время наиболее известны следующие схемы аудита ИБ:

- на соответствие Британскому стандарту BS 7799, часть 2;
- на соответствие международному стандарту ISO 27001;

- на соответствие требованиям Ассоциации аудита и управления информационными системами (The Information Systems Audit and Control Association & Fondation - ISACA);
- на соответствие требованиям Американского института общественных бухгалтеров (AICPA);
- на соответствие требованиям стандарта СТО БР ИББС 1.0-2006;
- на соответствие требованиям стандарта PCI DSS (VISA, Master Card).

Аудит безопасности в соответствии с ISO 27001:2005 (ГОСТ Р ИСО/МЭК 27001)

Истоки ISO/IEC 27001:2005 находятся в британском стандарте BS 7799, который был разработан в 1995 г. В 1999 г. первая часть BS 7799 была передана в Международную организацию по стандартизации (ISO) и в 2000 г. утверждена в качестве международного стандарта как ISO/IEC 17799:2000 (BS 7799-1:2000). Следующей его версией стал стандарт ISO/IEC 17799:2005.

В 1999 г. вышла в свет вторая часть британского стандарта: BS 7799-2:1999 Information Security management – Specification for ISMS (ISMS – Information Security Management System). В 2002 г. появилась новая, усовершенствованная редакция стандарта – BS 7799-2:2002. На ее основе 14 октября 2005 г. был принят стандарт ISO/IEC 27001:2005 . В России этот стандарт принят 31 декабря 2006 г. как ГОСТ Р ИСО/МЭК 27001 «Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Основные этапы внедрения стандарта ISO/IEC 27001:2005 при развертывании СУИБ следующие.

Этап 1. Аудит организации на соответствие требованиям ISO/IEC 27001:2005.

Этап 2. Разработка СУИБ. Оценка и анализ информационных рисков организации.

Этап 3. Внедрение СУИБ. Управление рисками. Обучение персонала.

Этап 4. Повторный аудит организации на соответствие требованиям ISO/IEC 27001:2005.

Этап 5. Сертификация в BSI Management Systems.

Построение корпоративной СУИБ представляет собой сложный, многоэтапный, циклический организационно-технологический процесс. Как показывает опыт реализации проектов по разработке СУИБ, внедрение данного стандарта целесообразно осуществлять в несколько последовательных этапов.

Рассмотрим каждый такой этап.

Первый этап разработки СУИБ – аудит компании на соответствие положениям ISO/IEC 27001:2005. Главная цель аудита – объективно оценить состояние действующей системы управления ИБ компании, ее адекватность целям и задачам бизнеса, а также разработать рекомендации по построению, внедрению и совершенствованию СУИБ.

Во время аудиторских работ, выполняемых консалтинговой компанией, решаются следующие основные задачи:

- анализ структуры организации;

-анализ защищаемой области деятельности компании и организационно-распорядительных документов;

- анализ структуры и функциональных особенностей используемых ИТ, в частности автоматизированной системы сбора, обработки, передачи и хранения информации;

- проверка выполнения требований ISO/IEC 27001:2005 к СУИБ;

- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, техническому и

аппаратно-программному обеспечению для создания, построения и совершенствования СУИБ.

В большинстве случаев решение перечисленных задач выполняется в четыре этапа.

1. Планирование мероприятий по аудиту. На данном этапе специалисты аудиторской компании собирают организационно-распорядительные документы, отраслевые стандарты, недокументированные проектные решения и другие рабочие материалы, которые могут иметь непосредственное отношение к созданию системы управления ИБ и информационных систем компании, способствующих использованию механизмов и средств обеспечения ИБ. Этот же этап включает разработку, согласование и утверждение планов мероприятий по аудиту.

2. Проверка на соответствие ISO/IEC 27001:2005: определение области деятельности и ключевых бизнес-процессов компании, которые необходимо защитить в первую очередь; анкетирование и интервьюирование сотрудников компании (разных уровней); анализ организационно-распорядительных и нормативных документов; анализ ИБ на соответствие ISO/IEC 27001:2005.

3. Оценка рисков ИБ – аналитический и инструментальный анализ информационных ресурсов компании, прежде всего ЛВС; консультации специалистов компании; оценка соответствия фактического и необходимого уровня безопасности информации; анализ рисков.

4. Систематизация результатов обследования и формирование отчетности. Предоставление итогового отчета руководству компании.

После выполнения аудиторских работ заказчик совместно с консалтинговой компанией приступают к разработке, внедрению (или совершенствованию) системы управления информационной безопасностью.

Основные задачи этого этапа:

- анализ структуры компании, функциональных особенностей построения бизнес-процессов и используемых в них ИТ. Определение защищаемой области деятельности компании;

- систематизация и определение ценности активов компании-заказчика, т. е составление перечня активов с указанием их собственника, места размещения, ответственного и т. д.;

- анализ рисков ИБ, определение возможных путей их реализации (несанкционированного воздействия на подсистемы и бизнес-процессы), классификация рисков по степени критичности, оценка вероятного ущерба от реализации угроз, расчет эффективности внедрения комплексных мероприятий по снижению рисков;

- разработка политики ИБ;

- определение процедур по снижению рисков;

- создание положения о применимости комплекса контролей (иначе – комплекса мероприятий по созданию СУИБ);

- разработка и внедрение СУИБ;

- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, техническому и аппаратно-программному обеспечению режима ИБ в организации;

- анализ и оценка результатов внедрения СУИБ.

Стандарт ISO/IEC 27001:2005 содержит целый ряд требований в отношении рисков.

Необходимо:

- определить подход к оценке риска в организации:

- определить метод оценки риска, подходящий для СМИБ, и установленные требования бизнеса в области информационной безопасности, а также правовые и инструктивные требования;

- определить критерии принятия рисков и установить приемлемый уровень риска.

Выбранная методология оценки риска должна обеспечить сравнимые и воспроизводимые результаты.

(Имеются различные методологии оценки риска. Примеры таких методологий обсуждаются в ISO/IEC TR 13335–3 Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT security (Руководство по менеджменту безопасности ИТ – Часть 3: Методы менеджмента безопасности ИТ).

Далее надо:

- идентифицировать риски:

- идентифицировать активы, относящиеся к области применения СМИБ, и определить собственников этих активов;

- идентифицировать угрозы этим активам;

- идентифицировать уязвимости, которые могут быть использованы этими угрозами;

- идентифицировать возможные воздействия, которые могут привести к утрате конфиденциальности, целостности и доступности активов;

- проанализировать и оценить риски:

- оценить ущерб бизнесу, который может быть нанесен в результате нарушения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

- оценить реальную вероятность возникновения такого нарушения безопасности в свете превалирующих угроз и уязвимостей, воздействия на соответствующие активы, а также применяемые меры контроля;

- оценить уровни рисков;

- определить, является ли риск приемлемым или требуется обработка риска с использованием критериев;

- определить и оценить различные варианты обработки рисков;

Возможные действия включают:

1) применение подходящих мер (средств) контроля;

2) сознательное и объективное принятие рисков при условии, что они четко удовлетворяют требованиям политики и критериям организации в отношении принятия рисков;

3) избежание рисков;

4) перенос связанных бизнес–рисков на сторонние организации, например на страховщиков или поставщиков;

Далее:

- выбрать цели и меры (средства) контроля для обработки рисков.

- получить одобрение руководства в отношении предлагаемых остаточных рисков;

- получить разрешение руководства на внедрение и эксплуатацию СМИБ;

- подготовить «Положение о применимости», которое содержит итоговые решения, касающиеся обработки риска. Обоснование исключений позволяет проверить, что ни одно средство контроля не было случайно упущено.

Аудит информационной безопасности в соответствии с СТО БР ИББС 1.0-2006

Банк России подготовил и принял в 2007 г. стандарт СТО БР ИББС – 1.1-2007 «Обеспечение информационной безопасности организации банковской системы Российской Федерации. Аудит информационной безопасности».

В стандарте сказано, что «**Внешний аудит ИБ организации банковской системы РФ; аудит информационной безопасности** – систематический, независимый и документируемый процесс получения свидетельств аудита деятельности организации БС РФ по обеспечению ИБ

и установления степени выполнения в организации БС РФ установленных критериев аудита ИБ, проводимый внешней по отношению к проверяемой независимой проверяющей организацией».

Данное определение предполагает, что критерии аудита могут быть различными. Однако ниже в том же стандарте сказано: **«Критерии аудита (самооценки) информационной безопасности; критерии аудита (самооценки) ИБ:** Совокупность требований в области информационной безопасности, определенных в соответствии с положениями СТО БР ИББС_1.0 или его частью, и характеризующая некоторый уровень информационной безопасности». Таким образом, аудит превращается фактически в оценку соответствия ИБ организации БС РФ требованиям стандарта СТО БР ИББС -1.0.

Из новых терминов и определений в стандарте присутствуют:

- аудитор (эксперт);
- аудиторская группа;
- выводы аудита информационной безопасности; выводы аудита ИБ;
- заказчик аудита информационной безопасности; заказчик аудита ИБ;
- заключение по результатам аудита информационной безопасности (аудиторское заключение); заключение по результатам аудита ИБ;
- область аудита информационной безопасности; область аудита ИБ;
- проверяемая организация;
- проверяющая организация (аудиторская организация);
- программа аудита информационной безопасности; программа аудита ИБ;
- свидетельства (доказательства) аудита (самооценки) информационной безопасности; свидетельства (доказательства) аудита (самооценки) ИБ;
- самооценка информационной безопасности организации банковской системы Российской Федерации; самооценка ИБ;
- технический эксперт.

За другими терминами и определениями предлагается обращаться к стандарту СТО БР ИББС -1.0. Это:

- банковская система Российской Федерации;
- активы организации банковской системы Российской Федерации;
- автоматизированная банковская система;
- роль в организации банковской системы Российской Федерации;
- банковский технологический процесс;
- информационная безопасность организации банковской системы Российской Федерации;
- менеджмент;
- система менеджмента информационной безопасности организации банковской системы Российской Федерации; СМИБ;
- осознание информационной безопасности;
- политика информационной безопасности организации банковской системы Российской Федерации;
- инцидент информационной безопасности организации банковской системы Российской Федерации;
- риск;
- менеджмент риска;
- риск нарушения информационной безопасности организации банковской системы Российской Федерации;
- мониторинг информационной безопасности организации банковской системы Российской Федерации (мониторинг ИБ);
- аудит информационной безопасности организации банковской системы Российской Федерации;
- оценка соответствия информационной безопасности организации банковской системы Российской Федерации установленным требованиям.

Обращает на себя внимание исходная концептуальная схема (парадигма) аудита информационной безопасности организаций БС РФ

(п. 4), заключающаяся в том, что в основе этой схемы «лежит, с одной стороны, желание собственника доказать достижение организацией БС РФ высокого уровня ИБ и таким образом повысить доверие к ней, с другой стороны - стремление аудиторов с помощью проведения независимой и компетентной оценки определить истинный (в пределах возможностей аудита ИБ) уровень организации работ в области ИБ и степень соответствия ИБ организации БС РФ установленным требованиям (критериям аудита)».

Причиной для регулярного проведения аудита ИБ в организации БС РФ является «возможное изменение внешней среды ведения бизнеса (деятельности) организации БС РФ, изменение и возрастание рисков ИБ вследствие естественных и/или преднамеренных изменений во внешней и внутренней среде организации БС РФ».

Для проведения аудита Банк России разработал и принял также стандарт СТО БР ИББС-1.2-2007 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки соответствия ИБ организаций БС РФ требованиям СТО БР ИББС-1.0-2006».

Цель этой методики – стандартизация подходов и способов оценки, используемых для определения уровня соответствия ИБ организации БС РФ требованиям стандарта Банка России СТО БР ИББС-1.0-2006 по направлениям оценки:

текущий уровень ИБ организации;

менеджмент ИБ организации;

осознание ИБ организации.

Для достижения цели методика решает следующие задачи: определение состава показателей ИБ и способов их оценивания и определение на этой основе итогового уровня соответствия ИБ организации требованиям СТО БР ИББС-1.0-2006.

При оценке используются групповые и частные показатели.

Групповые показатели ИБ – образуют структуру направлений оценки, детализируя оценки

- текущего уровня ИБ (М1-М8) – EV1,

- менеджмента (М9-М27) – EV2

- осознания ИБ (М28-М32) – EV3.

(Напомним: показатель ИБ – мера или характеристика для оценки ИБ.)

Оценки ГП (EV Mi) используются для получения оценки по направлениям (EV1, EV2 и EV3).

Частные показатели ИБ – входят в состав ГП и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV Mi.j), которые затем формируют оценки EV Mi ГП.

(ЧП – оценка степени выполнения какого-либо частного требования ИБ, умноженная на значимость требования. Далее в таблице это – Вычисленное значение показателя ИБ)

Приложение А в методике содержит формы для заполнения при проведении оценки. Каждая из форм содержит ГП ИБ, входящие в него ЧП ИБ, метрику (шкалу оценивания 0-0,25-0,5-0,75-1) для оценивания ЧП и коэффициенты значимости ЧП ИБ, используемые при вычислении ГП.

Рекомендуемые критерии выставления оценок ЧП ИБ.

Оценка ЧП ИБ – 0.

Требования не установлены во внутренних нормативных документах (ВНД) и не выполняются.

Требования частично установлены во ВНД, но не выполняются.

Оценка ЧП ИБ – 0,25.

Требования полностью установлены во внутренних нормативных документах (ВНД), но не выполняются;

Требования не установлены во ВНД и выполняются в неполном объеме.

Требования частично установлены во ВНД и выполняются в неполном объеме.

Оценка ЧП ИБ - 0,5.

Требования полностью установлены во ВНД и выполняются в неполном объеме.

Требования не установлены во ВНД, но выполняются в полном объеме.

Оценка ЧП ИБ - 0,75.

Требования частично установлены во ВНД, но выполняются в полном объеме.

Оценка ЧП ИБ – 1.

Требования полностью установлены во ВНД и выполняются в полном объеме.

Рекомендации применимы для большинства частных показателей и служат для большей объективности при выставлении оценок. При этом тенденция этих рекомендаций такова, что выполнение требований важнее их регламентации во внутренних документах организации.

Основные источники свидетельств:

- внутренние нормативные документы;
- документы третьих лиц;
- устные высказывания сотрудников;
- результаты наблюдений за деятельностью сотрудников.

Полученные свидетельства должны быть задокументированы в листах для сбора свидетельств.

По степени достоверности (от наибольшей к наименьшей) свидетельства аудита ИБ согласно стандарту СТО БР ИББС -1.2 делятся следующим образом:

- свидетельства, полученные от третьей стороны в письменном виде;
- свидетельства, полученные от проверяемой организации и

подтвержденные третьей стороной в письменном виде;

- свидетельства, полученные в ходе проведения аудиторских процедур (наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т. д.);
- свидетельства, полученные в форме документов;
- свидетельства, полученные в устной форме.

Текущий уровень ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить выполнение требований ИБ СТО БР ИББС-1.0 для следующих областей:

- назначение и распределение ролей, обеспечение доверия к персоналу;
- стадии жизненного цикла АБС;
- управление доступом и регистрация;
- антивирусная защита;
- использование ресурсов сети Интернет;
- использование средств криптографической защиты информации (СКЗИ);
- банковские платежные технологические процессы (БПТП);
- банковские информационные ТП (БИТП).

ГП по направлению оценки «менеджмент ИБ организации» оцениваются по стадиям циклической модели менеджмента ИБ.

- планирование системы менеджмента ИБ (СМИБ) (ГП М9-М13);

- реализация СМИБ (ГП М14-М18);

- проверка СМИБ (ГП М19-М23);

- совершенствование СМИБ (ГП М24-М27).

Уровень осознания ИБ организации определяется с помощью ГП и ЧП ИБ, позволяющих оценить уровень выполнения (соблюдения) общих и специальных принципов обеспечения ИБ организации, определенных в разделе 6 СТО БР ИББС-1.0-2006:

своевременность обнаружения проблем;

прогнозируемость развития проблем;

оценка влияния проблем на бизнес-цели;

адекватность защитных мер;

эффективность защитных мер;

использование опыта при принятии и реализации решений;

непрерывность принципов безопасного функционирования;

контролируемость защитных мер;

определенность целей;

знание своих клиентов и служащих;

персонификация и адекватное разделение ролей и ответственности;

адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки;

доступность услуг и сервисов;

наблюдаемость и оцениваемость обеспечения ИБ.

Если значение оценки EV1, EV2 или EV3 (то есть MIN) лежит в интервале…, то данному направлению оценки присваивается … уровень соответствия ИБ требованиям СТО БР ИББС-1.0-2006

Интервал 0–0,25 – нулевой уровень;

Интервал 0,25–0,5 – первый уровень;

Интервал 0,5–0,7 – второй уровень;

Интервал 0,7–0,85 – третий уровень;

Интервал 0,85–0,95 – четвертый уровень;

Интервал 0,95–1 включительно – пятый уровень.

Итоговый уровень R соответствия ИБ организации требованиям СТО БР ИББС-1.0-2006 определяется по наименьшему значению из трех оценок по направлениям оценки:

- оценки осознания ИБ организации (EV3);

- оценки менеджмента ИБ организации (EV2);

- оценки текущего уровня ИБ организации (EV1).

Полученное в результате оценки соответствия ИБ организации требованиям СТО БР ИББС-1.0 значение R является основой для формирования аудиторского заключения по результатам аудита ИБ.

Значения R, соответствующие четвертому и пятому уровням, являются рекомендуемыми Банком России. Значения R, соответствующие уровням с 0-го по 3-ий, не являются рекомендуемыми Банком России.

В Методике указаны в вопросах частных показателей необходимые документы по рискам ИБ:

План обработки рисков ИБ – 14.

План минимизации рисков ИБ – 14.2, 14.3, 14.4, 14.6, 14.5, 15.1.

План обработки (минимизации) рисков – 15.1.

Документ(ы) с результатами анализа и оценки рисков ИБ – 10.2.

Документы (база данных), содержащие описание изменений, внесенных в политику ИБ (частные политики ИБ) и план обработки рисков ИБ – 25.2.

Критерии для принятия рисков ИБ – 10.14.

Документ, в котором отражено принятие остаточных рисков – 13.1.

Таким образом, видно, что без должного внимания со стороны организации к вопросам управления рисками ИБ достичь требуемого уровня соответствия невозможно.

Комплекс «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Стандарты и рекомендации по стандартизации

Стандарты.

СТО БР ИББС – 0.0 Классификатор

СТО БР ИББС – 0.1 Термины и определения

СТО БР ИББС – 1.0 Общие положения

СТО БР ИББС – 1.1 Аудит информационной безопасности

СТО БР ИББС – 1.2 Методика оценки соответствия

Рекомендации.

РС БР ИББС – 2.0 Документы по обеспечению информационной безопасности

РС БР ИББС – 2.1 Руководство по самооценке

РС БР ИББС – 2.2 Методика классификации активов

РС БР ИББС – 2.3 Методика оценки рисков

Все перечисленные документы появились как результат большой аналитической работы и представляют лучшие практики в области информационной безопасности на примере банковского дела. Многие положения этих документов могут быть распространены и на другие направления деятельности.

ПРИЛОЖЕНИЕ

Некоторые определения из области управления информационным риском

Анализ риска – систематическое использование информации для выявления опасности и количественной оценки риска. [ГОСТ Р 51898–2002, статья 3.10]

Допустимый риск – риск, который в данной ситуации считается приемлемым при существующих общественных ценностях. [ГОСТ Р 51898–2002, статья 3.7]

Защитная мера – мера, используемая для уменьшения риска. [ГОСТ Р 51898–2002, статья 3.8]

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Примечания:

1. Термин «обработка риска» иногда используют для обозначения самих мер.
2. Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска. [ГОСТ Р 51897–2002, статья 3.4.1]

Операционный риск – риск прямых или косвенных потерь от неадекватных или имеющих недостатки внутренних процессов, людей и систем или от внешних событий. [Базель 2]

Информационный риск – риск возникновения убытков или ущерба в результате применения информационных технологий.

Остаточный риск – риск, остающийся после предпринятых защитных мер. [ГОСТ Р 51898–2002, статья 3.9]

Оценивание риска – основанная на результатах анализа риска процедура проверки, устанавливающая, не превышен ли допустимый риск.

[ГОСТ Р 51898–2002, статья 3.11]

Оценка риска – общий процесс анализа риска и оценивания риска.

[ГОСТ Р 51898–2002, статья 3.12]

Перенос риска – разделение с другой стороной бремени потерь или выгод от риска.

Примечания:

1. Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.
2. Перенос риска может быть осуществлен страхованием или другими соглашениями.
3. Перенос риска может создавать новый риск или модифицировать существующий риск.
4. Перемещение источника не является переносом риска.

[ГОСТ Р 51897–2002, статья 3.4.7]

Принятие риска – решение принять риск.

Примечание. Принятие риска зависит от критериев риска.

[ГОСТ Р 51897–2002, статья 3.4.10]

Риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898–2002, статья 3.2]

Риск информационной безопасности – риск возникновения убытков или ущерба в результате нарушения конфиденциальности, целостности и доступности информации.

Снижение риска – действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.

[ГОСТ Р 51897–2002, статья 4.4]

Ущерб – физическое повреждение или другой вред здоровью людей, имуществу или окружающей среде.

[ГОСТ Р 51898–2002, статья 3.3]

Литература

Обязательная:

1. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd. 1992. – 932 p. (Chapter 21. Moses R. Risk analysis and management.)

2. MG-3 «A Guide to RISK ASSESSMENT AND SAFEGUARD SELECTION for Information Technology Systems». 1996. – 73 p.

3. IT Security Guidance (ITSG), Canadian Handbook on Information Technology Security. 1998. – 272 p. (4. Common threats. – 37–45 p.; 7. IT Security Risk Management. – 71–83 p.; 18. Audit Trails. – 215–225 p.; 20. Assessing and Mitigating the Risks to Hypothetical IT System. – 247–272 p.) http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/mg9.pdf

4. MITRE, «NIMS Information Security Threat Methodology». 1998. – 35 p. http://www.mitre.org/work/tech_papers/tech_papers_98/nims_information/nims_info.pdf

5. Черешин Д.С., Кононов А.А., Новицкий Е.Г., Цыгичко В.Н. Методика оценки рисков нарушения информационной безопасности в автоматизированных информационных системах. Препринт. – М.: Институт системного анализа РАН, 1999.

6. IT Security Guidance (ITSG), Threat and Risk Assessment Working Guide, Canada. 1999 – 132 p. http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg04.pdf

8. GAO/AIMD-00-33: Information Security Risk Assessment–Practices of Leading Organization. 1999. – 50 p. http://www.gao.gov/special.pubs/ai00033.pdf

9. Федеральный закон от 7 августа 2001 г. N 119-ФЗ «Об аудиторской деятельности» (с изменениями от 14 декабря, 30 декабря 2001 г.)

10. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения». – 12 с.

11. ГОСТ Р 51901.1-2002, Менеджмент риска. Анализ риска технологических систем. – 27 с.

12. PD3002, Guide to BS7799 Risk Management, 2002, BSI.

13. Петренко С.А. Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.(4.2. Методы оценивания информационных рисков компании. – 216–231 с.)

14. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.: ил. (Гл. 13. Управление рисками. – 189–193.; Гл. 14. Методики оценки рисков – 194–199.)

15. Basel Committee on Banking Supervision «Risk Management Principles for Electronic Banking». 2003. – 35 p. http://www.bis.org/publ/bcbs98.pdf

16. Симонов С.В. Современные концепции управления информационными рисками. 2003**.** http://www.pmprofy.ru/content/rus/85/850-article.asp

17. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с. (Гл. 13. Управление рисками и построение систем сетевой безопасности. – 531–581 с.)

18. AS/NZS 4360:2004 Risk management. Australian/New Zealand Standard. – 39 p.

19. HB 436: 2004. Risk Management Guidelines. Companion to AS/NZS 4360:2004. – 131p.

20. ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management. (ГОСТ Р ИСО/МЭК 18044-проект, Информационная технология – Методы и средства

обеспечения безопасности – Менеджмент инцидентов информационной безопасности. 5.1.6 – Менеджмент и анализ рисков ИБ. 7.4 – Политики менеджмента рисков ИБ. 10.2 – Улучшение анализа рисков и менеджмента безопасности.)

21. ISO/IEC Guide 73: 2002, Risk management – Vocabulary – guidelines for use in standards.

22. NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. 2002. – 55 p.

23. ISO/IEC TR 13569:2005, Financial services – Information security guidelines. (ГОСТ Р ИСО/МЭК 13569-проект, Финансовые услуги – рекомендации по информационной безопасности. Раздел 8 – Анализ и оценка риска. Прил. С – Иллюстрация оценки риска.)

24. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная информация. Компания АйТи; ДМК Пресс, 2005. – 384 с.

25. Сазыкин Б. В. Управление операционным риском в коммерческом банке. – М.: Вершина, 2008. – 272 с.

26. BASEL II. Operational Risk Management/ Process Assessment Model/ v.1.00, 2005. – 30 p.
www.cssf.lu/fileadmin/files/Dossiers/**GRIF**/PAM_ORM_BALE**II**_V01_00.pdf

27. BSI-Standards 100-3, Risk Analysis based on IT-Grundschutz (Анализ рисков на основе «Руководства по защите ИТ для базового уровня защищенности»), ver. 2.0, 2005 – 19 p.

28. IT-Grundschutz Manual, BSI, «Руководстве по защите ИТ для базового уровня защищенности». 2004. http://www.bsi.bund.de/gshb. *http://www.bsi.de/english/gshb/manual/download/modules.pdf*

29. CISA Review Manual 2005. Ch. 7 Buiseness process evaluation and Risk Management. – 70 p.

30. Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2) http://www.csi.map.es/csi/pg5m20.htm

31. BS 7799-3:2006 – «Information security management systems - Guidelines for information security risk management».

32. Microsoft Solutions for Security, The Security Risk Management Guide, 2006. http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx

33. ISO/IEC 27005 Information technology – Security techniques – Information security risk management (draft) – Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности.

34. Курило А.П. и др. Обеспечение информационной безопасности бизнеса. – М.: БДЦ-пресс, 2005. – 512 с. (Оценка рисков. Экономика информационной безопасности. – 452–457 с.)

35. ГОСТ_Р_51901.2-2005 Менеджмент риска. Системы менеджмента надежности. – 12 с.

36. ГОСТ_Р_51901.5-2005 Менеджмент риска. Руководство по применению методов анализа надежности. – 72 с.

37. ГОСТ_Р_51901.14-2005 Менеджмент риска. Метод структурной схемы надежности. – 22 с.

38. ГОСТ_Р_51901.16-2005 Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки. – 35 с.

39. ГОСТ_Р_МЭК_61160-2006 Менеджмент риска. Формальный анализ проекта. – 26 с.

40. Галатенко В.А. Основы информационной безопасности. Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с. (7 лекция. Управление рисками).

41. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая

линия – Телеком, 2006. – 544 с. (4. Угрозы информации. – 139–172 с.; 5. Методы и модели оценки уязвимости информации. – 173–183 с.)

42. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с. (Политика оценки рисков. – 321–322 с.)

43. СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

44. СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». 2007. – 14 с. http://www.cbr.ru/credit/Gubzi_docs/st11.pdf

45. СТО БР ИББС-1.2-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006».

46. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. – М.: БДЦ-пресс, 2006. – 304 с.

47. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с. (10.4. Анализ рисков и управление рисками. 10.5. Программные средства, используемые для анализа и управления рисками. – 477–492 с.)

48. MAGERIT, VERSION 1.0, Risk Analysis and Management Methodology for Information Systems Procedures Handbook, Spain. – 213 p. http://www.epractice.eu/files/media/media_920.pdf

49. MAGERIT version 2, Methodology for Information Systems Risk Analysis and Management Book I: The method, Book II: Catalogue of elements, Book III: Techniques. http://www.csi.map.es/csi/pg5m20.htm

50. ISO 14971, Medical devices – Application of risk management to medical devices. Second edition, 2007-03-01.

51. ISO 13335-3 «Techniques for the management of IT Security» (Annex E Types of Risk Analysis Method. – 49–54 p.)

52. BS 31100 Code of Practice for risk management, 2007, Draft. – 44 p.

53. ISO 31000 CD «Risk management – Guidelines on principles and implementation of risk management» Doc/ISO/TMB/RMWG № 47 2007-06-15,

54. Видеотренинг Microsoft по Octave (управление рисками). http://www.securitymanagement.ru/f/showthread.php?t=9973

55. Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний http://dsec.ru/about/articles/ar_compare/ .

56. Crystal Ball – ПО для оценки рисков http://www.decisioneering.com/

57. Анализ рисков на http://www.securitymanagement.ru/f/forumdisplay.php?f=11

Дополнительная:

58. Basle Directive № 86, «Sound Practices for the Management and Supervision of Operational Risk» Basel Committee on Banking Supervision, Switzerland. May 2001.

59. Basle Directive № 91, «Risk Management Principles for Electronic Banking» Basel Committee on Banking Supervision, Switzerland. July 2002.

60. Information Systems Control Journal, ISACA, USA: Volume 5, 2002, «Risk Management in IT Projects», pages 37–39; Volume 2, 2003, «Risk

Assessment Tools: A Primer» pages 23–25; Volume 5, 2003, «Assessing and Preventing Risks from E-mail System Use» 33–35.

61. Gilbert I.E. Guide for selecting automated risk analysis tools. – 26 p.

62. Hoffman L. Modern methods for computer security and privacy. Prentice-Hall, Inc. 1977.

Русский перевод: Хоффман Л.Д. Современные методы защиты информации. – М.: Сов. радио, 1980.

63. Hsiao D., Kerr D., Mednick S. Computer security. Academic Press, 1979.

Русский перевод: Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. – М.: Мир, 1982.

64. Russel D., G.T.Gangemi Sr. Computer Security Basics. – O`Reilli & Associates, Inc., 1991. – 448 p.

65. Muftic S. Security Mechanisms for Computer Networks. Halsted Press.

Русский перевод: Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

66. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. Кн. 1 и 2.

67. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.

68. Горохов П.К. Информационная безопасность. Англо-русский словарь. – М.: Радио и связь, 1995. – 224 с.

69. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Яхтсмен, 1996.

70. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997. – 538 с.

71. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.

72. ГОСТ Р 51275-99, Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

73. ISO 9004, Системы менеджмента качества. Рекомендации по улучшению деятельности. Quality Management Systems – Guidelines for performance improvements. 2000. – 90 с.

74. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных: Учебное пособие. – М.: СИНТЕГ, 2000. – 248 с.

75. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности. – М: Радио и связь, 2000. – 192 с.

76. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

77. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учебное пособие. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.

78. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия – Телеком, 2001. – 148 с.

79. Barman S. Writing Information Security Policies. 2001.

Русский перевод: Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2002. – 208 с.

80. Голдовский И. Безопасность платежей в Интернете. – СПб : Питер, 2001. – 240 с.

81. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2002. – 368 с.

82. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

83. CMS Information Security Risk Assessment (RA) Methodology, CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS). 2002. – 20 p. http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/RA_meth.pdf

84. Pieprzyk J., Hardjono T., Seberry J. Fundamentals of Computer Security. Springer-Verlag Berlin Heidelberg. 2003. – 677 p.

85. Галатенко В.А. Стандарты информационной безопасности. Курс лекций. – М.: ИНТУИТ. РУ, 2004. – 328 с.

86. Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска. – М.: Изд. Дом ГУ ВШЭ, 2005. – 400 с. (Для моделирования рисков в страховых и пенсионных схемах и в финансах.)

87. Jones J.A., An Introduction to Factor Analysis of Information Risk (FAIR), A framework for understanding, analyzing, and measuring information risk. 2005. – 67 p.
http://nujia.norwich.edu/current/2_1_art01NUJIA.pdf

88. Ken Biery Jr. 2006, Aligning an information risk management approach to BS 7799-3:2005. 2006 – 79 p. www.sans.org/reading_room/whitepapers/auditing/1664.php

89. GCIO – Government Chief Information office, Guidelines/ Information Security Guidelines for NSG Government Agencies. Feb 2007, 111pp. (Ch.5 – Risk Management. – 28–46, Annex B. – Risk assessment. – 58–82).
http://www.gcio.nsw.gov.au/documents/Information%20Security%20Guideline%20V1.1.pdf

90. Stephenson P.R., A Formal Model for Information Risk Analysis Using Colored Petri Nets. 2004 – 18 p. FARES http://www.daimi.au.dk/CPnets/workshop04/cpn/papers/stephenson.pdf

91. Assessing Cyber-Threats in the Information Environment. 2004 – 19 p. http://www.glam.ac.uk/socschool/research/publications/technical/CS-04-01.pdf

92. Vidalis S. A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. 2004. – 33 p.
www.glam.ac.uk/socschool/research/publications/technical/CS-04-03.pdf

93. GCIO – Government Chief Information office, Project Risk Management Guideline, Sep. 2004. – 34 p.
http://www.gcio.nsw.gov.au/documents/Project_Risk_Man_0904.pdf

94. Чекалин А.А., Заряев А.В. и др. Защита информации в системах мобильной связи: Учебное пособие для вузов. – М.: Горячая линия – телеком, 2005. – 171 с. (Гл. 3. Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз. Гл. 4. Практические аспекты защиты информации в системах мобильной связи стандарта GSM. Гл. 6 Защита информации в перспективных системах мобильной связи.)

95. The Standard of Good Practice for Information Security, Inf. Sec. Forum-ISF, v.4.0-2003 (2005-New) – 240 p.
http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf .

96. Chris Ralph, Risk Analysis for HIPAA Compliancy. 2005. – 16 p.
http://www.giac.org/certified_professionals/practicals/ghsc/32.php

97. Доля А.А. Внутренние ИТ – угрозы в России – 2006. «Защита информации. Инсайд». № 2 март-апрель 2007. – 60–69 с.

98. Pfleeger C.P, Pfleeger S.L., Security in Computing, Prentice Hall Publishing. 2003.

99. Alberts, C & Dorofee, A, *Managing Information Security Risks*. Boston, Addison Wesley. 2003.

100. Jordon, E & Silcock, L *Beating IT Risks*, Chichester, John Wiley & Sons, Australia Ltd. 2006.

101. Slay, J & Koronios, A, *IT Security and Risk Managment*, John Wiley & Sons, Australia Ltd. 2006.

102. Peltier, TR, *Information Security Risk Analysis*, 2nd edn, Auerbach Publications. 2005.

103. Марков А.. Цирлов В. Управление рисками – нормативный вакуум информационной безопасности. Открытые системы. 2007, № 8.

104. Конеев И. Практическая оценка информационных рисков. Директор ИС. 2007, № 9

105. Конеев И. Классификация как основа управления информационными рисками. Директор ИС. 2006, № 5.

ОПИСАНИЕ КУРСА И ПРОГРАММА

Требования по управлению информационными рисками (рисками информационной безопасности) содержатся во многих международных и отечественных регламентирующих документах и обоснованы существующей практикой развития информационных технологий. Поэтому изучение проблем управления рисками и методов их решения является актуальным и востребованным в современном информационном обществе.

К настоящему времени накоплен достаточный опыт и знания по анализу рисков, в том числе и информационных, для того, чтобы отразить их в отдельном курсе. Конечно, некоторые общие подходы к этой проблематике содержатся в курсе «Основы информационной безопасности», но изложить весь материал, с учетом разнообразия существующих информационных систем, не представляется возможным. Данный курс призван решить эту задачу.

Рассматриваемая проблематика изучения информационных рисков достаточно новая по сравнению с финансовыми, банковскими и другими рисками. Но значимость ее повышается по мере возрастания зависимости общества от информационных технологий.

1.1. Цели и задачи курса.

Основная цель курса:

обеспечить комплексность и полноту подготовки бакалавриата по направлениям «Информационные технологии», «Прикладная математика и информатика», «Математика. Прикладная математика», «Автоматизация и управление» путем формирования у студентов знаний и навыков по вопросам управления информационными рисками, как неотъемлемой части обеспечения информационной безопасности.

Задачи курса:

ознакомить студентов с основными проблемами в области управления информационными рисками, а также с методами и средствами их решения; обеспечить необходимыми сведениями и навыками для последующего обучения по направлениям «Информационные технологии», «Прикладная математика и информатика», «Математика. Прикладная математика», "Автоматизация и управление".

1.2. Профессиональные навыки, умения и знания, приобретаемые в результате изучения дисциплины

Навыки и умения

Студент должен уметь:

анализировать риски информационной безопасности информационных систем;

оценивать существующие современные средства защиты информации;

выбирать и разрабатывать меры защиты информации при реализации информационных процессов;

иметь навыки работы со средствами автоматизации процессов управления рисками.

Знания

Студент должен знать:

общие проблемы информационной безопасности информационных систем;

основные виды информационных рисков, их взаимосвязь и отличия с другими видами рисков;

методы и средства управления информационными рисками;

методы и средства защиты информации и контроля широко используемых информационных технологий;

основные международные и отечественные стандарты и рекомендации по управлению информационными рисками.

1.3. Инновационность курса по содержанию и используемой литературе.

Для понимания инновационности курса необходимо представлять общее состояние в преподавании курсов по информационным технологиям и безопасности, а также определить факторы, влияющие на объективность появления новых направлений и тем в этой области.

Инновационность курса по содержанию обеспечена высокой динамикой развития информационных технологий, и большой зависимостью их от обеспечения информационной безопасности, в частности от многочисленных информационных рисков. Инновационность курса также основывается на необходимости осознанного выбора достаточного материала для введения студентов в данную проблематику из многочисленных публикаций с подходами разных организаций и исследователей к проблемам управления информационными рисками. При этом приходится соблюдать баланс между устоявшимися терминами и понятиями с непрерывно появляющимися новыми и не совсем общепринятыми.

Автор данного курса имел желание построить курс в соответствии с содержанием одной из доступных и качественных книг на русском языке с соответствующей тематикой. Это позволило бы облегчить как преподавание курса, так и обучение. В качестве основы-прототипа была выбрана книга Петренко С.А. и Симонова С.В. «Управление информационными рисками», выпущенная компанией АйТи в 2005 году.

Книга написана известными специалистами в области информационной безопасности и во многом основана на передовом зарубежном и отечественном опыте. Однако, за прошедшее с ее выхода время произошли существенные изменения в данной области, в частности в международной и отечественной практике, вышли новые стандарты и рекомендации по вопросам информационных рисков. В связи с этим должно быть переработано и дополнено содержание как книги, так и курса на ее основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых отраслевых стандартов. Также новизна содержания курса должна определяться выбором перспективных технологий для демонстрации решения проблем управления информационными рисками.

При разработке курса было необходимо ознакомиться с лучшими практиками преподавания данной тематики, чтобы критически их переработав создать собственный курс, адаптированный к конкретным условиям преподавания в России и в РУДН. К таким лучшим курсам по данной тематике можно отнести программу ISM201 “Information Risk Management ”(Управление рисками информационных систем), разработанного общепризнанным мировым лидером в области подготовки специалистов по вопросам информационной безопасности компанией MIS Training Institute (www.misti.com). Программа курса и ее перевод представлена в Приложении к отчету. Данная программа рассчитана на короткий интенсивный метод обучения и может служить только ориентиром для данного курса. К тому же в ней не отражена отечественная специфика и разработки в данном вопросе.

В настоящее время приобрело популярность получение международных сертификатов путем сдачи соответствующих квалификационных экзаменов, которые проводятся в виде тестов. Одними из наиболее признанных являются сертификаты CISA и CISSP, выдаваемые

Международным Информационным Консорциумом по Сертификации Защиты Систем (Information Security Certification Consortium (ISC)2 - www.isc2.org). Программа курса должна учитывать требования и соответствующие разделы программ этих экзаменов, чтобы в последующем позволить студентам сдать данные экзамены без больших дополнительных усилий.

Следует обратить внимание на согласование содержания данного курса и курса УМК «Основы информационной безопасности», где должны быть частично изложены и основы управления информационными рисками. Новые моменты в изучении данных вопросов должны обязательно присутствовать и заключаться в глубине и широте изучаемых тем.

Как ни странно, но инновационность курса связана и с языковыми различиями. Многие термины появляются в англоязычной литературе по разным причинам раньше чем у нас. Для многих понятий существуют различные обозначения и сочетания слов. Например, одному слову «цель» соответствуют разные слова на английском языке «aim, goal, object, target», слову «оценка» - «evaluation, assessment». Нахождение нужного перевода для появившихся ранее в зарубежной мировой литературе понятий оказывается сложной творческой задачей.

Отличительной особенностью данного курса должно явиться привлечение банковской тематики для демонстрации основных понятий и положений управления рисков. В настоящее время в России идет процесс формирования системы требований информационной безопасности для организаций банковской системы России, созданы несколько стандартов, система сертификации, методика проверки требований. Конечно, при этом использовался зарубежный опыт, но отечественные разработчики и специалисты по ИБ внесли много нового в этот процесс. Требования стандарта Банка России СТО БР ИББС -1.0-2006 «Обеспечение

информационной безопасности организаций банковской системы Российской Федерации. Общие положения» содержат требования по управлению рисками. В настоящее время Банк России готовит рекомендации по Методике оценки рисков РС БР ИББС – 2.3. Изучение и практическое применение этих документов является актуальным и новым направлением в области преподавания информационной безопасности в целом.

1.4. Инновационность курса по методике преподавания и организации учебного процесса.

В данном случае инновационность связана с необходимостью закрепления материала с помощью изучения новых коммерческих программных продуктов, реализующих и автоматизирующих некоторые процессы, связанные с управлением информационными рисками (например, RiskWatch, Авнгард и пр.). Возможно привлечение самих студентов к деятельности по автоматизации изученных методов анализа и оценки информационных рисков, обсуждение и оптимизация предложенных ими программ. Активно должны использоваться и источники из сети Интернет, прошедшие рецензирование специалистами в данной предметной области и рекомендованные ими.

Особенностью методики преподавания является не только выбор и компановка материала, но и направления в его изучении. В данном курсе изучение управления рисками идет на основе первоначального изучения стандартов и нормативно правовой базы передовых в технологическом плане стран (США, Канада, Великобритания, Германия, Австралия, Россия, …) и доходит до международной практики(ISO, ЕС, …). Такой подход диктуется не совсем устоявшейся практикой и научно-методической базой в данной области, которая продолжает изменяться и совершенствоваться в

настоящее время. Разные страны по разному развиваются, лидерство и лучшие практики меняются, и наблюдение и изучение этого процесса является основой для изучения студентами этой области.

1.5. Структура курса.

Виды учебных работ	**Объем работ, час.**	
	Всего	**8 сем.**
Выделено на дисциплину	72 (2 кредита)	72 (2 кредита)
Аудиторная работа:	46	46
- лекции	36	36
- семинары	-	-
- лабораторные занятия	10	10
Самостоятельная работа:	26	26
- курсовой проект	-	-
- курсовая работа	16	16
- домашнее задание	-	-
- самостоятельная проработка курса и подготовка к контрольным работам	10	10
Виды отчетности по дисциплине:		
- зачет	-	**-**
- экзамен	-	Экз.

Темы лекций.

Тема 1. Основные понятия и определения управления информационными рисками (2 часа).

Тема 2. Компоненты процесса управления информационными рисками и их особенности (2 часа).

Тема 3. Методы идентификации активов, угроз, уязвимостей, средств контроля (2 часа).

Тема 4. Возможные варианты обработки рисков и обоснование их выбора (2 часа).

Тема 5. Мониторинг и пересмотр составляющих информационных рисков и всего процесса управления информационными рисками (2 часа).

Тема 6. Политика информационной безопасности и управление информационными рисками (2 часа).

Тема 7. Разработка корпоративной методики анализа рисков (2 часа).

Тема 8. Оценка рисков экспертными методами (2 часа).

Тема 9. Американский стандарт NIST SP 800-30, Risk Management Guide for Information Technology Systems, 2002 (2 часа).

Тема 10. Германский стандарт BSI-Standards 100-3- Risk Analysis based on IT-Grundschutz, ver. 2.0, 2005 (2 часа).

Тема 11. Австралийские стандарты AS/NZS 4360:2004 Risk management. Australian/New Zealand Standard и HB 436: 2004. Risk Management Guidelines. Companion to AS/NZS 4360:2004 (2 часа).

Тема 12. Руководство фирмы Microsoft по управлению рисками безопасности Security Risk Management Guide, 2006 (2 часа).

Тема 13. Проект международного стандарта ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management (draft).(Информационные технологии – Методы безопасности-Управление рисками информационной безопасности) (2 часа).

Тема 14. сравнение методов анализа рисков OCTAVE, CRAMM, BS 7799-3, FIRM, SPRINT, Cobit, Ebios, Marion, Mehari (2 часа).

Тема 15. Отечественные стандарты по рискам. Вопросы гармонизации отечественных и международных стандартов по управлению рисками (2 часа).

Тема 16. Инструментальные средства анализа рисков (2 часа).

Тема 17. Аудит безопасности и анализ информационных рисков (2 часа).

Тема 18. Особенности аудита безопасности организаций банковской системы РФ (2 часа).

Система контроля знаний.

Форма итогового контроля знаний по курсу – экзамен.

Промежуточный контроль знаний в виде проверки выполненных лабораторных работ.

Система текущего контроля знаний учащихся по данному курсу строится по рейтинговому принципу: учащиеся в течение учебного семестра имеют возможность получать зачётные баллы за активную работу в течение семестра. Максимальное количество баллов, которые могут быть набраны таким образом, равно 100 ед. Если в течение семестра учащийся набирает достаточное количество баллов (80 – 100 ед.), он имеет возможность получить отличную оценку без ответа на экзаменационные билеты.

Программа курса УМК

2.1. Аннотированное содержание курса

Изучение данного курса обеспечивает студента сведениями о современном состоянии в области управления информационными рисками и первоначальными навыками оценки и анализа информационных рисков различных информационных систем с привлечением известных программных средств. Курс существенно расширяет и углубляет знания, полученные студентами при изучении дисциплины «Основы информационной безопасности». Материал курса основан на лучшей международной и отечественной практике, как государственных, так и общественных организаций.

Существенное место уделено вопросам управления рисками в процессе аудита информационной безопасности предприятия или организации. Наиболее полно эти вопросы рассматриваются для организаций банковской системы Российской Федерации, для чего изучаются требования и рекомендации Центрального Банка Российской Федерации, содержащиеся в принятых и разрабатываемых стандартах в области информационной безопасности.

В читаемой дисциплине излагаются:

- основные понятия и определения управления информационными рисками;

- технологии анализа информационных рисков;

- зарубежные, международные и отечественные стандарты по управлению информационными рисками;

- инструментальные средства анализа рисков;

- аудит безопасности и анализ информационных рисков

Для самостоятельной работы студентов выбираются темы из перечня тем известных отечественных и международных конференций и семинаров по проблемам информационной безопасности и управления рисками.

Лабораторные работы связаны с изучением и освоением известных готовых коммерческих программных продуктов для анализа информационных рисков.

2.2. Список обязательной и дополнительной литературы.

Далее представлена литература, которая предназначена для студентов и необходимая им для изучения курса. В разделе 2.5 будет представлена литература и Интернет - источники, которые использовались авторами при подготовке самого курса. В частности, они включают примеры программ некоторых зарубежных и отечественных курсов по информационным рискам.

При составлении списка учитывалась доступность литературы для студентов. По крайней мере, авторам курса она доступна или в бумажном виде или в электронном. Если это не так, то имеется указание и рекомендации на ее приобретение. Конечно, главный критерий выбора источника - это его качество. При выборе приходится искать компромисс между классическими и новейшими источниками, которые актуальны на данный определенный момент и еще не прошли проверку временем и практикой.

По возможности указываются страницы Интернет, с которых можно свободно скачать указанные необходимые для изучения курса материалы. Некоторые полезные книги отсканированы авторами и могут быть предоставлены студентам в электронном виде.

Обязательная:

1. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd., 1992. - 932 pp.(Chapter 21. Moses R. Risk analysis and management.)

2. MG-3 “A Guide to RISK ASSESSMENT AND SAFEGUARD SELECTION for Information Technology Systems”, 1996, 73 стр.

3. IT Security Guidance (ITSG), Canadian Handbook on Information Technology Security, 1998, 272 pp, (4. Common threats - 37-45pp, 7. IT Security Risk Management – 71-83, 18. Audit Trails – 215-225pp, 20. Assessing and Mitigating the Risks to Hypothetical IT System – 247-272pp) http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/mg9.pdf

4. MITRE, «NIMS Information Security Threat Methodology», 1998, 35pp, http://www.mitre.org/work/tech_papers/tech_papers_98/nims_information/nims_info.pdf

5. Черешин Д.С., Кононов А.А., Новицкий Е.Г., Цыгичко В.Н. Методика оценки рисков нарушения информационной безопасности в автоматизированных информационных системах. Препринт. – М.: Институт системного анализа РАН, 1999.

6. IT Security Guidance (ITSG), Threat and Risk Assessment Working Guide, Canada, 1999, 132 стр. http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg04.pdf

7. Threat and Risk Assessment Working Guide, 1999, 132стр. Canada.

8. GAO/AIMD-00-33: Information Security Risk Assessment–Practices of Leading Organization, 1999, 50 стр.
http://www.gao.gov/special.pubs/ai00033.pdf

9. Федеральный закон от 7 августа 2001 г. N 119-ФЗ «Об аудиторской деятельности» (с изменениями от 14 декабря, 30 декабря 2001 г.)

10. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения». 12 стр.

11. ГОСТ Р 51901.1-2002, Менеджмент риска. Анализ риска технологических систем. 27 стр.

12. PD3002, Guide to BS7799 Risk Management, 2002, BSI.

13. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.:БХВ-Петербург, 2003.-752 с.: ил. (Гл.13. Управление рисками 189-193, Гл.14. Методики оценки рисков 194-199.)

14. Basel Committee on Banking Supervision «Risk Management Principles for Electronic Banking» 2003, 35pp, http://www.bis.org/publ/bcbs98.pdf

15. Симонов С.В. Современные концепции управления информационными рисками, 2003, http://www.pmprofy.ru/content/rus/85/850-article.asp

16. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004.- 616с. (Гл.13. Управление рисками и построение систем сетевой безопасности. 531-581 стр.)

17. ISO GUIDE 73 Risk Management - Vocabulary - Guidelines for Use in Standards,

18. AS/NZS 4360:2004 Risk management. Australian/New Zealand Standard. 39 стр.

19. HB 436: 2004. Risk Management Guidelines. Companion to AS/NZS 4360:2004. 131 pp.

20. ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management. (ГОСТ Р ИСО/МЭК 18044-проект, Информационная технология - Методы и средства обеспечения безопасности - Менеджмент инцидентов информационной безопасности. 5.1.6 - Менеджмент и анализ рисков ИБ, 7.4 – Политики

менеджмента рисков ИБ, 10.2 – Улучшение анализа рисков и менеджмента безопасности).

21. ISO/IEC Guide 73: 2002, Risk management – Vocabulary – guidelines for use in standards.

22. NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, 2002, 55 стр.

23. ISO/IEC TR 13569:2005, Financial services — Information security guidelines.(ГОСТ Р ИСО/МЭК 13569- проект, Финансовые услуги – рекомендации по информационной безопасности. Раздел 8 –Анализ и оценка риска, Прил.С – Иллюстрация оценки риска.).

24. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная информация. Компания АйТи; ДМК Пресс, 2005.-384 с.

30pp

www.cssf.lu/fileadmin/files/Dossiers/**GRIF**/PAM_ORM_BALE**II**_V01_00.pdf

25. BSI-Standards 100-3, Risk Analysis based on IT-Grundschutz (Анализ рисков на основе « Руководства по защите ИТ для базового уровня защищенности»), ver. 2.0, 2005, 19p..

26. IT-Grundschutz Manual, BSI, http://www.bsi.bund.de/gshb , « Руководстве по защите ИТ для базового уровня защищенности». 2004.

27. CISA Review Manual 2005. Ch. 7 Buiseness process evaluation and Risk Management. 70pp.

28. Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2) http://www.csi.map.es/csi/pg5m20.htm

29. BS 7799-3:2006 – “Information security management systems - Guidelines for information security risk management”.

30. Microsoft Solutions for Security, The Security Risk Management Guide, 2006, http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx

31. ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management (draft) – Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности.

32. Курило А.П. и др. Обеспечение информационной безопасности бизнеса. М.: БДЦ-пресс,2005.-512 с. (Оценка рисков. Экономика информационной безопасности. 452-457)

33. ГОСТ_Р_51901.2-2005 Менеджмент риска. Системы менеджмента надежности. 12 стр.

34. ГОСТ_Р_51901.5-2005 Менеджмент риска. Руководство по применению методов анализа надежности. 72 стр.

35. ГОСТ_Р_51901.14-2005 Менеджмент риска. Метод структурной схемы надежности. 22 стр.

36. ГОСТ_Р_51901.16-2005 Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки. 35 стр.

37. ГОСТ_Р_МЭК_61160-2006 Менеджмент риска. Формальный анализ проекта. 26 стр.

38. Галатенко В.А. Основы информационной безопасности. Курс лекций. М.: ИНТУИТ. РУ, 2006_. – 205 с.(7 лекция. Управление рисками).

39. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.(4. Угрозы информации. 139-172 стр., 5. Методы и модели оценки уязвимости информации.173- 183 стр.)

40. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Компания АйТи, 2006.-400 с. (Политика оценки рисков, 321-322)

41. СТО БР ИББС -1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

42. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: БДЦ-пресс, 2006.-304 с.

43. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006.- 528 стр. (10.4. Анализ рисков и управление рисками. 10.5. Программные средства, используемые для анализа и управления рисками. 477-492 стр.)

44. MAGERIT, VERSION 1.0, Risk Analysis and Management Methodology for Information Systems Procedures Handbook, Spain, 213 стр., http://www.epractice.eu/files/media/media_920.pdf

45. MAGERIT version 2, Methodology for Information Systems Risk Analysis and Management Book I: The method, Book II: Catalogue of elements, Book III: Techniques, http://www.csi.map.es/csi/pg5m20.htm

46. СТО БР ИББС -1.1-2007, «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности», 2007.-14 стр. http://www.cbr.ru/credit/Gubzi_docs/st11.pdf

47. СТО БР ИББС-1.2-2007, «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006»

48. ISO 14971, Medical devices – Application of risk management to medical devices. Second edition, 2007-03-01.

Дополнительная литература

49. Basle Directive № 82, "Risk Management Principles for Electronic Banking," Basel Committee on Banking Supervision, Switzerland, May 2001

50. Basle Directive № 86, "Sound Practices for the Management and Supervision of Operational Risk," Basel Committee on Banking Supervision, Switzerland, May 2001

51. Basle Directive № 91, "Risk Management Principles for Electronic Banking," Basel Committee on Banking Supervision, Switzerland, July 2002

52. Information Systems Control Journal, ISACA, USA: Volume 5, 2002, "Risk Management in IT Projects," pages 37-39; Volume 2, 2003, "Risk Assessment Tools: A Primer," pages 23-25; Volume 5, 2003, "Assessing and Preventing Risks from E-mail System Use," 33-35

53. Gilbert I.E. Guide for selecting automated risk analysis tools, 26 pp.

54. Hoffman L. Modern methods for computer security and privacy. Prentice-Hall,Inc.,1977.

Русский перевод: Хоффман Л.Д. Современные методы защиты информации .-М.: Сов. радио, 1980.

55. Hsiao D., Kerr D., Mednick S. Computer security. Academic Press, 1979.

Русский перевод: Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. М.:Мир,1982.

56. Russel D., G.T.Gangemi Sr. Computer Security Basics. –O`Reilli & Associates, Inc., 1991. – 448 pp.

57. Muftic S. Security Mechanisms for Computer Networks. Halsted Press.

Русский перевод: Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

58. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 1994, Кн. 1 и 2.

59. Гайкович В., Першин А. Безопасность электронных банковских систем. –М.: Единая Европа, 1994.

60. Горохов П.К. Информацинная безопасность. Англо-русский словарь. – М.: Радио и связь, 1995. 224 с.-

61. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Яхтсмен, 1996.

62. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997 г., - 538 с., учебник (рекомендован Минобразованием России в качестве учебника для студентов ВУЗов).

63. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. – СПб.: НПО Мир и семья, 1997.

64. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.:Радио и связь, 1999. – 328 с.

65. ГОСТ Р 51275-99, Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

66. ISO 9004, СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА. РЕКОМЕНДАЦИИ ПО УЛУЧШЕНИЮ ДЕЯТЕЛЬНОСТИ. QUALITY MANAGEMENT SYSTEMS – GUIDELINES FOR PERFORMANCE IMPROVEMENTS, 2000, 90 стр.

67. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. М.: СИНТЕГ, 2000, -248 с.

68. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности, –М: Радио и связь, 2000. -192 с.

69. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телекомю 2000. – 452 с.

70. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учебное пособие. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.

71. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г.,-148 с.

72. Barman S. Writing Information Security Policies. 2001.

Русский перевод: Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2002.- 208 с.

73. Голдовский И. Безопасность платежей в Интернете. – СПб : Питер, 2001. – 240 с.

74. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. – М.: ФОРУМ: ИНФРА-Мб 2002. – 368 с.

75. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

76. CMS Information Security Risk Assessment (RA) Methodology, CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS), 2002, 20pp, http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/RA_meth.pdf

77. Pieprzyk J., Hardjono T., Seberry J. Fundamentals of Computer Security. Springer-Verlag Berlin Heidelberg, 2003. -677 p.

78. Галатенко В.А. Стандарты информационной безопасности. Курс лекций. М.: ИНТУИТ. РУ, 2004. – 328 с.

79. Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска. – М.: Изд. Дом ГУ ВШЭ, 2005.-400 с.(Для моделирования рисков в страховых и пенсионных схемах и в финансах).

80. Jones J.A., An Introduction to Factor Analysis of Information Risk (FAIR), A framework for understanding, analyzing, and measuring information risk, 2005, 67 pp,
http://nujia.norwich.edu/current/2_1_art01NUJIA.pdf

81. Ken Biery Jr. 2006, Aligning an information risk management approach to **BS 7799-3**:2005. 2006,79pp,
www.sans.org/reading_room/whitepapers/auditing/1664.php

82. GCIO – Government Chief Information office, Guidelines/ Information Security Guidelines for NSG Government Agencies. Feb 2007, 111pp. (Ch.5 – Risk Management, 28-46, Annex B.- Risk assessment, 58-82).
http://www.gcio.nsw.gov.au/documents/Information%20Security%20Guideline%20V1.1.pdf

83. Stephenson P.R., A Formal Model for Information Risk Analysis Using Colored Petri Nets, 2004, 18pp, FARES
http://www.daimi.au.dk/CPnets/workshop04/cpn/papers/stephenson.pdf

84. Assessing Cyber-Threats in the Information Environment, 2004, 19pp,
http://www.glam.ac.uk/socschool/research/publications/technical/CS-04-01.pdf

85. Vidalis S. A Critical Discussion of Risk and Threat Analysis Methods and Methodologies, 2004, 33pp
www.glam.ac.uk/socschool/research/publications/technical/CS-04-03.pdf

86. GCIO – Government Chief Information office, Project Risk Management Guideline, Sep 2004. 34pp
http://www.gcio.nsw.gov.au/documents/Project_Risk_Man_0904.pdf

87. Чекалин А.А., Заряев А.В., и др. Защита информации в системах мобильной связи: Учебное пособие для вузов. – М.: Горячая линия-телеком, 2005. – 171 с. (Гл.3 Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз. Гл.4 Практические аспекты защиты информации в системах мобильной связи

стандарта GSM. Гл.6 Защита информации в перспективных системах мобильной связи.)

88. The Standard of Good Practice for Information Security, Inf. Sec. Forum-ISF, v.4.0-2003 (2005-New), 240pp. http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf .

89. Chris Ralph, Risk Analysis for HIPAA Compliancy, 2005, 16pp, http://www.giac.org/certified_professionals/practicals/ghsc/32.php

90. Доля А.А. Внутренние ИТ - угрозы в России – 2006. «Защита информации. Инсайд», №2 март-апрель 2007. 60-69 стр.

91. Pfleeger C.P, Pfleeger S.L., Security in Computing, Prentice Hall Publishing, 2003.

92. Alberts, C & Dorofee, A, *Managing Information Security Risks*. Boston, Addison Wesley, 2003.

93. Jordon, E & Silcock, L *Beating IT Risks*, Chichester, John Wiley & Sons, Australia Ltd, 2006.

94. Slay, J & Koronios, A, *IT Security and Risk Managment*, John Wiley & Sons, Australia Ltd, 2006.

95. Peltier, TR, *Information Security Risk Analysis*, 2nd edn, Auerbach Publications, 2005.

Оригиналы международных стандартов и их лицензионные переводы на русский язык можно приобрести в интернет-магазине GlobalTrust.ru: http://shop.globaltrust.ru/show_cat.p...&grid=5001 .

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании", и Федеральным законом Российской Федерации от 1 мая 2007 г_ N 65-ФЗ “О внесении изменений в Федеральный закон “О техническом регулировании”.

Правила применения национальных стандартов Российской Федерации установлены в ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".

2.3. Темы рефератов, курсовых работ, эссе

Темы для самостоятельной работы студентов при подготовке рефератов и курсовых работ определяются на основе тематики известных признанных научных конференций и семинаров, рассматривающих вопросы безопасности ИТ систем. Среди таких мероприятий выделим следующие.

USENIX Security Symposium.

IEEE Symposium on Security and Privacy.

ACM Conference on Computer and Communications Security (CCS).

ISOC Network and Distributed System Security Symposium (NDSS).

International Symposium on Recent Advances in Intrusion Detection (RAID).

GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA).

Annual EICAR Conference.

Annual Computer Security Applications Conference (ACSAC).

International Conference on Applied Cryptography and Network Security (ACNS).

ACM Symposium on Information, Computer and Communications Security (ASIACCS).

European Symposium on Research in Computer Security (ESORICS).

Financial Cryptography and Data Security (FC).

ACM Workshop on Recurring Malcode (WORM).

DEFCON.

BlackHat.

The Virus Bulletin International Conference.

AVAR International Conference.

CanSecWest and EuSecWest Conferences.

Hack In The Box (HITB) Conference.

RSA Conference.

Chaos Communication Congress (CCC).

Труды большинства этих конференций и семинаров доступны для образовательных учреждений в сети Интернет на сайте http://www.springerlink.com/ .

Примеры тем.

- Управление рисками и защита информации в системах мобильной связи.

- Анализ рисков электронных платежных систем.

- Защита портативных электронных устройств в условиях рисков.

- Обнаружение сетевых атак и управление рисками.

- Анализ рисков и оценка затрат на информационную безопасность.

- Теория полезности в задачах оценки рисков.

- Риски информационной безопасности, связанные с аутсорсингом IT-сервисов.

- Страхование рисков электронной коммерции.

- Управление рисками и обеспечение непрерывности бизнеса.

- Угрозы безопасности беспроводных сетей.

2.4. Учебный тематический план курса

Раздел 1.
Введение. Основные понятия и определения управления информационными рисками.

Терминология и определения в публикациях на английском языке, сложности перевода. Сравнение с публикациями на русском языке.

Место управления рисками в общей системе управления информационной безопасности и защиты информации. Основные и дополнительные источники для изучения проблем управления рисками.

Компоненты процесса управления информационными рисками:

- установка контекста,
- учет(оценка) рисков(risk assessment),
- обработка рисков(risk treatment),
- принятие рисков(risk acceptance),
- коммуникация рисков(risk communication),
- мониторинг и пересмотр рисков.

Компоненты процесса оценки рисков:

- анализ рисков(risk analysis),
- оценивание рисков(risk evaluation).

Компоненты анализа рисков:

- идентификация рисков(идентификация активов, угроз, уязвимостей, влияния, средств контроля),

- количественная оценка рисков(risk estimation)(качественная, полуколичественная, количественная оценка, ценность активов и оценка влияния, вероятности угроз, оценка простоты использования уязвимостей).

Варианты обработки рисков:

- предотвращение риска,

- снижение риска,

- перенос риска,

- принятие риска.

Мониторинг и пересмотр составляющих информационных рисков и всего процесса управления информационными рисками. Итеративный подход к процессам управления рисками. Связь политики информационной безопасности и управления информационными рисками.

Раздел 2

Технологии анализа информационных рисков.

Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Измерение рисков. Выбор допустимого уровня рисков. Выбор средств защиты (контрмер) и оценка их эффективности.

Разработка корпоративной методики анализа рисков. Методы оценки информационных рисков.

Оценка рисков экспертными методами. Оценка субъективной вероятности, классификация методов получения субъективной вероятности. Методы оценок непрерывных распределений.

Высокоуровневая и детальная оценка рисков.

Раздел 3.

Управление информационными рисками и стандарты (зарубежные, международные, отечественные)

Стандарты и организации по стандартизации.

Американский стандарт NIST SP 800-30, Risk Management Guide for Information Technology Systems, 2002.

Германский стандарт BSI-Standards 100-3- Risk Analysis based on IT-Grundschutz, ver. 2.0, 2005.

Австралийские стандарты AS/NZS 4360:2004 Risk management. Australian/New Zealand Standard и HB 436: 2004. Risk Management Guidelines. Companion to AS/NZS 4360:2004.

Руководство фирмы Microsoft по управлению рисками безопасности Security Risk Management Guide, 2006.

Концепция управления рисками MITRE.

OCTAVE, CRAMM, BS 7799-3, FIRM, SPRINT, Cobit, , Ebios, Marion, Mehari, ….

Проект международного стандарта ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management (draft).(Информационные технологии – Методы безопасности- Управление рисками информационной безопасности)

Стандарты Интернет.

Федеральный закон РФ «О техническом регулировании» и поправки к нему. Отечественные стандарты ГОСТ по рискам. (ГОСТ Р 51898–2002, ГОСТ_Р_51901-2005, ГОСТ_Р_МЭК_61160-2006, и другие)Вопросы гармонизации отечественных и международных стандартов по управлению рисками.

Раздел 4

Программные средства, используемые для анализа и управления рисками.

Описание, анализ и сравнение современных программных продуктов по анализу рисков:

COBRA.
CRAMM.
RiskWatch.
Buddy System.
RA Software Tool.
IBM Tivoli Risk Manager.
Экспертная система «Авангард».

Изучение и практическое освоение данных и подобных средств может служить основой для проведения лабораторных работ(практических занятий). Сдерживающим моментом может быть только необходимость приобретения этих программных продуктов у соответствующих производителей. Но, некоторые производители(коммерческие фирмы) могут предоставить бесплатно свои демонстрационные версии или специальные версии для обучения.

Раздел 5

Аудит безопасности и анализ информационных рисков

Актуальность аудита безопасности. Основные понятия и определения. Отечественные законы и стандарты по аудиту.

Особенности аудита безопасности организаций банковской системы РФ. Система стандартов и рекомендаций Центрального Банка РФ. Требования ЦБ РФ по управлению информационными рисками.

2.5. Использованная для подготовки курса литература и Интернет - источники.

Данный материал предназначен для преподавателей, а не студентов, и демонстрирует объективность выбора тем курса. Этот материал также позволяет углубить знания в данной предметной области.

2.5.1. Программы некоторых курсов по информационным рискам

ISM201 “Information Risk Management ”(Управление информационными рисками)-
http://www.misti.com/default.asp?Page=10&pcID=3498
См. также: Программы курсов по информационной безопасности. Учебный центр МИКРОИНФОРМ, М.2007, 24-26 стр.

http://infosystem.ru/longkurs.php?fid=1177677961154892
Управление рисками информационной безопасности современной организации. Методики и практические аспекты, #IS 017, Академия Информационных Систем.

www.cisse.info/colloquia/cisse10/proceedings10/pdfs/papers/S01P04.pdf - A University Course in Information System Risk Analysis / Security Certification and accreditation. Schembari N.P., Univ. of Pennsylvania, 2006.

http://www.qaimea.com/pdfs/Information%20Security%20Risk%20Management.pdf программа курса «Information Security Risk Management» из Quality Assurance Institute Middle East and Africa.
http://www.insight.co.uk/files/courses/Information%20Security%20Risk%20Analysis%20and%20Management%20Overview%20Course%20(Datasheet).pdf Information Security Risk Analysis and Management Overview. A practical explanation of risk analysis and management tools and techniques.

http://courses.swinburne.edu.au/Subjects/ViewSubject.aspx?mi=300&id=5195 Information Systems Risk and Security, Unit Code: HIT8408.

http://www.isg.rhul.ac.uk - the Information Security Group. The ISG is one of the largest academic security groups in the world. The ISG also includes the Smart Card Centre of Excellence which it founded with Vodafone and Giesecke & Devrient.
http://www.isg.rhul.ac.uk/node/111 Risk Assessment, Duration/Units: 2 days/units.
Course Aims: The course enables participants to identify and prioritise the cost effective use of resources to protect business critical information assets from a breach of security. The course defines risk analysis and introduces risk management processes. The theory of risk analysis is considered in detail, supported by the practical use of methodologies.

http://www.bsi-global.com/en/Shop/Training-Detail-Pages/ISEB-Practitioner-Certificate-in-Information-Risk-Management/ ISEB Practitioner Certificate in Information Risk Management.
BSI Group.

http://www.professional.ie/course_details.php?id=3520 Information Risk Management．Professional Training Solutions Limited.
Description: Protecting critical information assets in a world of interconnected technologies challenges current security management practices, tools and methodologies. Strategies for addressing these issues need to assess organisational and technological risks in the context of the organisation's high-priority assets. This course provides managers and key decision-makers with a framework for evaluating and managing risk to an organisation's information assets.

2.5.2. Другие источники

Pattinson F. Certifying Information Security Management Systems, July 2007, www.net-security.org/dl/articles/CertifyingISMS.pdf 11 стр.

ENISA Result: Risk Management / Risk Assessment in European regulation, international guidelines and codes of practice, 2007, 105 стр.
http://www.enisa.europa.eu/rmra/files/rmra_regulation.pdf
ENISA - Inventory of Risk Management Methods and Tools
http://www.enisa.europa.eu/rmra/

http://www.nr.no/~abie/RiskAnalysis.htm Risk Analysis, Risk Assessment, Risk Management, страница Habtamu Abie.
http://portal.surrey.ac.uk/portal/page?_pageid=823,181361&_dad=portal&_schema=PORTAL - Risk Management at University of Surrey

http://www.prmia.org/ - Professional Risk Managers Association (PRMIA).

http://econpapers.repec.org/paper/boeboeewp - Bank of England working papers.

http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail_00.html Booklet: Retail Payment Systems, Section: Introduction.

2.6. Некоторые определения из области управления информационным риском

анализ риска: Систематическое использование информации для выявления опасности и количественной оценки риска.

[ГОСТ Р 51898–2002, статья 3.10]

допустимый риск: Риск, который в данной ситуации считается приемлемым при существующих общественных ценностях.

[ГОСТ Р 51898–2002, статья 3.7]

защитная мера: Мера, используемая для уменьшения риска.

[ГОСТ Р 51898–2002, статья 3.8]

обработка риска: Процесс выбора и осуществления мер по модификации риска.

Примечания

1 Термин «обработка риска» иногда используют для обозначения самих мер.

2 Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска.

[ГОСТ Р 51897–2002, статья 3.4.1]

операционный риск: Риск прямых или косвенных потерь от неадекватных или имеющих недостатки внутренних процессов, людей и систем или от внешних событий.

[Базель 2]

остаточный риск: Риск, остающийся после предпринятых защитных мер.

[ГОСТ Р 51898–2002, статья 3.9]

оценивание риска: Основанная на результатах анализа риска процедура проверки, устанавливающая, не превышен ли допустимый риск.

[ГОСТ Р 51898–2002, статья 3.11]

оценка риска: Общий процесс анализа риска и оценивания риска.

[ГОСТ Р 51898–2002, статья 3.12]

перенос риска: Разделение с другой стороной бремени потерь или выгод от риска.

Примечания

1 Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

2 Перенос риска может быть осуществлен страхованием или другими соглашениями.

3 Перенос риска может создавать новый риск или модифицировать существующий риск.

4 Перемещение источника не является переносом риска.

[ГОСТ Р 51897–2002, статья 3.4.7]

принятие риска: Решение принять риск.

Примечание – Принятие риска зависит от критериев риска.

[ГОСТ Р 51897–2002, статья 3.4.10]

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898–2002, статья 3.2]

снижение риска: Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.

[ГОСТ Р 51897–2002, статья 3.4.4]

ущерб: Физическое повреждение или другой вред здоровью людей, имуществу или окружающей среде.

[ГОСТ Р 51898–2002, статья 3.3]

Основным научным результатом проведённой работы явилась разработка описания и программы УМК «Управление информационными рисками», учитывающей основные современные тенденции развития ИТ, потребности рынка труда, в том числе с учетом международной и отечественной практики.

Разработка новой учебной программы осуществлена на основе аналитической работы по выявлению, отбору и систематизации открытых источников информации, а также работы по сравнительному анализу, оценке и отбору аналогичных учебных курсов, преподаваемых в зарубежных высших учебных заведениях.

Поиск и анализ литературы показал на отсутствие достаточного количества литературы на русском языке и наличие большого числа публикаций на английском языке, что требует написания специального учебного пособия по этому курсу.

Для практического освоения курса необходимо знакомство с современными программными продуктами по анализу рисков, которые разработаны и используются на практике многими предприятиями и организациями. Возможна и самостоятельная реализация методов оценки рисков силами кафедры или студентами для конкретных информационных систем.

Разработанный курс целесообразно изучать после изучения курса «Основы информационной безопасности», как развитие и углубление одного из важных его направлений.