Управление системой информационной безопасности

Вводная часть

В ходе данного занятия будет изучена систему управления информационной безопасности и ее содержание, а также анализ и управление рисками информационной безопасности.

Актуальность данного занятия обусловлена требованиями **ГОСТ 27002-2012** «Методы и средства обеспечения безопасности». После того как были определены требования к безопасности и риски безопасности и приняты решения в отношении обработки рисков, следует выбрать и внедрить такие меры и средства контроля и управления, которые обеспечат уверенность в снижении рисков до приемлемого уровня. Меры и средства контроля и управления могут быть выбраны из ГОСТ 27002 и других источников, а также могут быть разработаны новые меры и средства контроля и управления, удовлетворяющие специфическим потребностям организации. Выбор мер и средств контроля и управления зависит от решений организации, основанных на критериях принятия рисков, вариантах обработки рисков и общем подходе к менеджменту рисков, применяемом в организации. При этом необходимо также учитывать все соответствующие национальные и международные законы и нормы. Некоторые меры и средства контроля и управления, приведенные в ГОСТ 27002, рекомендуется рассматривать как руководящие принципы для управления информационной безопасностью и применять для большинства организаций. Более подробно такие меры и средства контроля и управления рассматриваются в ГОСТ 27002 под заголовком «Отправная точка информационной безопасности».

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Управление системой информационной безопасности.
2. Анализ и управление рисками информационной безопасности.

Рассмотрим первый учебный вопрос.

Первый учебный вопрос: «Управление системой информационной безопасности»

Данный учебный вопрос начнем с изучения сути понятия «управление».

Управление заключается в целенаправленном воздействии на объект управления с целью достижения им цели своего функционирования.

В данном случае, под **объектом управления** будем понимать совокупность элементов СИБ, целенаправленное воздействие на которые обеспечит выполнение задач информационной безопасности.

К управлению информационной безопасностью относятся силы управления и средства управления.

В соответствии с **ГОСТ 27000-2012** «Системы менеджмента информационной безопасности» и **ГОСТ 53114** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Система управления – система, включающая в себя политики, процедуры, рекомендации и связанные с ними ресурсы для достижения целей организации.

В части информационной безопасности система управления позволяет организации:

- удовлетворять требования безопасности клиентов и других заинтересованных лиц;
- улучшать планы и действия организации;
- соответствовать целям информационной безопасности организации;
- выполнять регулирующие требования, требования законодательства и отраслевые нормативные документы;
- организованно управлять информационными активами для облегчения непрерывного совершенствования и регулирования текущих организационных целей и внешних условий.

Управление информационной безопасностью организации – скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации.

Система управления информационной безопасности использует совокупность ресурсов для достижения целей организации, и включает в себя организационную структуру, политику, планирование действий, обязательства, методы, процедуры, процессы и ресурсы.

Таким образом, **система управления информационной безопасностью** – часть общей системы менеджмента организации (предприятия), основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

При этом, **ГОСТ Р ИСО/МЭК 27001** «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» определяет, что:

Целью построения системы менеджмента информационной безопасности бизнеса является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Термин «бизнес», в настоящем стандарте понимаемый в широком смысле, обозначает всю ту деятельность, которая является основой для целей существования организации.

Как уже было сказано, после определения требований к информационной безопасности и оценки рисков информационной безопасности для идентифицированных информационных активов (включая решения для обработки рисков информационной безопасности) должны быть выбраны и реализованы соответствующие меры и средства контроля и управления, чтобы гарантировать, что риски информационной безопасности уменьшены до уровня, приемлемого для организации.

Меры и средства контроля и управления могут быть выбраны с помощью стандарта ГОСТ 27002-2012 или из других соответствующих наборов средств управления. Также для удовлетворения специфических потребностей могут быть разработаны новые соответствующие меры и средства контроля и управления. Выбор средств управления безопасностью зависит от требований безопасности, принимающих во внимание критерии для принятия риска информационной безопасности, вариантов обработки риска и общего подхода управления рисками, применяемого организацией. Выбор и реализация средств управления могут быть документированы в Политике информационной безопасности.

Меры и средства контроля и управления, изложенные в ГОСТ 27002-2012, общепризнаны как лучшие методы, применимые к большинству организаций. Они были разработаны для того, чтобы удовлетворять требованиям организаций разной величины и структуры.

Отдельные меры и средства контроля и управления могут рассматриваться как подходящая отправная точка информационной безопасности. Такие меры и средства контроля и управления либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Законодательными мерами и средствами контроля и управления информационной безопасности для организации являются:

a) защита данных и конфиденциальность персональных данных;

b) защита документов организации;

c) права на интеллектуальную собственность.

Практические меры и средства контроля и управления информационной безопасности организации, включают:

a) документирование политики информационной безопасности;

b) распределение обязанностей по обеспечению информационной безопасности;

c) осведомленность, обучение и тренинг в области информационной безопасности;

d) корректирующая обработка в прикладных программах;

e) менеджмент технических уязвимостей;

f) менеджмент непрерывности бизнеса;

g) менеджмент инцидентов информационной безопасности и необходимое совершенствование.

Следует отметить, что, хотя все меры и средства контроля и управления являются важными, уместность какой-либо меры и средства контроля и управления должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что данный подход рассматривается как отправная точка информационной безопасности, он не заменяет выбор мер и средств контроля и управления, основанный на оценке рисков.

Организации или предприятию нужно вести различные виды деятельности и управлять ими для того, чтобы функционировать результативно. Любой вид деятельности, использующий ресурсы и управляемый для того, чтобы обеспечить возможность преобразования входных данных в выходные данные, можно считать процессом.

Выходные данные одного процесса могут непосредственно формировать входные данные следующего процесса. Обычно такая трансформация происходит в условиях планирования и управления. Применение системы процессов в рамках организации вместе с идентификацией и взаимодействием этих процессов, а также их управлением может быть определено как «процессный подход».

Процессный подход для СИБ, основан на операционном принципе, принятом в стандартах системы управления ISO и общеизвестном как процесс «План (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)» (**PDCA**):

- план – постановка целей и разработка планов (провести анализ ситуации в организации, наметить общие цели, поставить задачи и разработать планы для их достижения);

- осуществление – реализация планов (выполнить то, что было запланировано);

- проверка – проверка результатов (измерение/контроль степени соответствия достигнутых результатов плану);

- действие – коррекция и улучшение работы (учиться на ошибках, чтобы улучшить работу и достичь лучших результатов).

При этом, обращаю ваше внимание на разумную достаточность в планировании, что бы вы не погрязли в большом количестве различных планов, которые потребуют еще большего количества отчетных документов.

Далее рассмотрим содержание системы управления информационной безопасности.

В соответствии с ГОСТ 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» для

разработки системы управления информационной безопасности, организация должна осуществить следующее:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия;

b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:

1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;
2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;
3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ;
4) устанавливает критерии оценки рисков;
5) утверждается руководством организации. При этом необходимо отметить, что политика СМИБ имеет приоритет перед политикой ИБ. Эти политики могут быть изложены в одном документе;

c) определить подход к оценке риска в организации, для чего необходимо:

1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности;
2) разработать критерии принятия риска и определить приемлемые уровни риска. Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты;

d) идентифицировать риски, для чего необходимо:

1) идентифицировать активы в пределах области функционирования СМИБ и определить владельцев этих активов;
2) идентифицировать угрозы этим активам;
3) идентифицировать уязвимости активов, которые могут быть использованы угрозами;
4) идентифицировать последствия воздействия на активы в результате возможной утраты конфиденциальности, целостности и доступности активов;

e) проанализировать и оценить риски, для чего необходимо:

1) оценить ущерб для деятельности организации, который может быть нанесен в результате сбоя обеспечения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;
2) оценить реальную вероятность сбоя обеспечения безопасности с учетом превалирующих угроз, уязвимостей и их последствий,

связанных с этими активами, а также с учетом применяемых мер управления безопасностью;

3) оценить уровни рисков;

4) определить, являются ли риски приемлемыми или требуют обработки с использованием критериев допустимости рисков;

f) определить и оценить различные варианты обработки рисков. Возможные действия:

1) применение подходящих мер управления;

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

3) избежание рисков;

4) передача соответствующих деловых рисков сторонним организациям, например, страховщикам или поставщикам;

g) выбрать цели и меры управления для обработки рисков. Цели и меры управления должны быть выбраны и реализованы так, чтобы удовлетворять требованиям, определенным в процессе оценки и обработки рисков. Этот выбор должен учитывать критерии принятия рисков, а также нормативно-правовые требования и договорные обязательства;

h) получить утверждение руководством предполагаемых остаточных рисков;

i) получить разрешение руководства на внедрение и эксплуатацию СМИБ;

j) подготовить Положение об управлении СИБ, которое включает в себя следующее:

1) цели и меры управления, и обоснование этого выбора;

2) цели и меры управления, реализованные в настоящее время.

Для **внедрения и функционирования системы управления информационной безопасности** организация должна выполнить следующее:

a) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ;

b) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

c) внедрить меры управления для достижения целей управления;

d) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные. Измерение результативности мер управления позволяет руководителям и персоналу определить, в какой степени меры управления способствуют достижению намеченных целей управления;

e) реализовать программы по обучению и повышению квалификации сотрудников;

f) управлять работой СМИБ;

g) управлять ресурсами СМИБ;

h) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Для **проведения мониторинга и анализа системы управления информационной безопасности** организация должна осуществлять следующее:

a) выполнять процедуры мониторинга и анализа, а также использовать другие меры управления в следующих целях:

1) своевременно обнаруживать ошибки в результатах обработки;
2) своевременно выявлять удавшиеся и неудавшиеся попытки нарушения и инциденты ИБ;
3) предоставлять руководству информацию для принятия решений о ходе выполнения функций по обеспечению ИБ, осуществляемых как ответственными лицами, так и информационными технологиями;
4) способствовать обнаружению событий ИБ и, таким образом, предотвращать инциденты ИБ путем применения средств индикации;
5) определять, являются ли эффективными действия, предпринимаемые для устранения нарушения безопасности;

b) проводить регулярный анализ результативности СМИБ (включая проверку ее соответствия политике и целям СМИБ и анализ мер управления безопасностью) с учетом результатов аудиторских проверок ИБ, ее инцидентов, результатов измерений эффективности СМИБ, а также предложений и другой информации от всех заинтересованных сторон;

c) измерять результативность мер управления для проверки соответствия требованиям ИБ;

d) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения:

1) в организации;
2) в технологиях;
3) в целях деятельности и процессах;
4) в выявленных угрозах;
5) в результативности реализованных мер управления;
6) во внешних условиях, например, изменения нормативно-правовых требований, требований договорных обязательств, а также изменения в социальной структуре общества;

e) проводить внутренние аудиты СМИБ через установленные периоды времени. Внутренние аудиты, иногда называемые аудитами первой стороны, проводятся самой организацией (или внешней организацией от ее имени) для собственных целей;

f) регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;

g) обновлять планы ИБ с учетом результатов анализа и мониторинга;

h) регистрировать действия и события, способные повлиять на результативность или функционирование СМИБ.

Далее организуется непосредственное управление системой информационной безопасности.

Организация управления СИБ дает возможность решить две задачи управления системой информационной безопасности:

1. Задача количественной оценки текущего уровня информационной безопасности компании.

Выполнение этой задачи основано на оценке рисков ИБ на организационно-правовом, экономическом, инженерно-техническом и других уровнях обеспечения защиты информации.

2. Задача разработки и реализации комплексного плана совершенствования СИБ организации для достижения приемлемого уровня защищенности его информационных активов.

Для решения этой задачи необходимо:

- обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании;
- создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Решение названных задач открывает новые широкие возможности перед должностными лицами разного уровня по управлению СИБ.

Руководителям верхнего звена это поможет объективно и независимо оценить текущей уровень информационной безопасности организации, обеспечить формирование единой концепции безопасности, рассчитать, согласовать и обосновать необходимые затраты на защиту компании.

На основе полученной оценки ***начальники отделов и служб*** смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях).

Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, определить основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов организации (предприятия).

При выполнении данных работ целесообразнее всего использовать модель управления СИБ (рис. 1), основанную на использовании так называемых «Общих критериев», изложенных в стандарте информационной безопасности (ГОСТ Р ИСО/МЭК 15408-1), а также на проведении анализа рисков ИБ на основе требований международного стандарта «Управление информационной безопасностью» (ISO/IEC 17799).

Рисунок 1 – Модель управления СИБ

Представленный подход к управлению системой информационной безопасностью заключается в рассмотрении совокупности объективных внешних и внутренних факторов и их влияния на состояние информационной безопасности объекта, а также на сохранность материальных или информационных ресурсов.

При этом рассматриваются следующие объективные факторы, влияющие на модель СИБ:

- *угрозы информационной безопасности*, характеризующиеся вероятностью возникновения и вероятностью реализации;

- *уязвимости информационной системы* или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

- *величины рисков*, отражающих возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования. Риск удобнее всего представлять в виде вероятных финансовых потерь организации – прямых или косвенных.

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему обеспечения информационной безопасности необходимо построить таким образом, чтобы достичь заданного уровня риска.

Последовательность моделирования системы информационной безопасности строится следующим образом:

- для основных информационных ресурсов организации определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации, дезорганизации деятельности организации и нематериального ущерба от разглашения конфиденциальной информации и др.;

- описываются взаимосвязи ресурсов;

- определяются угрозы информационной безопасности и оцениваются вероятности их реализации;

- на основе построенной модели проводится выбор системы контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью.

Техническая документация, разрабатываемая в процессе реализации СИБ должна содержать набор требований безопасности информационной среды организации, эскизный проект, план защиты и др.

В общем виде разработка технической документации включает:

- уточнение функций защиты;

- определение принципов построения СИБ;

- разработку логической структуры СИБ;

- уточнение требований к СИБ;

- разработку методики создания системы;

- разработку программы испытаний на соответствие СИБ сформулированным требованиям.

Таким образом, мы рассмотрели основные вопросы управления системой информационной безопасности.

На этом изложение первого учебного вопроса завершено.

Второй учебный вопрос: «Анализ и управление рисками информационной безопасности»

При изучении предыдущих материалов мы рассмотрели, что существует два основных подхода к созданию системы защиты информации (рис.2).

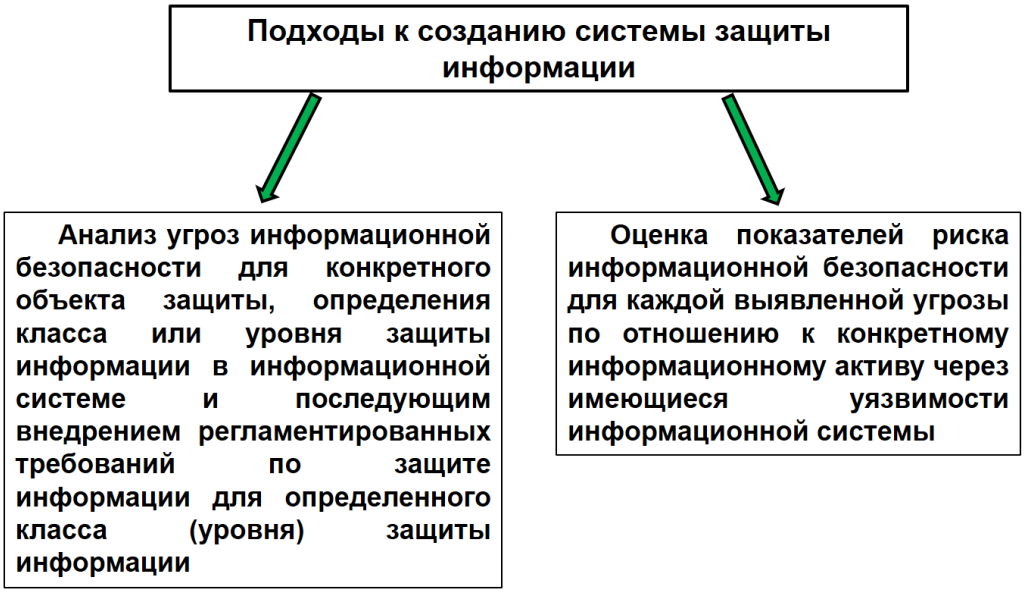

Рисунок 2 – Основные подходы к созданию системы защиты информации

Основные положения первого подхода вы изучили в ходе предыдущих занятий, а изученный вами материал в комплексе, позволяет перейти к изучению второго подхода, основанного на оценке показателей риска информационной безопасности для каждой выявленной угрозы по отношению к конкретному информационному активу через имеющиеся уязвимости информационной системы.

Управление рисками информационной безопасности требует соответствующей оценки риска и метода обработки риска. Это может включать в себя оценку затрат и преимуществ, законных требований, социальных, экономических и экологических аспектов, проблем заинтересованных лиц, приоритетов и других исходных данных, и переменных.

Результаты оценки риска информационной безопасности помогут выработать и провести соответствующие управленческие решения для действий и установления приоритетов для управления рисками

информационной безопасности, а также для реализации соответствующих средств управления безопасностью для защиты от этих рисков. **ГОСТ ИСО/МЭК 27005** «Менеджмент риска информационной безопасности» обеспечивает руководство менеджментом рисков информационной безопасности, включая рекомендации относительно оценки риска, обработки риска, принятия риска, коммуникации риска, контроля риска и анализа риска.

Подходы руководства различных отечественных организации к решению проблем обеспечения информационной безопасности можно выразить следующими тенденциями:

- примерно в 50% организаций не проводится контроля инцидентов в области информационной безопасности;

- примерно в 60% организаций для оценки СИБ не используют оценочные (расчетные) критерии;

- при использовании ***критериев оценки защищенности информационных ресурсов организации, приоритеты следующие*** (в сторону снижения):

а) корпоративные стандарты или собственная разработка;
б) результаты работы аудиторов;
в) требования международных стандартов в области ИБ;
г) количество инцидентов в области ИБ;
д) финансовые потери в результате инцидентов;
е) расходы на ИБ;
ж) степень достижения поставленных целей.

Понятие риска является краеугольным как для бизнеса, так и для системы организации информационной безопасности.

С точки зрения рисков следует иметь в виду два аспекта:

- во-первых, любую систему безопасности можно преодолеть, имея достаточно ресурсов и времени. Поэтому риски могут быть идентифицированы и уменьшены, но никогда не «уничтожены» полностью;

- во-вторых, все организации разные, поэтому процесс минимизации рисков для каждой организации имеет свои уникальные черты. Примеры других организации могут помочь, но адекватная оценка реальности - лучший помощник, ведь даже небольшие изменения в методике или организационной структуре могут повлечь значительные последствия, связанные с рисками. К тому же при внедрении нужны средства, учитывающие локальные особенности. Например, средства шифрования во всех развитых странах имеют свои системы стандартов, свои сертификаты и, соответственно, свои регламенты использования.

Рост экономики, усиливающаяся конкуренция порождают ***еще одну проблему безопасности*** – слияние организаций, поглощение мелких и средних компаний более крупными. При этом неизмеримо возрастают трудности межоперационного взаимодействия, возникает необходимость интеграции разнородных систем, что приводит к росту рисков.

Минимизация рисков, построение всеохватывающей системы информационной безопасности – процесс весьма сложный, длительный и

затратный. В мире нет ни одной организации, в которой реализован был бы весь набор средств и все необходимые, описанные в стандартах, процессы.

Выбор подходящих методов и степени защиты является субъективным процессом, и лишь отчасти регламентируемым нормативными актами.

Далее, товарищи студенты, рассмотрим суть термина «риски».

Под рисками в общем смысле слова понимается характеристика ситуации, имеющей неопределенность исхода, при обязательном наличии неблагоприятных последствий. Риск предполагает неуверенность, либо невозможность получения достоверного знания о благоприятном исходе в заданных внешних обстоятельствах.

Риск в узком смысле – измеряемая или рассчитываемая вероятность неблагоприятного исхода.

В соответствии с **ГОСТ 27000-2012** «Системы менеджмента информационной безопасности»:

Риск информационной безопасности – это потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации.

Управление риском информационной безопасности организации – скоординированные действия по руководству и управлению организацией в отношении риска информационной безопасности с целью его минимизации. (ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»).

Наличие системы управления рисками ***является обязательным компонентом общей системы обеспечения информационной безопасности на всех этапах жизненного цикла***.

На этапе управления рисками разрабатывается некоторая **стратегия управления рисками**. При этом возможны следующие подходы к управлению рисками информационной безопасности организации:

- уменьшение риска;
- уклонение от риска;
- изменение характера риска;
- принятие риска.

Уменьшение рисков информационной безопасности. Многие риски ИБ можно значительно уменьшить и часто за счет простых и дешевых контрмер. Например, управление паролями снижает риск несанкционированного доступа; инструктаж на рабочем месте по правилам пользования электронной почтой и системами мгновенных сообщений значительно снижает риск заражения вирусами и внедрения шпионских программ.

Уклонение от рисков информационной безопасности. От некоторых классов рисков ИБ можно уклониться. Например, вынесение Веб-сервера компании за пределы локальной сети (прокси-сервер) позволяет избежать риска несанкционированного проникновения в локальную сеть компании со стороны Веб-клиентов.

Изменение характера риска. Если не удается снизить риски ИБ или уклониться от них, то можно принять некоторые меры страховки.

Например:

- застраховать оборудование от пожара, стихийного бедствия и др.;
- заключить договор с поставщиками средств вычислительной техники о компенсации ущерба, связанного с нештатными ситуациями, вызванными сбоями и неисправностью технических средств.

Принятие рисков. От некоторых классов рисков ИБ нельзя избавиться вообще. Даже при применении полного комплекса контрмер некоторые из них уменьшаются, но остаются значимыми. При этом необходимо знать остаточную величину риска.

В результате в организации принимается стратегия управления рисками ИБ.

Система управления рисками в целом предназначена для поддержки принимаемых управленческих решений, основанных на учете возможных рисков.

Основными процессами управления рисками являются: установление контекста, оценка риска, обработка и принятие риска, мониторинг и пересмотр риска (ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»).

Цель управления рисками заключается в создании условий для достижения организацией своей цели или целей за счет:

- повышения безопасности ИТ-систем, которые хранят, обрабатывают или передают информацию в пределах или вне объекта;
- повышения информированности и осведомленности руководства относительно принятых решений по управлению риском для получения обоснованных объемов затрат, которые должны стать неотъемлемой частью общего бюджета ИТ;
- оказания помощи руководству в авторизации (или в аккредитации) своих ИТ-систем на базе документированной поддержки результатами, вытекающими из выполнения процессов управления риском.

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Рядом российских организаций были разработаны собственные методики анализа и управления рисками, разработано собственное программное обеспечение, которое, наряду с зарубежным, имеется на отечественном рынке.

С точки зрения построения информационных систем, решения вопросов информационной безопасности и управления рисками, Россия идет вслед за развитыми странами, что позволяет избегать некоторых распространенных ошибок.

Рассмотрим зарубежный опыт организации системы управления рисками информационной безопасности на основе наиболее влиятельных стандартов.

Многие зарубежные национальные институты стандартов, организации, специализирующиеся в решении комплексных проблем информационной безопасности, предложили схожие концепции управления информационными рисками. Так, наиболее распространенными являются концепции Британского стандарта BS 7799, Германского BSI, концепция национального института стандартов США NIST 800-30 и концепция MITRE.

Рассмотрим управление рисками в соответствии со стандартом NIST 800-30.

Система управления (информационными) рисками организации должна минимизировать возможные негативные последствия, связанные с использованием информационных технологий и обеспечить возможность выполнения основных бизнес - целей объекта.

Распространенная практика свидетельствует о том, что система управления рисками должна быть интегрирована в систему управления жизненным циклом информационной технологии (табл. 1).

Таблица 1. Управление рисками на различных стадиях жизненного цикла информационной технологии

Фаза жизненного цикла информационной системы	**Соответствие фазе управления рисками**
1. Предпроектная стадия ИС (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, отладка и конфигурирование	До начала функционирования ИС должны быть идентифицированы и приняты во внимания все классы рисков
4. Функционирование ИС	Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС
Прекращение функционирования ИС (информационные и вычислительные ресурсы более не используются по назначению и утилизируются)	Соблюдение требований информационной безопасности по отношению к выводимым информационным ресурсам

Далее рассмотрим пример практической реализации рассмотренной методики. Для этого сначала определим исходные показатели риска информационной безопасности.

Риск информационной безопасности ($R_{иб}$) определим, как функцию трех переменных: вероятности существования угрозы информационной безопасности организации ($P_у$), вероятности существования незащищённости

(уязвимости) информационной системы организации ($Р_{нз}$), и вероятности потенциального воздействия на информационную систему организации ($Р_{воз}$).

$$R_{иб} = F(Р_у; Р_{нз}; Р_{воз}) \quad (1)$$

Если любая из этих переменных приближается к нулю, то риск приближается к нулю, следовательно, для расчета величины риска информационной безопасности справедливым будет выражение 2.

$$R_{иб} = Р_у \times Р_{нз} \times Р_{воз} \quad (2)$$

Естественно, что выражение 2 справедливо для случая, когда переменные являются количественными величинами. Если же переменные – качественные величины, операция умножения становится не применимой. Таким образом, величина $R_{иб}$, рассчитанная в соответствии с выражением 2, в сущности, является *вероятностью понесения организации некоторых потерь*.

Если существует возможность оценить риски информационной безопасности в величинах ущерба организации, например в денежной, расчет проводится в соответствии с выражением 3

$$Y = R_{иб} \times Ц_{пот,} \quad (3)$$

Где: Y – возможный ущерб организации в результате риска информационной безопасности;

$Ц_{пот}$ – цена (стоимость) возможных потерь организации.

В случае, когда при определении величины риска приходится оперировать качественными величинами (высокий, средний, низкий), а это является наиболее распространенная ситуация, то необходимо прибегнуть к разработке шкал.

Шкалы могут быть прямыми (естественными) или косвенными (производными). Примерами прямых шкал являются шкалы для измерения физических величин, например, литры для измерения объемов, метры для измерения длины.

В ряде случаев прямых шкал не существует, приходится использовать либо прямые шкалы других свойств, связанных с интересующими нас, либо определять новые шкалы. Примером является шкала для измерения субъективного свойства «ценность информационного ресурса», которая может измеряться в производных шкалах, таких как стоимость восстановления ресурса, время восстановления ресурса и других. 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 его утраты он может быть восстановлен за время менее, чем критически допустимое, 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.

Примером субъективного критерия является оценка риска выхода из строя ПК владельцем информационного ресурса. Для этого обычно разрабатывается качественная шкала с несколькими градациями, например, низкий, средний, высокий уровень.

В методиках анализа рисков, как правило, используются субъективные критерии, измеряемые в качественных шкалах, поскольку:

- оценка должна отражать субъективную точку зрения владельца информационных ресурсов;
- должны быть учтены различные аспекты, не только технические, но и организационные, психологические, и другие.

Для получения субъективной оценки в рассматриваемом примере с оценкой риска выхода из строя компьютера, можно использовать либо прямую экспертную оценку, либо определить функцию, отображающую объективные данные (вероятность) в субъективную шкалу рисков.

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

Например, для оценки показателей риска возможно использование шкалы со следующими уровнями:

1 – *риск практически отсутствует*. Возможность наступления события имеет чисто теоретическое обоснование;

2 – *риск очень мал*. Наступление события маловероятно и последствия незначительны.

3 – *риск мал*. Наступление события невелико и последствия сравнительно невелики.

4 – *риск средний*. Вероятность наступления события примерно 0,5 и средняя тяжесть последствий;

5 – *риск значительный*. Значительная вероятность наступления события и последствия будут серьезными;

6 – *риск велик*. Большая вероятность наступления события и последствия будут тяжелыми;

7 – *риск очень велик*. Событие, скорее всего, наступит, и негативные последствия будут критическими.

При использовании подобной шкалы разрабатывается матрица для определения рисков информационной безопасности организации, для чего по

одной оси показывается уровень угроз ИБ организации, на другой – уровень уязвимости СИБ и вероятность воздействия на нее (табл.2).

Таблица 2

Матрица рисков информационной безопасности объекта «Х»

Цена потери	**Уровень угрозы**								
	Низкий			Средний			Высокий		
	Уровень уязвимости								
	Низкий	Средний	Высокий	Низкий	Средний	Высокий	Низкий	Средний	Высокий
Низкая	**1**	**2**	**3**	**2**	**3**	**4**	**3**	**4**	**5**
Средняя	**2**	**3**	**4**	**3**	**4**	**5**	**4**	**5**	**6**
Высокая	**3**	**4**	**5**	**4**	**5**	**6**	**5**	**6**	**7**

Применение матрицы рисков организуется следующим образом. Если уровень угрозы информационной безопасности определен нами как средний, а уровень уязвимости информационной системы, или ее элемента – как высокий, то при низкой цене потери будем иметь величину риска равной 4, что соответствует *среднему его значению* и следующей качественной характеристике: *вероятность наступления события примерно 0,5 и средняя тяжесть последствий.*

Такой подход может быть воспринят достаточно формальным, но в таблице 1 показан лишь принцип формирования матрицы рисков. Для каждой организации данная матрица будет индивидуальной. Количество градаций для каждого измерения матрицы может быть выбран с учетом конкретных особенностей: для более точного определения, необходимо увеличение их числа до 6-7, для более грубого – 3-4.

Далее приступаем к оценке угроз и уязвимостей.

Для оценки угроз и уязвимостей информационной безопасности могут быть использованы следующие методы, которые основаны на:

- экспертных оценках;
- анализе статистических данных;
- учете факторов, влияющих на уровни угроз и уязвимостей.

В настоящее время, товарищи студенты, подобные «бумажные» методики реализованы в виде специального программного обеспечения как зарубежного – программные комплексы CRAMM, Risk Watch, Cobra и другие, а также отечественные, перечень которых скромнее - АванГард и Digital Security. Но, прежде чем применять программное обеспечение, необходимо понять суть происходящих процессов в данной области.

Рассмотрим применение наиболее распространенного в настоящее время метода, основанного на учете факторов, влияющих на уровни угроз и уязвимостей. Данный метод применяется в наиболее популярном в настоящее время программном комплексе CRAMM. При этом в качестве примера возьмем один из классов рисков «*Использование чужого идентификатора сотрудниками организации*».

Для *оценки угроз* выбраны следующие косвенные факторы:

- статистика по зарегистрированным инцидентам;
- тенденции в статистке по подобным нарушениям;

- наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей;

- морально-этические качества персонала;

- возможность извлечь выгоду из изменения обрабатываемой в системе информации;

- наличие альтернативных способов доступа к информации;

- статистика по подобным нарушениям в других информационных системах организации.

Для *оценки уязвимостей* выбраны следующие косвенные факторы:

- количество рабочих мест (пользователей) в системе;

- размер рабочих групп;

- осведомленность руководства о действиях сотрудников (в различных аспектах);

- характер используемого на рабочих местах оборудования и программного обеспечения;

- полномочия пользователей.

Для использования косвенных факторов предложены тесты с вопросами, предполагающими несколько фиксированных вариантов ответов, которые в дальнейшем оцениваются определенным количеством баллов.

Итоговая оценка угрозы и уязвимости данного класса определяется путем суммирования баллов. Сначала оцениваем границы шкалы путем полярных ответов на вопросы, а затем оцениваем промежуточные ее значения.

Так, получаем, что при оценке степени серьезности угрозы, шкала (по количеству баллов) будет следующая:

- до 9 - Очень низкая;
- от 10 до 19 – Низкая;
- от 20 до 29 – Средняя;
- от 30 до 39 – Высокая;
- 40 и более - Очень высокая.

При оценке степени уязвимости, шкала (по количеству баллов) будет следующая:

- до 9 – Низкая;
- от 10 до 19 – Средняя;
- 20 и более – Высокая.

Таким образом осуществляется оценка показателей риска информационной безопасности для каждой выявленной угрозы по отношению к конкретному информационному активу через имеющиеся уязвимости информационной системы.

Чрезвычайно важной представляется деятельность по анализу рисков информационной безопасности организации. Результаты данного анализа используются далее при выборе средств защиты, оценке эффективности существующих и проектируемых подсистем информационной безопасности.

На этом изложение второго учебного вопроса завершено.

Литература

1. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»

2. ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»

3. ГОСТ 27002-2012 «Методы и средства обеспечения безопасности»

4. Федеральный закон Российской Федерации №149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации»

5. ГОСТ Р ИСО/МЭК 15408-12012 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

6. ISO/IEC 17799 «Управление информационной безопасностью»

7. Невский А.Ю., Баронов О.Р. Система обеспечения информационной безопасности хозяйствующего субъекта: учебное пособие. – М.: Издательский дом МЭИ, 2009 г.

Заключение

Из представленного учебного материала вам необходимо уяснить систему обеспечения информационной безопасности и ее содержание, а также анализ и управление рисками информационной безопасности.

Доцент кафедры БИТ Д.Власкин