Тема 1 Организация безопасного удаленного доступа

Лекция 6. Анализ рисков и результатов деятельности по управлению компьютерными инцидентами

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

1. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры.

2. Анализ результатов деятельности по управлению компьютерными инцидентами

3. Анализ рисков информационной безопасности объектов мониторинга

Стадия реагирования на компьютерные инциденты состоит из следующих последовательных этапов:

- определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
- локализация компьютерного инцидента;
- выявление последствий компьютерного инцидента;
- ликвидация последствий компьютерного инцидента;
- закрытие компьютерного инцидента.

Параллельно с перечисленными действиями по реагированию на КИ могут проводиться:

- фиксация материалов, связанных с возникновением компьютерного инцидента;
- установление причин и условий возникновения компьютерного инцидента даже после закрытия компьютерного инцидента.

Выполнение данных этапов не влияет на закрытие компьютерного инцидента.

На данном этапе специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры, на которых имеются признаки зарегистрированного компьютерного инцидента, с целью их дальнейшей локализации. На рисунке представлена схема организационного процесса этапа определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры.

Схема организационного процесса этапа определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры

Для определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры следует изучить их состояние, допускается использование программных и/или программно-технических средств, предназначенных:

1) для получения доступа к файловой системе;

2) получения доступа к журналам регистрации событий без опасности:

а) операционной системы;

б) средств защиты информации (антивирусные средства, средства обнаружения компьютерных атак и иные средства защиты информации);

в) прикладного программного обеспечения;

3) сканирования файловой системы с целью выявления вредоносного ПО;

4) проведения инвентаризации программно-технических средств;

5) проведения анализа уязвимостей;

6) оценки работоспособности и производительности элементов информационной инфраструктуры;

7) получения информации из службы каталогов;

8) получения параметров сетевых настроек и информации о сетевой активности элементов информационной инфраструктуры;

9) анализа сетевого трафика, циркулирующего между элементами информационной инфраструктуры, а также другими 193 функционирующими в сети Интернет ресурсами, в том числе зафиксированного в момент возникновения компьютерного инцидента (при наличии такой возможности);

10) обнаружения компьютерных атак.

Локализация компьютерного инцидента

На этапе локализации компьютерного инцидента специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на ограничение функционирования элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент, с целью предотвращения его дальнейшего распространения. На рисунке представлена схема организационного процесса этапа локализации компьютерного инцидента.

Первый учебный вопрос.

К примерам возможных действий, которые могут выполняться при локализации компьютерных инцидентов, можно отнести:

– применение блокировок (использование межсетевого экрана). Блокировки с использованием межсетевых экранов предназначены для предотвращения несанкционированного воздействия. Например, с использованием межсетевого экрана можно заблокировать информационные потоки с IP-адресов, с которых распространяется вредоносное или шпионское ПО, а также IP-адресов почтовых ре трансляторов, источников фишинга и спама. Почтовые блокировки включают в себя фильтрацию вложений, строк темы и адреса отправителей. Для предотвращения доступа к неразрешенным или вредоносным веб-сайтам или хостам (узлам) могут применяться блокировки URL-адресов и доменных имен;

– отключение (изоляция, исключение).

Отключение зараженного элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) от локальной вычислительной сети может предотвратить заражение остальной части информационной инфраструктуры. Отключение зараженного элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) от сети Интернет или любых других общедоступных сетей связи может предотвратить несанкционированный доступ и, соответственно, нарушение конфиденциальности, целостности и доступности информации. В некоторых случаях целесообразно осуществлять мониторинг вредоносной активности, ограничив при этом возможности злоумышленника атаковать другие информационные ресурсы;

– выключение.

Если дальнейшее функционирование элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) приведет к уничтожению (потере) данных, может быть принято решение о прекращении функционирования элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом). Следует учитывать, что выключение элемента информационной инфраструктуры может отрицательно сказаться на работе конкретных пользователей, сервисов и различных критических процессов. Данное решение должно приниматься в координации с соответствующим руководителем и/или ответственными за эксплуатацию информационных ресурсов организации;

– изменение маршрутизации с целью устранения маршрута действия злоумышленника, препятствуя ему в получении доступа к информационным ресурсам, которые могут являться объектами атаки, и блокирования механизмов передачи (распространения) вредоносного ПО;
– отключение или блокирование процессов, которые могли быть использованы злоумышленником;
– отключение учетных записей пользователей, которые могли быть использованы злоумышленником.
Любые изменения в информационных ресурсах, включая действия по локализации компьютерного инцидента, могут привести к потере (уничтожению) информации, связанной с возникновением компьютерного инцидента (цифровых свидетельств). Следует убедиться, что вся информация, необходимая для установления причин и условий возникновения компьютерных инцидентов (цифровые свидетельства), собрана в полном объеме перед внесением каких-либо системных изменений.

Выявление последствий компьютерного инцидента

На этапе выявления последствий компьютерного инцидента специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на обнаружение признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент. При выявлении признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент, специалисты, входящие в состав рабочей группы реагирования на компьютерный инцидент, должны провести детальный анализ имеющихся данных о компьютерном инциденте. На рисунке представлена схема организационного процесса этапа выявления последствий компьютерного инцидента.

Первый учебный вопрос.

Первый учебный вопрос.

К примерам признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в компьютерный инцидент, которые выявляются в ходе анализа имеющихся данных о компьютерном инциденте, можно отнести следующее:

- нештатная сетевая активность элемента информационной инфраструктуры;-
- созданные, модифицированные, удаленные файлы, каталоги, параметры настройки ОС, средств защиты информации, прикладного ПО;
- отклонения от эталонных (допустимых) параметров конфигурации ОС, средств защиты информации, прикладного ПО;
- отклонения от эталонного (допустимого) состава прикладного ПО, установленного в ОС;

- отклонения от эталонного (допустимого) содержания системных и защищаемых файлов;
- выполненные потенциально вредоносные команды, в том числе расположенные в оперативной памяти;
- признаки, идентифицирующие источник компьютерной атаки;
- признаки сбоев, перезагрузок, остановок и других нарушений в штатной работе ОС, средств защиты информации, прикладного ПО;
- признаки нарушений функционирования сетевых служб, аномального использования системных ресурсов;
- другая информация, характерная для отдельных типов компьютерных инцидентов и компьютерных атак.

Ликвидация последствий компьютерного инцидента

На этапе ликвидации последствий компьютерного инцидента специалистами, входящими в состав рабочей группы реагирования на компьютерный инцидент, должны выполняться действия, направленные на устранение последствий негативного влияния компьютерного инцидента на информационный ресурс (по возможности) и/или восстановление элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом) и/или обрабатываемой в нем информации. На рисунке представлена схема организационного процесса этапа ликвидации последствий компьютерного инцидента.

Первый учебный вопрос.

К примерам возможных действий, которые могут быть выполнены для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне сети, можно отнести:

1) внесение изменений в параметры настроек ОС, средств защиты информации и прикладного ПО, функционирующего в информационных ресурсах, вовлеченных в компьютерный инцидент;

2) отключение неиспользуемых функций телекоммуникационного оборудования (например, отключение уязвимых сервисов или протоколов, которые использовались для распространения вредоносного ПО);

3) смена аутентификационной информации скомпрометированных учетных записей пользователей:

а) на телекоммуникационном оборудовании;

б) средствах межсетевого экранирования;

в) средствах защиты от компьютерных атак, направленных на отказ в обслуживании;

4) внесение изменений в правила фильтрации межсетевых экранов;

5) внесение изменений в параметры очистки трафика в средствах защиты от компьютерных атак, направленных на отказ в обслуживании;

6) подключение резервных ресурсов (каналы связи, серверное оборудование, виртуальные машины, оборудование из состава запасных инструментов и принадлежностей);

7) миграция (перемещение) виртуальных машин в сторонние виртуальные инфраструктуры.

К примерам возможных мер, которые могут быть приняты для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне прикладного ПО, можно отнести:

- выполнение настройки безопасной конфигурации прикладного или специального ПО, вовлеченного в компьютерный инцидент;
- восстановление из актуальных резервных копий файлов, баз данных, конфигурационных файлов, подвергшихся модификации при компьютерном инциденте;
- восстановление удаленных файлов, в том числе с использованием специальных инструментальных средств;
- удаление ПО, вовлеченного в компьютерный инцидент, и всех его файлов с последующей установкой актуальной версии данного ПО и актуальных обновлений безопасности.

К примерам возможных мер, которые могут быть приняты для ликвидации последствий компьютерного инцидента, приведшего к негативным последствиям на уровне ОС, можно отнести:

- удаление вредоносного ПО;
- отмена изменений, внесенных вредоносным ПО (например, удаление созданных вредоносным ПО файлов, отмена выполненных изменений в конфигурации и настройках ОС, удаление созданных вредоносным ПО учетных записей);
- смена аутентификационной информации для скомпрометированных учетных записей пользователей в ОС;
- восстановление средств защиты информации, функционирующих в среде ОС;
- восстановление ОС в целом;
- настройка безопасной конфигурации средств защиты информации, функционирующих в среде ОС;
- настройка безопасной конфигурации ОС;
- переустановка ОС и прикладного ПО с последующей установкой актуальных обновлений безопасности.

Первый учебный вопрос.

Закрытие компьютерного инцидента Решение о закрытии компьютерного инцидента принимается по результатам проверки специалистом, ответственным за реагирование на компьютерный инцидент (руководителем рабочей группы реагирования на компьютерный инцидент), в ходе которой определяется полнота выполненных и запротоколированных действий по реагированию на компьютерный инцидент, выполненных на каждом этапе реагирования на компьютерный инцидент. Карточки компьютерных инцидентов после закрытия соответствующих компьютерных инцидентов не должны удаляться, так как они могут быть использованы в дальнейшем как типовые шаблоны действий по реагированию на аналогичные компьютерные инциденты и при проведении анализа деятельности по их управлению. Карточки закрытых компьютерных инцидентов могут использоваться в качестве типовых шаблонов действий по реагированию на аналогичные компьютерные инциденты в организации с целью формирования базы знаний, доступной специалистам, входящим в состав рабочих групп реагирования на компьютерные инциденты, при работе с новыми компьютерными инцидентами.

Анализ результатов деятельности по управлению компьютерными инцидентами

Общие положения

Стадия анализа результатов деятельности по управлению компьютерными инцидентами включает в себя следующие этапы:

- приобретение и накопление опыта по результатам управления компьютерными инцидентами;
- разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов;
- оценка результатов и эффективности реагирования на компьютерные инциденты.

Второй учебный вопрос.

Приобретение и накопление опыта по результатам управления компьютерными инцидентами

Процесс приобретения и накопления опыта является важной составляющей ведения деятельности по управлению компьютерными инцидентами. После завершения всех этапов реагирования на компьютерный инцидент важно, чтобы организация приобрела и накопила опыт управления компьютерными инцидентами.
Приобретение и накопление опыта по результатам управления компьютерными инцидентами позволяет:

- идентифицировать методы и способы обнаружения и регистрации компьютерных инцидентов и реагирования на компьютерные инциденты, которые показали свою эффективность в отношении уже закрытых компьютерных инцидентов;
- доработать (актуализировать) документацию в части управления компьютерными инцидентами, в том числе политику управления компьютерными инцидентами и план реагирования на компьютерные инциденты.

Второй учебный вопрос.

Все изменения (корректировки, дополнения), предлагаемые к внесению в план реагирования на компьютерные инциденты, относящиеся к этапам обнаружения и регистрации компьютерных инцидентов и реагирования на компьютерные инциденты, должны быть надлежащим образом проверены и протестированы, т. е. должны быть проведены тренировки по отработке мероприятий плана реагирования на компьютерные инциденты в соответствии с положениями.

Второй учебный вопрос.

Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов По результатам реагирования на компьютерные инциденты и установления причин и условий их возникновения следует разрабатывать рекомендации по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов, которые могут включать предложения:

- по принятию дополнительных мер защиты информации в соответствии с нормативными правовыми актами и методическими документами уполномоченных федеральных органов исполнительной власти (ФСБ России и ФСТЭК России), в том числе по доработке (актуализации) и/или разработке документации, регламентирующей вопросы обеспечения безопасности организации;
- повышению защищенности информационных ресурсов от компьютерных атак;
- устранению технических причин и условий, способствующих проведению деструктивного воздействия на информационные ресурсы.

Оценка результатов и эффективности реагирования на компьютерные инциденты

После завершения всех этапов реагирования на компьютерный инцидент следует проводить оценку результатов и эффективности предпринятых действий. Такая оценка направлена на определение эффективности тех или иных процессов и процедур реагирования на компьютерные инциденты.

Мониторинг эффективности защитных мер и процессов управления ИБ с учетом результатов оценки/переоценки рисков ИБ и уровней остаточных и приемлемых рисков ИБ является важной составляющей СУИБ.

Второй учебный вопрос.

Реализация данного процесса в организации предназначена для достижения следующих целей:

- повышение эффективности используемых и внедряемых защитных мер;
- повышение эффективности процессов, реализуемых в рамках СУИБ;
- предоставление данных руководству для анализа эффективности процесса ОИБ в организации.

Для объективной оценки эффективности функционирования и эксплуатации процессов управления ИБ и защитных мер можно ввести следующий метод. Для каждого из процессов управления ИБ, а также при необходимости для групп защитных мер вводятся показатели (в данном случае обобщенные характеристики свойств СУИБ или процесса управления ИБ), они регулярно измеряются и оцениваются. Для каждого из показателей определяется целевое значение, к которому необходимо стремиться.

В случае если текущее значение показателя отличается от целевого, формируются соответствующие предложения по улучшению. Предложения по улучшению того или иного процесса управления ИБ или по модификации существующих защитных мер могут быть сформулированы в виде запросов на корректирующие или предупреждающие действия, т. е. стать входными данными для процесса управления корректирующими и предупреждающими действиями. Мониторинг показателей позволяет увидеть, улучшается или ухудшается ситуация в рамках процессов управления ИБ и функционирования защитных мер.

Для оценки СУИБ используются два основных параметра, которые должны задаваться и быть адекватными назначению процесса управления ИБ, требованиям законодательства и его внутренних и внешних потребителей, целям деятельности организации:

Второй учебный вопрос.

результативность (effectiveness) – степень реализации запланированной деятельности и достижения запланированных результатов;

эффективность (efficiency) – соотношение между достигнутым результатом (характеристикой результативности) и использованными затратами (время, финансы и т. д.), обеспечившими его получение.

Можно сказать, что результативность зависит от качества решений по отношению к целям (делать правильные вещи), а эффективность – от качества действий (делать вещи правильно).

Второй учебный вопрос.

Для определения эффективности СУИБ как соотношения между достигнутым уровнем ОИБ, полученным при управлении ИБ на основе СУИБ, и использованными ресурсами, обеспечившими его получение, необходимо выбрать критерий, в соответствии с которым можно судить о степени эффективности СУИБ. Эффективность управления ИБ представляет собой экономическую категорию, отражающую вклад управленческой деятельности в области ОИБ в конечный результат – уровень ИБ организации и определяемую степенью реализации целей организации в области ОИБ и ее интегрального показателя – при были.

Оценка эффективности СУИБ – это системный процесс получения объективных данных о ее текущем состоянии, процессах и событиях, происходящих в ней, устанавливающий уровень их соответствия определенным критериям. Для количественного выражения эффективности критерий должен быть охарактеризован определенным числовым значением и соответствовать оцениваемому явлению, быть универсальным и простым в применении, давать однозначную и полную оценку.

Второй учебный вопрос.

Эффективность СУИБ как вспомогательной системы организации проявляется, главным образом, в косвенном, а не прямом эффекте, поэтому она не может быть определена каким-то одним показателем. Необходимо разработать целую систему показателей.

Совершенствование СУИБ создает благоприятные условия для повышения эффективности деятельности организации в целом при снижении удельных затрат на аппарат управления организации, включая и управление ИБ.

Ключевые показатели эффективности СУИБ интегрируются в систему управления рисками ИБ.

В зависимости от выбранного для оценки критерия можно разделить способы оценки СУИБ организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям

Второй учебный вопрос.

Способ оценки по эталону сводится к сравнению деятельности и средств управления ИБ организации с требованиями, закрепленными в эталоне. По сути, проводится оценка соответствия СУИБ организации установленному эталону, связанная с прямым или косвенным определением выполнения/невыполнения и правильностью и недостатками реализации соответствующих требований – законодательства РФ, отраслевых требований, требований нормативных, методических и организационно-распорядительных документов, требований национальных и международных стандартов в области ИБ.

Основные этапы оценки по эталону включают выбор эталона и формирование на его основе критериев оценки, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование общей оценки.

Второй учебный вопрос.

Риск-ориентированная оценка представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в ин формационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры. Цель этого подхода – показать, что все процессы управления рисками ИБ в организации созданы, внедрены и действуют надлежащим образом. В результате формируется оценка способности организации эффективно управлять рисками ИБ для достижения своих целей деятельности. Основные этапы риск ориентированной оценки включают идентификацию рисков ИБ, определение адекватных процессов управления рисками ИБ и ключевых индикаторов рисков ИБ, формирование на их основе критериев оценки, сбор свидетельств оценки, измерение риск-факторов, формирование общей оценки.

Второй учебный вопрос.

Способ оценки ИБ на основе экономических показателей оперирует понятными для деятельности аргументами о необходимости обеспечения и совершенствования СУИБ. Часто для этого используются следующие экономические показатели:

– отдача на инвестиционный капитал (Return of Investments, ROI) – процентное отношение прибыли (или экономического эффекта) от проекта к инвестициям, необходимым для реализации этого проекта (в общем случае под инвестициями понимают ТСО);

– совокупная стоимость владения (Total Cost of Ownership, TCO), которая позволяет сделать выводы о целесообразности реализации проекта в области ОИБ на основании оценки затрат. Все затраты делятся на две категории – прямые и косвенные. Под косвенными затратами, как правило, понимаются скрытые расходы, возникающие в процессе эксплуатации СУИБ. Прямые затраты составляют от 5 до 21 % от общей суммы затрат на использование ИТ. Расчет ТСО предполагает оценку не только первоначальных затрат на различных этапах всего жизненного цикла системы.

Оба показателя – TCO и ROI – являются статичным, не учитывающими изменения ситуации в области ОИБ во времени, а все ИС, сети и сама СУИБ с течением времени подвергаются постоянным изменениям, появляются новые угрозы ИБ и уязвимости систем. Поэтому для анализа эффективности инвестиций в СУИБ применяют систему динамических показателей, основанных на методе дисконтированных потоков денежных средств (Discounted Cash Flows, DCF). Будущие поступления денежных средств (снижение ущерба) дисконтируются, т. е. приводятся к текущей стоимости. Для этого применяют ставку дисконтирования (норму доходности), ее величина отражает риски, связанные с обесцениванием денег из-за инфляции и с возможностью неудачи инвестиционного проекта, который может не принести ожидаемого эффекта. Чем выше риски, связанные с проектом, тем больше значение ставки дисконтирования.

Также ставка дисконтирования определяется показателем средне взвешенной стоимости капитала (Weighted Average Cost of Capital, WACC) – средней нормой дохода на вложенный капитал. Обычно WACC рассматривается как минимальная норма отдачи, которая должна быть обеспечена инвестиционным проектом.
Для оценки эффективности инвестиций используют показатель чистой текущей стоимости (Net Present Value, NPV) – текущей стоимости будущих денежных потоков инвестиционного проекта с учетом дисконтирования и за вычетом инвестиций. При значении NPV > 0 считается, что вложение средств эффективно.
Можно также рассчитать внутренний коэффициент отдачи (Internal Rate of Return, IRR). Для этого необходимо найти такую ставку дисконтирования – точку безубыточности, при которой значение RPV = 0. В этой точке дисконтированный поток затрат равен дисконтированному потоку доходов. Таким образом, внутренний коэффициент отдачи – это та минимальная ставка, при которой инвестиции окупают все затраты, в том числе затраты на привлечение средств.

Но далеко не весь ущерб от реализации угроз ИБ можно однозначно выразить в денежном эквиваленте. Например, причинение урона интеллектуальной собственности организации может привести к потере позиций на рынке, потере постоянных и временных конку рентных преимуществ или снижению стоимости торговой марки. Поэтому нередко даже при наличии рассчитанных показателей ROI и TCO решение о создании СУИБ принимается на основе качественной оценки возможных эффектов.

Любой метод оценки эффективности СУИБ является всего лишь набором математических формул и логических выкладок. Поэтому качество информации, необходимой для принятия решения о целесообразности инвестиций в СУИБ, в первую очередь будет зависеть от исходных данных, на основе которых производились вычисления.

Второй учебный вопрос.

Под результативностью СУИБ будем понимать свойство СУИБ выполнять поставленную цель по управлению и, следовательно, по обеспечению ИБ в организации в заданных условиях использования и с определенным качеством. Установление измеримых целей особенно способствует организации работ по управлению ИБ и оптимальному функционированию СУИБ, ориентированной на результат, – организация в условиях ее деятельности достигает поставленных целей с наибольшим эффектом. Управление ИБ результативно, если ставятся цели, которые организация в этой области способна достичь (целеполагание и стратегия), и последовательно в своем движении к поставленным целям (планирование и контроль).

Второй учебный вопрос.

Показатели результативности СУИБ характеризуют степень ее приспособленности к выполнению поставленных перед ней задач в области управления и обеспечения ИБ организации и являются обобщающими показателями оптимальности функционирования СУИБ.

Показателями результативности СУИБ могут быть, например, изменение количества инцидентов ИБ, квалификация пользователей в области ИБ и т. п. Чем ближе измеренные фактические значения целевых показателей к плановым, тем выше результативность СУИБ.

Комплексный учет показателей эффективности и результативности СУИБ предполагает комплексный подход к организации обеспечения ИБ и управления ею, когда на соответствие определенным правилам проверяется, контролируется и поддерживается не только программно-техническая составляющая, но и организационно административные меры по обеспечению ИБ организации.

Второй учебный вопрос.

Оценку результатов и эффективности действий, предпринятых на каждом этапе реагирования на компьютерный инцидент, целесообразно проводить в отношении компьютерных инцидентов со средним, высоким и критическим уровнями влияния и на основании задокументированных результатов реагирования. После завершения всех этапов реагирования на компьютерный инцидент следует проводить рабочие совещания со специалистами всех подразделений, участвующих в деятельности по управлению компьютерными инцидентами, на стадиях обнаружения и регистрации компьютерных инцидентов и реагирования на компьютерные инциденты.

Второй учебный вопрос.

На рабочем совещании целесообразно обсудить следующие вопросы:

- оценка достаточности и эффективности процессов и процедур реагирования на компьютерные инциденты, изложенных в плане;
- предложения по включению в план реагирования на компьютерные инциденты дополнительных процессов и процедур, которые могли бы повысить эффективность действий, выполняемых на стадиях обнаружения и регистрации компьютерных инцидентов и реагирования на компьютерные инциденты;
- предложения по использованию дополнительных инструментальных средств с целью повышения эффективности реагирования и установления причин и условий возникновения компьютерных инцидентов;
- оценка эффективности обмена информацией о компьютерных инцидентах между всеми сторонами, принимающими участие на стадиях обнаружения и регистрация компьютерных инцидентов и реагирования на компьютерные инциденты.

Второй учебный вопрос.

Оценка результатов и эффективности реагирования на компьютерные инциденты может осуществляться на основании следующих показателей:

- среднее время проведения проверки признаков возможного возникновения компьютерных инцидентов;
- среднее время определения вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
- среднее время локализации компьютерных инцидентов;
- среднее время выявления последствий компьютерных инцидентов;
- среднее время ликвидации последствий компьютерных инцидентов;
- среднее время реагирования на компьютерные инциденты;
- процент компьютерных инцидентов, для которых были нарушены сроки выполнения этапов реагирования.

Анализ рисков информационной безопасности объектов мониторинга

Вопросы управления рисками рассматриваются на административном уровне ИБ, поскольку только руководство организации может выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ. Управление рисками, равно как и выработка собственной поли тики безопасности, нужны только для тех организаций, ТКС и/или обрабатываемые данные которых можно считать нестандартными. Типовой организации достаточно стандартного набора защитных мер, выбранного на основе представления о типичных рисках или без анализа рисков, в соответствии с российским законодательством в области информационной безопасности. Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество доку ментов, во втором – достаточно определиться лишь с несколькими параметрами.

Базовый уровень безопасности – минимальный набор регуляторов безопасности, необходимый для защиты информационной системы, определяемый из потребностей телекоммуникационной сети (ТКС) в обеспечении доступности, конфиденциальности и целостности.

Риск – уровень воздействия на производственную деятельность организации (включая миссию, функции, образ, репутацию), ее активы (ресурсы) и персонал, являющегося следствием эксплуатации информационной системы и зависящего от потенциального воздействия угрозы и вероятности ее осуществления (реализации).

Риски, связанные с информационными технологиями, – общее воздействие на производственную деятельность с учетом:

1) вероятности того, что определенный источник угроз использует или активизирует определенную уязвимость информационной системы;
2) результирующего воздействия, если угроза будет реализована.

Риски, связанные с информационными технологиями, являются следствием законодательной ответственности или производственных потерь по причине:

- несанкционированного (злоумышленного, незлоумышленного, случайного) доступа к информации; незлоумышленных ошибок и/или упущений;
- разрушения ТКС в результате стихийных бедствий или техногенных катастроф;
- неспособности проявлять должную аккуратность и старательность при реализации и/или эксплуатации ТКС.

Третий учебный вопрос.

Остаточный риск – остающийся, потенциальный риск после применения всех контрмер. С каждой угрозой ассоциирован свой остаточный риск.

Совокупный (суммарный, полный) риск – возможность осуществления вредоносного события при отсутствии мер по нейтрализации рисков.

Анализ рисков – процесс идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительных контрмер, ослабляющих (уменьшающих) это воздействие. Анализ рисков – синоним термина "оценка рисков" – является частью управления рисками, включает в себя анализ угроз и уязвимостей.

Управление рисками – процесс, включающий оценку рисков, анализ экономической эффективности, выбор, реализацию и оценку контрмер, а также формальное санкционирование ввода системы в эксплуатацию. В процессе управления рисками принимаются во внимание и анализируются эффективность действий и законодательные ограничения.

Нейтрализация (уменьшение, ослабление) рисков – определение приоритетов, оценка и реализация контрмер, должным образом уменьшающих риски.

Терпимость по отношению к риску – уровень риска, который считается допустимым для достижения желаемого результата.

Оценка риска – это систематический анализ вероятного ущерба системе в результате нарушений ИБ с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации, вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по УИБ.

Третий учебный вопрос.

Современные методики по анализу рисков ИБ, проектированию и сопровождению систем безопасности позволяют:

- произвести количественную оценку текущего уровня без опасности, задать допустимые уровни рисков, разработать план мероприятий по обеспечению требуемого уровня безопасности с использованием организационных и технических механизмов ЗИ;
- рассчитать и экономически обосновать размер необходимых вложений при создании СЗИ, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередное блокирование наиболее опасных уязвимостей;
- разработать проект внедрения необходимых элементов СЗИ, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренной СЗИ в соответствии с изменяющимися условиями работы, модификацией технологических процессов и модернизацией технических средств защиты.

Третий учебный вопрос.

Прежде чем приступить к любым действиям, связанным с анализом риска, организация должна иметь стратегию проведения такого анализа, причем составные части этой стратегии должны быть отражены в содержании политики безопасности. Методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям организации. Приведенные ниже варианты стратегии представляют собой четыре разных подхода к анализу риска, основное различие между которыми состоит в степени глубины проводимого анализа (при этом не рассматривается вариант стратегии анализа риска, заключающийся в отсутствии каких-либо защитных мер, и допускается, что появление различных видов риска неизвестного уровня и интенсивности вполне реально):

1. Базовый подход (с низкой степенью риска) – используется для всех информационных систем (ИС) независимо от уровня риска, которому подвергаются системы.
2. Неформальный подход – применяется к проведению анализа риска – обращается особое внимание на ТКС, которые подвергаются наибольшему риску.
3. Детальный анализ риска – используется при формальном под ходе ко всем ТКС.
4. Комбинированный подход – предполагается проводить предварительный анализ высокого уровня риска для всех элементов ТКС, обращая особое внимание на значимость системы и уровень риска, которому она подвергается.

Если элементы имеют важное значение для деятельности организации и/или подвержены высокому уровню риска, в первую очередь проводят детальный анализ. Для остальных следует ограничиться базовым подходом. Таким образом, комбинированный вариант, сочетающий лучшие свойства базового и неформального под ходов, позволяет при сведении к минимуму времени и усилий, затраченных на идентификацию должных защитных мер, обеспечить необходимую защиту систем с высоким уровнем риска.

Комбинированный подход имеет следующие преимущества:

- использование быстрого и простого предварительного анализа риска позволит обеспечить принятие программы анализа риска;
- существует возможность быстро оценить оперативное состояние программы обеспечения безопасности организации;
- ресурсы и средства могут быть вложены туда, где они при несут максимальный эффект, так как в первую очередь будут направлены в системы, в наибольшей степени нуждающиеся в обеспечении безопасности;
- проведение последующих мероприятий будет более успешным.

Единственный потенциальный недостаток данного подхода состоит в следующем: поскольку предварительный анализ риска про водят исходя из предположения о его возможном высоком уровне, отдельные системы могут быть ошибочно отнесены к системам, не требующим проведения детального анализа риска. К этим системам в дальнейшем будут применены базовые методы обеспечения без опасности. При необходимости можно будет вернуться к их рассмотрению с тем, чтобы удостовериться, не требуют ли они более тщательного анализа по сравнению с базовым подходом.

Использование комбинированного варианта с анализом высокого уровня риска в сочетании с базовым подходом и (если необходимо) детальным анализом риска обеспечивает большинству организаций наиболее эффективное решение проблем. Прежде всего проводят предварительный анализ высокого уровня риска, чтобы установить, какой из вариантов (базовый или детальный) лучше под ходит для конкретной системы информационных технологий. В ходе проведения такого предварительного анализа рассматривают значимость систем информационных технологий и обрабатываемой с их помощью информации, а также уровень риска с учетом вида деятельности организации. В данном случае придерживаются следующего общего правила: если прекращение функционирования данной системы ИТ может причинить ущерб или принести убытки организации, отрицательно повлиять на ее деятельность или активы, то для оценки потенциального риска проводят его детальный анализ. Во всех других случаях достаточная безопасность системы может быть обеспечена путем применения базового подхода.

Третий учебный вопрос.

Цель обеспечения безопасности с помощью базового подхода состоит в том, чтобы подобрать для организации минимальный набор защитных мер для всех или отдельных систем информационных технологий. Используя базовый подход, можно применять соответствующий ему базовый уровень безопасности в организации и, кроме того, дополнительно использовать результаты детального анализа риска для обеспечения безопасности систем информационных техно логий с высоким уровнем риска или систем, играющих важную роль в деятельности организации. Применение базового подхода позволяет снизить затраты организации на исследование результатов анализа риска.

Третий учебный вопрос.

С помощью базового подхода возможно обеспечить удовлетворительную защиту путем использования справочных материалов (каталогов) по защитным мерам безопасности, с помощью которых можно подобрать набор средств для защиты ИС от наиболее часто встречающихся угроз. Базовый уровень безопасности может быть установлен в соответствии с потребностями организации, при этом в проведении детальной оценки угроз, рисков и уязвимости систем не будет необходимости, достаточно выбрать из справочных материалов (каталогов) по защитным мерам безопасности соответствующие пункты, которые подходят для рассматриваемой системы информационных технологий. При наличии в системе установленных защитных мер их необходимо сравнить с рекомендуемыми в каталогах. Защитные меры, которые отсутствуют в системе, но могут быть в ней использованы, должны быть реализованы.

Детальный анализ риска для ИС предполагает идентификацию всех возможных рисков и оценку их уровня. Необходимость проведения детального анализа риска может быть определена без лишних затрат времени и средств после анализа высокого уровня риска для всех систем с последующим изучением результатов детального анализа, проведенного только для критических систем или систем с высоким уровнем риска.

Анализ риска проводится путем идентификации нежелательных событий, создающих неблагоприятные ситуации, и определения вероятности их появления. Нежелательные события также могут негативно влиять на рабочий процесс или сотрудников организации. Такое неблагоприятное воздействие нежелательных событий является сложным сочетанием возможных видов ущерба, наносимого стоимости активов, подвергающихся риску.

Вероятность такого события зависит от того, насколько привлекательным является данный актив для потенциального нарушителя, от возможности реализации угроз и простоты эксплуатации уязвимости. Результаты анализа 136 риска позволяют идентифицировать ИС с высоким уровнем риска и выбрать меры по обеспечению безопасности, которые могут быть использованы для снижения уровня идентифицированного риска до приемлемого.

Результаты детального анализа риска позволяют проводить вы бор обоснованных защитных мер как части процесса управления риском. Требования, предъявляемые к выбранным мерам защиты, должны быть зафиксированы в политике безопасности и соответствующем ей плане безопасности.

Основные этапы алгоритма управления рисками

Установление границ рассмотрения
Прежде чем получить исходные данные для идентификации и оценки активов, необходимо определить границы рассмотрения. Тщательное определение границ на этой стадии анализа риска позволяет избежать ненужных операций и повысить качество анализа риска. Установление границ рассмотрения должно четко определить, какие из перечисленных ниже ресурсов подлежат учету при рассмотрении результатов анализа риска.

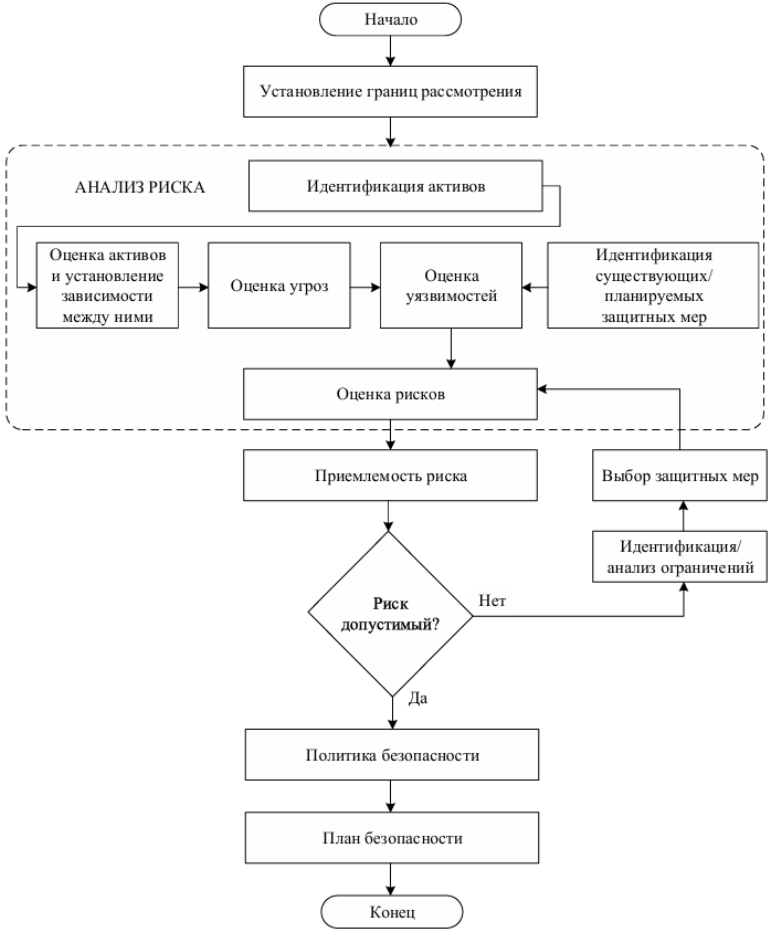
Для конкретной ТКС учитывают:

- активы ТКС (аппаратные средства, информационное обеспечение, информация);
- служащих (персонал организации и сторонних организаций, субподрядчики);
- условия осуществления производственной деятельности;
- деловую деятельность (операции).

Идентификация активов

Актив ТКС является компонентом или частью общей системы, в которую организация напрямую вкладывает средства, и требует за щиты со стороны организации. При идентификации активов следует иметь в виду, что любая ТКС включает в себя не только аппаратные средства и программное обеспечение.

Третий учебный вопрос.



Управление риском с использованием его детального анализа

Третий учебный вопрос.

Могут существовать следующие типы активов:

- информация/данные (файлы);
- аппаратные средства (компьютеры, принтеры);
- программное обеспечение, включая прикладные программы (программы обработки текстов);
- оборудование для обеспечения связи;
- программно-аппаратные средства (гибкие магнитные диски, CD-ROM, программируемые ROM);
- документы (контракты);
- фонды (в банковских автоматах);
- продукция организации;
- услуги (информационные, вычислительные);
- оборудование, обеспечивающее условия работы;
- конфиденциальность и доверие при оказании услуг;
- персонал организации;
- престиж (имидж) организации.

Активы, включенные в установленные границы рассмотрения, должны быть обнаружены, и наоборот, любые активы, выведенные за границы рассмотрения, должны быть рассмотрены еще раз с тем, чтобы убедиться, что они не были забыты или упущены.

Оценка активов и установление зависимости между ними

После того как все цели процесса идентификации активов были достигнуты и составлен перечень всех активов рассматриваемой ИС, должна быть определена их ценность исходя из важности для дея тельности организации и возможности обеспечения безопасности, т. е. насколько могут пострадать деятельность организации и другие активы ИС от утечки, искажения, недоступности и/или разрушения информации. Таким образом, идентификация и оценка активов, проведенные на основе учета интересов организации, являются основным фактором в определении риска.

Исходные данные для оценки должны быть получены от владельцев и пользователей активов. Специалист(ы), проводящий(е) анализ риска, должен(ны) составить перечень активов; при этом следует запросить содействие лиц, непосредственно занимающихся планированием деятельности, финансами, ИС и другими соответствующими направлениями деловой активности для определения ценности каждого из активов. Полученные данные соотносят со стоимостью создания и обслуживания актива, а также с возможностью негативного воздействия на деятельность, связанного с нарушением конфиденциальности, целостности, доступности, достоверности и надежности информации. Независимо от используемой шкалы оценок, в ходе проведения оценки необходимо рассмотреть проблемы, связанные с уровнем возможного ущерба, причиной которого могут быть:

- нарушение законодательства и/или технических норм;
- снижение уровня деловой активности;
- потеря/ухудшение репутации;
- нарушение конфиденциальности личной информации;
- возникновение угрозы личной безопасности;
- нарушение конфиденциальности в финансовых вопросах;
- неблагоприятные последствия деятельности правоохранительных органов;
- нарушение общественного порядка;
- финансовые потери;
- нарушение непрерывного функционирования организации;
- угроза экологического ущерба.

Следует также выявить виды зависимости одних активов от других, поскольку их наличие может оказать влияние на оценку активов. Данные о зависимостях, существующих между отдельными активами, будут способствовать идентификации некоторых видов угроз и определению конкретных уязвимостей, а использование данных о зависимостях даст уверенность в том, что активы оценены в соответствии с их реальной ценностью и уровень безопасности выбран обоснованно.

Уровни ценности активов, от которых зависят другие активы, могут быть изменены в следующих случаях:

- если уровни ценности зависимых активов (например, данных) ниже или равны уровню ценности рассматриваемого актива (напри мер, ПО), то этот уровень останется прежним;
- если уровни ценности зависимых активов (например, данных) выше, то уровень ценности рассматриваемого актива (например, ПО) необходимо повысить с учетом уровня соответствующей зависимо сти либо уровней ценности других активов.

Конечными результатами данного этапа являются составление перечня активов и их оценка с учетом таких показателей, как раскрытие информации (сохранение конфиденциальности), изменение данных (сохранение целостности), невозможность доступа и разрушения информации (сокращение доступности), а также стоимость замены.

Конечными результатами данного этапа являются составление перечня активов и их оценка с учетом таких показателей, как раскрытие информации (сохранение конфиденциальности), изменение данных (сохранение целостности), невозможность доступа и разрушения информации (сокращение доступности), а также стоимость замены.