**Лекция № 1**

**Сущность информации**

**Первый учебный вопрос: «Понятие информации и ее виды. Виды и способы защиты информации»**

**ГОСТ Р 57321.1-2016** «Менеджмент знаний. Менеджмент знаний в области инжиниринга. Часть 1. Общие положения, принципы и понятия» определяет значение слова «Основы»:

Далее рассмотрим ***понятие «информация»***. В **Федеральном Законе №149** от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации» дано понятие информации:

**Информация** – сведения (сообщения, данные) независимо от формы их представления.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Этим же законом определены **виды информации**, представленные на рисунке 1.

Далее, товарищи студенты, подробнее рассмотрим некоторые дополнительные категории информации, которые нам необходимы.

Информация, подразделяемая ***по назначению*:**

* *массовая* – содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума;
* *специальная* – содержит специфический набор понятий, при использовании происходит передача сведений, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация;
* *секретная* – доступ, к которой предоставляется узкому кругу лиц и по закрытым (защищённым) каналам;
* *личная* – набор сведений о какой-либо личности, которые определяют социальное положение и типы социальных взаимодействий внутри популяции.

Информация, подразделяемая ***по способу восприятия*:**

* *визуальная* – воспринимается органами зрения;
* *аудиальная* – воспринимается органами слуха;
* *тактильная* – воспринимается тактильными рецепторами; *- обонятельная* – воспринимается обонятельными рецепторами; *- вкусовая* – воспринимается вкусовыми рецепторами.

Далее, информация, подразделяемая ***по форме отображения*:**

*текстовая* – что передается в виде символов, предназначенных

обозначать лексемы языка; *числовая* – в виде цифр и знаков, обозначающих математические

действия; *графическая* – в виде изображений, событий, предметов, графиков; *звуковая* – устная или в виде записи передача лексем языка аудиальным

путем; *мультимедиа* – информация любого вида, передаваемая через

компьютерные средства.

**Ключевым аспектом для вас, с позиции защиты информации, являются свойства информации, характеризующиеся как факторы окружающей среды человека**:

* нейтральная информация;
* агрессивная информация;  ложная информация;
* защищаемая информация.

Рассмотрим, что включают в себя данные категории.

**Нейтральная информация** – сведения (сообщения, данные), которые в стандартной картине мира не описываются в ценностных категориях (к такой информации неприменимы оценки хорошо или плохо – это есть, было, будет и только).

**Агрессивная информация** – сведения (сообщения, данные), навязываемые человеку различными информационными способами для достижения конкретных целей. При этом агрессивная информация может быть истинной или ложной.

**Ложная информация** – сведения (сообщения, данные), характеризующие какое-либо действие, свойства, и прочую информацию неверно или не до конца верно.

**Защищаемая информация** – сведения (сообщения, данные), являющиеся предметом собственности и подлежащие защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (**ГОСТ Р 50922-2006**. «Защита информации. Основные термины и определения»).

В соответствии с **ГОСТ Р 50922-2006**. «Защита информации. Основные термины и определения»:

**Защита информации** – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

С позиций системного подхода **к защите информации предъявляются определенные требования**:

* обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявления ее узких и слабых мест и противоправных действий;
* безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;
* планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции;
* защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
* методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;
* эффективность защиты информации означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз;
* четкость определения полномочий и прав определенным видам информации;
* предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
* сведение к минимуму числа общих для нескольких пользователей средств защиты;
* учет случаев и попыток несанкционированного доступа к конфиденциальной информации; обеспечение степени конфиденциальной информации;
* обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Рассмотренные требования по защите информации сформировали **принципы защиты информации**:

1. ***Комплексность***. Предполагает:

а) обеспечение безопасности обслуживающего персонала, материальных и финансовых ресурсов от всех возможных угроз всеми доступными законными средствами, методами и мероприятиями;

б) обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, во всех технологических процессах и операциях их создания, обработки, использования и уничтожения;

в) способность системы защиты информации к развитию и совершенствованию в соответствии с изменяющимися внешними и внутренними условиями.

1. ***Своевременность*** – упреждающий характер мер защиты информации. Предполагает постановку задач по комплексной защите информации на стадии проектирования (создания) системы ее защиты на основе анализа известных и прогнозирования возможных угроз безопасности информации, которые могут появиться в будущем после запуска системы защиты в эксплуатацию (реализацию).
2. ***Непрерывность*** – постоянное поддержание работоспособности и развитие системы защиты информации.
3. ***Активность*** – настойчивость в достижении целей и задач защиты информации. Предполагает постоянный маневр силами и средствами защиты информации, а также принятие нестандартных мер защиты.
4. ***Законность*** – разработка системы защиты информации на основе действующего законодательства, а также иных нормативных актов, регламентирующих безопасность информации. В ходе последующей реализации системы защиты информации – применение всех законных методов и средств обнаружения и пресечения правонарушений в области безопасности информации.
5. ***Обоснованность***. Заключается в том, что все методы и средства защиты информации должны быть научно обоснованными и современными, соответствовать последним достижениям науки и техники. В своей совокупности они должны отвечать всем установленным требованиям и нормам по защите информации.
6. ***Экономическая целесообразность*** – затраты на разработку и реализацию (обеспечение заданных параметров) системы защиты информации не должны превышать размеры потенциального ущерба, который может наступить в результате нарушения безопасности защищаемой информации.
7. ***Специализация***. Предполагает привлечение к разработке и внедрению методов и средств защиты информации специализированных субъектов, имеющих государственную лицензию на определенный вид деятельности в сфере оказания услуг по защите информации. Применяемые ими средства защиты информации должны быть сертифицированы по требованиям безопасности информации.
8. ***Взаимодействие и координация деятельности***. Предусматривает организацию четкого взаимодействия между всеми субъектами защиты информации, действующими в рамках единой системы защиты информации, а также координацию их усилий и осуществляемых работ в этой сфере для достижения общих целей. Заключается в интеграции и последовательности деятельности по защите конкретных информационных ресурсов.
9. ***Совершенствование***. Предусматривает совершенствование и разработку новых законодательных, организационных и технических мер защиты информации под воздействием объективных и субъективных факторов.
10. ***Централизация управления***. Предполагает наличие единого координационного центра (субъекта), занимающегося общими вопросами управления системой защиты информации, а также единых требований по обеспечению безопасности информации.

В целом защищаемая информация представляет собой объект защиты информации с определенными элементами. Рассмотрим содержание объекта защиты информации.

**Объект защиты информации** – это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с ***целью защиты информации***.

Типичные **объекты защиты информации**:

1. Лица, допущенные к работе с охраняемой законом информацией либо имеющие доступ в помещения, где эта информация обрабатывается.
2. Объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров.
3. Охраняемая законом информация – информация, доступ к которой ограничен в соответствии с законодательством России (сведения (сообщения, данные), составляющие государственную, банковскую, коммерческую, налоговую, служебную, профессиональную, семейную и иную тайну, включая персональные данные физических лиц).
4. Материальные носители охраняемой законом информации.
5. Средства защиты информации.
6. Технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации.

При этом **носитель защищаемой информации** – это физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Защищаемый объект информатизации** – это объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

**Защищаемая информационная система** – это информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Как было сказано выше, элементы объекта защиты информации необходимо защищать в соответствии с целью защиты информации.

В соответствии с требованиями **федерального закона** **№ 149** от 08.07.2006 г. «Об информации, информационных технологиях и защите информации» **целями защиты информации являются**:

1. Предотвращение утечки, хищения, утраты, искажения, подделки информации.
2. Предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
3. Предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Данные цели реализуются замыслом защиты информации.

**Замысел защиты информации** – это основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Содержание технических и организационных мероприятий будет рассмотрено на следующих занятиях дисциплины.

При этом необходимо обратить внимание на то, что для эффективного выполнения технических и организационных мероприятий, необходимых для достижения цели защиты информации, создается система защиты информации.

**Система защиты информации** – это совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Основными **элементами системы защиты информации** являются:

* объект защиты информации;
* виды защиты информации;
* способы защиты информации;  средства защиты информации;  силы защиты информации.

Пред **системой защиты информации стоят** следующие **задачи**:

1. Проведение единой политики, организация и координация работ по защите информации в оборонной, экономической, политической, научнотехнической и других сферах деятельности.
2. Исключение или существенное затруднение добывания информации средствами разведки.
3. Предотвращение утечки информации по техническим каналам и несанкционированного доступа к ней.
4. Предупреждение вредоносных воздействий на информацию, ее носителей, а также технические средства ее создания, обработки, использования, передачи и защиты.
5. Принятие правовых актов, регулирующих общественные отношения в области защиты информации.
6. Анализ состояния и прогнозирование возможностей технических средств разведки, а также способов их применения.
7. Формирование системы информационного обмена сведениями об осведомленности иностранных разведок о силах, методах, средствах и мероприятиях, обеспечивающих защиту информации внутри страны и за ее пределами.
8. Организация сил, разработка научно обоснованных методов, создание средств защиты информации и контроля за ее эффективностью.
9. Контроль состояния защиты информации в органах государственной власти, учреждениях, организациях и на предприятиях всех форм собственности, использующих в своей деятельности охраняемую законом информацию.

На этом изложение первого учебного вопроса завершено.

**Второй учебный вопрос: «Виды и способы защиты информации»**

При изучении данного учебного вопроса рассмотрим, что представляет собой система защиты информации. При этом содержание объекта защиты информации на сегодняшнем занятии мы изучать не будем, т.к. этому вопросу посвящено следующее занятие и мы сразу приступаем к изучению следующего элемента – виды защиты информации.

В системе защиты информации применяются следующие **виды защиты информации**:

* + правовая защита информации;
  + организационная защита информации;
  + техническая защита информации;
  + криптографическая защита информации;  физическая защита информации.

Кратко рассмотрим эти понятия.

**Правовая защита информации** – это защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Государство также определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности. Например, глава 28 [«Преступления в сфере компьютерной информации»](http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/) в **Уголовном кодексе Российской Федерации**, включает три статьи: Статья 272 «Неправомерный доступ к компьютерной информации»;

Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;

Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационнотелекоммуникационных сетей».

**Организационная защита информации** – это защита информации, основанная на решении, определяющим регламент работы пользователей с конфиденциальной информацией, порядок работы с документацией и носителями данных и подбор кадров.

**Техническая защита информации** – это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

**Средство защиты информации** – это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

***Технические средства защиты информации*** – это любые электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей. Они препятствуют доступу к информации, в том числе с помощью её маскировки.

К *техническим средствам защиты информации* относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить.

*Программные средства защиты информации* – это простые и комплексные программы, предназначенные для решения задач, связанных с обеспечением информационной безопасности.

Примером комплексных решений служат DLP-системы и SIEMсистемы.

*DLP-системы* («Data Leak Prevention» дословно «предотвращение утечки данных») соответственно служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков.

*SIEM-системы* («Security Information and Event Management», что в переводе означает «Управление событиями и информационной безопасностью») обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM-система представлена приложениями, приборами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.

Программные средства требовательны к мощности аппаратных устройств, и при установке необходимо предусмотреть дополнительные резервы.

**Криптографическая защита информации** – это защита информации с помощью ее криптографического преобразования.

Криптография считается одним из самых надежных способов защиты данных, ведь она охраняет саму информацию, а не доступ к ней. Криптографически преобразованная информация обладает повышенной степенью защиты.

**Криптографическое средство защиты информации** – это средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

**Физическая защита информации** – это защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Физическая защита информации характеризуется постоянно действующим ***комплексом сил и средств защиты***.

***Силами физической защиты информации*** являются сотрудники, обеспечивающие выполнение данного функционала.

***Средство физической защиты информации*** – это средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

К ***объектам физической защиты информации*** могут быть отнесены:

охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Рассмотренные виды защиты информации комплексно применяются в различных способах защиты информации.

**Способ защиты информации** – это порядок и правила применения определенных принципов и средств защиты информации.

К **способам защиты информации** относится:

* защита информации от утечки;
* защита информации от несанкционированного воздействия;
* защита информации от непреднамеренного воздействия;
* защита информации от разглашения, защита информации от несанкционированного доступа;
* защита информации от преднамеренного воздействия;
* защита информации от разведки (иностранной разведки).

Кратко рассмотрим эти понятия.

**Защита информации от утечки** – это защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации разведками (иностранными разведками) и другими заинтересованными субъектами.

Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

**Защита информации от несанкционированного воздействия** – это защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**Защита информации от непреднамеренного воздействия** – это защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**Защита информации от разглашения** – это защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

**Защита информации от несанкционированного доступа** – это защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

**Защита информации от преднамеренного воздействия** – это защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

**Защита информации от разведки (иностранной разведки)** – это защита информации, направленная на предотвращение получения защищаемой информации разведкой (иностранной разведкой).

Эффективность рассмотренных видов и способов защиты информации зависит от качества и уровня средств и сил защиты информации.

**Средство контроля эффективности защиты информации** – это средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

Необходимо также отметить, что **эффективность защиты информации** – это степень соответствия результатов защиты информации цели защиты информации.

При этом основой для оценки эффективности защиты информации являются требования к защите информации, определяемые законодательно.

Таким образом, **требование по защите информации** – это установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

**Показатель эффективности защиты информации** – это мера или характеристика для оценки эффективности защиты информации.

**Норма эффективности защиты информации** – это значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

Итак, последний элемент системы защиты информации – силы защиты информации.

**Силы защиты информации** – совокупность органов и (или) исполнителей работ, связанных с защитой информации в интересах владельца информации (структурное подразделение, выполняющее задачи управления функционированием данной системы).

**Конфиденциальная информация**

**Первый учебный вопрос: «Конфиденциальная информация»**

В рассматриваемом ранее нами **Федеральном законе № 149 от 08.07.2006 г. «Об информации, информационных технологиях и о защите информации»** дано понятие **«конфиденциальной информации»**.

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Одним из ***Принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации*** является:

2) установление ограничений доступа к информации только федеральными законами

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите, содержащейся в них информации

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

Статья 9. Ограничение доступа к информации.

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

1. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
2. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим государственную тайну, коммерческую тайну, служебную тайну и иную тайну (например, профессиональную тайну), обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
3. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
4. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.
5. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.
6. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.
7. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

***Статья 16.*** ***Защита информации***.

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного

доступа;

1. реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

***Статья 17.*** ***Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации***).

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Для понимания вопросов конфиденциальности информации, необходимо изучить еще ряд документов.

Одним из них является **Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской**

**Федерации»**.

Основными положениями данного закона являются понятия:

**Критическая информационная инфраструктура** - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Объекты критической информационной инфраструктуры** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Безопасность критической информационной инфраструктуры** - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

**Компьютерная атака** - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

**Компьютерный инцидент** - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки. ***Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры***.

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1. законность;
2. непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры; 3) приоритет предотвращения компьютерных атак.

***Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации***

2. *К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся*:

1. подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
2. организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее - национальный координационный центр по компьютерным инцидентам);
3. подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

3. *Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются* технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

**Статья 7. Категорирование объектов критической информационной инфраструктуры**.

1. ***Категорирование объекта*** ***критической информационной инфраструктуры*** представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Далее в Законе раскрываются вопросы категорирования ***объектов*** ***критической информационной инфраструктуры***, которые вы изучите самостоятельно

**Задание на самостоятельную подготовку**:

* + изучить Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» в полном объеме и быть готовым им руководствоваться в ходе учебного процесса.

Следующий документ, определяющий вопросы конфиденциальной информации, является **Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера»**.

**Перечень сведений конфиденциального характера** 1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

1. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с [Гражданским кодексом Российской Федерации](http://docs.cntd.ru/document/9027690) и Федеральными законами (служебная тайна).
2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с Федеральными законами от 20 апреля 1995 года № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и [от 20 августа 2004 года № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»,](http://docs.cntd.ru/document/901906975) другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.
3. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с [Конституцией Российской Федерации](http://docs.cntd.ru/document/9004937) и Федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
4. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с [Гражданским кодексом Российской Федерации](http://docs.cntd.ru/document/9027690) и федеральными законами (коммерческая тайна).
5. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
6. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с [Федеральным законом от 2 октября 2007 года № 229-ФЗ «Об исполнительном производстве».](http://docs.cntd.ru/document/902063102)

Таким образом, данный Указ определяет виды конфиденциальной информации, которые мы более подробно рассмотрим в следующем учебном вопросе. На этом изложение первого учебного вопроса завершено.

**Второй учебный вопрос: «Виды конфиденциальной информаций»**

Рассмотренный в предыдущем вопросе «Перечень сведений конфиденциального характера» определяет следующие виды конфиденциальной информации:

* + персональные данные;
  + государственную тайну;
  + коммерческую тайну;
  + служебную тайну;
  + иная тайна в соответствии с законодательством (например, врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Рассмотрим содержание некоторых категорий.

Первая категория – «**персональные данные**».

Данная категория определена **Федеральным законом № 152 от 14 июля 2006 года «О персональных данных»**.

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-

телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным (*часть в редакции, введенной в действие с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года*).

Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1. обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
2. организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с

законодательством об архивном деле в Российской Федерации;

1. обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Рассмотрим основные положения данного закона:

Статья 2. **Цель настоящего Федерального закона**.

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. **Основные понятия, используемые в настоящем Федеральном законе.**

В целях настоящего Федерального закона используются следующие основные понятия:

1. **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
2. **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
3. **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
4. **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
5. **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Статья 5. **Принципы обработки персональных данных.**

1. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
2. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
3. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. **Условия обработки персональных данных:**

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
2. обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
3. обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
   1. обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.
4. обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
5. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
6. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
7. обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
8. обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
9. обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;
   1. обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве» и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных», в порядке и на условиях, которые предусмотрены указанным Федеральным законом (*Пункт дополнительно включен с 1 июля 2020 года Федеральным законом от 24 апреля 2020 года N 123-ФЗ*);
10. осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (*далее - персональные данные, сделанные общедоступными субъектом персональных данных*);
11. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;
    1. обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27 мая 1996 года № 57-ФЗ «О государственной охране».
12. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.
13. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора)
14. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.
15. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. **Конфиденциальность персональных данных.**

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 8. **Общедоступные источники персональных данных.**

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 11. **Биометрические персональные данные**.

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**.

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. Обеспечение безопасности персональных данных достигается, в частности:
3. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
4. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
5. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
6. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
7. учетом машинных носителей персональных данных;
8. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
9. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
10. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
11. контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1. уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
2. требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
3. требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Следующая категория – «**государственная тайна**».

**Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (**федеральный закон Российской Федерации № 5485-1 от 21.07.1993 «О государственной тайне»**). ***Степени секретности сведений*** (грифы секретности): особой важности; совершенно секретно; секретно.

***Перечень сведений, отнесенных к государственной тайне*** (*утв.*

*Указом Президента РФ от 30 ноября 1995 г. N 1203*): 1) сведения в военной области;

1. сведения в области экономики, науки и техники;
2. сведения в области внешней политики и экономики;
3. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам,

предприятиям, учреждениям и организациям; о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах

Российской Федерации; о состоянии здоровья высших должностных лиц Российской

Федерации; о фактах нарушения законности органами государственной власти и их

должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Рассмотрим **содержание коммерческой тайны**.

Федеральным законом **Российской Федерации** № 98 от 29 июля 2004 г. «О коммерческой тайне» (*с изменениями и дополнениями от: 2 февраля, 18 декабря 2006 г., 24 июля 2007 г., 11 июля 2011 г., 12 марта 2014 г., 18 апреля 2018 г.*) определены следующие положения.

**Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

**Информация, составляющая коммерческую тайну** – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны

Для **обозначения ценности конфиденциальной коммерческой информации** используются три категории:

* «коммерческая тайна - строго конфиденциально»; - «коммерческая тайна - конфиденциально»; - «коммерческая тайна».

Используется и другой подход к **градации ценности коммерческой информации**:

* «строго конфиденциально - строгий учет»; - «строго конфиденциально»; - «конфиденциально».

**Режим «Коммерческая тайна»** вступает в силу после выполнения следующих мер:

1. Определен перечень информации, составляющей коммерческую тайну.
2. Ограничен доступ к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.
3. Организован учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.
4. Урегулированы отношения по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.
5. Нанесен на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включен в состав реквизитов документов, содержащих такую информацию, гриф «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

**Режим коммерческой тайны не может быть установлен** лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1. содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
2. содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
3. о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
4. о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и

безопасности населения в целом;

1. о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
2. о задолженности работодателей по выплате заработной платы и социальным выплатам;
3. о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
4. об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
5. о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
6. о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
7. обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

Должностные лица несут ответственность в соответствии с законодательством Российской Федерации за неправомерное отнесение сведений к коммерческой тайне, а также за не отнесение сведений к коммерческой тайне в случаях, предусмотренных законодательством Российской Федерации.

Рассмотрим **содержание служебной тайны**.

Федеральным законом «О служебной тайне» (Проект № 124871-4) определены следующие положения.

**Служебная тайна** – это охраняемая законом конфиденциальная информация о деятельности государственных органов, организаций, доступ к которой ограничен в силу служебной необходимости.

**Режим служебной тайны** – совокупность правовых, организационных, технических и иных мер, принимаемых уполномоченными должностными лицами органов государственной власти и организаций,обеспечивающих ограничения на распространение сведений, составляющих служебную тайну, и на доступ к этим сведениям.

Сведения, составляющие служебную тайну (служебная тайна) – конфиденциальные сведения, образующиеся в процессе управленческой деятельности органа или организации, распространение которых препятствует реализации органом или организацией предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом или организацией в соответствии с их компетенцией в установленном законодательством порядке.

**Сведения, относящиеся к служебной тайне**: сведения, поступившие от физических и юридических лиц, других органов государственной власти и организаций, доступ к которым ограничен в соответствии с федеральными законами, при наличии на документах, содержащих эти сведения или сопроводительных документах грифа «Служебная тайна».

**Не подлежат отнесению к служебной тайне сведения**:

содержащиеся в законодательных и иных правовых актах, устанавливающих права, свободы, обязанности граждан и порядок их реализации, а также правовой статус органов государственной власти, органов местного самоуправления, организаций; о чрезвычайных ситуациях, происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, а также о стихийных бедствиях, их официальных прогнозах и последствиях; в области экологии, метеорологии, демографии, эпидемиологии и санитарии, культуры, сельского хозяйства, о состоянии преступности и другие сведения, необходимые для обеспечения безопасности граждан и населения в целом;

**Угрозы информации**

**Первый учебный вопрос: «Угрозы информации»**

Угрозы безопасности, которые могут быть реализованы, например, с помощью скрытых каналов, включают в себя:

* внедрение вредоносных программ и данных;
* подачу злоумышленником команд агенту для выполнения; - утечку криптографических ключей или паролей; - утечку отдельных информационных объектов.

Для дальнейшего изучения угроз безопасности информации вы должны знать ряд понятий, определенных в **ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

**Угроза** – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

**Угроза информационной безопасности организации** – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Формой реализации или проявления угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств информационной безопасности объекта или объектов защиты организации.

**Ущерб** – отрицательные последствия, возникающие вследствие причинения вреда активам организации.

**Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

**Безопасность информации (данных)** – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

В ходе занятий мы уже несколько раз встречаемся с терминами

«конфиденциальность», «доступность» и «целостность», и в дальнейшем не раз будем к ним обращаться. Термин «конфиденциальность информации» мы рассмотрели на предыдущем занятии. Поэтому напомню его формулировку и рассмотрим содержание категорий «доступность» и «целостность».

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (**ГОСТ Р 50922** «Защита информации. Основные термины и определения»).

**Доступность информации (ресурсов информационной системы)** – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно

**Целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Возвращаясь к **ГОСТ Р 53114** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», вы должны изучить следующие понятия:

**Уязвимость** – внутренние свойства объекта, создающие восприимчивость к воздействию источника риска, которое может привести к какому-либо последствию.

**Атака** – попытка преодоления системы защиты информационной системы.

Степень «успеха» атаки зависит от уязвимости и эффективности системы защиты.

**Сетевая атака** – действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

**Сетевой протокол** – совокупность семантических и синтаксических правил, определяющих взаимодействие программ управления сетью, находящейся на одном компьютере, с одноименными программами, находящимися на другом компьютере.

Угрозы и ущерб связаны между собой. Угрозы становятся возможными по причине уязвимостей в информационной системе.

Угроза может причинить ущерб активам организации, таким как информация, процессы и системы. Угрозы могут возникать в результате природных явлений или действий людей, они могут быть случайными или умышленными.

Должны быть установлены и случайные, и преднамеренные источники угроз. Угрозы могут проистекать как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться в общем и по виду (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные угрозы, не будет упущена, но объем требуемой работы, несмотря на это, сокращается. Некоторые угрозы могут влиять более чем на один актив. В таких случаях они могут быть причиной различных влияний в зависимости от того, на какие активы оказывается воздействие.

Для определения и количественной оценки вероятности возникновения угроз данные могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в области ИБ, экспертов в области физической безопасности, специалистов юридического отдела и других структур, а также от юридических организаций, метеорологических служб, страховых компаний, национальных правительственных учреждений. При анализе угроз должны учитываться аспекты среды и культуры. Опыт, извлеченный из инцидентов, и предыдущие оценки угроз должны быть учтены в текущей оценке. При необходимости для заполнения перечня общих угроз может быть целесообразным справиться в других реестрах угроз (возможно, специфичных для конкретной организации или бизнеса). Списки угроз и их статистику можно получить от промышленных предприятий, федерального правительства, юридических организаций, страховых компаний и т.д. Используя списки угроз или результаты предыдущих оценок угроз, не следует забывать о том, что происходит постоянная смена значимых угроз, особенно, если изменяются бизнес-среда или информационные системы.

**Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы информационной безопасности.**

Рассмотрим содержание объекта угрозы информационной безопасности.

Данная категория определяется методическим документом «Методика оценки угроз безопасности информации» (*утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г*.).

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям - объекты воздействия.

Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации.

Исходными данными для определения возможных **объектов угрозы являются**:

а) общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России;

б) описания векторов компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий, и типах доступа, внешних и внутренних интерфейсах);

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационнотелекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

Объекты воздействия и виды воздействия на них должны быть конкретизированы применительно к архитектуре и условиям функционирования систем и сетей, а также областям и особенностям деятельности обладателя информации и оператора.

Товарищи студенты! Мы рассмотрели, что исходными данными для определения возможных объектов воздействия являются, в том числе общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России.

Что представляет собой ***Банк данных угроз безопасности информации*** и ***модель угроз***?

Целью создания и ведения настоящего Банка данных угроз безопасности информации является повышение информированности заинтересованных лиц о существующих угрозах безопасности информации в информационных (автоматизированных) системах.

Банк данных угроз безопасности информации предназначен для заказчиков, операторов, разработчиков информационных (автоматизированных) систем и их систем защиты, разработчиков и производителей средств защиты информации, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

Банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Сведения об угрозах безопасности информации и уязвимостях программного обеспечения, содержащиеся в Банке данных угроз безопасности информации, не являются исчерпывающими и могут быть дополнены по результатам анализа угроз безопасности информации и уязвимостей в конкретной информационной (автоматизированной) системе с учетом особенностей ее эксплуатации (рис.1).



Рисунок – 1 Банк данных угроз безопасности информации

При определении угроз безопасности информации учитываются структурно-функциональные характеристики системы защиты информации, включающие наличие элементов автоматизированной системы управления, физические, логические, функциональные и технологические взаимосвязи в системе защиты информации, в том числе взаимодействие автоматизированной системы управления с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, режимы функционирования системы защиты информации, а также иные особенности ее построения и функционирования.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурнофункциональных характеристик системы защиты информации, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Банк данных угроз безопасности информации постоянно обновляется

(рис. 2).

Визуально Банк данных угроз безопасности информации содержит следующие данные:

1. Общие сведения об угрозе безопасности информации:

* идентификатор угрозы безопасности информации;
* наименование угрозы безопасности информации;
* описание угрозы безопасности информации;
* источник угрозы (характеристика и потенциал нарушителя);
* объект воздействия угрозы безопасности информации;

2. Последствия воздействия угрозы безопасности информации

* нарушение конфиденциальности (1 или 0);
* нарушение целостности (1 или 0);
* нарушение доступности (1 или 0);

3. Дополнительные сведения об угрозы безопасности информации: - дата включения угрозы в банк угроз безопасности информации; - дата последнего изменения данных.

Аналогично можно получить сведения по уязвимостям.

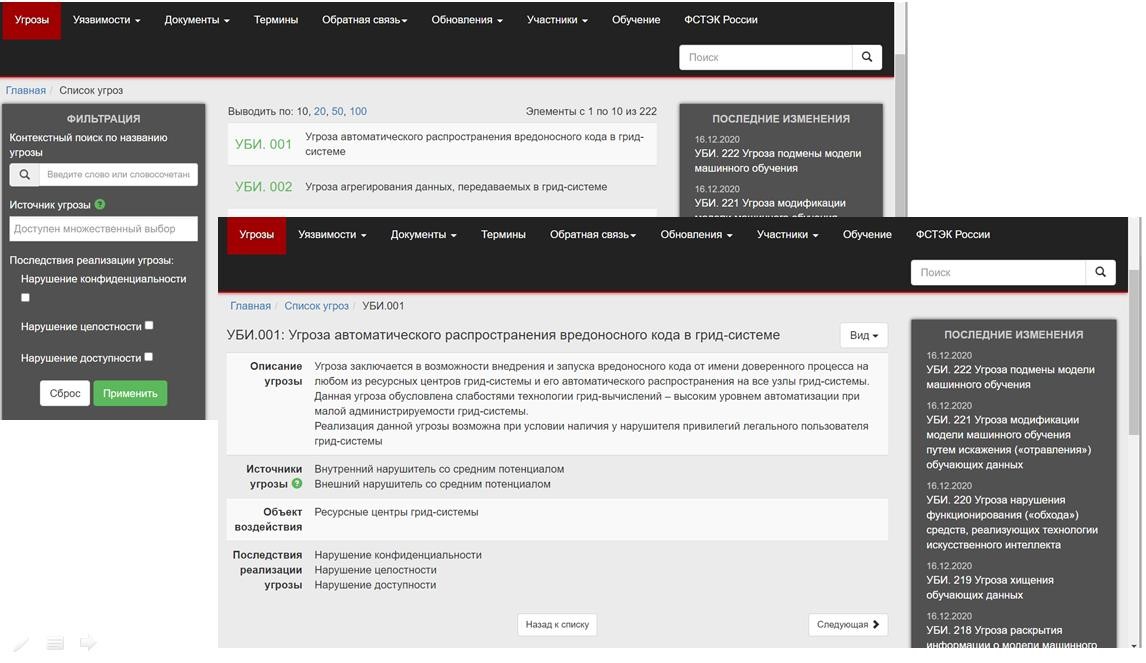


Рисунок – 2 Структура банка данных угроз безопасности информации

Следующей элемент, являющийся исходными данными для определения возможных объектов воздействия– это ***модель угроз безопасности информации***. Она должна содержать описание системы защиты информации и угроз безопасности информации для каждого из уровней системы защиты информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования системы защиты информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России. ***Порядок моделирования угроз безопасности*** представлен на рисунке 3 в виде схемы.

Данный порядок включает в себя пять этапов, выполняемых в определенной последовательности. Общая схема процесса, представленная в Методике, выглядит следующим образом.

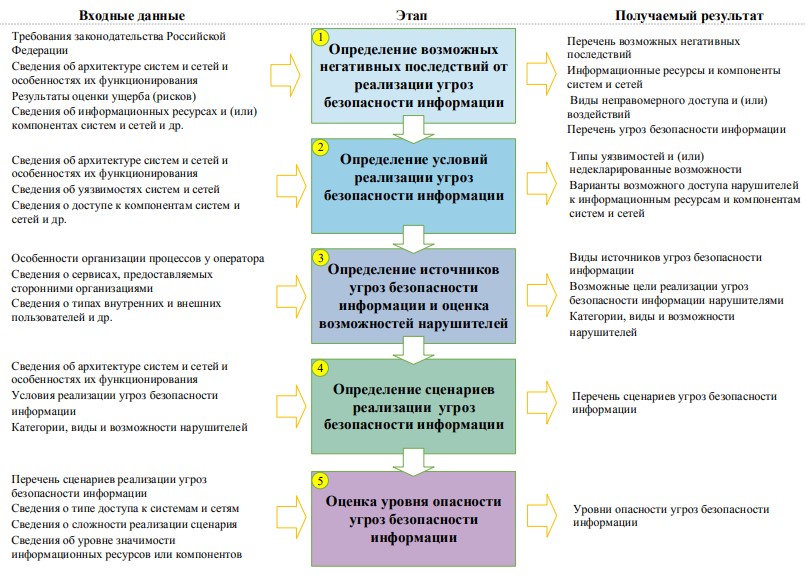


Рисунок 3 – Порядок моделирования угроз безопасности

За ***определение актуальности угрозы безопасности информации*** отвечают этапы с первого по четвертый. В соответствии с Методикой, угроза безопасности будет являться актуальной при наличии хотя бы одного сценария ее реализации и, если ее реализация приведет к каким-либо негативным последствиям для обладателя информации (оператора) или государства.

Цель пятого этапа – ***определить опасность каждой из актуальных угроз***. По сути, ***данная характеристика носит исключительно информационный характер*** и не оказывает прямого влияния ни на итоговый документ, формируемый по результатам моделирования, ни на возможные варианты нейтрализации угрозы. Можно предположить, что данный параметр должен использоваться для определения очередности закрытия угрозы, однако малое число возможных значений показателя – «низкий», «средний», «высокий» – не позволяют сделать это с достаточной степенью детализации. Более того, любая из дошедших до данного шага угроз должна быть так или иначе закрыта, поэтому забыть про «неопасную» угрозу попросту не получится. Таким образом, истинная цель данного параметра остается не раскрытой в полной мере.

Стоит отметить, что работы по моделированию угроз безопасности должны проводиться либо обладателем информации (оператором) самостоятельно, либо с привлечением лицензиатов ФСТЭК.

Подробнее рассмотрим ***порядок определения актуальности угроз безопасности***.

На ***первом этапе*** предлагается определить ***все возможные негативные последствия от реализации угроз безопасности***. Помогать в этом должна либо проведенная ранее [оценка ущерба (рисков)](https://acribia.ru/services/analysis) от нарушения основных критических процессов, либо экспертная оценка, либо информация, получаемая от эксплуатирующих информационную систему подразделений.

При любом выбранном подходе, необходимо определить информационные ресурсы, обеспечивающие выполнение критических процессов (непосредственно информация, программно-аппаратные средства, средства защиты информации и иные) и основные виды неправомерного доступа по отношению к каждому из ресурсов. Методичка содержит перечень основных видов ресурсов и неправомерного доступа к ним, а также примеры определения возможных негативных последствий.

1. На ***втором этапе*** необходимо определить наличие ***потенциальных уязвимостей и их типы, наличие недекларированных возможностей в информационных системах, а также необходимость доступа к системе для реализации каждой из угроз безопасности***.

В качестве основного метода выявления потенциальных уязвимостей в информационной системе на этапе ее эксплуатации является тестирование на проникновение, проводимое в том числе с учетом функциональных возможностей и настроек средств защиты.

1. Следующим, ***третьим этапом*** является ***определение нарушителей безопасности***, как **источника угроз информационной безопасности** и оценка их возможностей. В качестве источников угроз предлагается рассматривать как антропогенные, так и техногенные: первые рассматриваются абсолютно для всех информационных систем, тогда как вторые – только для тех систем, для которых предъявляются требования к устойчивости и надежности функционирования.

Подход к определению возможных ***антропогенных источников угроз – нарушителей*** – является стандартным и заключается в выявлении конкретных видов нарушителей, их потенциала и возможностей при реализации угроз в отношении защищаемой информационной системы. Стоит отметить, что при наличии связи информационной системы с Интернетом, внешний нарушитель как минимум с низким потенциалом всегда рассматривается в качестве актуального источника угроз.

Необходимо обратить внимание, что согласно Методике, нарушитель может обладать одним из четырех уровней потенциала (базовый, базовый повышенный, средний и высокий).

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей.

Основными **видами нарушителей**, подлежащих оценке, являются:

* специальные службы иностранных государств;
* террористические, экстремистские группировки;
* преступные группы (криминальные структуры);
* отдельные физические лица (хакеры);
* конкурирующие организации;
* разработчики программных, программно-аппаратных средств;
* лица, обеспечивающие поставку программных, программноаппаратных средств, обеспечивающих систем;
* поставщики услуг связи, вычислительных услуг;
* лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
* лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
* авторизованные пользователи систем и сетей;
* системные администраторы и администраторы безопасности; - бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов.

Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба).

Возвращаемся к схеме модели угроз, показанной выше на рис. 3.

4. На четвертом этапе осуществляется **анализ возможных тактик и техник реализации угроз**. Для определения возможных сценариев атак, Методика предлагает использовать приведенные в ней тактики и техники, а также дополнительную информацию из БДУ ФСТЭК или иных баз данных компьютерных атак (здесь имеются в виду матрица ATT&CK и аналогичные походы).

Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации.

На этапе эксплуатации систем и сетей для каждой возможной угрозы безопасности информации определяется множество возможных сценариев ее реализации в интересах оценки эффективности принятых технических мер по защите информации (обеспечению безопасности), в том числе средств защиты информации. При этом множество сценариев определяется для каждого актуального нарушителя и уровней его возможностей в соответствии с полученными результатами инвентаризации систем и сетей, анализа уязвимостей и (или) тестирования на проникновение, проведенных с использованием автоматизированных средств.

На этапе эксплуатации определение сценариев реализации угрозы включает:

а) анализ исходных данных на систему или сеть, предусматривающий в том числе анализ документации, модели угроз безопасности информации, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;

б) проведение инвентаризации информационных систем и сетей и

определение объектов воздействия и их интерфейсов;

в) определение внешних интерфейсов, которые могут быть

задействованы при реализации угроз безопасности информации;

г) определение внутренних интерфейсов, которые могут быть

задействованы при реализации угроз безопасности информации;

д) выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;

е) проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;

ж) поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также результатов инвентаризации, анализа уязвимостей и тестирования на проникновение;

з) составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

На этом изложение первого учебного вопроса завершено.

**Второй учебный вопрос: «Классификация угроз информационной безопасности»**

Угрозы чрезвычайно разнообразны, поэтому мы рассмотрим их общую классификацию. В частности, угрозы можно классифицировать по их носителям, по целям, по причиненному ущербу, по наличию умысла, по степени подготовленности и профессионализму нарушителей, по скрытности исполнения, по удаленности от объекта защиты и еще множеству различных признаков.

**Классификацию угроз информационной безопасности** можно разделить на четыре большие группы:

1. ***По аспекту ИБ***: угрозы конфиденциальности, угрозы целостности, угрозы доступности.
2. ***По сфере воздействия на информационную систему***: внутри или вне рассматриваемой АИС; угрозы, возникновение которых обусловлено человеческим фактором. Угрозы со стороны инсайдеров (лиц, имеющих доступ к скрытой и достоверной информации) являются наиболее опасными.
3. ***По компонентам АИС, на которые нацелена угроза***: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура; угрозы, связанные с техническими и программными средствами, используемыми при разработке и эксплуатации информационных систем.
4. ***По природе возникновения***: естественные (объективные) и искусственные (субъективные); техногенные угрозы, возникающие вследствие форс-мажорных обстоятельств.

Рассмотрим данную классификацию угроз информационной безопасности.

**Первая группа угроз – угрозы по аспекту ИБ.** *угрозы конфиденциальности, угрозы целостности, угрозы доступности.*

*Угрозы конфиденциальности* реализуются, если защищаемая информация, обладающая действующей или потенциальной ценностью в силу ее неизвестности третьим лицам, становится достоянием этих лиц (одного или многих).

В некоторых случаях угрозу конфиденциальности может нести не только раскрытие содержания скрываемой информации, но ставший известным сам факт существования такой информации. Например, тайной может являться не только содержание международного договора или финансовой сделки, но и сам факт такого соглашения.

*Угрозы целостности информации* выражаются в ее несанкционированной или непреднамеренной модификации. Т.е. угрозы изменения ее содержания.

Правомерен вопрос: какое количество информации необходимо изменить, чтобы наступила угроза целостности? Это, безусловно, зависит от вида информации. Если защищаемая информация представляет собой текст, запись голоса, музыкальное произведение, рисунок, то порча или искажение ее части могут не привести к потере качества.

Угроза целостности представляет опасность не только для данных. Модификация компьютерной программы, делающая возможной перехват управления компьютером с целью совершения шпионских или деструктивных действий, тоже является разновидностью угроз целостности. Нарушение целостности информации вредит двум ее прагматическим качествам – полноте и достоверности. Косвенным следствием угрозы целостности является утрата доверия к источнику или носителю информации.

*Угрозы доступности* выражаются в том, что защищаемая информация оказывается заблокированной, т. е. в течение некоторого времени недоступной для ее собственника, владельца или пользователя. При этом информация сохраняется в неизменном виде и не становится достоянием третьих лиц. Блокирование информации может произойти по какой-либо из перечисленных ниже причин:

* поломки ключа или замка от сейфа, в котором хранятся носители конфиденциальной информации;
* забывчивости пользователя, приводящей к утрате пароля для расшифровывания электронного документа;
* повреждения служебной области данных на магнитном или оптическом диске либо неисправности устройства считывания/записи данных (если поврежден участок носителя, где была записана защищаемая информация, следует говорить об угрозах целостности).

Угроза доступности реализуется и в том случае, если информация временно оказывается заблокированной для автоматизированной информационной системы. Например, страшные по своим возможным последствиям переключения на посторонние задачи компьютерных систем, управляющих ядерной реакцией или движением транспорта, тоже являются примерами угроз доступности информации.

Собственник, организующий защиту своей информации, должен ясно представлять себе характер потенциальных угроз и четко осознавать, что с помощью одного и того же набора средств и методов защитить информацию от всех трех типов угроз невозможно.

**Вторая группа угроз – угрозы по сфере воздействия на информационную систему**.

*Внутри или вне рассматриваемой АИС; угрозы, возникновение которых обусловлено человеческим фактором. Угрозы со стороны инсайдеров (лиц, имеющих доступ к скрытой и достоверной информации) являются наиболее опасными*.

Источники угроз ИБ можно разделить на внутренние и внешние.

К ***внутренним*** источникам угроз информационной безопасности относятся:

* внутренние нарушители информационной безопасности;
* аппаратные средства, используемые в информационной системе (рабочие станции, серверы, принтеры, внешнее оборудование,

источники бесперебойного питания и другие);

* программные средства (системное и прикладное программное обеспечение);
* сетевое оборудование (маршрутизаторы, коммутаторы, модемы, каналы связи и т.д.);
* системы жизнеобеспечения (системы энергоснабжения, системы кондиционирования и водоснабжения).

К ***внешним*** источникам угроз информационной безопасности относятся:

* внешние нарушители информационной безопасности ИС;  форс-мажорные обстоятельства.

*По мотивации воздействия на информационные ресурсы и системы*, источники угроз ИБ можно разделить на преднамеренные и случайные.

*Преднамеренные (умышленные) угрозы* связаны с корыстными стремлениями людей (злоумышленников).

*Случайные (неумышленные) угрозы* вызваны ошибками в проектировании элементов информационных систем, в программном обеспечении, в действиях сотрудников и т.п.

*Угрозы, обусловленные человеческим фактором*.

Данный класс угроз весьма обширен, к нему относятся угрозы, возникающие вследствие умышленных или неумышленных действий человека:

* *неправомерные действия авторизованных пользователей в системах и приложениях*, что выражается в использовании нарушителем учетной записи, к которой ему разрешен доступ, в неразрешенных целях, в том числе неправомерные действия в системах управления сетями телекоммуникаций, биллинговых, финансовых и технологических системах. Эти же угрозы могут исходить и от других категорий лиц: администраторов, временных и удалённых пользователей, программистов, партнёров;
* *отказ в обслуживании*, т.е. выполнение намеренных действий, направленных на возникновение отказа в обслуживании в системах, приложениях, базах и сетях передачи данных. Такой вид угроз может исходить от администраторов, технического персонала, внешних злоумышленников, программистов, партнёров; авторизованных, удалённых и временных пользователей;
* *внедрение вредоносного или разрушающего программного обеспечения*, включающего вирусы, «троянских коней», «червей», «логические бомбы» и приводящее к сбою или нарушению в работе компонентов информационных систем, а также получению полного контроля над уязвимой системой. К такому виду угроз могут быть причастны внешние злоумышленники; авторизованные, удалённые и временные пользователи, партнёры (конкуренты), разработчики, программисты, технический персонал, администраторы;
* *подмена имени пользователя авторизованными пользователями*, выражающаяся в получении доступа (например, с помощью использования чужой учетной записи) авторизованными пользователями к информации, доступ к которой им запрещен. Данный вид угроз может исходить от авторизованных, удалённых и временных пользователей; технического персонала, партнёров (конкурентов) и администраторов;
* *подмена имени пользователя посторонними лицами*, выражающаяся в получении посторонними лицами доступа к информации под именем авторизованного пользователя. Основная угроза в этом случае может исходить от внешних злоумышленников и посетителей.
* *неправомерное использование системных ресурсов*, связанное с использованием аппаратного и программного обеспечения информационной системы в нерабочих целях, например, компьютерные игры, просмотр фильмов, использование доступа в Интернет в целях, не относящихся к выполнению функциональных обязанностей; использование ресурсов для несанкционированного выполнения работ для сторонних организаций и в личных целях. Эти угрозы могут исходить от авторизованных, удалённых и временных пользователей, технического персонала, программистов, администраторов;
* *ошибки в операциях*, выражающиеся в совершении ошибок сотрудниками организации при выполнении операций, связанных с эксплуатацией программно-аппаратных средств информационной системы. Данные угрозы могут исходить в основном от администраторов и партнёров организации;
* *ошибки в обслуживании* *аппаратного обеспечения*, т.е. компьютерной, множительной техники, сетевого оборудования и прочего в процессе технического обслуживания аппаратных средств техническим персоналом;
* *ошибки пользователя при работе с приложениями*. К данным угрозам могут быть причастны авторизованные, удалённые и временные пользователи, а также партнёры;
* *проникновение в корпоративную сеть*. Данная угроза может быть реализована одним из следующих способов:
* проникновение хакера в систему с использованием, например, атаки с переполнением буфера;
* проникновение в систему с подменой участника сетевого соединения;
* проникновение в систему с подменой IP-, MAC-адресов;
* осуществление атаки с заведомым введением в заблуждение и другие.

В любом случае, подобные угрозы исходят от внешних

злоумышленников;

 *манипулирование информацией*. К данной угрозе относятся:

* подмена информации на веб-сайте организации, партнеров;
* рассылка заведомо ненужной адресату информации

(бомбардирование спамом);

* внедрение ложных сообщений;
* намеренное нарушение очередности доставки информации;
* намеренная задержка доставки информации;
* намеренный сбой маршрутизации;
* перехват, изменение и перенаправление сообщения атакующей стороной посредством посылки сообщения через скомпрометированную рабочую станцию или компьютер злоумышленника.

Эти виды угроз исходят от внешних злоумышленников, администраторов, технического персонала, авторизованных, удалённых и временных пользователей, партнёров (конкурентов), программистов;  *перехват информации*. К данной угрозе относятся:

* пассивный перехват информации;
* активный перехват информации;
* несанкционированный мониторинг трафика.

Эти виды угроз исходят от авторизованных, удалённых и временных пользователей; технический персонал, внешние злоумышленники, программисты, партнёры (конкуренты) и администраторы;

 *отрицание приема/передачи сообщений*. К данной угрозе относятся следующие случаи:

* пользователи сети отрицают, что они посылали сообщение (отрицание передачи);
* пользователи сети отрицают, что они приняли сообщение (отрицание приема).

К данным угрозам могут быть причастны авторизованные, удалённые и временные пользователи, технический персонал, программисты, администраторы и партнёры;

* *кражи* *персоналом документов, а также имущества, находящихся в помещениях организации*. К этому могут быть причастны обслуживающий и технический персонал, пользователи, программисты, администраторы;
* *кражи посторонними лицами* документов, а также имущества, в том числе, осуществившими незаконное проникновение в помещения организации. Данный вид угроз исходит от посетителей и временных пользователей;
* *умышленная порча имущества сотрудниками организации* путем совершения актов вандализма и причинения физического ущерба техническим средствам, носителям информации, системам жизнеобеспечения. Такие угрозы могут исходить от обслуживающего и технического персонала, пользователей, программистов и администраторов;
* *умышленная порча имущества посторонними лицами, не являющимися сотрудниками организации*, в том числе, осуществившими незаконное проникновение на объекты организации. Эти угрозы могут исходить от посетителей и временных пользователей.

В соответствии **с ГОСТ Р 27005-2010** «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», особое внимание следует уделять источникам угроз, происходящих от деятельности человека.

Задание на самостоятельную подготовку: изучить ГОСТ Р 27005-2010 в полном объеме и быть готовым им руководствоваться в ходе учебного процесса.

**Третья группа угроз – угрозы по компонентам АИС, на которые нацелена угроза.**

*данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура; угрозы, связанные с техническими и программными средствами, используемыми при разработке и эксплуатации информационных систем*.

Угрозы компонентов АИС целесообразно рассматривать по трем группам отказов:

- отказ пользователей работать с ИС; - внутренний отказ информационной системы; - отказ поддерживающей инфраструктуры.

Применительно к *отказам пользователей* рассматриваются следующие угрозы:

*нежелание работать с информационной системой* (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями, и техническими характеристиками);

*невозможность работать с системой в силу отсутствия соответствующей подготовки* (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.); *невозможность работать с системой в силу отсутствия технической поддержки* (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками *внутренних отказов* являются: *нарушение* (случайное или умышленное) от установленных правил

эксплуатации; *выход системы из штатного режима эксплуатации* в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

* ошибки при (пере)конфигурировании системы;
* отказы программного и аппаратного обеспечения;
* разрушение данных;
* разрушение или повреждение аппаратуры.

По отношению к *поддерживающей инфраструктуре* рекомендуется рассматривать следующие угрозы:

нарушение работы (случайное или умышленное) систем связи,

электропитания, водо- и/или теплоснабжения, кондиционирования; разрушение или повреждение помещений;

невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

**Четвертая группа угроз – угрозы по природе возникновения**: *естественные (объективные) и искусственные (субъективные); техногенные угрозы, возникающие вследствие форс-мажорных обстоятельств*.

**Естественные угрозы** – это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

**Искусственные угрозы** – угрозы, вызванные деятельностью человека:

*непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

*преднамеренные* (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

**Основные непреднамеренные искусственные угрозы АИС**:

* неумышленные физические действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
* неумышленная порча носителей информации;
* запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);
* самостоятельная установка и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами, нарушающих целостность и доступность конфиденциальной информации;
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* ввод ошибочных данных.

**Основные преднамеренные искусственные угрозы АИС:**

* физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* хищение носителей конфиденциальной информации
* чтение остаточной информации из оперативной памяти, внешних запоминающих устройств;
* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя

(«маскарад»);

* вскрытие шифров криптозащиты информации;
* незаконное подключение к телекоммуникационным системам и линиям связи.

На этом изложение учебного вопроса завершено.

**Каналы утечки информации**

**Первый учебный вопрос: «Каналы утечки информации. Виды и классификация каналов утечки информации»**

В **ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» определены термины в области утечки информации.

**Утечка информации** – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

К каналам утечки информации относится разглашение информации и получение информативного сигнала злоумышленником посредством ее перехвата.

**Разглашение информации** – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

**Информативный сигнал** – сигнал, по параметрам которого может быть определена защищаемая информация.

Данный информативный сигнал перехватывается техническими средствами, применяемыми злоумышленниками.

**Перехват информации** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Т.е. под перехватом понимают получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации.

Существует два метода перехвата: непосредственный перехват и электромагнитный перехват.

**Непосредственный перехват** – это перехват, осуществляемый либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

**Электромагнитный перехват** – это перехват, осуществляемый за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д., т.е. перехват с технических средств, имеющих побочные электромагнитные излучения и наводки. Данный перехват может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Таким образом, **канал утечки информации** – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Необходимо отметить, что каналы утечки информации характеризуются как скрытые каналы.

В соответствии с **ГОСТ Р 53113.1-2008** «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов».

**Скрытый канал** – это канал, непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Для создания канала утечки информации или скрытого канала применяется агент нарушителя.

**Агент нарушителя** – это лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

Рассмотрим ***типовой механизм функционирования скрытого канала***.

Скрытые каналы используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на автоматизированную информационную систему, которая не обнаруживается средствами контроля и защиты.

Опасность скрытых каналов основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации.

Общая схема механизма функционирования скрытых каналов в автоматизированной информационной системе представлена на рис. 2.

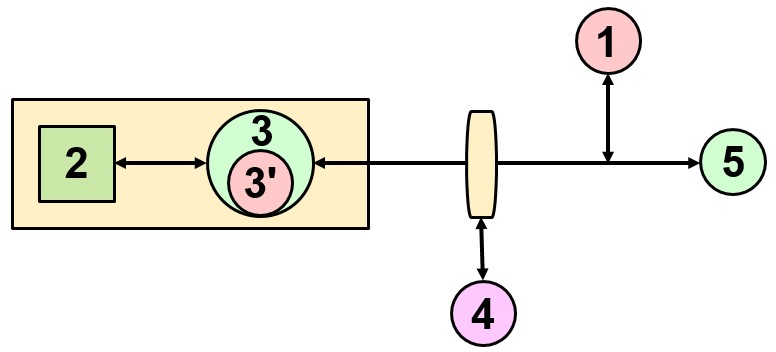


Рисунок 2 – Схема механизма функционирования скрытых каналов в автоматизированной информационной системе

где:

1. – нарушитель безопасности (злоумышленник), целью которою валяется НСД (информации ограниченною доступа либо несанкционированное влияние на АИС;
2. – информация ограниченного доступа либо критически важная функция;
3. – субъект, имеющий санкционированный доступ к 2;

3' – агент нарушителя безопасности, находящийся в замкнутом контуре с 2 и взаимодействующий с 2 от имени субъекта 3;

1. – инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий(ее) информационное взаимодействие 3. пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды;
2. – субъект, находящийся вне замкнутого контура, с которым 3 осуществляет санкционированное информационное взаимодействие.

Взаимодействие между субъектами 3 и 5 является санкционированным и необходимым для правильной работы АИС. Задача агента *3* заключается в том, чтобы обеспечить регулярное интерактивное взаимодействие между агентом и злоумышленником. Агент должен передать информацию ограниченного доступа 2 злоумышленнику *1* либо по команде злоумышленника *1* оказать воздействие на критически важную функцию 2. Скрытность канала взаимодействия между злоумышленником *1* и агентом *3'* заключается в том, что субъект *3,* инспектор *4* и субъект 5 не обнаруживают факт передачи информации или команды.

Скрытые каналы позволяют злоумышленнику регулярно интерактивно осуществлять взаимодействие со своим агентом, внедренным в автоматизированную информационную систему.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, электробытовые приборы и др.

К **факторам, способствующим утечки информации** относятся:

* недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
* использование не аттестованных технических средств обработки конфиденциальной информации;
* слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами.

Следует помнить о **внутренних каналах утечки информации**, связанных с действиями администрации и обслуживающего персонала, с качеством организации режима работы, тем более что обычно им не придают должного внимания. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированное копирование и т. п.

К **внешним каналам утечки информации** относятся:

* телекоммуникационные сети, линии связи и коммунальные сети, выходящие за пределы контролируемой зоны;
* электромагнитные, визуально-оптические, материальновещественные, информационные, выходящие за пределы контролируемой зоны.

Все **каналы проникновения в систему и утечки информации** разделяют на прямые и косвенные.

Под ***косвенными*** понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы.

В качестве косвенных каналов утечки информации большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения с установленными в них основными и вспомогательными техническими средствами, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

***Прямые каналы*** могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов. Для использования прямых каналов необходимо проникновение в помещения, где расположены компоненты системы.

Кроме этого, по**типу основного средства**, используемого для реализации угрозы все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

**По способу получения информации** потенциальные каналы утечки информации можно разделить на:

* акустические (включая и акустопреобразовательные). Связаны с распространением звуковых волн в воздухе или упругих колебаний в других средах;
* электромагнитные (в том числе магнитные и электрические);
* визуально-оптические (наблюдение, фотографирование). В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.;
* материально-вещественные (бумага, фото, магнитные носители,

отходы и т. п.);

* информационные. Связаны с доступом к элементам телекоммуникационных систем, носителям информации, самой вводимой и выводимой информации, к программному обеспечению, а также с подключением к линиям связи.

Иной возможности для переноса информации в природе не существует.

В соответствии с **ГОСТ Р 53113.2-2009** «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов» **классификация скрытых каналов по механизму передачи информации** подразделяют на:

* скрытые каналы по памяти;
* скрытые канал по времени;
* скрытые статистические каналы;
* скрытые каналы по пропускной способности.

**Скрытые каналы по памяти** основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий - считывает ее. Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация. Скрытые каналы по памяти предполагают использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты.

Скрытые каналы по памяти, в свою очередь, подразделяют на:

* скрытые каналы, основанные на сокрытии информации в структурированных данных;
* скрытые каналы, основанные на сокрытии информации в неструктурированных данных.

***Скрытые каналы, основанные на сокрытии информации в структурированных данных***, используют встраивание данных в информационные объекты с формально описанной структурой и формальными правилами обработки. Например, внутренний формат файлов, используемых современными текстовыми процессами, содержит ряд полей, не отображаемых при редактировании файла, поэтому они могут быть использованы для вставки скрытой информации.

***Скрытые каналы, основанные на сокрытии информации в неструктурированных данных***, используют встраивание данных в информационные объекты без учета формально описанной структуры (например, запись скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения).

**Скрытые каналы по времени** предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени. Например, в многозадачной операционной системе центральный процессор является разделяемым информационно вычислительным ресурсом для прикладных программ. Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные.

**Скрытый статистический канал** использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре скрытого канала. Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

**Скрытые каналы по пропускной способности** подразделяют на:

- канал с низкой пропускной способностью; - канал с высокой пропускной способностью.

***Скрытый канал является каналом с низкой пропускной способностью***, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

***Скрытый канал является каналом с высокой пропускной*** способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого данные информационные объекты являются ценными. Для решения сложных задач может использоваться комбинация скрытых каналов, опирающихся на различные механизмы передачи.

Таким образом, существуют следующие виды **каналов утечки информации** относят:

#  акустическое излучение информативного речевого сигнала;

* электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы контролируемой зоны (территория, здание, часть здания, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);
* виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
* несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
* воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
* хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
* побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
* наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны;
* радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах

(элементах) технических средств;

* радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации «закладок», модулированные информативным сигналом;
* радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

#  прослушивание ведущихся телефонных и радиопереговоров;

 просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств. На этом изложение первого учебного вопроса завершено.

**Второй учебный вопрос: «Физические процессы каналов утечки информации»**

Для принятия правильного решения по защите информации необходимо понимание физических процессов, создающих возможность утечки информации по рассмотренным в предыдущем вопросе каналам утечки информации.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве излучения, которые в той или иной степени связаны с обрабатываемой информацией и являются объектом для перехвата.

Правомерно предполагать, что образованию каналов утечки информации способствуют также определенные обстоятельства и причины технического характера (несовершенство схемных решений, эксплуатационный износ элементов изделия).

В любых технических средствах существуют те или иные физические преобразователи, которые выполняют соответствующие им функции, основанные на определенном физическом принципе действия. Однако помимо основных своих функций такие преобразователи в соответствии со своей физической природой способны порождать и дополнительные каналы утечки. Знание всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Входе изучения второго учебного вопроса мы рассмотрим физические процессы для типовых каналов утечки информации, это:

1. Акустические каналы утечки информации;
2. Вибрационные, каналы утечки информации;
3. Преобразователи информации:
   * преобразователи аудиоинформации;
   * индуктивные преобразователи. Микрофонный эффект;
   * пьезоэлектрический преобразователь;
   * оптические преобразователи;
4. Электромагнитные каналы утечки;
5. Визуально-оптические каналы утечки;
6. Информационные каналы утечки информации.

В соответствии с представленными типами каналов утечки информации, мы начнем с **акустических каналов утечки информации**.

Наиболее ценной акустической информацией чаще всего является речь. Частоты речевых сигналов 16 – 20 000 Гц.

Один и тот же звук разные люди произносят по-разному (своего рода речевой почерк). Звуки речи не одинаково информативны: гласные содержат мало информации о смысле речи, а глухие согласные наиболее информативны.

***Мерой силы звукового ощущения*** является громкость звука. Минимальная громкость соответствует порогу слышимости, максимальная – порогу болевого ощущения. Оба порога зависят от частоты звука. Человеческому уху свойственно изменение порога слышимости: в условиях тишины слышен писк комара, а в условиях шума трудно услышать громкую речь.

Качество речи оценивается ее разборчивостью, представляющей собой статистическую характеристику речи, принимаемой на фоне шумов. ***Разборчивость*** – это отношение числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу переданных по каналу элементов. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону. Разборчивость речи определяется экспериментально с помощью так называемых артикуляционных испытаний. Объективные измерительные и расчетные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. Формантами называются максимумы текущего спектра речи, которые заполняют весь речевой диапазон. Доказано, что восприятие человеком формант обладает свойством аддитивности, т. е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи. В акустических измерениях используются октавные или третьоктавные частотные полосы. Для октавного анализа вклады частот русской речи равны следующим значениям:

Частотная полоса, кГц – 0,25; 0,5; 1; 2; 4; 8.

Разборчивость формант, % – 6,7; 12,5; 21,2; 29,4; 25; 5,2.

От качественного приема (без искажений и помех) каждой частотной полосы зависит суммарная разборчивость. Предельное значение разборчивости формант, при которой возможно понимание смысла речевого сообщения, равно 15 %, что соответствует 25 %-й разборчивости слогов. Задача оценки канала утечки сводится к измерению или вычислению разборчивости речи и сравнению полученного значения с предельным.

Важным является то, какое качество принятого сигнала может обеспечить используемый канал. Для оценки *акустического канала* при работе с речевой информацией также применяется такая характеристика, как разборчивость речи. Она зависит от следующих факторов:

* ослабления речи в канале;
* реверберации звука (это процесс постепенного уменьшения интенсивности звука при его многократных отражениях);
* уровня вибрационных и акустических шумов в местах установки датчиков;
* чувствительности самих датчиков.

Оперативная оценка этих факторов осложняется тем, что вибрационные и акустические сигналы не поддаются точному расчету. Качество каналов съема оценивают экспериментальным путем с помощью акустических измерений, имитирующих ситуацию контроля информации, кроме компьютерной информации.

***Шумы и помехи***, возникающие в месте установки датчика, вызываются многочисленными естественными источниками: автомобильным транспортом, работой механических машин, технических средств в помещениях, разговорами в смежных помещениях и т. п. Характерная особенность шумов – их не стационарность, т. е. изменение уровня во времени. Эти изменения зависят от времени суток (вечером уровни шумов намного меньше, чем днем), от дня недели (в выходные дни уровни шумов снижаются), от погодных условий. Наибольшие шумы – уличные, которые создаются автомобильным транспортом, листвой (при наличии ветра), а также дворовые. В здании источниками шумов являются люди (разговоры, шаги), работа механизмов, водопровода, лифта. Средние значения акустических шумов на улице составляют 60...75 дБ и зависят от интенсивности движения автомашин в районе расположения объекта. Разница в уровне шумов от максимального до минимального может составлять до 30 дБ. Следует иметь в виду, что существующая норма допустимого уровня акустических шумов в рабочих помещениях равна 50 дБ. Этот уровень можно брать в качестве расчетного, если неизвестны конкретные показатели шумности в смежных посторонних помещениях. Все приведенные значения шумов даны для широкополосных источников помех, которые не различаются человеческим ухом, но маскируют акустическую информацию для шпионской аппаратуры.

Поэтому помехи предназначены для скрытия (маскировки) полезного акустического сигнала, распространяющегося в виде акустических колебаний. Маскирующие свойства помех проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона.

Таким образом, ***акустические колебания*** в помещении складываются из шумов источников, находящихся внутри помещения, и шумов источников вне помещения.

***Основные пути прохождения акустических волн из помещения***:

* воздушный перенос: прохождение через открытые окна, двери, щели, поры, вентиляционные воздуховоды;
* материальный перенос: прохождение через материал стены или по трубам отопления, газопровода, водопровода в виде продольных колебаний;
* мембранный перенос: передача колебаний посредством поперечных колебаний перегородки (стекла, стены и пр.).

При рассмотрении первого пути говорят об акустическом канале утечки, второй и третий образуют вибрационный канал.

В воздушных каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными мини передатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с телефонного аппарата.

Поэтому, создавая защиту от акустических каналов утечки информации, необходимо определить фактический уровень разговорной речи (аудио записи), уровень естественных шумов и рассчитать требуемый уровень маскирующих шумов и помех.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

Следующий тип каналов утечки информации – **вибрационные, или структурные, каналы утечки информации**. В данных каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т.

п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие обычно в ближнем инфракрасном диапазоне волн и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров (рис. 3).

Следующий тип каналов утечки информации – **преобразователи информации.**

***Преобразователи аудиоинформации***. Преобразователем является прибор, который преобразует изменения одной физической величины в изменения другой.

Акустическая энергия, возникающая при разговоре, может вызвать акустические (т. е. механические) колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению или изменению электромагнитного излучения.

*Любой преобразователь характеризуется определенными параметрами*. Наиболее важными из них являются:

* чувствительность – отношение изменения выходного сигнала к изменению сигнала на его входе;
* разрешающая способность – наибольшая точность, с которой осуществляется преобразование;
* линейность – равномерность изменения выходного сигнала в зависимости от входного;
* инертность (время отклика) – время установления выходного сигнала в ответ на изменение входного сигнала;
* рабочая полоса частот – частотный диапазон, в пределах которого воздействие на входе преобразователя создает на выходе допустимый уровень сигнала.

*По физической природе имеется значительное количество различных первичных преобразователей информации, среди которых выделяются следующие группы*:

* индуктивные;
* емкостные;
* пьезоэлектрические;
* оптические преобразователи.

Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

***Индуктивные преобразователи. Микрофонный эффект***. Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС (электродвижущая сила) индукции в такой катушке сводятся к следующему. Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению 70 ЭДС индукции на концах катушки. Она зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Данный эффект непосредственно используется в электродинамических микрофонах, поэтому получил название микрофонного эффекта.

Индуктивные преобразователи информации (рис. 4) подразделяются на:

* электромагнитные;
* электродинамические;

К *электромагнитным преобразователям* относятся такие устройства как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы.

Типичный образец индуктивного акустоэлектрического преобразователя – электромеханический вызывной звонок телефонного аппарата, микрофонный эффект которого проявляется при положенной телефонной трубке. По тому же принципу образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения. Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов.

В магнитоэлектрическом измерительном приборе имеются подвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения. Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции (рис. 5).

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит.

Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не применяется для конкретных измерений.

Примерами индукционных акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

***Трансформатор*** состоит из двух (или более) изолированных друг от друга катушек (обмоток) с разными числами витков и замкнутого сердечника из мягкой стали или феррита (рис. 6).

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в разы, соответствующие коэффициенту трансформации.

Трансформаторы обладают важным свойством – магнитострикцией.

*Магнитострикция* – изменение размеров и формы кристаллического тела при намагничивании – вызывается изменением энергетического состояния кристаллической решетки в магнитном поле и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико.

Обратное по отношению к магнитострикции явление – Виллариэффект, т. е. изменение намагничиваемости тела при его деформации.

Виллари-эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах способен преобразовывать механические колебания в электрические.

***Емкостные преобразователи***. Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

Емкость конденсатора зависит от расстояния между пластинами. Воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости (рис. 7).

Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что система пластин вдвигается в другую систему пластин, образуя конденсатор переменной емкости. Изменяющееся акустическое давление, воздействуя на такой конденсатор, изменяет его емкость, а, следовательно, и характеристики устройства, в котором он установлен.

***Пьезоэлектрический преобразователь***. Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии называется прямым пьезоэлектрическим эффектом. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. У пьезокристаллов наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле, зарядив металлические обкладки, то она поляризуется и деформируется, например, сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом (рис. 8).

Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах, генераторах электрического микрофона.

***Оптические преобразователи***. К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно (рис. 9).

Что касается технических каналов утечки информации, то в оптических системах опасным является акустооптический эффект. **Акустооптический эффект** – это явление преломления, отражения или рассеяния света, вызванное упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием звуковых колебаний. Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования – микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах).

Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки – создание лучших условий отражения на границе сердцевина-оболочка и защита от излучения в окружающее пространство (рис.10).

Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломления. В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации.

Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т. е. приводит к изменению интенсивности, причем пропорционально значению этого давления.

При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом осуществляется амплитудная модуляция излучения, проходящего по волокну, что способствует утечки информации.

Следующий тип канала утечки информации – **электромагнитные каналы утечки**.

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Вокруг проводника, по которому протекает ток I, вызванный напряжением U, создается магнитное поле с напряженностью H и электрическое поле с напряженностью Е.

Изменение во времени тока приводит к изменению во времени электрического и магнитного полей. Вызванные изменением тока в проводнике изменяющиеся во времени электрическое и магнитное поля представляют собой единое изменяющееся электромагнитное поле, распространяющееся в пространстве, свойства которого целиком и полностью описываются уравнениями Максвелла.

Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Поле делится на две зоны: ближнюю и дальнюю.

В дальней зоне (начиная от расстояний, больших 6λ от источника возмущения) электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами. Дальняя зона – это область пространства, в которой распространение от источника существенно превышает длину волны. Граница между дальней и ближней зонами находится на расстоянии около 0,5 м от источника излучения для частоты 100 МГц и 50 м для частоты 1 МГц.

В ближней зоне преобладает магнитная либо электрическая составляющая поля. Сильные магнитные поля, как правило, создаются цепями с низким волновым сопротивлением, большим током и малым перепадом напряжений.

Для поля с преобладающей электрической компонентой волновое сопротивление существенно больше, а для преобладающего магнитного поля – существенно меньше значения волнового сопротивления для плоской волны (Z = 377 Ом).

Изменение тока во времени может носить импульсный характер или подчиняться любому другому закону. Каждый такой процесс на основе известного из математики преобразования Фурье может быть представлен в виде суммы гармонических колебаний с различными амплитудами для каждой частоты, причем частоты изменяются в пределах от нуля до бесконечности. Зависимость амплитуд этих гармонических составляющих от частоты – это спектр сигнала (в рассматриваемом случае – электромагнитного излучения). Спектр характеризует распределение энергии в поле излучения. В зависимости от того, на каких частотах устройство излучает наиболее интенсивно, излучатели электромагнитных сигналов подразделяют на низкочастотные, высокочастотные и оптические.

*Низкочастотными излучателями* электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне этих устройств наиболее мощным выступает магнитное поле информативного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот.

К *группе высокочастотных излучателей относятся* ВЧ-

автогенераторы, модуляторы ВЧ-колебаний и устройства, генерирующие паразитные высокочастотные колебания по различным причинам и в различных условиях.

Источниками сигнала выступают ВЧ-генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы компьютеров, модуляторы ВЧ колебаний. Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации за счет нежелательной положительной обратной связи.

В качестве высокочастотного излучателя рассматривается любое устройство, содержащее элементы с нелинейными характеристиками (диоды, транзисторы, микросхемы), порождающими нежелательные составляющие высокочастотного характера.

Спектр излучения обычно не поддается аналитическому расчету, т. к.

его форма зависит от многих факторов; прежде всего это следующие:

* рабочие частоты устройства, их гармоники и комбинационные частоты;
* расположение и длина проводников;
* расположение и конструкция реактивных элементов (конденсаторов и индуктивных катушек);
* тип корпуса, наличие в нем щелей, отверстий и т. п.

При анализе спектра следует разделять информативное ПЭМИ и неинформативное ПЭМИ, а также реальные возможности восстановления информации из принятого ПЭМИ.

***Наиболее опасными являются следующие виды излучений и наводок***:

* электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, напряжение, частота или фаза которого изменяются по закону информационного сигнала);
* электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство);
* электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом);
* наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС);
* просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала);
* просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);
* съем информации с использованием закладных устройств, представляющих собой минипередатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны.

Особое внимание следует обратить на перехват информации при ее передаче по каналам связи. Это вызвано тем, что в данном случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам, особенно в случае использования радиоканала. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств.

***Электромагнитный канал перехвата информации*** широко применяется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

***Электрический канал перехвата информации***, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям.

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи.

Следующий тип каналов утечки информации – **визуально-оптические каналы утечки**.

В последнее время стало уделяться большое внимание утечке визуальной информации, получаемой в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п.

Для документирования результатов наблюдения проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

Следующий тип каналов утечки информации – **информационные каналы утечки информации**.

Информационный канал может быть разделен на следующие каналы:

* канал коммутируемых линий связи;
* канал выделенных линий связи;
* канал локальной сети;
* канал машинных носителей информации;
* канал терминальных и периферийных устройств.

Утечка информации из канала связи при использовании специальных технических средств съема информации была рассмотрена выше.

В последнее время наиболее динамично развиваются методы съема компьютерной информации. В этом направлении используются:

* аппаратные закладки; • вредоносные программы.

Основные возможности несанкционированного доступа связаны с использованием специального математического обеспечения, включающего в себя такие составляющие, как компьютерные вирусы, «логические бомбы», «троянские кони», программные закладки и т. п.

***Вредоносная программа*** – программа, предназначенная для несанкционированного копирования, модификации, блокирования, уничтожения компьютерной информации.

Часто вредоносная программа доставляется к месту постоянного размещения через привлекательную для пользователя программу («троянскую» программу). То есть для «троянской» программы характерно наличие встроенной структуры или функции, скрытно выполняющей вредоносные действия. При запуске или на этапе инсталяции параллельно идут два процесса: документированный и недокументированный.

Вредоносные программы можно разделить на две большие категории:

1. вирусы. Основные свойства вирусов: паразитическое существование, размещение внутри программного файла или в другом месте, способность к саморазмножению – копированию, выраженные деструктивные функции. Основная угроза со стороны вирусов – угроза целостности;
2. программные закладки. Основные свойства: скрытность работы на всех этапах жизненного цикла, явно выраженные «шпионские» функции, частое отсутствие механизма саморазмножения, хотя возможно наличие механизма самоликвидации.

В настоящее время известно большое количество программных закладок, основные функции которых следующие:

* слежение за пользователем;
* раскрытие паролей, ключей;
* изучение обрабатываемой информации.

Вредоносные программы могут быть внедрены в прикладные программы, утилиты и сервисные программы, подсистему безопасности, реестр, ядро, командный интерпретатор, BIOS, драйверы устройств, аппаратные средства. ВП, внедренные на уровень ядра и ниже, невидимы для пользователя. На этом изложение второго учебного вопроса завершено.

**Основы системы информационной безопасности**

**Первый учебный вопрос: «Понятие концепции и политики информационной безопасности»**

Защита информационных активов посредством определения, достижения, поддержания и улучшения информационной безопасности очень важна для того, чтобы позволить организации достигать своей цели, а также поддерживать и повышать уровень соответствия законодательству и репутации. Эти скоординированные действия, направляющие реализацию подходящих средств управления и рассматривающие недопустимые риски информационной безопасности, являются общеизвестными как элементы менеджмента информационной безопасности.

Инструменты и механизмы информационной безопасности включают в себя процессы и процедуры ограничения и разграничения доступа, информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); использование методов надежного хранения, преобразования и передачи информации; нормативно административное побуждение и принуждение.

В соответствии с **ГОСТ 27002-2012** «Методы и средства обеспечения безопасности»:

**Информационная безопасность организации** – это состояние защищенности интересов организации в условиях угроз в информационной сфере.

***Защищенность*** достигается обеспечением совокупности свойств информационной безопасности – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации.

Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

При этом **цель информационной безопасности (организации)** рассматривается как заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).

***Результатом обеспечения ИБ*** может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Для нормативно-правового обеспечения ИБ организации создается система документов по ИБ.

**Система документов по информационной безопасности в организации** – это объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

Товарищи студенты, основополагающим документом по информационной безопасности организации (предприятия) является Концепция информационной безопасности. Рассмотрим содержание данного документа.

**Концепция информационной безопасности** организации (предприятия) представляет собой документ, в котором определены:

* основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с

определением стоимости ресурсов и степени их критичности для предприятия;

* основные принципы защиты, определяющие стратегию обеспечения информационной безопасности и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности предприятия;
* модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования;
* модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;
* требования безопасности, определяемые по результатам анализа рисков;
* меры обеспечения безопасности организационного и программнотехнического уровня, предпринимаемые для реализации перечисленных требований;
* ответственность сотрудников предприятия за соблюдение установленных требований информационной безопасности при эксплуатации информационной системы предприятия.

При этом необходимо учитывать, что риски и эффективность средств управления информационной безопасности меняются в зависимости от складывающихся обстоятельств, поэтому каждая организация обязана выполнять следующие обязанности:

* контролировать и оценивать эффективность имеющихся средств управления и процедур информационной безопасности;
* идентифицировать появляющиеся риски для их рассмотрения;
* выбирать, реализовывать и улучшать должным образом соответствующие меры и средства контроля и управления информационной безопасности.

Товарищи студенты! В соответствии с изученным ранее материалом, системы защиты информации могут рассматриваться по различным уровням, например, система защиты информации государства, отрасли, ведомства, организации или личности. Но система защиты информации для любого уровня определяется «Политикой безопасности информации».

При этом каждая ***организация должна установить свою политику и цели для системы информационной безопасности***. Данная политика необходима, чтобы установить взаимосвязь между всеми элементами системы информационной безопасности и скоординировать все процессы, протекающие в ней, что в свою очередь позволит эффективно достигать цели информационной безопасности организации при использовании системы менеджмента. А т.к. вы будете специалистами по направлению «Информационная безопасность организации», то далее мы будем рассматривать понятие «Политика безопасности информации (в организации)».

Политика безопасности организации может состоять из принципов безопасности и директив для организации в целом. Она должна отражать более широкий круг аспектов политики организации, включая аспекты, которые касаются прав личности, законодательных требований и стандартов.

Политика информационной безопасности может содержать принципы и директивы, специфичные для защиты конфиденциальной, ценной или иной важной для организации информации. Содержащиеся в ней принципы строятся на основе принципов политики безопасности и, таким образом, согласованы с ними.

При разработке и проведении Политики информационной безопасности в жизнь целесообразно руководствоваться следующими принципами:

* невозможность миновать защитные средства;
* усиление самого слабого звена;
* невозможность перехода в небезопасное состояние;
* минимизация привилегий;
* разделение обязанностей;
* эшелонированность обороны;
* разнообразие защитных средств;
* простота и управляемость информационной системы;
* обеспечение всеобщей поддержки мер безопасности;
* адекватность (разумная достаточность);
* системность;
* прозрачность для легальных пользователей; - равностойкость звеньев.

Кратко рассмотрим суть некоторых принципов.

***Принцип невозможности перехода в небезопасное состояние*** означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если механизм турникета ломается, турникет должен оставаться в закрытом состоянии, препятствуя проходу людей.

***Принцип минимизации привилегий*** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

***Принцип разделения обязанностей*** предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

***Принцип эшелонированности обороны*** предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

***Принцип разнообразия защитных средств*** рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен ***принцип простоты и управляемости информационной системы*** в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

***Принцип всеобщей поддержки мер безопасности*** носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

***Принцип адекватности*** (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Вряд ли руководитель потратит деньги на металлическую дверь, суперзамок и сигнализацию, если в помещении нет конфиденциальной информации.

***Системность***. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забывать о важности системного подхода. Он состоит в том, что система защиты должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств.

***Прозрачность для легальных пользователей***. Можно заставлять пользователей перед каждой операцией для надежной идентификации вводить 10-значный пароль, прикладывать палец к сканеру и произносить кодовую фразу. Но необходимо учитывать, что это будет затруднять доступ пользователей к информации, поэтому необходимо создавать рациональные способы доступа.

***Равностойкость звеньев***. Звенья – это элементы защиты, преодоление любого из которых означает преодоление всей защиты (например, окно и дверь в равной степени открывают злоумышленнику путь в защищаемое помещение). Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае прочность защиты (или ее уровня) определяется прочностью самого слабого звена.

Таким образом, в соответствии с рассматриваемым **ГОСТ 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»:

**Политика информационной безопасности организации** – формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

***Правила информационной безопасности включают***:

* физическую безопасность объекта. Т.е., охрана территории предприятия должна регулироваться общими правилами. Также доступ на объект рекомендуется контролировать, чтобы избежать риска проникновения злоумышленника;
* безопасность персонала. Сюда относят обеспечение надлежащих условий труда, распределение сотрудников по отделам с конкретными рабочими задачами, в том числе и по информационной безопасности;
* административную и сетевую безопасность – это правила разграничения доступа к данным и практическая реализация алгоритмов защиты локальных сетей предприятия.

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности.

**Политики информационной безопасности должны содержать**:

* предмет, основные цели и задачи политики безопасности;
* условия применения политики безопасности и возможные ограничения;
* описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
* права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;
* порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в актуальной, доступной и понятной форме.

В соответствии с ранее рассматриваемым **ГОСТ 27002** «Методы и средства обеспечения безопасности»:

**Цель Политики информационной безопасности** – обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами, и нормами.

Высшее руководство организации должно установить четкое направление Политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках организации.

***Цели Политики информационной* *безопасности относятся к одной или нескольким из следующих категорий***:

* защита ресурсов;
* аутентификация;
* авторизация; - целостность; - конфиденциальность; - аудит безопасности.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники.

Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

**Основными задачами Политики информационной безопасности являются**:

* разработка требований по обеспечению информационной безопасности;
* контроль выполнения установленных требований по обеспечению информационной безопасности;
* повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
* разработка нормативных документов для обеспечения информационной безопасности организации;
* выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности организации;
* организация антивирусной защиты информационных ресурсов

организации;

* защита информации организации от несанкционированного доступа и утечки по техническим каналам связи;
* организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководителю организации.

Таким образом, мы рассмотрели *предмет, основные цели и задачи политики безопасности*. Далее рассмотрим *условия применения политики безопасности и возможные ограничения*.

Выяснение того, что, от кого и от чего мы будем защищать - большой шаг на пути к ответу на главный вопрос: как защищать?

Итак, следует определить политику применительно к различным элементам защиты:

***Политика управления паролями*** (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований. Политика на этом уровне также может устанавливать запрет хранения записанных паролей, запрет сообщать кому-либо свой пароль (в том числе руководителям и администраторам информационных систем) и другие аналогичные ограничения. ***Политика установки и обновления версий программного обеспечения*** не является внутриорганизационной политикой безопасности, но фактически должна либо напрямую использоваться государственными учреждениями и предприятиями, имеющими доступ к информации, составляющей государственную тайну РФ, как политика безопасности, либо ее положения должны быть прямо перенесены во внутренние политики информационной безопасности таких учреждений и предприятий.

***Политика приобретения информационных систем и их элементов*** (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

***Политика доступа сторонних пользователей (организаций)*** в информационные системы предприятия может содержать перечень основных ситуаций возможности доступа, критериев и процедур его осуществления, распределение ответственности сотрудников компании.

***Политика в отношении разработки программного обеспечения*** может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств сторонним специализированным организациям, а также в отношении приобретения и использования тиражируемых программных библиотек компаний производителей.

***Политики использования отдельных универсальных информационных технологий*** в масштабе всего предприятия могут включать в себя политику использования электронной почты (e-mail); политику использования средств шифрования данных; политику защиты от компьютерных вирусов и других вредоносных программ; политику использования модемов и других аналогичных коммуникационных средств; политику использования Инфраструктуры публичных ключей; политику использования технологии Виртуальных частных сетей (VirtualPrivateNetwork- VPN).

***Политика использования электронной почты*** может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.

***Политика использования коммуникационных средств*** может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами. Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.).

Политика информационной безопасности может составлять часть документа по общей Политике безопасности организации. Если Политика информационной безопасности распространяется за пределами организации, следует принимать меры в отношении неразглашения конфиденциальной информации.

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики информационной безопасности. Пересмотр Политики информационной безопасности заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к менеджменту информационной безопасности в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре Политики информационной безопасности следует учитывать результаты пересмотров методов управления. Для этого должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

***Входные данные для пересмотра Политики информационной безопасности*** должны включать информацию:

* об ответной реакции заинтересованных сторон;
* о результатах независимых пересмотров;
* о состоянии предотвращающих и корректирующих действий; - о результатах предыдущих пересмотров методов управления;
* о выполнении процесса и соответствии политике информационной безопасности;
* об изменениях, которые могли бы повлиять на подход организации к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств бизнеса, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;
* о тенденциях в отношении угроз и уязвимостей;
* о доведенных до сведения инцидентах информационной безопасности; - о рекомендациях, данных соответствующими органами.

***Выходные данные пересмотра*** Политики информационной безопасности должны включать любые решения и действия относительно:

* улучшения подхода организации к менеджменту информационной безопасности и ее процессов;
* улучшения мер и средств контроля и управления, и целей их применения; - улучшения распределения ресурсов и(или) обязанностей.

Пересмотренная Политика должна быть утверждена руководством. **Соответствие Политикам безопасности и стандартам, техническое соответствие**.

***Цель проведения соответствия:*** обеспечить уверенность в соответствии систем политикам безопасности организации и стандартам.

Безопасность информационных систем необходимо регулярно пересматривать.

Такие пересмотры необходимо осуществлять по отношению к соответствующим политикам безопасности, а технические платформы и информационные системы должны подвергаться проверке на предмет соответствия применимым стандартам безопасности и документированным мерам, и средствам контроля и управления безопасности.

Руководители должны обеспечить уверенность в том, что все процедуры безопасности в пределах их зоны ответственности выполняются правильно, для того чтобы достичь соответствия политикам и стандартам безопасности.

Руководители должны регулярно анализировать соответствие обработки информации в пределах их зоны ответственности политикам и стандартам безопасности, а также любым другим требованиям безопасности.

Если в результате проведения анализа было ***выявлено какое-либо несоответствие***, руководителям следует:

* определить причины несоответствия;
* оценить необходимость действий с целью обеспечения уверенности в том, что несоответствие не повторится;
* определить и реализовать соответствующее корректирующее действие; - проанализировать предпринятое корректирующее действие.

Результаты анализа и корректирующих действий, предпринятых руководителями, необходимо регистрировать, и эти записи следует сохранять для аудита информационной безопасности. Руководители должны сообщать результаты лицам, проводящим независимые проверки, если такая независимая проверка имела место в зоне их ответственности.

На этом изложение первого учебного вопроса завершено.

**Второй учебный вопрос: «Цель и задачи системы информационной безопасности»**

Проблемы информационной безопасности уже более 30 лет находятся в центре внимания специалистов и, можно считать, что за это время были достигнуты следующие результаты:

* проблема информационной безопасности получила всеобщее признание;
* созданы методологические основы информационной безопасности;
* налажено производство средств информационной безопасности;
* организована система подготовки и повышения квалификации специалистов в области информационной безопасности;
* создана государственная система информационной безопасности;
* накоплен богатый опыт практического решения задач защиты информации в системах различного масштаба и назначения.

Приведенное выше, дает основание утверждать, что проблема информационной безопасности имеет определенный базис для дальнейшего целенаправленного развития.

Адекватная защита информационных ресурсов объекта является сегодня обязательным требованием бизнеса. Методы атак на информационные и коммуникационные системы постоянно совершенствуются. С ростом значимости информационных технологий для бизнеса, преступления, связанные с нарушением требований информационной безопасности, все чаще носят направленный характер и совершаются из корыстных побуждений, зачастую, организованными группами лиц.

Товарищи студенты, основой безопасности любой организации является комплексная безопасность.

***Комплексная безопасность*** – система взглядов и практических действий, направленных на создание и поддержание таких условий, которые обеспечивают деятельность всего комплекса мер безопасности, направленных на достижение целей его функционирования.

***Система комплексной*** *безопасности* включает в себя следующие составляющие подсистемы:

* правовую безопасность; - кадровую безопасность;
* финансовую безопасность;
* инженерно-техническую безопасность;
* экономическую безопасность;
* ***информационную безопасность*;** - и другие.

Темпы развития информационных технологий и появления новых продуктов и технологий, а также их специфика должны быть учтены средствами и системами защиты IT-ресурсов. Таким образом, усложнение информационных технологий в целом, сопровождается возрастающей степенью зависимости бизнеса от их применения.

В связи с этим, процесс обеспечения информационной безопасности становится непрерывным, а применяемые меры должны носить комплексный характер.

Для решения этих задач в организации (предприятии) создается система информационной безопасности.

Данная система информационной безопасности представляет модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов для достижения деловых целей, основанную на оценке риска и на принятии уровней риска организации, разработанную для эффективного рассмотрения и управления рисками.

Анализ требований для защиты информационных активов и применение соответствующих средств управления, чтобы обеспечить необходимую защиту этих информационных активов, способствует успешной реализации системы информационной безопасности.

Следующие основные **принципы** способствуют созданию **системы информационной безопасности**:

* понимание необходимости создания системы информационной безопасности всеми должностными лицами;
* назначение ответственности за информационную безопасность;
* соединение административных обязанностей и интересов

заинтересованных лиц;

* возрастание социальных ценностей;
* оценка риска, определяющая соответствующие меры и средства контроля и управления для достижения допустимых уровней риска;
* безопасность это неотъемлемый, важный элемент информационных сетей и систем;
* активное предупреждение и выявление инцидентов информационной безопасности;
* обеспечение комплексного подхода к менеджменту информационной безопасности;
* непрерывная переоценка и соответствующая модификация системы информационной безопасности.

**Роль системы информационной безопасности в организации** заключается в совокупности определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

К субъектам относятся лица из числа руководителей организации, ее персонал или инициируемые от их имени процессы по выполнению действий над объектами.

Объектами могут быть техническое, программное, программнотехническое средство, информационный ресурс, над которыми выполняются действия.

Товарищи студенты, на предыдущих занятиях было акцентировано ваше внимание на то, что основными документами, определяющим требования к информационной безопасности для бизнеса являются ГОСТы Р ИСО/МЭК 27001 – 27008.

**Требования**, предъявляемые **к системе информационной безопасности**, структурированы и сгруппированы по нескольким направлениям.

1. Группа требований, обусловленных характером информации, циркулирующей в информационной системе объекта. К ним относятся:

* степени конфиденциальности информации;
* объемы информации, циркулирующей в информационной системе; - интенсивность обработки информации.

2. Группа требований, обусловленных архитектурой информационной системы объекта. К ним можно отнести:

* пространственные размеры информационной системы;
* территориальную распределённость информационной системы; - структурированность компонентов информационной системы.

3. Группа требований, обусловленных условиями функционирования информационной системы объекта. К ним отнесем:

* расположение информационной инфраструктуры системы на территории объекта;
* степень обустроенности информационной инфраструктуры; - развитость информационных коммуникаций.

4. Группа требований, обусловленных технологией обработки информации в системе. К ним будем относить:

* масштабируемость системы;
* стабильность функционирования;
* доступность технологических решений;
* структурированность технологии обработки информации в системе.

5. Группа требований, обусловленных организацией функционирования информационной системы объекта. К ним можно отнести:

* общую организацию функционирования системы;
* степень и качество укомплектованности кадрами;
* уровень подготовки и мотивации кадров;
* уровень производственной (технологической) дисциплины.

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

**Система информационной безопасности** – это функциональная подсистема системы комплексной безопасности объекта, объединяющая силы, средства и объекты защиты информации, организованные и функционирующие по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации.

**Целью** **системы информационной безопасности** является создание таких условий функционирования информационной системы объекта, при которых обеспечивается выполнение требований по конфиденциальности, доступности и целостности информации, принадлежащей ему.

При этом, **информационная безопасность бизнеса** – это свойство информации сохранять конфиденциальность, целостность и доступность.

В соответствии с целью СИБ, формируются требования к основным характеристикам информации, составляющим сущность ее безопасности в качестве некоторых свойств или условий функционирования информационной системы объекта, определенных **Федеральным законом** **№ 149** «Об информации, информационных технологиях и о защите информации».

В соответствии с требованиями к безопасности информации сформулируем **задачи СИБ**. К таковым можно отнести:

1. Предупреждение появления угроз информационной безопасности.

Реализация этой задачи носит упреждающий характер и должна способствовать такому построению, которое обеспечивает полную невозможность (в идеале) или минимальную возможность появления дестабилизирующих факторов в различных условиях ее функционирования.

1. Обнаружение появившихся угроз и предупреждение их воздействия на информационную систему объекта.

Данная задача решается осуществлением комплекса мероприятий, в результате проведения которых появившиеся угрозы должны быть обнаружены до момента их воздействия на информационную систему и, непосредственно, на информацию, а также должно быть обеспечено недопущение воздействия угроз в условиях их появления и обнаружения.

1. Обнаружение воздействия угроз на информационную систему объекта и локализация этого воздействия.

Решение данной задачи заключается в непрерывном контроле средств, комплексов, систем обработки, хранения и защиты информации с целью своевременного обнаружения фактов воздействия на них угроз.

1. Ликвидация последствий воздействия угроз на информационную систему объекта.

Данная задача решается путем восстановления конфиденциальности, целостности и доступности активов организации, подвергнувшихся угрозам. Анализ причин совершения угроз и принятие мер по недопущению подобных инцидентов информационной безопасности впредь.

Для примера рассмотрим вариант с двумя акустическими закладками – активной (имеющей собственное энергетическое поле) и пассивной (не имеющей собственное энергетическое поле), которые заложены в зале для совещаний.

При выполнении 1 задачи определяются угрозы для зала совещаний и принимаются меры по защите информации. При выполнении 2 задачи обследуется зал и обнаруживается активная закладка. В ходе совещания выполняется 3 задача и, например, обнаруживается пассивная закладка, которая уничтожается или блокируется. При выполнении 4 задачи для обеих закладок проводится разбирательство по факту их установки, и определяются меры по недопущению подобных инцидентов впредь и оценивается ущерб организации.

(**Слайд № 23**). Проведем детальный анализ создаваемой системы информационной безопасности (рис.1).



Рис.1. Укрупненная структура СИБ

Под ***силами*** ***системы информационной безопасности*** будем понимать совокупность органов и (или) исполнителей работ, связанных с защитой информации в интересах данного объекта. Следовательно, под силами СИБ подразумевается существование некоторого структурного подразделения, выполняющего задачи управления функционированием данной системы. Характер и масштабы сил СИБ будут зависеть от масштаба объекта, характера и степени конфиденциальности имеющейся информации, а также от объема затрат на выполнение указанных задач. Более детально анализ сил информационной безопасности объекта будет проведен в ходе следующих занятий. Но главным органом системы информационной безопасности является **служба информационной безопасности** организации – организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации.

***Средства*** ***системы информационной безопасности*** – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты информационных ресурсов объекта от внутренних и внешних воздействий.

Под ***объектами системы информационной безопасности*** будем понимать *информационные ресурсы,* т.е. любые виды активов информационной системы объекта: структурированная и неструктурированная информация, документы, вычислительная техника, коммуникационное и сетевое оборудование, оргтехника и др., относящиеся к конфиденциальной информации.

***Система обеспечения информационной безопасности*** будет рассмотрена на следующем занятии.

Необходимо отметить, что для успешного внедрения системы информационной безопасности в организации решающими факторами зачастую являются следующие:

* соответствие целей, политик и процедур информационной безопасности целям бизнеса;
* подход и основы для внедрения, поддержки, мониторинга и улучшения информационной безопасности, которые согласуются с корпоративной культурой;
* видимая поддержка и обязательства со стороны руководства всех уровней;
* четкое понимание требований информационной безопасности, оценки рисков и менеджмента рисков;
* эффективный маркетинг информационной безопасности среди всех руководителей, сотрудников и других сторон для достижения осведомленности;
* распространение руководящих указаний политики информационной безопасности и соответствующих стандартов среди всех руководителей, сотрудников и других сторон;
* обеспечение финансирования деятельностей по менеджменту информационной безопасности;
* обеспечение соответствующей осведомленности, обучения и тренинга;
* создание эффективного процесса менеджмента инцидентов информационной безопасности;
* внедрение системы измерений, используемых для оценивания, эффективности менеджмента информационной безопасности и предложений по ее улучшению.

При этом информационная безопасность неразрывно связана с ее нарушениями, и вы также должны понимать значение этого понятия.

**Нарушение информационной безопасности организации** – это случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

На предыдущих занятиях мы рассматривали компьютерные инциденты. Но кроме этого, существуют **инциденты информационной безопасности** – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность организации.

**Инцидентами информационной безопасности** являются:

* утрата услуг, оборудования или устройств;
* системные сбои или перегрузки;
* ошибки пользователей;
* несоблюдение политики или рекомендаций по ИБ;
* нарушение физических мер защиты;
* неконтролируемые изменения систем;
* сбои программного обеспечения и отказы технических средств; - нарушение правил доступа (ГОСТ Р ИСО/МЭК 27001-2006, пункт 3.6). На этом изложение второго учебного вопроса завершено.

**Третий учебный вопрос: «Применение системного подхода к созданию системы информационной безопасности»**

Исходя из основных положений системного анализа, будем рассматривать обозначенную систему информационной безопасности, как функционирование сложной системы в совокупности со всесторонним ее обеспечением.

Оценка соответствия системы информационной безопасности организации установленным требованиям – это деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований информационной безопасности.

Особенностью системного подхода к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы.

Системный подход к созданию системы информационной безопасности базируется на следующих методологических принципах:

* конечной цели - абсолютного приоритета конечной (глобальной) цели;
* единства - совместного рассмотрения системы как целого и как совокупности частей (элементов);
* связности - рассмотрения любой части системы совместно с ее связями с окружением;
* модульного построения - выделения модулей в системе и рассмотрения ее как совокупности модулей;
* иерархии - введения иерархии частей (элементов) и их ранжирования;
* функциональности - совместного рассмотрения структуры и функции с приоритетом функции над структурой;
* развития - учета изменяемости системы, ее способности к развитию, расширению, замене частей, накапливанию информации;
* децентрализации - сочетания в принимаемых решениях и управлении централизации и децентрализации;
* неопределенности - учета неопределенностей и случайностей в системе.

В качестве системного подхода к реализации работ по созданию системы информационной безопасности приведем положения американской концепции системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security), которая строится на 7 этапах реализации.

Первый этап (анализ объекта защиты) состоит в определении того, что нужно защищать и проводится по следующим направлениям:

* какая информация нуждается в защите;
* наиболее важные элементы (критические) защищаемой информации;
* срок жизни критической информации (время, необходимое конкуренту для реализации добытых сведений);
* определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;
* классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материальнотехнического обеспечения производства, подразделения управления и т.д.).

Второй этап заключается в выявлении угроз. Он происходит по следующим направлениям:

* определяется, кого может заинтересовать защищаемая информация;
* оцениваются методы, используемые конкурентами для получения этой информации;
* оцениваются вероятные каналы утечки информации;
* разрабатывается система мероприятий по пресечению действий конкурента.

Третий этап заключается в анализе эффективности принятых и постоянно действующих подсистем безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.).

На четвертом этапе проводится определение необходимых мер защиты. На основе проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

Пятый этап включает рассмотрение руководителями фирмы (организации) представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.

На шестом этапе осуществляется реализация принятых дополнительных мер безопасности с учетом установленных приоритетов.

На седьмом этапе осуществляется контроль и доведение до персонала фирмы реализуемых мер безопасности.

Более наглядно данный подход отобразить схемой (рис. 2), из которой видно, что данный процесс является циклическим.

Рассматриваемый метод требует серьезной аналитической работы, проводимой аналитической группой по следующим основным направлениям:

* информация о рынке и конкурентном окружении;
* информация о производстве и продукции;
* информация об организационных особенностях предприятия и его финансах.

Известно, что основополагающим принципом создания различных систем безопасности является принцип равно прочности, который предполагает сбалансированность уровней защищенности информационной системы объекта, которые вносят все составляющие системы информационной безопасности организации. Следовательно, говорить о серьезной защите информации в информационной системе объекта возможно только в том случае, когда будет обеспечено комплексное применение всех мер и средств ее защиты.

**Выявлени**

**е**

**угроз ИБ**

**Контроль и**

**доведение до**

**персонала**

**реализуемых**

**мер**

**Что подлежит**

**защите?**

**Реализация**

**принятых**

**дополнительны**

**х мер защиты**

**Рассмотрение**

**руководством**

**предложений**

**по мерам**

**защиты**

**Определение**

**необходимых**

**мер**

**защиты**

**Анализ**

**эффективности**

**принятых мер**

**защиты**

**Циклический**

**характер**

**работы**

Рис.2. Концепция системного подхода к созданию защиты конфиденциальной информации (OPSEC Operation Security),

На этом изложение второго учебного вопроса завершено.

**Управление системой информационной безопасности**

**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 270022012, 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:

1. защита данных и конфиденциальность персональных данных;
2. защита документов организации;
3. права на интеллектуальную собственность.

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

1. документирование политики информационной безопасности;
2. распределение обязанностей по обеспечению информационной

безопасности;

1. осведомленность, обучение и тренинг в области информационной

безопасности;

1. корректирующая обработка в прикладных программах;
2. менеджмент технических уязвимостей;
3. менеджмент непрерывности бизнеса;
4. 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:

1. 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;
2. 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, нормативноправовые 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;

1. 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;

1. 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;
2. 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;
3. 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;

1. 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 нормативноправовые требования и договорные обязательства;
2. получить утверждение руководством предполагаемых остаточных

рисков;

1. получить разрешение руководства на внедрение и эксплуатацию

СМИБ;

1. 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:

1. разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ;
2. реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;
3. внедрить меры управления для достижения целей управления;
4. 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;
5. реализовать программы по обучению и повышению квалификации

сотрудников;

1. управлять работой СМИБ;
2. управлять ресурсами СМИБ;
3. 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:

1. 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;

1. 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;
2. измерять результативность мер управления для проверки

соответствия требованиям ИБ;

1. 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 нормативноправовых требований, требований договорных обязательств, а также изменения в социальной структуре общества;

е) 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;

1. регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;
2. обновлять планы ИБ с учетом результатов анализа и мониторинга;
3. 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.

1. 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.

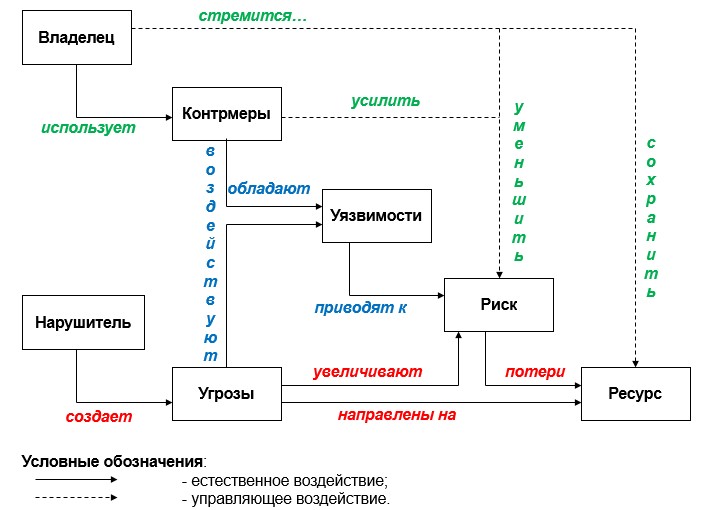
***Руководителям верхнего звена*** это поможет объективно и независимо оценить текущей уровень информационной безопасности организации, обеспечить формирование единой концепции безопасности, рассчитать, согласовать и обосновать необходимые затраты на защиту компании.

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).

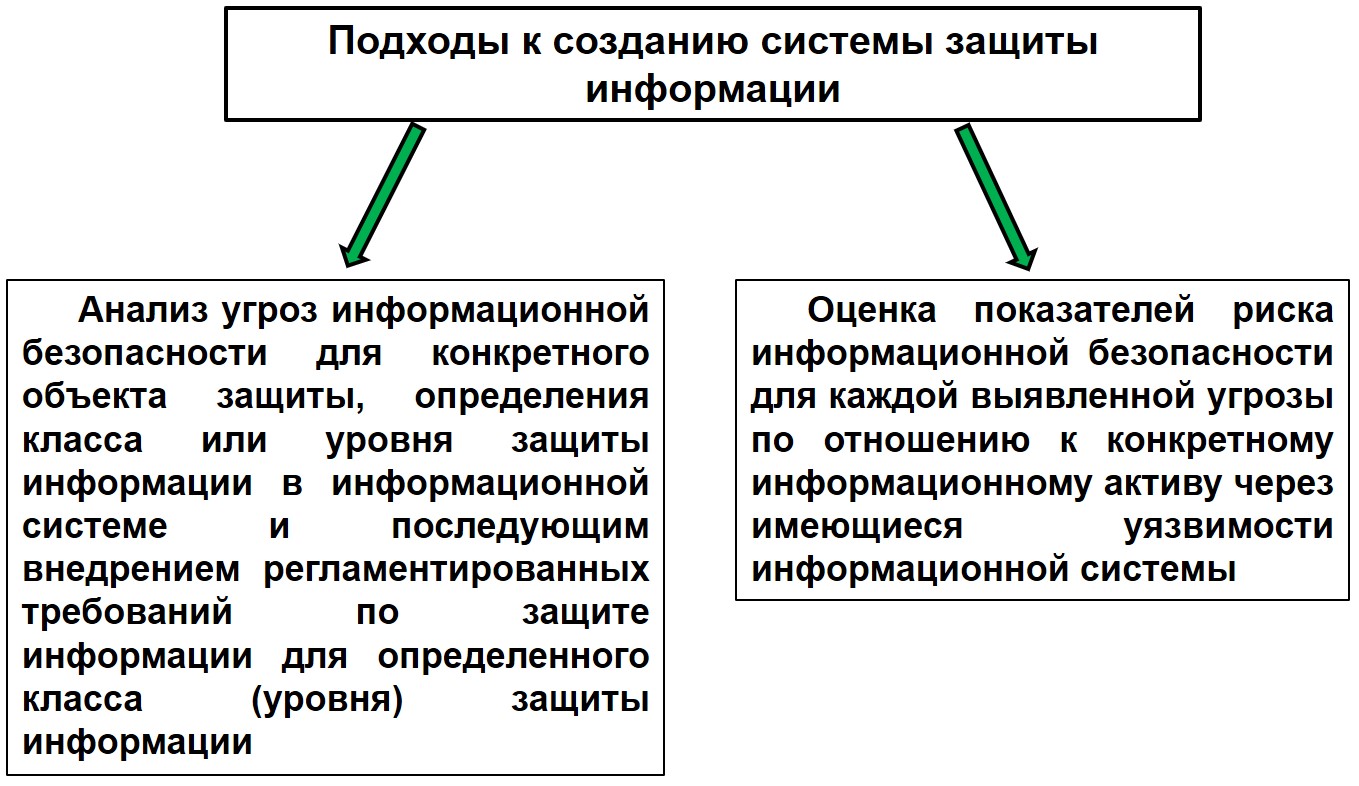


Рисунок 2 – Основные подходы к созданию системы защиты информации

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.

C 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*** (Rиб) определим, как функцию трех переменных: вероятности существования угрозы информационной безопасности организации (Pу), вероятности существования незащищённости (уязвимости) информационной системы организации (Pнз), и вероятности потенциального воздействия на информационную систему организации (Pвоз).

Rиб = F(Pу; Pнз; Pвоз) (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.

Rиб = Pу х Pнз х Pвоз (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 Rиб, 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 = Rиб х Цпот, (3)

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

Цпот – 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.

**Основы системы обеспечения информационной безопасности**

# Вводная часть

В ходе данного занятия будет рассмотрено понятие «системы обеспечения информационной безопасности» и ее содержание.

**Актуальность** данного занятия определена растущим уровнем угроз, рисков для предприятий и организаций любого типа, что приводит к необходимости искать современные методы защиты информации, позволяющие системно решить задачу обеспечения информационной безопасности.

С конца 2018 года Правительством Российской Федерации разрабатывается Концепция суверенного Рунета, внедрение которой способно существенно повысить уровень защиты информации. Эта тема привлекает повышенное внимание экспертного сообщества.

Кроме этого, обеспечение безопасности информации требует вложения серьезных финансовых ресурсов. Если компания может позволить себе соизмерять потенциальные расходы, связанные с внедрением современных информационных технологий, с ущербом, который может быть причинен утечкой информации, то государство обязано обеспечить максимально возможную степень защиты. Реализация концепции национального Рунета, импортозамещение в области производства электронной техники и разработки программного обеспечения должны решить задачу обеспечения информационной безопасности в стране.

Поэтому совершенствование системы обеспечения информационной безопасности на предприятиях, фирмах и организациях очень важно в современном мире.

В ходе занятия будет рассмотрен следующий учебный вопрос:

1. Основы системы обеспечения информационной безопасности на предприятии (в организации).

**Первый учебный вопрос: «Основы системы обеспечения информационной безопасности на предприятии (в организации)»**

В соответствии с Доктриной информационной безопасности Российской Федерации (утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

**Организационную основу системы обеспечения информационной безопасности** составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания

Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

**Участниками системы обеспечения информационной безопасности** являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежнокредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих **принципах**:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

**Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности** являются:

а) обеспечение защиты прав и законных интересов граждан и

организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных

направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса

мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного,

контрразведывательного, научно-технического, информационно-

аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

**Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности** являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-

технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

В соответствии с ранее изучаемым **ГОСТ 53114** «Обеспечение информационной безопасности в организации»:

**Обеспечение информационной безопасности организации** – это деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

**Мероприятия обеспечения** **информационной безопасности** – это совокупность действий, направленных на разработку и (или) практическое применение способов и средств обеспечения информационной безопасности. **Критерий обеспечения информационной безопасности организации** – это показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.

**Эффективность обеспечения информационной безопасности** – это связь между достигнутым результатом и использованными ресурсами для обеспечения заданного уровня информационной безопасности.

Рассмотрим методологию системы обеспечения информационной безопасности.

На предыдущем занятии мы рассмотрели схему информационной безопасности, которая содержит объекты информационной безопасности, силы информационной безопасности и средства информационной безопасности. Кроме этого, для эффективной работы системы информационной безопасности создается система обеспечения информационной безопасности, функционал которой направлен на обеспечение сил и средств информационной безопасности, которые в свою очередь будут обеспечивать надежную защиту конфиденциальной информации (рис. 1).



Рисунок 1 – Система информационной безопасности

В соответствии со схемой, **систему обеспечения информационной безопасности рассмотрим по двум направлениям**:

* обеспечение сил информационной безопасности; - обеспечение средств информационной безопасности.

Итак, первое направление – **обеспечение сил информационной безопасности**.

Данное направление содержит такие аспекты, как:

* подготовка специалистов информационной безопасности;
* трудоустройство специалистов информационной безопасности;
* обеспечение трудовой деятельности (выполнение функциональных обязанностей) специалистом информационной безопасности;
* увольнение специалиста информационной безопасности или сотрудника, имевшего доступ к конфиденциальной информации или привлекавшегося к выполнению задач информационной безопасности.

Как мы рассмотрели на предыдущих занятиях, к силам информационной безопасности организаций относятся структурные подразделения, выполняющие задачи управления системой информационной безопасности организации.

Поэтому к сотрудникам службы информационной безопасности предъявляется ряд квалификационных требований, которые мы рассмотрим на следующих занятиях. Но данные квалификационные требования формируются у сотрудников не одномоментно, а за определенный промежуток времени – от нескольких месяцев до нескольких лет.

Основными этапами в ***подготовке специалистов информационной безопасности*** являются:

* подготовка специалистов информационной безопасности в учебных образовательных организациях и центрах различного уровня образования (средне-специального, технического, бакалавриата, специалитета, магистратуры);
* повышение квалификации в зависимости от его базового уровня и занимаемой должности. Повышение квалификации также осуществляется в учебных образовательных организациях и центрах и может осуществляться как с отрывом от производства, так и без отрыва от производства;
* переподготовка специалистов информационной безопасности направлена на получение знаний и умений нового уровня в данной области деятельности. Как правило, переподготовка специалиста осуществляется при его переходе на другую должность.

Для достижения требуемого уровня квалификации разрабатывается ФГОСТ по специальности «Информационная безопасность», а для каждой специализации разрабатываются квалификационные и трудовые требования, т.е. определяется, что должен знать специалист информационной безопасности, что он должен уметь и какими навыками владеть.

Поэтому по окончании обучения проводится итоговая государственная аттестация, выпускники защищают диплом или проект.

При этом необходимо отметить, что в подготовке соответствующего специалиста может быть заинтересовано государство или ведомство, а организация или предприятие может быть заинтересовано в подготовке конкретного сотрудника (или будущего сотрудника).

Как любой вид деятельности подготовка (переподготовка и повышение квалификации) специалистов информационной безопасности обеспечивается: - нормативно-правовой базой, включая и лицензирование деятельности; - финансированием подготовки специалистов информационной

безопасности;

- обеспечением государственных, муниципальных и других социальных гарантий на период обучения, повышения квалификации и переподготовки специалиста.

Следующий этап в жизни специалиста информационной безопасности – его ***трудоустройство***.

На данном этапе государство, ведомство или организация должны создать и обеспечить наличие рабочих мест формированием отделов или служб информационной безопасности. По окончании обучения, в соответствии с квотами государства или ведомства, выпускники получают рабочие места от «Заказчиков», так же в учебные заведения приезжают представители различных организаций, и в соответствии со своими требованиями отбирают кандидатов на работу в данные организации. Например, в МЭИ есть отдел помощи в трудоустройстве выпускникам, и каждый желающий может подать в этот отдел свои документы. Но вы должны понимать, что успех вашего трудоустройства напрямую будет зависеть от показателей вашей успеваемости, уровня полученных знаний и умений.

Но, к сожалению, в настоящее время вопросы трудоустройства всех выпускников учебных заведений слабо урегулированы, и специалисты, зачастую, самостоятельно занимаются трудоустройством.

При трудоустройстве, как правило, проходит отбор кандидатов. Т.е. проходит собеседование, тестирование или другие способы определения уровня подготовки кандидатов. Соответствующими сотрудниками организации определяются общие и отраслевые требования к специалисту информационной безопасности.

Поэтому трудоустройство также сопровождается нормативно-правовым и финансовым обеспечением, но при этом добавляется кадровое обеспечение.

Следующий этап – ***обеспечение трудовой деятельности*** (выполнение функциональных обязанностей) специалистом информационной безопасности.

Данный этап характеризуется объемом выполняемых обязанностей по информационной безопасности. Но в выполнении задач информационной безопасности участвуют:

* сотрудники службы информационной безопасности;
* руководство организации и начальники различных отделов;
* сотрудники охраны организации;
* сотрудники различных отделов, имеющие доступ к конфиденциальной информации или привлекаемые к выполнению задач информационной безопасности.

Все сотрудники, привлекаемые к выполнению задач информационной безопасности, обеспечиваются должностными обязанностями, договорами и инструкциями, определяющими их функционал.

Кроме этого, указанные сотрудники должны проходить регулярное обучение без отрыва от производства и сдавать зачеты (проверки) по вопросам информационной безопасности. Успешная сдача зачетов и проверок должна стимулироваться руководством организации. При этом, обращаю ваше внимание, все вопросы обучения указанных сотрудников осуществляется службой информационной безопасности.

Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их функциональных обязанностей.

Обучение, обеспечивающее доступ к конфиденциальной информации, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями организации в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Постоянное обучение должно охватывать требования безопасности, правовую ответственность, управление бизнесом, а также обучение правильному использованию средств обработки информации, например, процедуре начала сеанса, использованию пакетов программ и информации об ответственности за нарушение требований по информационной безопасности.

Деятельность, связанная с обеспечением доступа к конфиденциальной информации, обучения и тренинга в отношении безопасности должна быть адекватной и соответствовать роли, обязанностям и квалификации лица, и должна включать информацию об известных угрозах, о контактном лице для получения дополнительной консультации по безопасности, а также о соответствующих каналах для сообщения об инцидентах информационной безопасности. Обучение с целью повышения уровня доступа к конфиденциальной информации направлено на то, чтобы дать возможность отдельным лицам распознавать проблемы и инциденты информационной безопасности, и реагировать в соответствии с их функциональными обязанностями.

Кроме этого, обучение сотрудников в процессе трудовой деятельности, т.е. без отрыва от производства, может осуществляется в форме так называемого «наставничества», более опытными сотрудниками в данной области.

Поэтому выполнение трудовых обязанностей в области информационной безопасности также сопровождается нормативно-правовым, финансовым, кадровым обеспечением и добавляется организационное обеспечение и аудит информационной безопасности.

Следующий этап – ***увольнение*** ***специалиста информационной безопасности или сотрудника, имевшего доступ к конфиденциальной информации или привлекавшегося к выполнению задач информационной безопасности***.

Данный этап характеризуется причинами увольнения:

* увольнение сотрудника на пенсию по достижении соответствующего возраста;
* переход сотрудника в другую организацию или назначение сотрудника на новую должность, функционал которой не требует выполнения работ с конфиденциальной информацией;
* увольнение сотрудника по решению руководителя организации (сокращение штатов, в связи с нарушением требований информационной безопасности или в результате создания сотрудником инцидента информационной безопасности).

Все эти причины определяют режим прекращения доступа увольняемого сотрудника к конфиденциальной информации организации и возложение на него обязательства не разглашать в последующем ту конфиденциальную информацию, к сведениям которой он имел доступ. Данные обязательства подкрепляются договором, в котором могут указываться и возможные ограничения для данного сотрудника по выезду за границу или трудоустройство в конкурирующие организации, а также мероприятиями по контролю за соблюдением настоящего обязательства.

Основными видами обеспечения данного этапа являются нормативноправовое, организационное, финансовое и кадровое обеспечение организации.

Далее рассмотрим второе направление системы обеспечения информационной безопасности – **обеспечение средств информационной безопасности.**

Как мы рассматривали на предыдущих занятиях, к **средствам обеспечения информационной безопасности** относятся: техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Поэтому средства обеспечения информационной безопасности содержат такие этапы «жизни», как:

* приобретение сертифицированных программных, программнотехнических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
* категорирование программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
* установка, настройка, проведение испытаний и ввод в эксплуатацию программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности;
* техническое обслуживание и ремонт программных, программнотехнических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности в процессе их

эксплуатации;

* списание и утилизация программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации.

Итак, первый этап системы обеспечения средств информационной безопасности – **приобретение сертифицированных программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**

Важным элементом является сертификация приобретаемых средств. Использование компанией несертифицированной продукции в сфере деятельности, требующей обязательной сертификации средств защиты информации, может повлечь за собой серьезные последствия: от больших штрафов до уголовной ответственности для руководителей.

Сертификация осуществляется ФСТЭК – это процедура получения документа, подтверждающего, что средство защиты информации соответствует требованиям нормативных и методических документов ФСТЭК России.

Сертификация ФСТЭК для средств защиты информации создана для того, чтобы обеспечить:

* защиту конфиденциальной информации строго определенного уровня;
* возможность для потребителей выбирать качественные и эффективные средства защиты информации;
* содействие формированию рынка защищенных информационных технологий и средств их обеспечения.

Поэтому данный этап сопровождается нормативно-правовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **категорирование программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**

Данный этап регламентирован **приказом ФСТЭК** России от 2 июня 2020 года **№ 76** «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)».

**Категорирование** – определение уровней доверия для программных и программно-технических средств технической защиты информации, средств обеспечения безопасности информационных технологий, включая защищенные средства обработки информации, характеризующие безопасность применения данных средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа, а также для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Для дифференциации требований по безопасности информации к средствам информационной безопасности устанавливается **6 уровней доверия**. Самый низкий уровень - шестой, самый высокий - первый.

Средства информационной безопасности, соответствующие ***6 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных.

Средства информационной безопасности, соответствующие ***5 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 2 категории, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Средства информационной безопасности, соответствующие ***4 уровню доверия***, применяются в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

При проведении сертификации средства защиты информации должно быть подтверждено соответствие средства настоящим Требованиям.

Устанавливается следующее **соответствие классов средств защиты информации и средств вычислительной техники уровням** доверия:

* средства защиты информации 6 класса должны соответствовать 6 уровню доверия;
* средства защиты информации 5 класса должны соответствовать 5 уровню доверия;
* средства защиты информации 4 класса и средства вычислительной техники 5 класса должны соответствовать 4 уровню доверия.

Данные уровни доверия определяются ***наличием возможных уязвимостей*** программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности.

Основой в данном вопросе являются опубликованные в различных источниках сведения о технических уязвимостях. Контроль технических уязвимостей следует осуществлять эффективным, систематическим и повторяемым способом, с проведением измерений с целью подтверждения его эффективности. Эти подходы должны касаться эксплуатируемых систем и любых других используемых прикладных программ.

При этом необходимо получать своевременную информацию о технических уязвимостях используемых средств информационной безопасности, оценивать незащищенность организации в отношении таких уязвимостей и принимать соответствующие меры для рассмотрения, связанного с ними риска. Данная информация позволяет эффективно управлять техническими уязвимостями.

Специальная информация, необходимая для управления техническими уязвимостями, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии применяемых средств информационной безопасности (например, какое программное обеспечение установлено на каких системах) и специалистах, отвечающих в организации за программное обеспечение.

Аналогично, своевременное действие должно предприниматься в ответ на выявление потенциальных технических уязвимостей.

Для создания эффективного процесса менеджмента в отношении технических уязвимостей необходимо выполнять следующие мероприятия:

1. в организации необходимо определять и устанавливать роли и обязанности, связанные с менеджментом технических уязвимостей, включая мониторинг уязвимостей, оценку риска проявления уязвимостей, исправление программ, слежение за активами и любые другие координирующие функции;
2. информационные ресурсы, которые будут использоваться для выявления значимых технических уязвимостей и обеспечения осведомленности о них, следует определять для программного обеспечения и другой технологии на основе списка инвентаризации активов; эти информационные ресурсы должны обновляться вслед за изменениями, вносимыми в опись, или, когда найдены другие новые или полезные ресурсы;
3. необходимо определить временные параметры реагирования на

уведомления о потенциально значимых технических уязвимостях;

1. после выявления потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать внесение исправлений в уязвимые системы и (или) применение других мер и средств контроля и управления;
2. в зависимости от того, насколько срочно необходимо рассмотреть техническую уязвимость, предпринимаемое действие следует осуществлять в соответствии с мерами и средствами контроля и управления, связанными с менеджментом изменений, или следуя процедурам реагирования на инциденты информационной безопасности;
3. если имеется возможность установки патча, следует оценить риски, связанные с его установкой (риски, создаваемые уязвимостью, необходимо сравнить с риском установки патча);
4. перед установкой патчи следует тестировать и оценивать для обеспечения уверенности в том, что они являются эффективными и не приводят к побочным эффектам, которые нельзя допускать; если нет возможности установить патч, следует рассмотреть другие меры и средства контроля и управления, например:
   1. отключение сервисов, связанных с уязвимостью;
   2. адаптацию или добавление средств управления доступом, например, межсетевых экранов на сетевых границах;
   3. усиленный мониторинг для обнаружения или предотвращения реальных атак;
   4. повышение осведомленности об уязвимостях;
5. в контрольный журнал следует вносить информацию о всех

предпринятых процедурах;

1. следует регулярно проводить мониторинг и оценку процесса менеджмента технических уязвимостей в целях обеспечения уверенности в его эффективности и действенности;
2. в первую очередь следует обращать внимание на системы с высоким

уровнем риска.

Следующий элемент – ***процесс получения разрешения на использование средств обработки информации***.

При этом необходимо определить и реализовать процесс получения разрешения у руководства на использование новых средств обработки информации.

В отношении процесса получения разрешения следует рассмотреть следующие мероприятия:

1. на новые средства должны быть получены соответствующие разрешения руководства пользователей, утверждающего их цель и использование. Разрешение следует также получать от администратора, ответственного за поддержку среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие требования и политики безопасности соблюдаются;
2. аппаратные средства и программное обеспечение, где необходимо, следует проверять на предмет совместимости с другими компонентами системы;
3. использование персональных или находящихся в частной собственности средств обработки информации, например, ноутбуков, домашних компьютеров или карманных устройств для обработки деловой информации может являться причиной новых уязвимостей, поэтому следует определять и реализовывать необходимые меры и средства контроля и управления. В настоящее время при удаленной работе многих сотрудников данный пункт является очень актуальным.

Таким образом, данный этап также сопровождается нормативноправовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **установка, настройка, проведение испытаний и ввод в эксплуатацию программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности**.

Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.

Документально оформленные процедуры должны быть подготовлены для действий системы, связанных со средствами обработки информации и связи, таких как процедуры запуска и завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обращения с носителями информации, управление работой в машинном зале и работы с почтой, а также процедуры обеспечения безопасности.

Данные процедуры должны содержать детальные инструкции по выполнению каждой работы, включая:

1. обработку и управление информацией;
2. резервирование;
3. требования в отношении графика работ, включая взаимозависимости между системами, время начала самой ранней работы и время завершения самой последней работы;
4. инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит;
5. необходимые контакты на случай неожиданных эксплуатационных

или технических проблем;

1. специальные инструкции по управлению выводом данных и обращению с носителями информации, например, использование специальной бумаги для печатающих устройств или управление выводом конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе;
2. перезапуск системы и соответствующие процедуры восстановления

на случай системных сбоев;

1. управление информацией, содержащейся в контрольных записях и

системных журналах.

Эксплуатационные процедуры и документально оформленные процедуры действий системы должны рассматриваться как официальные документы, а изменения в них должны санкционироваться руководством. Если технически возможно, менеджмент информационных систем необходимо осуществлять единообразно, используя одни и те же процедуры, инструментальные средства и утилиты.

Эксплуатируемые системы и прикладное программное обеспечение должны быть предметом строгого контроля управления изменениями. В частности, необходимо рассмотреть следующие аспекты:

1. определение и регистрацию существенных изменений;
2. планирование и тестирование изменений;
3. оценку возможных последствий, включая последствия для

безопасности, таких изменений;

1. формализованную процедуру утверждения предполагаемых

изменений;

1. подробное информирование об изменениях всех заинтересованных

лиц;

1. процедуры возврата в исходный режим, включая процедуры и обязанности в отношении отмены и последующего восстановления в случае неудачных изменений и непредвиденных обстоятельств.

С целью обеспечения уверенности в надлежащем контроле всех изменений в оборудовании, программном обеспечении или процедурах, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в контрольном журнале.

Таким образом, данный этап также сопровождается нормативноправовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **техническое обслуживание и ремонт программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности в процессе их эксплуатации**.

Техническое обслуживание средств информационной безопасности должно проводиться в соответствии с целями обеспечения его непрерывной доступности и целостности.

В отношении технического обслуживания средств информационной безопасности следует рассмотреть следующие мероприятия:

1. оборудование должно обслуживаться в соответствии с

рекомендуемыми поставщиком периодичностью и спецификациями;

1. техническое обслуживание и ремонт оборудования должны

проводиться только авторизованным персоналом;

1. следует хранить записи обо всех предполагаемых или фактических

неисправностях и всех видах профилактического обслуживания;

1. если запланировано техническое обслуживание оборудования, следует принимать соответствующие меры и средства контроля и управления, при этом необходимо учитывать, будет ли техническое обслуживание проводиться персоналом организации или за ее пределами; при необходимости, конфиденциальная информация из оборудования должна быть удалена, или специалисты по техническому обслуживанию и ремонту должны иметь соответствующий допуск;
2. должны соблюдаться все требования, устанавливаемые технической

документацией.

Отдельного внимания заслуживает безопасность средств информационной безопасности, находящихся вне помещений организации.

При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, следует учитывать различные риски, связанные с работой вне помещений организации.

Независимо от права собственности использование оборудования для обработки информации вне помещений организации должно быть санкционировано руководством.

Следующие рекомендации необходимо учитывать в отношении защиты оборудования, используемого вне помещений организации:

1. оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах; во время поездок портативные компьютеры нужно перевозить как ручную кладь и по возможности маскировать;
2. необходимо соблюдать инструкции изготовителей по защите оборудования, например, по защите от воздействия сильных

электромагнитных полей;

1. для работы вне контролируемой зоны организации следует определить соответствующие меры и средства контроля и управления, исходя из оценки рисков, например, использование запираемых шкафов для хранения документов, соблюдение политики «чистого стола», управление доступом к компьютерам и связь с офисом по защищенным сетям (ИСО/МЭК 18028

«Сетевая Безопасность»);

1. с целью защиты оборудования, используемого вне помещений организации, должно проводиться адекватное страхование, покрывающее указанные риски. Риски безопасности, например, связанные с повреждением, воровством и подслушиванием, могут значительно отличаться для различных объектов и должны учитываться при определении наиболее подходящих мер и средств контроля и управления.

Еще один элемент – ***техническая проверка прикладных программ после изменений эксплуатируемой системы***.

При внесении изменений в эксплуатируемые системы прикладные программы, имеющие большое значение для бизнеса, следует анализировать и тестировать с целью обеспечения уверенности в том, что не оказывается неблагоприятного воздействия на функционирование или безопасность организации.

Этот процесс должен охватывать:

1. анализ мер и средств контроля и управления прикладными программами и процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями эксплуатируемой системы;
2. обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, необходимые при изменениях эксплуатируемой системы;
3. обеспечение уверенности в том, что уведомления об изменениях эксплуатируемой системы поступают своевременно, чтобы дать возможность перед их реализацией провести соответствующие тесты и анализы;
4. обеспечение уверенности в том, что соответствующие изменения

вносятся в планы обеспечения непрерывности бизнеса.

Определенной группе лиц или отдельному специалисту следует вменять в обязанность проведение мониторинга уязвимостей, версий патчей поставщиков и их установок.

Следующий элемент – ***ограничения на изменения пакетов программ***.

Необходимо избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все сделанные изменения.

Насколько возможно и допустимо с практической точки зрения пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

1. риск в отношении встроенных мер и средств контроля и управления,

и процедур обеспечения целостности;

1. необходимость получения согласия поставщика;
2. возможность получения требуемых изменений от поставщика в

качестве стандартной программы обновления;

1. возможные последствия в случае, если организация станет ответственной за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ.

Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

Таким образом, данный этап также сопровождается нормативноправовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Следующий этап системы обеспечения средств информационной безопасности – **списание и утилизация программных, программнотехнических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации.**

Безопасная утилизация программных, программно-технических средств, веществ и (или) материалов, предназначенных или используемых для информационной безопасности, не пригодных для дальнейшей эксплуатации является не менее важным этапом.

Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

Носители данных, содержащие конфиденциальную информацию, необходимо физически уничтожать, или информацию необходимо разрушить, удалить или перезаписать способами, делающими исходную информацию невосстановимой, а не использовать стандартные функции удаления и форматирования.

Поврежденные устройства, содержащие конфиденциальные данные, могут потребовать проведения оценки рисков с целью определения элементов, которые должны быть физически разрушены, направлены на ремонт или списаны.

При этом всегда необходимо помнить, что конфиденциальная информация всегда может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования.

Таким образом, данный этап также сопровождается нормативноправовым, финансовым, инженерно-техническим и программно-аппаратным обеспечением.

Подводя итог выше изложенному материалу, необходимо отметить, что анализ всех мероприятий системы обеспечения средств информационной безопасности показал, что основными видами обеспечения данного направления являются нормативно-правовое, организационное, финансовое, инженерно-техническое и программно-аппаратное обеспечение организации.

Таким образом возникла необходимость систематизировать информацию о системе обеспечения информационной безопасности, ее составе и функционале.

**Система обеспечения информационной безопасности** – совокупность правовых, организационных и технических мероприятий, органов, сил, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба собственнику информации.

*Данная формулировка определена РЕШЕНИЕМ Совета глав правительств СНГ. «О концепции информационной безопасности государств - участников содружества независимых государств в военной сфере».* **Цель СОИБ заключается** в обеспечении устойчивого функционирования организации (предприятия) для достижения им своих целей, которое достигается выполнением требований по конфиденциальности, доступности и целостности принадлежащих ему активов.

**Задачи СОИБ**:

1. Предотвращение угроз безопасности организации (предприятия), защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ, обеспечение стабильной производственной деятельности всех подразделений объекта.
2. Повышение качества предоставляемых услуг и гарантий безопасности.

Для решения этих задач необходимо выполнить следующие **мероприятия СОИБ**:

* отнести информацию к категории ограниченного доступа;
* прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению нормального функционирования и развития организации;
* создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
* создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических и прочих мер, и средств обеспечения безопасности;
* создать условия для максимально возможного возмещения и (или) локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

Выше изложенные положения определяют **состав системы обеспечения информационной безопасности**:

* подсистема организационно-правового обеспечения;
* подсистема кадрового обеспечения;
* подсистема финансово-экономического обеспечения;
* подсистема инженерно-технического обеспечения;
* подсистема программно-аппаратного обеспечения;
* подсистема аудита информационной безопасности.

Данные подсистемы, представляющие собой единую СОИБ полностью охватывают весь перечень работ по ее созданию в интересах объекта, организации функционирования этой системы и поддержания ее в состоянии готовности к решению возложенных на нее задач.

*Подсистема организационно-правового обеспечения* должна обеспечить:

* во-первых, формирование правового поля для выполнения мероприятий обеспечения информационной безопасности, путем учета требований законодательства РФ в данной предметной области;
* во-вторых, обеспечение выполнения концептуальных разработок, а также практических ограничительных и режимных мероприятий по обеспечению информационной безопасности в интересах объекта.

При этом, **организационные мероприятия обеспечения информационной безопасности** – мероприятия обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Таким образом, для обеспечения информационной безопасности организации, создан универсальный перечень режимных (организационных) мероприятий, включающий:

* физическую защиту сотрудников, являющихся потенциальными носителями конфиденциальной информации;
* постоянный контроль и проверка персонала с целью устранения возможностей для совершения мошенничества, предотвращения возможного сговора между сотрудниками и, например, клиентами;
* ограничение прав доступа сотрудников к информации, которое должно регламентироваться только характером выполняемых ими должностных обязанностей;
* налаженную и постоянно действующая система внутреннего контроля, включающая проведение плановых, внезапных и скрытых контрольных проверок;
* проведение предупредительной активной политики аудита информационной безопасности.

*Подсистема кадрового обеспечения* должна базироваться на созданной системе подготовки специалистов в области информационной безопасности, иметь систему подбора специалистов, основывающуюся на деятельности кадрового органа объекта, а также, систему работы с сотрудниками.

*Подсистема финансово-экономического обеспечения* обеспечивает выполнение функции использования результатов анализа финансовоэкономической деятельности организации с целью определения возможных масштабов финансирования деятельности по обеспечению информационной безопасности.

Кроме этого, обеспечивает работы по моделированию и оценке затрат на обеспечение ИБ, а также, по определению минимально достаточного уровня затрат, т.е. оптимизационные расчеты.

*Подсистема инженерно-технического обеспечения* охватывает совокупность работ по инженерно-техническому оборудованию элементов (объектов) информационной инфраструктуры организации.

Кроме этого, по обеспечению видеонаблюдения, противопожарной защиты на объектах, и защиты информации, в том числе и компьютерной, от утечек по различным каналам.

*Подсистема программно-аппаратного обеспечения* обеспечивает выполнение функций защиты информации в информационной системе, а также самих элементов информационной системы от различных угроз применением различных программных и программно-аппаратных решений.

*Подсистема аудита информационной безопасности* предназначена для обеспечения контроля и проверок качества функционирования всех подсистем и элементов СОИБ применением методик анализа рисков информационной безопасности, а также различных форм проведения проверок. На этом изложение учебного вопроса завершено.