Лекция № 1
Сущность информации

Вводная часть

На сегодняшнем занятии вы ознакомитесь с понятиями «информация», «защита информации», видами и способами защиты информации.

Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты во всем мире. Количество случаев посягательства на информационную безопасность растет на 4-5 % каждые полгода. При этом необходимо отметить, что для хакеров не существует авторитетов. Например, в ноябре 2021 года они разослали от имени центрального банка РФ письма с вирусами в 50 российских банков. При этом подразделение ЦБ РФ по работе с информацией отмечает, что в 2021 году существенно выросло количество атак на компании, информационные массивы которых защищены гораздо меньше, чем банковские или государственные. Все это говорит о растущей актуальности проблемы обеспечения безопасности информации. Поэтому в современном мире информационная безопасность – это жизненно необходимое условие обеспечения интересов человека, общества и государства. Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – экономике, обороне, политике, а также в социальной сфере.

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Понятие информации и ее виды.
2. Виды и способы защиты информации.

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

В первом учебном вопросе рассмотрим составляющие осваиваемой специальности по каждой категории – «основы», «информация» и «безопасность», а на следующих занятиях данные категории мы будем рассматривать комплексно. Все изучаемые термины и положения вы должны знать, т.к. эти знания позволяют специалистам любой направленности правильно излагать и понимать все процессы в области информационной безопасности.

Данные категории, в первую очередь, определены законодательно.

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

Основы менеджмента знаний в области инжиниринга включают: цель, задачи, мероприятия и привлекаемые для этого силы и средства. Т.е., в ходе изучения дисциплины вы должны изучить цель, задачи, мероприятия, организацию, силы и средства информационной безопасности и составляющих ее элементов.

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.

В соответствии со схемой на рисунке, информация бывает общедоступной и ограниченного доступа.

В свою очередь информация ограниченного доступа подразделяется на государственную тайну и конфиденциальную информацию. Более подробно содержание государственной тайны и конфиденциальной информации мы рассмотрим на следующем занятии.

Кроме этого, информация разделяется по назначению и распространению.

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;

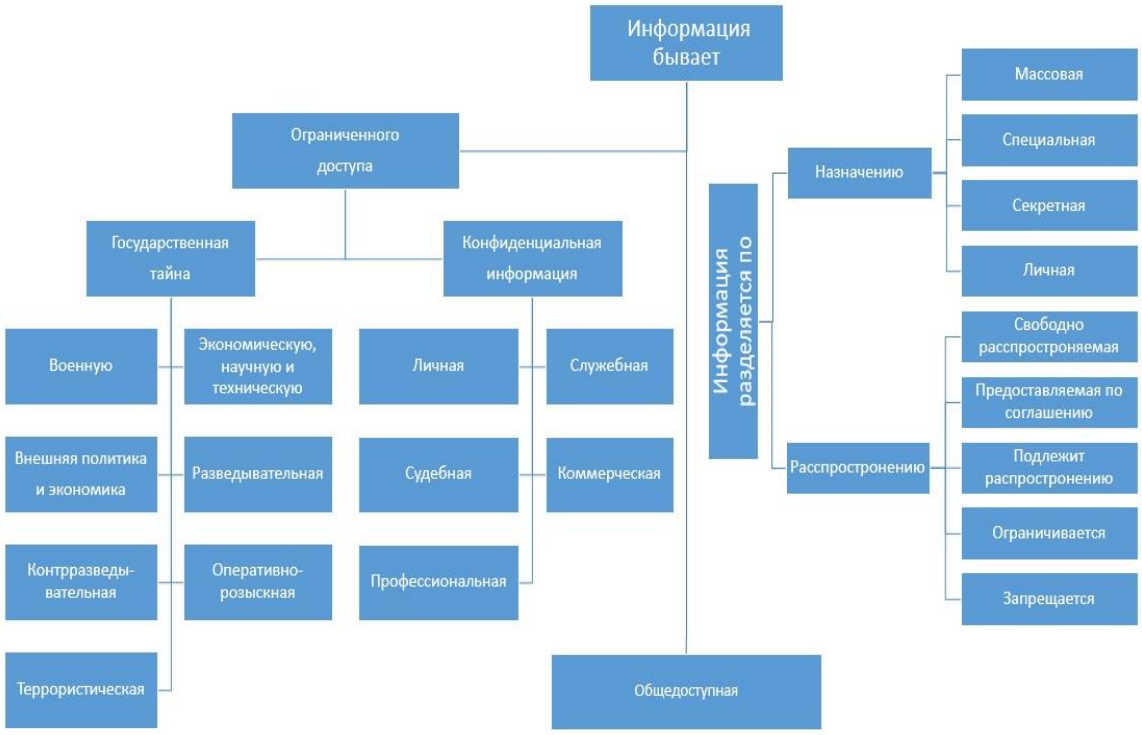

Рисунок 1 – Виды информации

- *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.

При этом хочу обратить ваше внимание на то, что конфиденциальная информация может иметь любое отображение в соответствии с представленными формами и видами на слайдах.

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.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

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»).

Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Из представленных выше категорий вы будете изучать вопросы защиты информации.

Итак, что же такое «защита информации»?

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.

2. ***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).

3. ***Непрерывность*** – постоянное поддержание работоспособности и развитие системы защиты информации.

4. ***Активность*** – настойчивость в достижении целей и задач защиты информации. Предполагает постоянный маневр силами и средствами защиты информации, а также принятие нестандартных мер защиты.

5. ***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.

6. ***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.

7. ***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.

8. ***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.

9. ***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.

10. ***Совершенствование***. Предусматривает совершенствование и разработку новых законодательных, организационных и технических мер защиты информации под воздействием объективных и субъективных факторов.

11. ***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, научно-технической 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.

Правовую основу (законодательные средства) информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами «Об информации, информационных технологиях и о защите информации», законы Российской Федерации «О безопасности», «О связи», «О государственной тайне» и различными подзаконными актами. Не соблюдение данных законов влечет за собой угрозы информационной безопасности, которые могут привести к значительным последствиям, что в свою очередь наказуемо в соответствии с этими законами в плоть до уголовной ответственности.

Государство также определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности. Например, глава 28 «Преступления в сфере компьютерной информации» 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 информационно-телекоммуникационных 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.

Регламент определяет разграничение доступа и временные показатели работы пользователей с конфиденциальной информацией. Правила разграничения доступа к защищаемой информации разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

Правила устанавливаются руководством компании совместно со службой безопасности и поставщиком, который внедряет систему безопасности.

Цель – создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа.

Порядок работы с документацией и носителями данных определяет организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации. Так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями. Например, нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

Для снижения влияния этих аспектов необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы или сводили к минимуму возможность возникновения угроз конфиденциальной информации.

В данной организационной деятельности по защите информации для сотрудников служб безопасности информации определен большой объем должностных обязанностей.

Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации.

С точки зрения регламентации деятельности персонала важным станет оформление системы запросов на допуск к интернету, внешней электронной почте, другим ресурсам. Отдельным элементом станет получение электронной цифровой подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам электронной почты. И многие другие аспекты, которые вы изучите в ходе обучения.

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 SIEM-системы.

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.

Внедрение средств криптографической защиты информации предусматривает создание программно-аппаратного комплекса, архитектура и состав которого определяется, исходя из потребностей конкретного

заказчика, требований законодательства, поставленных задач и необходимых методов, и алгоритмов шифрования.

Сюда могут входить программные компоненты шифрования (криптопровайдеры), средства организации VPN сетей, средства удостоверения, средства формирования и проверки ключей и электронной цифровой подписи.

Средства шифрования могут поддерживать алгоритмы шифрования ГОСТ и обеспечивать необходимые классы криптозащиты в зависимости от необходимой степени защиты, нормативной базы и требований совместимости с иными, в том числе, внешними системами. При этом средства шифрования обеспечивают защиту всего множества информационных компонент в том числе файлов, каталогов с файлами, физических и виртуальных носителей информации, целиком серверов и систем хранения данных.

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 средствам физической защиты относятся: замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами. Группа дополняется средствами систем безопасности, например, видеокамерами, видеорегистраторами, датчиками, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения технических средств для снятия информации.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

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.

Таким образом, средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Важным средством для защиты информации является средство контроля эффективности 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).

Т.е. под силами защиты информации подразумевается существование некоторого структурного подразделения, выполняющего задачи управления функционированием данной системы.

Характер и масштабы сил защиты информации будут зависеть от масштаба объекта, характера и степени конфиденциальности имеющейся

информации, а также от объема затрат на выполнение указанных задач. Более детально анализ сил защиты информации в организации будет проведен в ходе следующих занятий.

На этом изложение второго учебного вопроса завершено.

Литература

1. Национальный стандарт Российской Федерации ГОСТ Р 57321.1 «Менеджмент знаний. Менеджмент знаний в области инжиниринга. Часть 1. Общие положения, принципы и понятия».

2. Федеральный закон №149 от 7.07.2006г. «Об информации, информационных технологиях и о защите информации».

3. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».

4. Уголовный кодекс Российской Федерации

5. Национальный стандарт Российской Федерации ГОСТ Р 7.0.97-2016 «Организационно-распорядительная документация».

6. Национальный стандарт Российской Федерации ГОСТ Р 7.0.8-2013 «Делопроизводство и архивное дело».

7. Межгосударственный стандарт ГОСТ 2.105-95 «Общие требования к текстовым документам».

Заключение

Из представленного учебного материала необходимо уяснить, что такое «информация», «защита информации», виды и способы защиты информации, а также требованиями законодательных документов в области защиты информации.

Доцент кафедры БИТ Д.Власкин