ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.13 Основы информационной безопасности

Направление подготовки (специальность) *09.03.01 Информатика и вычислительная техника*
Профиль образовательной программы **"***Автоматизированные системы обработки информации и управления***"**

Форма обучения *очная*

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1.1 Лекция №1, 2 (4 часа).

Тема: «Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности.»

1.1.1 Вопросы лекции:

1. Основные понятия, термины и определения.

2. Основы государственной политики в области информационной безопасности

1.1.2 Краткое содержание вопросов:

1. Основные понятия термины и определения.

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое *информационная безопасность*. Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2. административный – комплекс мер, предпринимаемых локально руководством организации;
3. процедурный уровень – меры безопасности, реализуемые людьми;
4. *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

2. Основы государственной политики в области информационной безопасности

Основу правового обеспечения информационной безопасности России помимо нормативно-правовых актов составляют концептуальные документы. Они принимаются на уровне Президента РФ, Правительства РФ и других органов государственной власти. В частности, такими документами являются Доктрина информационной безопасности РФ и Стратегия национальной безопасности РФ до 2020 года.

Концепция (от лат. conceptio) - генеральный замысел, определяющий стратегию действий. Концепция защиты информации - это система взглядов на сущность, цели, принципы и организацию защиты информации.

Концепция защиты информации предполагает:

1. Определение понятия, сущности и целей защиты информации.
2. Какую информацию необходимо защищать, каковы критерии отнесения ее к защищаемой.
3. Дифференциацию защищаемой информации: а) по степеням конфиденциальности, б) по собственникам и владельцам.
4. Определение состава и классификации носителей защищаемой информации.
5. Определение источников, видов и способов дестабилизирующего воздействия на информацию, причин, обстоятельств и условий воздействий, каналов, методов и средств несанкционированного доступа к информации.
6. Определение методов и средств защиты информации.
7. Кадровое обеспечение защиты информации.

То есть концептуальные документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов.

Стратегия национальной безопасности до 2020 года была утверждена президентом Д. Медведевым 12 мая 2009 года. Стратегия – это "официально признанная система стратегических национальных приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу".

Документ содержит 6 разделов:

1. Общие положения
2. Современный мир и Россия: состояние и тенденции развития
3. Национальные интересы Российской Федерации и стратегические национальные приоритеты
4. Обеспечение национальной безопасности
5. Организационные, нормативные правовые и информационные основы реализации настоящей Стратегии
6. Основные характеристики состояния национальной безопасности в составе 112 отдельных пунктов

В Общих положениях дается перечень основных понятий в области национальной безопасности:

- национальная безопасность - состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

- национальные интересы Российской Федерации - совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства;

- угроза национальной безопасности - прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства;

- стратегические национальные приоритеты - важнейшие направления обеспечения национальной безопасности, по которым реализуются конституционные права и свободы граждан Российской Федерации, осуществляются устойчивое социально-экономическое развитие и охрана суверенитета страны, ее независимости и территориальной целостности;

- система обеспечения национальной безопасности - силы и средства обеспечения национальной безопасности;

- силы обеспечения национальной безопасности - Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации;

- средства обеспечения национальной безопасности - технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению.

"Концептуальные положения в области обеспечения национальной безопасности базируются на фундаментальной взаимосвязи и взаимозависимости Стратегии национальной безопасности Российской Федерации на период до 2020 года и Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года". Важно подчеркнуть, что Документ ориентирован именно на национальную

безопасность, то есть на безопасность интересов государства в целом. При этом задача обеспечения национальной безопасности признается комплексной задачей, для решения которой в Стратегии представлены следующие направления деятельности:

- Повышение качества жизни российских граждан;
- Экономический рост;
- Наука, технология и образование;
- Здравоохранение;
- Культура;
- Экология живых систем и рациональное природопользование.

В заключительной части описаны основные характеристики состояния национальной безопасности, а именно:

1. уровень безработицы (доля от экономически активного населения);
2. децильный коэффициент (соотношение доходов 10% наиболее и 10% наименее обеспеченного населения);
3. уровень роста потребительских цен;
4. уровень государственного внешнего и внутреннего долга в процентном отношении от валового внутреннего продукта;
5. уровень обеспеченности ресурсами здравоохранения, культуры, образования и науки в процентном отношении от валового внутреннего продукта;
6. уровень ежегодного обновления вооружения, военной и специальной техники;
7. уровень обеспеченности военными и инженерно-техническими кадрами.

Для сравнения: в Европе децильный коэффициент находится в диапазоне 6-8, в США – 10-12, в России, по данным Российской академии наук, 14-17. Этот параметр является наиболее значимым при определении состояния национальной безопасности, и одной из основных задач на данный момент является его максимальное уменьшение.

В целом, Стратегия национальной безопасности РФ до 2020 года стала принципиально новым документом, основной целью которого является планирование развития системы национальной безопасности, в том числе цели, меры и порядок действий для ее обеспечения. Стратегия стала своего рода ответом на новую международную обстановку и отразила взгляды и планы руководства РФ в отношении внешней политики.

Если Стратегия ориентирована на вопросы национальной безопасности, то основополагающим концептуальным документом в области информационной безопасности является Доктрина информационной безопасности, утвержденная 9 сентября

2000 года. Доктрина информационной безопасности РФ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

В Доктрине выделены четыре составляющие национальных интересов в области информационных отношений:

- Соблюдение прав и свобод человека в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.;
- Информационное обеспечение внутренней и внешней государственной политики страны;
- Развитие информационных технологий в соответствии со временем;
- Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Дается следующее определение информационной безопасности - состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [2.2].

Таким образом, понятие информационной безопасности здесь является более расширенным, чем рассмотренное нами в предыдущей лекции.

В соответствии с Доктриной угрозы информационной безопасности подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина, индивидуальному, групповому и общественному сознаниям, духовному возрождению России. Примером данного вида угроз может быть незаконное ограничение доступа к информации, намеренное дезинформирование или прослушивание телефона.

- угрозы информационному обеспечению государственной политики России. Сюда относится нарушение работы государственных СМИ, монополизация информационного рынка России.
- угрозы развитию российской индустрии информации. Интересным является то, что закупка органами государственной власти зарубежных средств информатизации приравнивается в Доктрине к угрозе, так как мешает отечественным производителям развиваться. Отток высококвалифицированных специалистов также относится к данному типу угроз.
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Этот вид угроз наиболее близок к пониманию, так как именно к нему относятся угрозы "классических" атак и воздействий. Сюда относятся противоправные сбор и обработка информации, хищение, утечка по техническим каналам и несанкционированный доступ к информации. В ходе курса мы подробнее остановимся на данном виде угроз.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации. Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

- Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.
- Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

- Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

Важно отметить, что Доктрина не является нормативно-правовым документом, то есть не обязательна к исполнению ни государством, ни его органами власти, ни гражданами, ни организациями. Доктрина разрабатывается для определенного исторического этапа развития и реализовывается в дальнейшем в виде законов, нормативных актов и практических мер, которые будут рассмотрены далее.

1. 2 Лекция №3,4 (4 часа).

Тема: Аттестация объектов информатизации по требованиям безопасности информации.

1.2.1 Вопросы лекции:

1. Общие сведения об аттестации.

2**.** Структура системы аттестации.

3. Порядок проведения аттестации.

1.2.2 Краткое содержание вопросов:

1. Общие сведения об аттестации

Деятельность по аттестации объектов *информатизации* по *требованиям безопасности* информации осуществляет ФСТЭК России (бывш. Гостехкомиссия России). Для начала дадим *определение* объекта *информатизации*.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта *информатизации*, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что *объект* соответствует требованиям стандартов или иных нормативно-технических документов по *безопасности информации*, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право

обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.

Аттестация производится в порядке, установленном "Положением по аттестации объектов *информатизации* по *требованиям безопасности* информации" от 25 ноября 1994 года. *Аттестация* должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте *информатизации*.

Аттестация является обязательной в следующих случаях:

- *государственная тайна*;
- при защите государственного информационного ресурса;
- управление экологически опасными объектами;
- ведение секретных переговоров.

Во всех остальных случаях *аттестация* носит добровольный характер, то есть может осуществляться по желанию заказчика или владельца объекта *информатизации*.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта *информатизации* в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:

- защита от НСД, в том числе *компьютерных вирусов*;
- защита от утечки через ПЭМИН;
- защита от утечки или воздействия на информацию за счет специальных устройств, встроенных в объект *информатизации*.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня *работ*:

- анализ исходных данных по аттестуемому объекту *информатизации*;
- предварительное ознакомление с аттестуемым объектом *информатизации*;
- проведение экспертного обследования объекта *информатизации* и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте *информатизации* с помощью специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по *сертификациисредств защиты информации* по *требованиям безопасности* информации;
- проведение комплексных аттестационных испытаний объекта *информатизации* в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта *информатизации* и утверждение заключения по результатам аттестации.

Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по *сертификации средств защиты информации* по *требованиям безопасности* информации".

Все *расходы* по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

2. Структура системы аттестации

В *структуру системы* аттестации входят:

- федеральный орган по *сертификации средств защиты информации* и аттестации объектов *информатизации* по *требованиям безопасности* информации – ФСТЭК России;
- органы по аттестации объектов *информатизации* по *требованиям безопасности* информации;
- испытательные центры (лаборатории) по *сертификации* продукции по *требованиям безопасности* информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов *информатизации*).

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов *информатизации*.

В качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.

Органы по аттестации:

- аттестуют объекты *информатизации* и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах *информатизации*, и за их эксплуатацией;
- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";
- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов *информатизации*, участвуют в их разработке;
- ведут *информационную базу* аттестованных этим органом объектов *информатизации*;
- осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

- организует обязательную аттестацию объектов *информатизации*;
- создает системы аттестации объектов *информатизации* и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов *информатизации*;
- аккредитует органы по аттестации объектов *информатизации* и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов *информатизации*;
- рассматривает апелляции, возникающие в процессе аттестации объектов *информатизации*, и контроля за эксплуатацией аттестованных объектов *информатизации*;
- организует периодическую публикацию информации по функционированию системы аттестации объектов *информатизации* по *требованиям безопасности* информации.

Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте *информатизации*.

Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе "Сведения о Системе *сертификации средств защиты информации* по *требованиям безопасности* информации".

Заявители:

- проводят подготовку объекта *информатизации* для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
- привлекают органы по аттестации для организации и проведения аттестации объекта *информатизации*;
- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
- привлекают, в необходимых случаях, для проведения испытаний несертифицированных *средств защиты информации*, используемых на аттестуемом объекте *информатизации*, испытательные центры (лаборатории) по *сертификации*;
- осуществляют эксплуатацию объекта *информатизации* в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";
- извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и *средств защиты информации* (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
- предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта *информатизации*, прошедшего обязательную аттестацию.

Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

- приемо-сдаточную документацию на объект *информатизации*;
- акты *категорирования* выделенных помещений и объектов *информатизации*;
- инструкции по эксплуатации *средств защиты информации*;
- технический паспорт на аттестуемый объект;
- документы на эксплуатацию (*сертификаты соответствия требованиям безопасности* информации) ТСОИ;
- *сертификаты соответствия требованиям безопасности* информации на ВТСС;
- *сертификаты соответствия требованиям безопасности* информации на технические средства защиты информации;
- акты на проведенные скрытые работы;

- протоколы измерения звукоизоляции выделенных помещений и эффективности *экранирования* сооружений и кабин (если они проводились);
- протоколы измерения величины сопротивления заземления;
- протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
- данные по уровню подготовки кадров, обеспечивающих защиту информации;
- данные о *техническом обеспечении* средствами контроля эффективности защиты информации и их метрологической поверке;
- нормативную и методическую документацию по защите информации и контролю эффективности защиты.

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта *информатизации* по согласованию с аттестационной комиссией.

- пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
- перечень объектов *информатизации*, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых технических *средств защиты информации* с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной *подстанции*, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания с указанием мест расположения объектов *информатизации* и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;

- планы объектов *информатизации* с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схему системы заземления объекта с указанием места расположения заземлителя;
- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (*подстанции*), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены).

3. Порядок проведения аттестации

Порядок проведения аттестации объектов *информатизации* по *требованиям безопасности* информации включает следующие действия:

1. подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов *информатизации* по *требованиям безопасности*". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.
2. предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;
3. испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
4. разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.

5. заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

6. проведение аттестационных испытаний объекта *информатизации*. В ходе аттестационных испытаний выполняется следующее:

- анализ организационной структуры объекта *информатизации*, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определяется правильность *категорирования* объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по *сертификации*;
- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по *безопасности информации*;
- проводятся комплексные аттестационные испытания объекта *информатизации* в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта *информатизации* в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта *информатизации*[6.2]

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен включать:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;

- перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
- перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов;
- выводы по результатам испытаний [6.4]

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю [2]. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

7. оформление, регистрация и выдача "Аттестата соответствия" (если заключение по результатам аттестации утверждено).

8. осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов *информатизации*;

9. рассмотрение апелляций. В случае, если заявитель не согласен с отказом в выдаче "Аттестата соответствия", он может подать апелляцию в вышестоящий орган по аттестации или в ФСТЭК. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.

Аттестат соответствия должен содержать:

- регистрационный номер;
- дату выдачи;
- срок действия;
- наименование, адрес и местоположение объекта *информатизации*;
- категорию объекта *информатизации*;
- класс защищенности автоматизированной системы;
- гриф секретности (конфиденциальности) информации, обрабатываемой на объекте *информатизации*;
- организационную структуру объекта *информатизации* и вывод об уровне подготовки специалистов по защите информации;
- номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;

- перечень руководящих документов, в соответствии с которыми проводилась аттестация;
- номер и дата утверждения заключения по результатам аттестационных испытаний;
- состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических *средств защиты информации*, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;
- организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;
- перечень действий, которые запрещаются при эксплуатации объекта *информатизации*;
- список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и *средств защиты информации*.

Аттестат соответствия подписывается руководителем аттестационной комиссии и утверждается руководителем органа по аттестации.

Аттестат соответствия выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта *информатизации* и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие *безопасность* информации (состав и структура технических средств, условия размещения, используемое *программное обеспечение*, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

1. 3 Лекция №5,6 (4 часа).

Тема: «Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну.»

1.3.1 Вопросы лекции:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне".

2. Организационно-технические меры защиты сведений, составляющих государственную тайну.

1.3.2 Краткое содержание вопросов:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В настоящем Законе используются следующие основные понятия:

- 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;

- носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

- система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

- допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

- доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

- гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

- средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной

тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Государственную тайну составляют:

1) сведения в военной области;

2) сведения в области экономики, науки и техники;

3) сведения в области внешней политики и экономики;

4) 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.

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 настоящего Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

2. Организационно-технические меры защиты сведений, составляющих государственную тайну.

Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

5. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности и осуществляются во

взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

Главными направлениями работ по защите информации являются:

- обеспечение эффективного управления системой защиты информации;

- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;

- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

- разработка организационно-технических мероприятий по защите информации и их реализация;

- организация и проведение контроля состояния защиты информации.

Основными организационно-техническими мероприятиями по защите информации являются:

- лицензирование деятельности предприятий в области защиты информации;

- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

- категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

- обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;

- оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

- разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;

- разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;

- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

1. 4 Лекция №7,8 (4 часа).

Тема: «Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны.»

1.4.1 Вопросы лекции:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

2. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

3. Организационно-технические меры защиты коммерческой тайны.

1.4.2 Краткое содержание вопросов:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

В настоящем Федеральном законе используются следующие основные понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";

14) страница сайта в сети "Интернет" (далее также - интернет-страница) - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет";

15) доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";

16) сетевой адрес - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

17) владелец сайта в сети "Интернет" - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте;

18) провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет";

19) единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

20) поисковая система - информационная система, осуществляющая по запросу пользователя поиск в сети "Интернет" информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети "Интернет" для доступа к запрашиваемой информации, расположенной на сайтах в сети "Интернет", принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания

государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

2. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

Принят Государственной Думой 9 июля 2004 года. Одобрен Советом Федерации 15 июля 2004 года.

Цели и сфера действия Федерального закона:

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Основные понятия, используемые в настоящем Федеральном законе:

1) 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;

2) 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;

3) обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

4) доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее

обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

5) передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

6) контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

7) предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

8) разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

3. Организационно-технические меры защиты коммерческой тайны.

Меры по охране коммерческой тайны определены в Федеральном законе от 29.07.2004 N 98-ФЗ "О коммерческой тайне" в статье 10 «Охрана конфиденциальности информации»

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "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).

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

1. 5 Лекция №9, 10 (4 часа).

Тема: «Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.»

1.5.1 Вопросы лекции:

1. Сведения не составляющие государственную тайну.

2. Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

1.5.2 Краткое содержание вопросов:

1. Сведения не составляющие государственную тайну.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию определены в Законе РФ от 21.07.1993 N 5485-1 "О государственной тайне" в статье 7.

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. Граждане вправе обжаловать такие решения в суд.

2. Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства

вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании».

Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

- неправомерного блокирования информации (обеспечение доступности информации).

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка системы защиты информации информационной системы;

- внедрение системы защиты информации информационной системы;

- аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

1. 6 Лекция №11, 12 (4 часа).

Тема: «Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

1.6.1 Вопросы лекции:

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1.6.2 Краткое содержание вопросов:

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), 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.

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;

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

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или

общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
-выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение

доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а

также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных,

анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

1. 7 Лекция №13, 14, 15 (6 часов).

Тема: «Нормативно-правовые, морально-этические, административные, физические и технические меры»

1.7.1 Вопросы лекции:

1. Нормативно-правовые меры.
2. Морально-этические меры.
3. Административные меры.
4. Физические и технические меры

1.7.2 Краткое содержание вопросов

1. Нормативно-правовые меры.

К нормативно-правовым мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией, закрепляющие нрава и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Нормативно-правовые меры направлены на решение следующих вопросов:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий но доступу к информации;
- нрава должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

На созданную в 1992 г. Гостехкомиссию России но защите информации были возложены обязанности но координации, организационно-методическому руководству, разработке и финансированию научно-технических программ, лицензированию деятельности предприятий и сертификации продукции.

В настоящее время защита секретной информации в автоматизированных системах осуществляется Федеральной службой по техническому и экспортному контролю (ФСТЭК), созданной но Указу Президента РФ от 01.01.2001 г. № 000 «О системе и структуре федеральных органов исполнительной власти».

В состав государственной системы ЗИ входят системы лицензирования деятельности предприятий по оказанию услуг в области защиты информации и сертификации продукции по требованиям безопасности информации.

Система лицензирования направлена на создание условий, при которых право заниматься работами по защите информации предоставляется только организациям, имеющим соответствующее разрешение (лицензию) на этот вид деятельности. А система сертификации технических и программных средств по требованиям безопасности информации направлена на защиту потребителя продукции и услуг от недобросовестной работы исполнителя. К сожалению, в этих вопросах Россия значительно отстала от развитых зарубежных стран.

Важным организационным документом системы защиты информации (СЗИ) является «Положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ». Этим документом установлен единый в стране порядок исследований, разработок, введения в действие и эксплуатации защищенных от НСД средств автоматизации.

Исходя из практических потребностей, в Положении определены различные варианты разработки защищенных средств ВТ. среди которых предусматривается:

- разработка защищенного общепрограммного обеспечения (ОНО) - ОС, СУБД, сетевого ПО;

- разработка защищенных программных средств (ПС) на базе ОНО, находящегося в эксплуатации и поставляемого вместе с незащищенными СВТ;

- разработка защищенных ПС на базе импортных программных прототипов.

2. Морально-этические меры

К морально-этическим мерам противодействия угрозам безопасности относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаными (например, общепризнанные нормы честности, патриотизма и т. д.), так и оформленными в некий свод (кодекс) правил или предписаний. Например, "Кодекс профессионального поведения членов Ассоциации пользователей

ЭВМ США" рассматривает как неэтичные действия, которые умышленно или неумышленно:

- нарушают нормальную работу компьютерных систем;
- вызывают неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т. п.);
- нарушают целостность информации (хранимой и обрабатываемой);
- нарушают интересы других законных пользователей и т. н.

Социально-психологическое обеспечение ЗИ во многом зависит также от своевременной проверки благонадежности, от расстановки работников в соответствии с их способностями и личными качествами, формирования у каждого члена коллектива осознанного понимания важности и необходимости соблюдения требований режима конфиденциальности. Идеальным считается работник, обладающий такими личными качествами, как честность, принципиальность (строгое следование основным правилам), исполнительность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная оценка собственных возможностей и способностей, умеренная склонность к риску, осторожность, умение хранить секреты, тренированное внимание, неплохая память.

Меньше всего утечек информации наблюдается в Японии, что связано с системой «пожизненного найма», и воспитанием чувств преданности и патернализма, когда работники одной организации считают себя членами единой, большой семьи.

В целом, нормативно-правовая база и моральные устои современного общества оказались не готовы к столь быстрому скачку в развитии информационных технологий, что проявилось прежде всего при интеграции России в единое информационное пространство Европы и мира с использованием сетей типа Интернет. В настоящее время отсутствуют способы и средства контроля ценности информационных ресурсов, транслируемых через границы (происходит утечка технологий и «ноу-хау»).

Для отработки механизма взаимодействия в информационном пространстве необходимо разработать законы, регулирующие отношения в этой области.

3. Административные меры

Административные меры защиты - это меры организационного характера. Они регламентируют:

- процессы функционирования системы обработки данных.
- использование ее ресурсов,
- деятельность персонала,

- порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т. н.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т. н.

Административные меры являются той основой, которая объединяет различные меры защиты в единую систему.

Выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты должно быть возложено на специальную службу - службу компьютерной безопасности.

Обязанности должностных лиц должны быть определены таким образом, чтобы при эффективной реализации ими своих функций, обеспечиваюсь разделение их полномочий и ответственности.

4. Физические и технические меры

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов).

- разграничение доступа к ресурсам, регистрацию и анализ событий, криптографическое закрытие информации.

- резервирование ресурсов и компонентов систем обработки информации и др.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

2.1. Практическое занятие №1,2 (4 часа)

Тема: «Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности»

2.1.1. Задание для работы:

1. Основные понятия, термины и определения.

2. Основы государственной политики в области информационной безопасности

2.1.2 Краткое описание проводимого занятия:

1. Основные понятия термины и определения.

Термин "*информационная безопасность*" может иметь различный смысл и трактовку в зависимости от контекста. ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

2. Основы государственной политики в области информационной безопасности

Основу правового обеспечения информационной безопасности России помимо нормативно-правовых актов составляют концептуальные документы. Они принимаются на уровне Президента РФ, Правительства РФ и других органов государственной власти. В частности, такими документами являются Доктрина информационной безопасности РФ и Стратегия национальной безопасности РФ до 2020 года.

Концепция (от лат. conceptio) - генеральный замысел, определяющий стратегию действий. Концепция защиты информации - это система взглядов на сущность, цели, принципы и организацию защиты информации.

Стратегия национальной безопасности до 2020 года была утверждена президентом Д. Медведевым 12 мая 2009 года. Стратегия – это "официально признанная система стратегических национальных приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу".

Документ содержит 6 разделов:

1. Общие положения

2. Современный мир и Россия: состояние и тенденции развития

3. Национальные интересы Российской Федерации и стратегические национальные приоритеты

4. Обеспечение национальной безопасности

5. Организационные, нормативные правовые и информационные основы реализации настоящей Стратегии

6. Основные характеристики состояния национальной безопасности в составе 112 отдельных пунктов

Задача обеспечения национальной безопасности признается комплексной задачей, для решения которой в Стратегии представлены следующие направления деятельности:

- Повышение качества жизни российских граждан;
- Экономический рост;
- Наука, технология и образование;
- Здравоохранение;
- Культура;
- Экология живых систем и рациональное природопользование.

В целом, Стратегия национальной безопасности РФ до 2020 года стала принципиально новым документом, основной целью которого является планирование

развития системы национальной безопасности, в том числе цели, меры и порядок действий для ее обеспечения. Стратегия стала своего рода ответом на новую международную обстановку и отразила взгляды и планы руководства РФ в отношении внешней политики.

Основополагающим концептуальным документом в области информационной безопасности является Доктрина информационной безопасности, утвержденная 9 сентября 2000 года. Доктрина информационной безопасности РФ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

В Доктрине выделены четыре составляющие национальных интересов в области информационных отношений:

- Соблюдение прав и свобод человека в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.;
- Информационное обеспечение внутренней и внешней государственной политики страны;
- Развитие информационных технологий в соответствии со временем;
- Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

1.1.3 Результаты и выводы:

Ознакомление с основными понятиями, терминами и определениями. С основами государственной политики в области информационной безопасности

2.2 Практическое занятие № 3, 4, 5 (6 часов).

Тема: Аттестация объектов информатизации по требованиям безопасности информации.

2.2.2 Задание для работы:

1. Общие сведения об аттестации.

2**.** Структура системы аттестации.

3. Порядок проведения аттестации.

2.2.2 Краткое описание проводимого занятия:

1. Общие сведения об аттестации

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России. Для начала дадим определение объекта информатизации.

Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа подтверждается, что *объект* соответствует требованиям стандартов или иных нормативно-технических документов по *безопасности информации*, утвержденных ФСТЭК России.

Аттестация является обязательной в следующих случаях:

- *государственная тайна*;
- при защите государственного информационного ресурса;
- управление экологически опасными объектами;
- ведение секретных переговоров.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня *работ*:

- анализ исходных данных по аттестуемому объекту *информатизации*;
- предварительное ознакомление с аттестуемым объектом *информатизации*;
- проведение экспертного обследования объекта *информатизации* и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте *информатизации* с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по *сертификации средств защиты информации* по *требованиям безопасности* информации;

- проведение комплексных аттестационных испытаний объекта *информатизации* в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта *информатизации* и утверждение заключения по результатам аттестации.

Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по *сертификации средств защиты информации* по *требованиям безопасности* информации".

Все *расходы* по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

2. Структура системы аттестации

В *структуру системы* аттестации входят:

- федеральный орган по *сертификации средств защиты информации* и аттестации объектов *информатизации* по *требованиям безопасности* информации – ФСТЭК России;
- органы по аттестации объектов *информатизации* по *требованиям безопасности* информации;
- испытательные центры (лаборатории) по *сертификации* продукции по *требованиям безопасности* информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов *информатизации*).

Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

- приемо-сдаточную документацию на объект *информатизации*;
- акты *категорирования* выделенных помещений и объектов *информатизации*;
- инструкции по эксплуатации *средств защиты информации*;
- технический паспорт на аттестуемый объект;
- документы на эксплуатацию (*сертификаты соответствия требованиям безопасности* информации) ТСОИ;
- *сертификаты соответствия требованиям безопасности* информации на ВТСС;

- *сертификаты соответствия требованиям безопасности* информации на технические средства защиты информации;
- акты на проведенные скрытые работы;
- протоколы измерения звукоизоляции выделенных помещений и эффективности *экранирования* сооружений и кабин (если они проводились);
- протоколы измерения величины сопротивления заземления;
- протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
- данные по уровню подготовки кадров, обеспечивающих защиту информации;
- данные о *техническом обеспечении* средствами контроля эффективности защиты информации и их метрологической поверке;
- нормативную и методическую документацию по защите информации и контролю эффективности защиты.

3. Порядок проведения аттестации

Порядок проведения аттестации объектов *информатизации* по *требованиям безопасности* информации включает следующие действия:

1. подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов *информатизации* по *требованиям безопасности*". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.

2. предварительное ознакомление с аттестуемым объектом – производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;

3. испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

4. разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.

5. заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

6. проведение аттестационных испытаний объекта *информатизации*.

2.2.3 Результаты и выводы:

Ознакомились с аттестацией объектов информатизации по требованиям безопасности информации.

2. 3 Практическое занятие № 6,7 (4 часа).

Тема: «Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне". Организационно-технические меры защиты сведений, составляющих государственную тайну.»

2.3.1 Задание для работы:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне".

2. Организационно-технические меры защиты сведений, составляющих государственную тайну.

2.3.2 Краткое описание проводимого занятия:

1. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В настоящем Законе используются следующие основные понятия:

- 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;

- носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

- система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений,

составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

- допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

- доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

- гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

- средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

2. Организационно-технические меры защиты сведений, составляющих государственную тайну.

Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

Главными направлениями работ по защите информации являются:

- обеспечение эффективного управления системой защиты информации;

- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;

- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

- разработка организационно-технических мероприятий по защите информации и их реализация;

- организация и проведение контроля состояния защиты информации.

2.3.3 Результаты и выводы

Ознакомились с законом РФ от 21.07.1993 N 5485-1 "О государственной тайне"; с организационно-техническими мерами защиты сведений, составляющих государственную тайну.

2. 4 Практическое занятие № 8,9 (4 часа).

Тема: «Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне". Организационно-технические меры защиты коммерческой тайны.»

2.4.1 Задание для работы:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

2. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

3. Организационно-технические меры защиты коммерческой тайны.

2.4.2 Краткое описание проводимого занятия:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

2. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

Принят Государственной Думой 9 июля 2004 года. Одобрен Советом Федерации 15 июля 2004 года.

Цели и сфера действия Федерального закона:

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

3. Организационно-технические меры защиты коммерческой тайны.

Меры по охране коммерческой тайны определены в Федеральном законе от 29.07.2004 N 98-ФЗ "О коммерческой тайне" в статье 10 «Охрана конфиденциальности информации»

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую

информацию, грифа "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).

2.4.3 Результаты и выводы:

Ознакомились с Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации, с Федеральным законом от 29.07.2004 N 98-ФЗ "О коммерческой тайне", с организационно-техническими мерами защиты коммерческой тайны.

2. 5 Практическое занятие № 10, 11 (4 часа).

Тема: «Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

2.5.1 Задание для работы:

1. Сведения не составляющие государственную тайну.

2. Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2.5.2 Краткое описание проводимого занятия:

1. Сведения не составляющие государственную тайну.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию определены в Законе РФ от 21.07.1993 N 5485-1 "О государственной тайне" в статье 7.

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.

2. Защита информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании».

2.5.3 Результаты и выводы:

Ознакомились с защитой информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2.6 Практическое занятие № 12, 13 (4 часа).

Тема: «Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

2.6.1 Задание для работы:

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2.6.2 Краткое описание проводимого занятия:

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), 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.

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных,

нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

- регистрация событий безопасности;

- антивирусная защита;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

-выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

2.6.3 Результаты и выводы:

Ознакомились с ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных", с требования к защите персональных данных при их обработке в информационных системах персональных данных, с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. 7 Практическое занятие № 14, 15 (4 часа).

Тема: «Нормативно-правовые, морально-этические, административные, физические и технические меры»

2.7.1 Задание для работы:

1. Нормативно-правовые меры.

2. Морально-этические меры.

3. Административные меры.

4. Физические и технические меры

2.7.2 Краткое описание проводимого занятия:

1. Нормативно-правовые меры.

К нормативно-правовым мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией, закрепляющие нрава и обязанности участников информационных

отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Нормативно-правовые меры направлены на решение следующих вопросов:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий но доступу к информации;
- нрава должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

2. Морально-этические меры

К морально-этическим мерам противодействия угрозам безопасности относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаными (например, общепризнанные нормы честности, патриотизма и т. д.), так и оформленными в некий свод (кодекс) правил или предписаний.

Социально-психологическое обеспечение ЗИ во многом зависит также от своевременной проверки благонадежности, от расстановки работников в соответствии с их способностями и личными качествами, формирования у каждого члена коллектива осознанного понимания важности и необходимости соблюдения требований режима конфиденциальности. Идеальным считается работник, обладающий такими личными качествами, как честность, принципиальность (строгое следование основным правилам), исполнительность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная оценка собственных возможностей и способностей, умеренная склонность к риску, осторожность, умение хранить секреты, тренированное внимание, неплохая память.

3. Административные меры

Административные меры защиты - это меры организационного характера. Они регламентируют:

- процессы функционирования системы обработки данных.

- использование ее ресурсов,

- деятельность персонала,

- порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;

- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);

- мероприятия, осуществляемые при подборе и подготовке персонала системы;

- организацию охраны и надежного пропускного режима;

- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т. н.);

- организацию явного и скрытого контроля за работой пользователей;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т. н.

4. Физические и технические меры

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов).

- разграничение доступа к ресурсам, регистрацию и анализ событий, криптографическое закрытие информации.

- резервирование ресурсов и компонентов систем обработки информации и др.

2.7.3 Результаты и выводы:

Ознакомились с нормативно-правовыми, морально-этическими, административными, физическими и техническими мерами.