ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра мультисервисных сетей и информационной безопасности

А.В. Крыжановский

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания к практическим занятиям

Самара

2018

УДК 681.3.067

ББК 32.973-018.2

К

Рекомендовано к изданию методическим советом ПГУТИ, протокол №62, от 15.05.2018 г.

Рецензент:

заведующий кафедрой АЭС ФГБОУ ВО ПГУТИ,

д.т.н., проф. Росляков А.В.

Крыжановский, А.В.

К Организационное и правовое обеспечение информационной безопасности: методические указания к практическим занятиям/ А.В. Крыжановский– Самара: ПГУТИ, 2018. – 86 с.

Методические указания разработаны в соответствии ФГОС ВО направлений подготовки 10.05.02 (ИБТС) и 10.03.01 (ИБ) и предназначены студентам факультета ТР для методического обеспечения проведения практических занятий по дисциплине «Организационное и правовое обеспечение информационной безопасности» с целью закрепления полученных теоретических знаний, выработки умения применять действующую законодательную базу в области информационной безопасности, а также получения практических навыков по созданию систем защиты информации.

Содержится материал по организационным и правовым аспектам защиты информации, раскрывающий основные положения нормативно-правовых актов информационного права, принципы и методы создания систем информационной безопасности.

При подготовке методических указаний использованы раздаточные материалы, любезно предоставленные доцентом кафедры « Безопасность информационных систем» Самарского государственного университета Родичевым Юрием Андреевичем, за что выражаю ему самую искреннюю благодарность.

Содержание

Введение

Современное понятие защиты информации находится в центре внимания исследователей в различных странах уже несколько десятков лет и ассоциируется, как правило, с проблемами создания систем защиты информации на различных уровнях её использования. Несмотря на то, что существует еще большое количество неразрешенных и спорных вопросов в теории информационной безопасности, в настоящее время сложилась типовая структура системы защиты информации, используемая большинством развитых стран мира.

Под ***защитой информации*** в общем виде понимают соединение в единое целое отдельных элементов, механизмов, процессов, явлений, мероприятий, мер и программ их взаимосвязей, способствующих реализации целей защиты и обеспечению структурного построения системы защиты.

Структурно-типовая система защиты информации (рис.В.1) представляет собой совокупность отдельных взаимосвязанных элементов, реализующих следующие её виды:

Правовая защита информации – защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая защита информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является основой для морально – этических норм в области защиты информации [2].

Организационная защита информации – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание *системы защиты,* побуждающих персонал соблюдать правила защиты конфиденциальной информации. Организационные меры связаны с установлением *режима конфиден-*

циальности в организации.

Техническая или ***инженерно-техническая*** защита, основывающаяся на использовании технических устройств, узлов, блоков, элементов, систем, как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации, сооружений и т.д.;

Программно-аппаратная защита, предполагающая использование программного обеспечения информационных систем, комплексов и систем, а также аппаратных устройств, встроенных в состав технических средств и систем обработки информации.

В качестве отдельного вида наиболее эффективных средств защиты информации выделяются ***математические*** или ***криптографические*** *методы,* которые могут быть реализованы в виде технических устройств, программ и программно-аппаратных средств.

Рассмотренные виды в основном обеспечивают надежную защиту информации в различных системах ее обработки и различных условиях их функционирования. Однако опыт практического обеспечения безопасности информации в России и за рубежом показывает, что для надежной защиты, в условиях обязательного участия человека, массовости решения задач защиты необходимо использовать психологические и морально-этические виды, а в ряде случаев и страховые.

Под ***психологическими*** видами защиты понимаются допускаемые нормами права и морали методы и средства изучения психофизиологических особенностей и возможностей людей, а также психологического воздействия на людей с целью оценки соответствия их требованиям для допуска к обработке защищаемой информации.

Под ***морально-этическими*** видами защиты понимаются нормы и правила, которые не имеют юридической силы, но их нарушение ведет к

потере авторитета, возникновению дополнительных трудностей и другим негативным последствиям для человека и организации [3].

Страховая защита информации – защита информации, предусматривающая возмещение убытков от её уничтожения или модификации путем получения страховых выплат.

Очевидно, что в ряде стран при построении систем защиты в типовую модель вносят изменения. Так, во Франции элементы правовой и организационной защиты информации рассматривают в едином ракурсе, а в программно-аппаратной защите наоборот выделяют отдельно программные и аппаратные методы и средства защиты информации.

Среди перечисленных видов защиты базовыми являются правовая, организационная и техническая защита информации.

1 Структура государственной системы обеспечения информационной безопасности в РФ

Нормативно – правовое обеспечение информационной безопасности представляет собой совокупность законодательных актов и нормативов, регламентирующих общую организацию работ по защите информации, создание и функционирование систем защиты информации. Организационное обеспечение информационной безопасности состоит из системы государственных органов и должностных лиц, ответственных за организацию работ и обеспечение информационной безопасности, а также контролирующих и судебных органов, осуществляющих надзор и решение правовых вопросов в данной области.

Организационная структура системы обеспечения информационной безопасности представлена на рис.1.1.

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры по координации работ в области информационной безопасности.

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры по координации работ в области информационной безопасности.

Основным международным органом является Организация Объединенных Наций и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбе с преступлениями в сфере информационных технологий. Спорные вопросы на межгосударственном уровне решает международный суд.

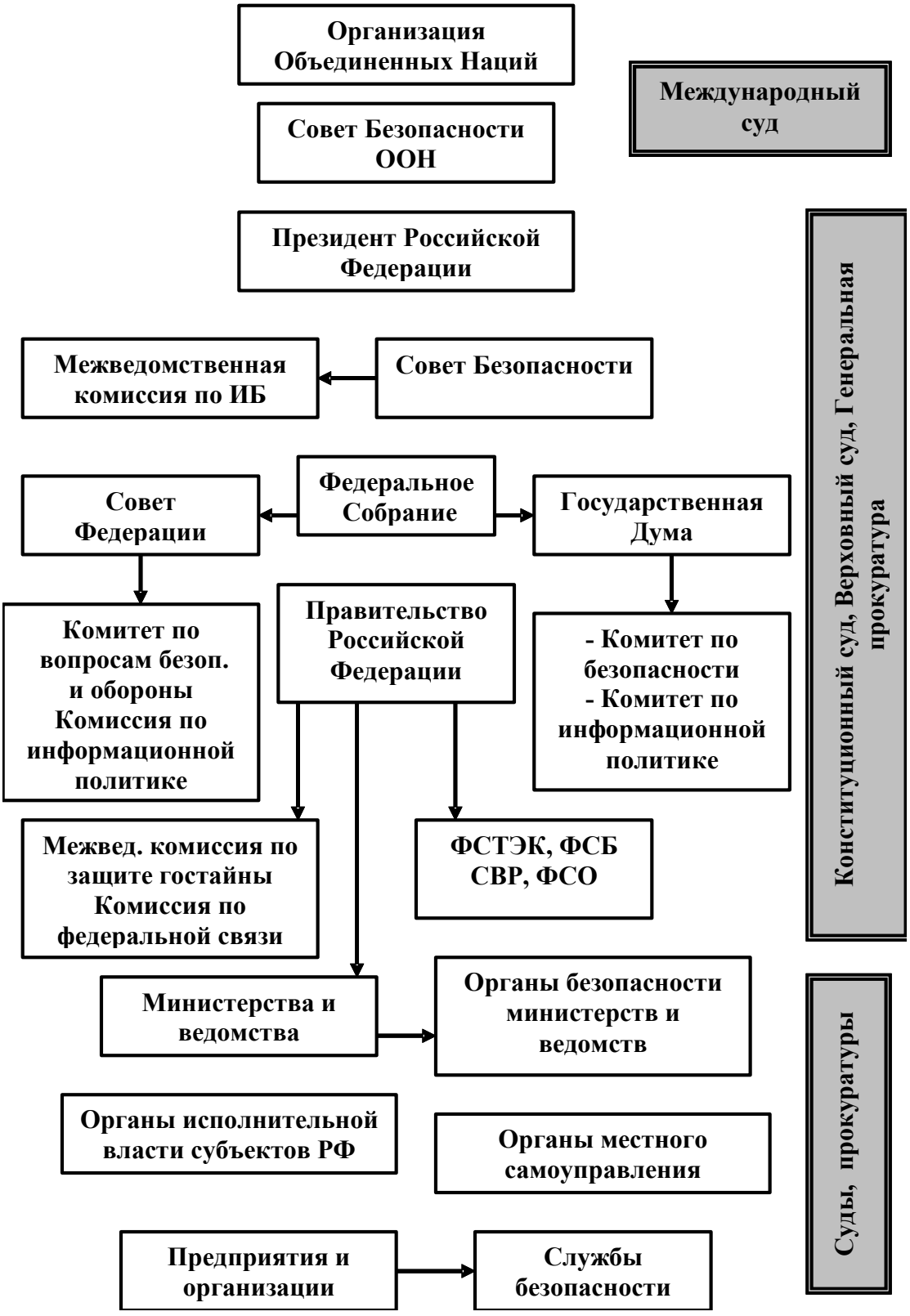

Рис. 1.1- Структура органов обеспечения информационной безопасности

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального уровня, уровня субъектов Российской Федерации, ведомственных структур, а также служб предприятий и организаций.

Основными элементами организационной структуры системы обеспечения информационной безопасности Российской Федерации на федеральном уровне являются: Президент Российской Федерации, Совет Безопасности, Совет Федерации, Государственная Дума, Правительство Российской Федерации, федеральные органы исполнительной власти, государственные и межведомственные комиссии, создаваемые Президентом и Правительством Российской Федерации для решения вопросов в соответствии с предоставленными им полномочиями, определяемыми Положениями о комиссиях.

Федеральные министерства и ведомства могут в своем составе создавать соответствующие службы и подразделения для решения вопросов обеспечения информационной безопасности на отраслевом уровне.

Контролирующими и правоохранительными органами федерального уровня, обеспечивающими соблюдение нормативно – правовых норм, являются: Конституционный суд, Верховный суд, Генеральная прокуратура.

Следующим уровнем в системе обеспечения информационной безопасности являются органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, которые могут также создавать различные комиссии. Нижним уровнем системы обеспечения информационной безопасности являются структурные подразделения и должностные лица предприятий и организаций.

Информацию об органах государственной власти Российской Федерации можно получить на информационном портале «Сервер органов государственной власти Российской Федерации» http://www.gov.ru. Он со-

держит ссылки на сайты федеральных и региональных органов исполнительной власти, а также сайты Президента, Федерального Собрания (Совета Федерации и Государственной думы), Совета Безопасности, Генеральной прокуратуры, Конституционного, Верховного и Арбитражного судов Российской Федерации, Счетной Палаты, Центральной избирательной комиссии.

Президент Российской Федерации (http://www.kremlin.ru) в пределах своих полномочий создает, реорганизует и руководит органами по обеспечению информационной безопасности, определяет приоритетные направления государственной политики в данной области.

Совет Безопасности Российской Федерации (http://www.scrf.gov.ru) является конституционным совещательным органом, осуществляющим подготовку решений Президента Российской Федерации по вопросам обеспечения защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики в области обеспечения национальной (в том числе информационной) безопасности.

Правовую основу деятельности Совета Безопасности составляют Конституция Российской Федерации, федеральные законы Российской Федерации, международные договоры Российской Федерации, указы и распоряжения Президента Российской Федерации, а также Положение о Совете Безопасности, утверждаемое Президентом Российской Федерации.

Совет Безопасности проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, разрабатывает важнейшие концептуальные документы в области национальной безопасности и предложения в области обеспечения информационной безопасности, координирует деятельность органов по обеспечению информационной безопасности, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Россий-

ской Федерации решений Президента в этой области.

Указом президента от 28 октября 2005 года № 1244 «Об утверждении Положения о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности» (с изменениями от 12 июня 2006 года) утверждено Положение о специальной Межведомственной комиссии при Совете Безопасности по информационной безопасности.

Палаты Федерального Собрания (Совет Федерации и Государственная Дума) формируют систему законодательных актов в области информационной безопасности в соответствии с Конституцией Российской Федерации.

Совет Федерации имеет комитет по вопросам безопасности и обороны и комиссию по информационной политике. Комиссия по информационной политике создана Постановлением Совета Федерации от 30 января 2002 года № 106. Ее создание было обусловлено необходимостью детального изучения и мониторинга информационной ситуации, а также требованиями дальнейшего совершенствования законодательной базы в интересах большей ее ориентации на формирование единого информационного пространства, решения других вопросов информационной политики Российской Федерации.

К предмету ведения комиссии были отнесены следующие вопросы правового обеспечения:

- государственная политика в сфере средств массовой информации, информационных технологий и информатизации;

- развитие единого информационного пространства Российской Федерации;

- издательская и полиграфическая деятельность;

- информационный обмен, развитие компьютерных сетей общего пользования;

- распространение периодических изданий, книжной и иной печатной, аудио- и видеопродукции;

- межгосударственное сотрудничество в информационной сфере.

В составе Государственной Думы сформированы два комитета: Комитет по безопасности и Комитет по информационной политике.

Правительство Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, обеспечивает разработку и реализацию федеральных программ в области информационной безопасности.

Функции Правительства определены Федеральным Конституционным законом «О правительстве Российской Федерации» от 17 декабря 1997 года № 2-ФКЗ с последующими уточнениями и изменениями конституционными законами от 31.12.1997 № 3-ФКЗ, от 19.06.2004 № 4-ФКЗ, от 03.11.2004 № 6-ФКЗ, от 01.06.2005 № 4-ФКЗ, от 30.01.2007 № 1-ФКЗ, от 02.03.2007 № 3-ФКЗ.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства, решений Президента и Правительства Российской Федерации в области обеспечения информационной безопасности. В пределах своей компетенции они разрабатывают нормативные правовые акты в области информационной безопасности и представляют их в установленном порядке Президенту и в Правительство Российской Федерации.

Указом Президента Российской Федерации от 20 мая 2004 года № 649 «Структура федеральных органов исполнительной власти» (в ред. Указов Президента от 28.07.2004 N 976, от 13.09.2004 N 1168, от 11.10.2004 N 1304, от 18.11.2004 N 1453, от 01.12.2004 N 1487, от 22.07.2005 N 855, от 05.09.2005 N 1049, от 03.10.2005 N 1158, от 11.05.2006 N 473, от 30.06.2006 N 658, от 05.02.2007 N 119, от 12.03.2007 N 320) утверждены следующие службы, связанные с обеспечением информационной безопасности: Федеральная служба по техническому и экспортному

контролю, Федеральная служба безопасности, Федеральная служба охраны, Служба внешней разведки.

Межведомственные и государственные комиссии, создаваемые Президентом и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Указом Президента Российской Федерации от 8 ноября 1995 года № 1108 создана Межведомственная комиссия по защите государственной тайны, которая является основным органом, координирующим действия государственных структур по вопросам защиты информации. Указом Президента от 6 октября 2004 года № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны» заново определены основные направления работы комиссии. Постановлением Правительства от 3 декабря 2004 года № 728 «О персональном составе Межведомственной комиссии по защите государственной тайны» определен персональный состав комиссии.

Постановлением Правительства Российской Федерации от 13 апреля 2006 года № 213 «О правительственной комиссии по федеральной связи» создана специальная комиссия по федеральной связи и утверждено Положение о комиссии. К основным функциям Комиссии относится определение приоритетов в реализации основных направлений развития федеральной связи с учетом задач государственного управления, обороны и безопасности государства, обеспечения правопорядка, координация деятельности федеральных органов исполнительной власти по развитию российской инфраструктуры связи, обеспечению ее интеграции с международными сетями связи, развитию технологий и средств защиты информации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства, решений Президента и Правитель-

ства Российской Федерации в области обеспечения информационной безопасности, а также по вопросам реализации федеральных программ в этой области. Совместно с органами местного самоуправления они осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности, вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности.

Органы судебной власти и прокуратуры осуществляют правосудие по делам о преступлениях, связанных с информационной сферой.

2 Структура нормативных правовых актов в области информационной безопасности

Правовое обеспечение информационной безопасности заключается в исполнении существующих или введении новых законов, постановлений и других документов, регулирующих юридическую ответственность должностных лиц, технических специалистов и пользователей за действия (или бездействие), повлекшие утечку, утрату или модификацию защищаемой информации, а также злоумышленников за совершение преднамеренного несанкционированного доступа к информации и нарушение процессов ее обработки.Всякий документ (акт), принятый уполномоченным законом органом или лицом, является правовым, поскольку он регулирует правовые отношения. Принятые правовые документы могут быть обязательными для исполнения, либо носить рекомендательный характер.

Обязательные для исполнения акты являются нормативными правовыми актами.

Международные, государственные и ведомственные нормативные акты регламентируют основные понятия и концепции информационной безопасности на межгосударственном и государственном уровне, что позволяет ввести единые стандарты и критерии в области защиты информации. В соответствии со статьей 15 Конституции Российской Федерации «Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора».

Структуру нормативных правовых актов в области информационной безопасности можно представить в виде схемы, изображённой на рис. 2.1.

Рис. 2.1- Структура нормативно-правовых актов в области информационной безопасности

Современная база международных актов в области информационной безопасности включает в себя декларации, конвенции, соглашения, рекомендации, а также стандарты. Основными целями использования международных документов являются:

1 Приведение отечественных нормативных документов в области защиты информации в соответствие с международными.

2 Выработка государственной политики в области информатизации в соответствии с мировыми тенденциями развития глобального информационного общества.

3 Предоставление отечественным разработчикам информационных технологий средств и методов создания аппаратно-программных средств и технологий, соответствующих международным стандартам и делающих их конкурентоспособными на международном рынке товаров и услуг.

4 Предоставление соответствующим специалистам правил и критериев оценки защищенности информационных технологий для различных сфер применений.

5 Подготовка кадров специалистов в области информатизации и информационной безопасности, соответствующих современным потребностям глобального информационного общества.

Информационное обеспечение управленческих, финансовых, технологических и производственных бизнес-процессов является основой экономической устойчивости организации, а информация становится важным корпоративным ресурсом, который необходимо защищать.

Для обеспечения конфиденциальности, целостности и доступности информации, а также сохранения устойчивости функционирования информационных систем в условиях угроз, реализуемых посредством целенаправленных деструктивных информационных воздействий на критически важные объекты информационной инфраструктуры, в организации формируются требования к обеспечению ИБ.

Формирование требований к обеспечению ИБ осуществляется с учетом:

– юридических, законодательных, регулирующих и договорных требований, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг;

– результатов оценки рисков организации. Посредством оценки рисков осуществляется выявление актуальных угроз активов организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;

– принципов и целей в отношении обработки информации, определенных организацией.

Формирование требований к обеспечению ИБ организации и информационных систем осуществляется с учетом нормативных и правовых актов РФ, а также с учетом разработанных стандартов и рекомендаций, апробированных на практике и признанных профессиональными сообществами специалистов в области ИБ.

Законодательную и нормативную базу в области обеспечения ИБ в РФ можно представить как совокупность правовых актов, организационно-распорядительных, нормативных, методических и отраслевых документов по технической защите информации.

Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств . Важно обратить внимание, что техническая защита – это не только защита от утечки информации по техническим каналам утечки, но и защита от НСД, от математического воздействия, от вредоносных программ и т.п. Объектами технической защиты информации могут быть:

— объект информатизации;

— информационная система;

— ресурсы информационной системы;

— информационные технологии;

— программные средства;

— сети связи.

Законодательная и нормативная база в области обеспечения ИБ РФ представлена на рис.2.2.

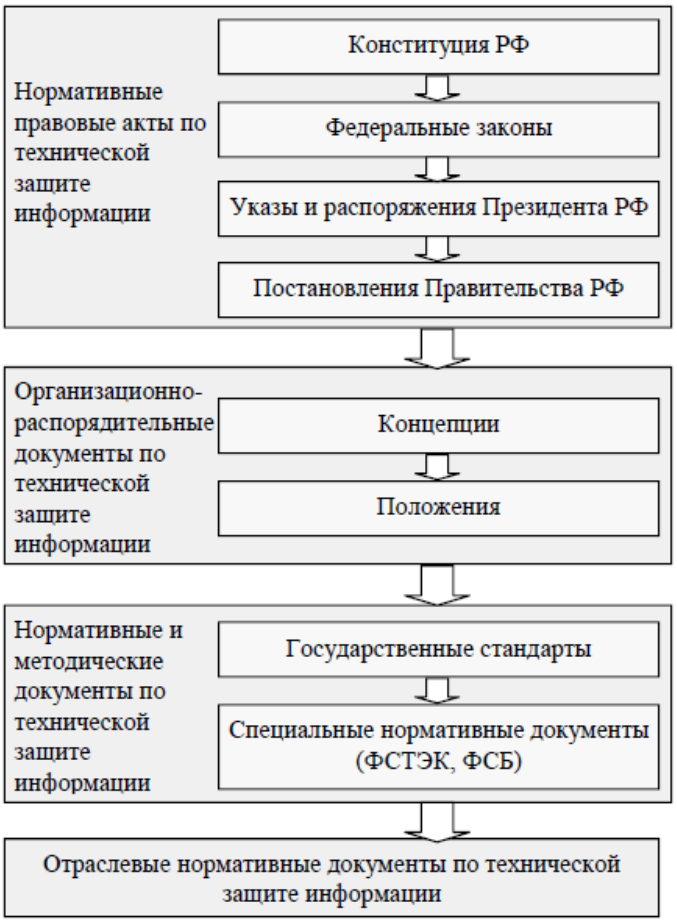

Рис.2.2 – Законодательная и нормативная база в области обеспечения ИБ РФ

Нормативный правовой акт – это письменный официальный документ, принятый (изданный) в определенной форме правотворческим орга-

ном в пределах его компетенции и направленный на установление, изменение или отмену правовых норм.

Все нормативные документы, действующие в настоящее время в Российской Федерации можно разделить по типу на две группы.

1. Документы, составляющие нормативную правовую базу и определяющие правовое пространство в области информатизации и защиты информации (федеральные законы, кодексы, указы президента, постановления правительства).

2. Документы, составляющие нормативно-техническую базу в области информационных технологий и защиты информации (стандарты, критерии, и другие документы, непосредственно определяющие организационные и технические требования по защите информации, порядок их выполнения и контроля эффективности принимаемых мер защиты).

По назначению все документы федерального уровня можно разделить на следующие группы.

1. Документы, составляющие концептуальную основу защиты информации.

2. Пакет федеральных законов и кодексов, определяющих систему защиты информации.

3. Пакет нормативных правовых актов в виде указов Президента, постановлений Правительства Российской Федерации, межведомственных и ведомственных (отраслевых) руководящих документов и стандартов, регулирующих механизмы исполнения требований к системе обеспечения информационной безопасности государства.

Среди документов федерального уровня следует особо отметить документы, регламентирующие порядок лицензирования деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием и сертификацией средств защиты информации.

Ведомственные нормативные документы разрабатываются в целях развития и конкретизации положений федеральных документов по защите информации, с учетом ведомственной (отраслевой) специфики.

Органы законодательной и исполнительной власти субъектов Российской власти, а также органы местного самоуправления в пределах своей компетенции, также могут разрабатывать нормативные правовые акты в области информационной безопасности. Указанные акты не должны противоречить соответствующим актам федерального и международного уровня.

Согласно требованиям нормативно-правовых документов на предприятиях и в учреждениях должен также действовать комплекс мер по обеспечению защиты информации. Этот комплекс должен основываться на нормативно-правовых и нормативно-технических документах в области защиты информации федерального и отраслевого уровней.

Нормативные документы уровня предприятия, учреждения или организации, разрабатываются в дополнение и в целях конкретизации нормативных правовых актов, нормативной и методической документации технического характера отраслевого уровня. В состав документов уровня предприятия входит также проектная и эксплуатационная документация по создаваемым и эксплуатируемым объектам информатизации, инструкции и регламенты по эксплуатации информационных систем и средств защиты, а также организационно-распорядительная документация предприятия (приказы, распоряжения, должностные инструкции сотрудников и др.).

В связи с возрастанием важности задач обеспечения информационной безопасности многие предприятия разрабатывают и утверждают в виде специального документа концепцию информационной безопасности. На основании концепции затем разрабатывается политика безопасности, которая конкретизирует положения концепции применительно к конкрет-

ным функциональным подсистемам единой информационной системы предприятия

3 Основные нормативно-правовые документы Российской Федерации в области защиты информации

Система нормативных правовых актов Российской Федерации в области информационной безопасности состоит из нескольких уровней от международного до уровня предприятия. К числу международных актов относятся документы, которые подписаны от имени Российской Федерации. Ниже приведен список основных нормативных правовых документов, касающихся защиты информации.

3.1Международные документы

1. «Конвенция, учреждающая Всемирную организацию интеллектуальной собственности» (Стокгольм, 1967. Вступила в силу для СССР 26.04.1970).
2. «Всемирная конвенция об авторском праве» (Женева, 6 сентября 1952 года. Пересмотрена в Париже 24 июля 1971 года. Вступила в силу для СССР 27 мая 1973 года).
3. «Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года». Российская Федерация присоединилась 13 марта 1995 года.
4. «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» Ратифицирована законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ.
5. «Окинавская Хартия глобального информационного общества» Окинава. 22 июля 2000 года.

6. Декларация принципов. «Построение информационного общества – глобальная задача в новом тысячелетии». Всемирная встреча на высшем уровне по вопросам информационного общества. Женева. 10 декабря 2003 года.
7. «Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций» (Рим, 26 октября 1961 г. Вступила в силу для Российской Федерации 26 мая 2003 года).
8. «Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм» (Женева, 29 октября 1971 г.; вступила в силу для Российской Федерации 13.03.1995 г.).
9. «Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации» (Минск 1.06.2001)

Ратифицировано Российской Федерацией законом 164-ФЗ от 1.10.2008 г. со следующей оговоркой:

«Российская Федерация оставляет за собой право отказать в исполнении запроса полностью или частично, если исполнение запроса может нанести ущерб ее суверенитету или безопасности.».

Конвенция Совета Европы о компьютерных преступлениях. СДСЕ № 185. (Будапешт. Открыта для подписания 23.11.2001, вступила в силу 1.07.2004. Не подписана Российской Федерацией).

3.2 Зарубежные нормативы

«Оранжевая книга» – гос. стандарт США «Критерии оценивания безопасности надежных вычислительных систем» (1984г.).

«Европейские критерии безопасности информационных технологий» (1991 г.).

«Федеральные критерии безопасности информационных технологий» США.

«Канадские критерии безопасности компьютерных систем»(1993г.)

«Единые критерии оценивания безопасности информационных технологий» (Великобритания, Германия, Канада, Нидерланды, США, Франция 1997 г.)

Единый международный стандарт оценивания безопасности информационных технологий (ISO/IEC 15408: 1999 «Общие критерии») ISO/IEC 15408:2002 ISO/IEC 15408:2005 ISO/IEC 15408:2008

«**Общие критерии»** обобщили содержание и опыт использования «Оранжевой книги» и ее интерпретаций. «Общие критерии» - наиболее полная на сегодняшний день совокупность требований безопасности информационных технологий. Соглашение о взаимном признании оценок, полученных на основе Общих критериев подписали 26 стран (на 31.12.2013 г.). В рамках Соглашения в 17 странах действуют аккредитованные органы по сертификации.

Аналоги в России: ГОСТ Р ИСО/МЭК 15408:2002 ГОСТ Р ИСО/МЭК 15408:2005 ГОСТ Р ИСО/МЭК 15408:2008

Руководящие документы Гостехкомиссии РФ (ч. 1, 2,3): «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Введены Приказом Гостехкомиссии от 19.06.2002 г. № 187)

Часть 1 РД определяет виды требований безопасности, основные конструкции представления требований безопасности и содержит основные методические положения по оценке безопасности ИТ.

Часть 2 РД содержит каталог функциональных требований безопасности.

Часть 3 РД содержит каталог требований доверия к безопасности и оценочные уровни доверия.

ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасносности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.

Часть 2. Функциональные требования безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ.

Часть 3. Требования доверия к безопасности.

Гостехкомиссией России в 2003 году разработан ряд **методических документов** в соответствии со стандартом ГОСТ Р ИСО/МЭК 15408:

Руководство по разработке профилей защиты и заданий по безопасности.

Положение по разработке профилей защиты и заданий по безопасности.

Руководство по формированию семейств профилей защиты

Руководство по регистрации профилей защиты

Последние версии стандартов ГОСТ Р ИСО/МЭК 15408:

ГОСТ Р ИСО/МЭК 15408-1-2012 ГОСТ Р ИСО/МЭК 15408-2-2013
ГОСТ Р ИСО/МЭК 15408-3-2013

Российские стандарты по менеджменту ИБ:

ГОСТ Р ИСО/МЭК 27001-2006 аналог ISO/IEC 27001:2005
ГОСТ Р ИСО/МЭК 27002-2012 аналог ISO/IEC 27002:2005

Российские стандарты по безопасности сетей:

ГОСТ Р ИСО /МЭК 27033-1-2011 аналог ISO/IEC 27033-1:2009

ГОСТ Р ИСО /МЭК 27033-3-2014 аналог ISO/IEC 27033-3:2010

3.3 Концептуальные документы Российской Федерации

1. «Конституция Российской Федерации» от 12 декабря 1993 года.
2. «Доктрина информационной безопасности Российской Федерации». Утверждена Указом Президента Российской Федерации от 5.12.2016 № 646.
3. «Концепция национальной безопасности Российской Федерации». Утверждена Указом Президента Российской Федерации от 10.01.2000 № 24).
4. «Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года». Распоряжение Правительства РФ от 27 сентября 2004 г. № 1244-р.
5. «Концепции создания системы персонального учета населения Российской Федерации». Утверждена Распоряжением Правительства РФ от 9 июня 2005 года № 748-р.
6. «Концепция региональной информатизации до 2010 года». Одобрена распоряжение Правительства РФ от 17 июля 2006 г. № 1024-р.
7. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением Государственной технической комиссии от 30 марта 1992 года.
8. Стратегия развития информационного общества в Российской Федерации на период 2017-2030 годы. Утверждена Указом Президента РФ № 203 от 9.05.2017 г.

9. «Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года», утверждена распоряжением Правительства РФ от 17.11.2008 г. № 1662-р;

10. Концепция развития национальной системы стандартизации РФ на период до 2020 года (одобрена распоряжением Правительства РФ от 24.09.2012 г. N 1762-р).
11. Государственная Программа Российской Федерации «Инфор – мационное общество (2011 - 2020 годы)» (распоряжением Прави - тельства РФ от 20.10.2010 № 1815-р;
12. «Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года.» Распоряжение Правительства от 1.11.2013 г. № 2036-р
13. Основы государственной политики Российской Федерации в облас ти международной информационной безопасности на период до 2020 года. (Утверждены Президентом РФ 24 июля 2013 г., № Пр-1753)
14. Стратегия национальной безопасности Российской Федерации Утверждена Указом Президента РФ № 683 от 31.12.2015 г.
15. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Утверждена Президентом РФ 12 декабря 2014 г. № К 1274.

3.4 Федеральные законы Российской Федерации

1. «О средствах массовой информации» № 2124-1. от 27 декабря 1991 года.
2. «Об оперативно-розыскной деятельности» 144-ФЗ от 12 августа 1995 года.

3. «Уголовный кодекс Российской Федерации» № 63-ФЗ от 13.06.1996 .
4. «О лицензировании отдельных видов деятельности» № 99-ФЗ от 4.05.11.

Утратил силу № 128-ФЗ от 8.08.2001 «О лицензировании отдельных видов деятельности».

5. «Кодекс РФ об административных правонарушениях» от 30.12.2001.
6. «Трудовой Кодекс Российской Федерации» от 30.12.2001.
7. «О Федеральной службе безопасности» № 40-ФЗ от 3 апреля 1995 года .
8. «О внешней разведке» № 5-ФЗ от 10 января 1996 года
9. «Об электронной подписи» № 63-ФЗ.от 6.04.2011

Утратил силу закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ

10. «О техническом регулировании» № 184-ФЗот 27.12.2002

Утратили силу:

«О сертификации продукции и услуг» № 5151-1 от 10.06.1993 г.

«О стандартизации» № 5154-1 от 10.06.1993 г.

9. «О персональных данных» от 27.07.2006 № 152-ФЗ.
10. «О рекламе» № 38-ФЗ от 13.03.2006
11. О государственной тайне № 5485-1 от 21.07.1993
12. О коммерческой тайне № 98-ФЗ от 29.07.2004
13. «О защите детей от информации, причиняющей вред их здоровью и развитию» № 436-ФЗ от 29.12.2010. Вступил в силу 1.09.2012.
14. «Гражданский кодекс Российской Федерации» от 30.11.1994 (ч. 4 вступила в силу с 1 января 2008 года)

Утратили силу законы:

от 23.09.1992 № 3520-1 "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров";

от 23.09.1992 № 3523-1 "О правовой охране программ для электрон-

ных вычислительных машин и баз данных";

от 23.09.1992 № 3526-1 "О правовой охране топологий интегральных микросхем";

от 9.07.1993 № 5351-1 “Об авторском праве и смежных правах”;

от 23.09.1992 № 3517-1 «Патентный закон».

15. «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Утратили силу законы:

«Об информации, информатизации и защите информации» от 20.02.1995;

«Об участии в международном информационном обмене» от 4.06.1996

16. «О связи» от 07.07.2003 № 126-ФЗ (ред. от 21.07.2014)

Утратил силу закон «О связи» от 16.02.1995 г. № 15-ФЗ.

17. «О национальной платежной системе» от 27.06.2011 № 161-ФЗ.

18. «О стандартизации в Российской Федерации» от 29.06.2015 № 162-ФЗ .

19. «О безопасности критической информационной инфраструктуры Российской Федерации».Принят 26.07.2017 г. № 187-ФЗ (вступ. в силу с 1.01.2018 г.).

3.5 Структура законодательства в области ИБ:

- об информации, информационных технологиях и о защите информации;
- о персональных данных;
- об интеллектуальной собственности;
- о тайнах;
- о связи и Интернет;
- о техническом регулировании;
- об электронной подписи;

- о лицензировании деятельности в области ИБ;

- о средствах массовой информации и рекламе;

новое направление:

- о безопасности критической информационной инфраструктуры.

Нормативная правовая база по каждому направлению состоит из одного или нескольких базовых федеральных законов и нормативных документов федеральных органов государственной власти.

Доктрина информационной безопасности РФ-совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ: осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно- технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления

Средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности

4 Структура информационных ресурсов

Анализ определений понятий «информация» и «информационный ресурс», приведенных в различных источниках, показывает, что в настоящее время отсутствует их единое общепринятое определение.

В Федеральном Законе 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» дано определение информации, как сведения (сообщения, данные) независимо от формы их представления.

В литературе приводится ряд классификаций информации по различным признакам и критериям.

В данном разделе приведена классификация информации (информационных ресурсов) с точки зрения ее правового статуса (Рис. 4.1). Основанием для такой классификации является трактовка информации в ряде Федеральных законов Российской Федерации, Указов Президента и постановлений правительства.

В соответствии с Федеральным законом 149-ФЗ вся информация в зависимости от категории доступа к ней делится на общедоступную и ограниченного доступа. Информация в зависимости от порядка распространения подразделяется на: свободно распространяемую; информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению; распространение ограничивается или запрещается.

Виды информации ограниченного распространения: государственная тайна; коммерческая тайна; профессиональная тайна; служебная тайна; информация о частной жизни; личная и семейная тайна; персональные данные.

Рис.4. 1- Структура информационных ресурсов

Федеральный Закон «О государственной тайне» от 21 июля 1993 года № 5485-I (с последующими изменениями) определяет основные понятия и отношения в сфере информации, содержащей государственную тайну. Он устанавливает степени секретности информации и соответству-

ющие им грифы секретности носителей: «особой важности», «секретная» и «совершенно секретная».

Отношения, связанные с обработкой персональных данных, регулируются федеральным законом «О персональных данных» от 27 июля 2006 года № 152-ФЗ. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Вопросы, связанные с обеспечением защиты персональных данных работников, регулирует также «Трудовой кодекс» Российской Федерации от 30 декабря 2001 года № 197-ФЗ (глава 14, с изменениями и дополнениями).

Защиту информации, содержащей сведения о личной жизни, обеспечивает статья 24 Конституции Российской Федерации: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.». Уголовный Кодекс Российской Федерации предусматривает соответствующее наказание (статья 137) за: «Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации».

В соответствии с Федеральным законом 149-ФЗ запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Информация, содержащая сведения, связанные с производственной и хозяйственной деятельностью, в законодательных актах Российской федерации делится на следующие типы: коммерческая тайна, про-

фессиональная тайна, объекты авторского права и смежных прав, объекты патентного права, для служебного пользования.

Правовые вопросы, связанные с информацией, содержащей коммерческую тайну, регулируются Федеральным законом «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ (с изменениями и дополнениями от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ) и статьей 139 Гражданского кодекса Российской Федерации от 30 ноября 1994 года № 51-ФЗ (часть 1 с изменениями, внесенными Федеральным законом от 29.12.2006 № 258-ФЗ, часть 2 с изменениями от 18.12.2006 № 231-ФЗ, часть 3 с изменениями, внесенными Федеральными законами от 18.12.2006 № 231-ФЗ, от 29.12.2006 № 258-ФЗ, часть 4 в соответствии с Федеральным законом от 18.12.2006 № 231-ФЗ вступает в силу с 1 января 2008 года.).

Закон определяет перечень сведений, которые не могут составлять коммерческую тайну, круг лиц и организаций, кому необходимо представлять информацию, содержащую коммерческую тайну, а также права обладателя такой информации. Статья 139 Гражданского кодекса гласит: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Основные принципы правового регулирования авторских и смежных прав определяет Федеральный закон «Об авторском праве и смежных правах» от 9 июля 1993 года № 5351-1 (с изменениями и дополнениями от 20.07.2004 № 72-ФЗ). Однако данный закон утрачивает силу с 1 января 2008 года в связи с принятием Закона № 231-ФЗ от 18.12.2006 г. о введении в действие части четвертой Гражданского кодекса.

Правовое регулирование объектов промышленной собственности (изобретений, полезных моделей и промышленных образцов) предусмат-

ривает «Патентный Закон» от 23 сентября 1992 года № 3517-1 (с изменениями и дополнениями от 27.12.2000 № 150-ФЗ, от 30.12.2001 N 194-ФЗ, от 24.12.2002 N 176-ФЗ, от 07.02.2003 N 22-ФЗ, от 02.02.2006 N 19-ФЗ). Данный закон также утратил силу с 01.01.2008 г. в связи с принятием Закона № 231-ФЗ от 18.12.2006 г.

С 1 января 2008 года вместо двух вышеуказанных законов введена в действие часть четвертая Гражданского кодекса, которая регулирует права на результаты интеллектуальной деятельности и средства индивидуализации. Ряд законодательных актов Российской Федерации вводят понятия профессиональной тайны – конфиденциальные сведения, полученные в результате выполнения профессиональной деятельности. В соответствии с законом 149-ФЗ «Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда».

В Гражданском Кодексе введены понятия «банковской тайны» (статья 857), «тайна страхования» (статья 946). В состав банковской тайны входят сведения о счетах, вкладах, операциях и другая информация, полученная сотрудниками банков при выполнении своих профессиональных обязанностей. Тайну страхования составляют сведения о страхователе. Понятие «банковской тайны» определено также в законе «О банках и банковской деятельности» от 2 декабря 1990 года № 395-1 (с изменениями и дополнениями от 3.02.1996 г. № 17-ФЗ).

Федеральным законом «Об аудиторской деятельности» от 7 августа 2001 года № 119-ФЗ введено понятие «аудиторской тайны» - сведения, по-

лученные при осуществлении аудиторской деятельности. В законе «О связи» от 7 июля 2003 года № 126-ФЗ введено понятие «тайны связи» - тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и почтовой связи.

Законом «Об адвокатской деятельности и адвокатуре Российской Федерации» от 31 мая 2002 года № 63-ФЗ введено понятие «адвокатской тайны» - сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 года № 5487-1 вводят понятие «врачебной тайны» - информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе заболевания и иные сведения, полученные при обследовании и лечении.Налоговый кодекс Российской Федерации (ч. 1 от 31 июля 1998 г. № 146-ФЗ, ч. 2 от 5 августа 2000 г. № 117-ФЗ) вводит понятие «налоговой тайны» - сведения о налогоплательщике, полученные налоговым органом. Постановлением Правительства российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Федеральных органах исполнительной власти» утверждено соответствующее Положение. Оно определяет общий порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. На соответствующих документах, проставляется пометка "Для служебного пользования".

4.1 Законодательство о безопасности критической информационной инфраструктуры (КИИ)

Эффективное правовое регулирование в этой сфере было затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности КИИ в России.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» вступил в силу с 1.01.2018 г**.**

Критическая информационная инфраструктура включает в себя информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Закон устанавливает основные принципы обеспечения безопасности КИИ, полномочия Президента, Правительства и органов государственной власти РФ в области обеспечения безопасности КИИ, права и обязанности субъектов, порядок осуществления оценки безопасности, порядок категорирования и ведения реестра значимых объектов КИИ.

Основополагающие документы в сфере безопасности КИИ

Указ Президента РФ № 31С от 15.01.2013 г. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ФСБ, система «СОПКА»).

Распоряжение Правительства РФ от 15.04.2013 N 611-р «Об утверждении перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи РФ».

Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента РФ № 683 от 31.12.2015 г.

Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 5.12.2016 № 646.

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации .Утверждена Президентом РФ 12 декабря 2014 г. № К 1274.

Одновременно приняты и с 1.01.2018 г. вступили в силу поправки к законам: «О связи», «О государственной тайне», УК РФ, УПК РФ.

Неправомерное воздействие на критическую информационную инфраструктуру РФ может повлечь за собой **уголовную ответственность в виде лишения свободы до 10 лет (ст. 274-1 УК РФ)**.Предварительное следствие по преступлениям в сфере КИИ будет производиться следователями органов ФСБ. Меры по обеспечению безопасности критической информационной инфраструктуры РФ и о состоянии ее защищенности от компьютерных атак отнесены к сведениям, составляющим государственную тайну**.**

Категорирование объекта КИИ - установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Категорирование объекта КИИ осуществляется исходя из:

- социальной значимости,
- политической значимости,
- экономической значимости,
- экологической значимости,
- значимости для обеспечения обороны страны, безопасности государства и правопорядка.

Устанавливаются три категории значимости объектов КИИ - первая, вторая и третья.

В целях учета значимых объектов КИИ федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, ведет реестр значимых объектов КИИ.

4.2 Законодательство о персональных данных

Базовый закон - № 152-ФЗ «О персональных данных», а также ряд других законов и нормативных документов.

«Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

Предмет регулирования: отношения, возникающие при осуществлении обработки этих данных как с применением ИТ, так и без их применения.

Цель регулирования: защита прав и свобод человека при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни.

Основные угрозы безопасности этих прав заключаются в неправомерном использовании собираемых персональных данных операторами.

4.3 Законодательство об интеллектуальной собственности

Базовый закон – Гражданский Кодекс РФ (часть 4), а также ряд других законов и нормативных документов, в том числе международных Конвенций о защите авторских прав.

Предмет регулирования: отношения, возникающие в связи с правовой охраной интеллектуальных прав на объекты интеллектуальной собственности.

Виды прав в сфере ИТ:

- авторское право;

- право смежное с авторским;
- патентное право;
- право на топологию интегральных микросхем;
- право на секрет производства (ноу-хау);
- право на средства индивидуализации товаров, услуг, юридических лиц, предприятий (фирменное наименование, товарный знак и др.);
- право на использование результатов интеллектуальной деятельности в составе единой технологии.

4.4 Законодательство о тайнах

Базовые законы: «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 21.12.2013); «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014), а также ряд других законов и нормативных документов.

Предмет регулирования: отношения, связанные с отнесением информации к конкретному виду тайны, распоряжением этой информацией, охраной ее конфиденциальности.

Режим соответствующей тайны образуется совокупностью правовых, организационных, технических и иных мер, принимаемых обладателем информации, по регламентированию порядка отнесения информации к виду тайн, ее распоряжением и обеспечением защиты.

Нормативные акты по видам тайн (более 60)

Гостайна - Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне», Указ Президента РФ №1203 от 30.11.1995 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

Коммерческая тайна – Закон РФ №98-ФЗ от 29.07.2004 «О коммерческой тайне».

Персональные данные – Закон РФ №152-ФЗ от 27.07.2006 «О персональных данных».

Налоговая тайна – «Налоговый кодекс РФ».

Банковская тайна – Закон РФ от 02.12.1990 №395-1 «О банках и банковской деятельности».

Врачебная тайна – Закон РФ от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

Адвокатская тайна – Закон РФ от 31.05.2002 №63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации".

Тайна связи – Закон РФ от 07.07.2003 № 126-ФЗ "О связи".

Тайна следствия – Уголовно-процессуальный кодекс.

Тайна усыновления – Семейный кодекс.

Аудиторская тайна – Закон РФ от 30.12.2008 №307-ФЗ "Об аудиторской деятельности".

и другие виды тайн.

4.5 Законодательство о лицензировании деятельности

Базовый закон – «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ (ред. от 21.07.2014), а также ряд других законов и нормативных документов.

Предмет регулирования: регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности.

Лицензирование отдельных видов деятельности осуществляется **в** целях предотвращения ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, обороне и безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности.

4.6 Законодательство о связи и Интернет

Базовый закон – «О связи» от 07.07.2003 № 126-ФЗ (ред. от 21.07.2014), а также ряд других законов и нормативных документов.

Предмет регулирования**:** установление правовых основ деятельности в области связи на территории РФ и на находящихся под юрисдикцией РФ территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Цели:

- создание условий для оказания услуг связи на всей территории РФ;
- содействие внедрению перспективных технологий и стандартов;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
-создание условий для обеспечения потребностей в связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

4.7Законодательство об электронной подписи

Базовый закон – «Об электронной подписи» от 6.04.2011 № 63-ФЗ.

Утратил силу закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ.

Предмет регулирования: закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

4.8 Законодательство о средствах массовой информации и рекламе

Базовые законы – «О средствах массовой информации» от27.12.1991 № 2124-1 (ред. от 24.11.2014); «О рекламе» от 13.03.2006 № 38-ФЗ (ред. от 21.07.2014).

Предмет регулирования: деятельность средств массовой информации и отношения, возникающие в процессе производства, размещения и распространения рекламы.

Закон «О средствах массовой информации» регламентирует правовое положение учредителей, редакций, журналистов, дает определение основных понятий в сфере масс-медиа, описывает права и обязанности журналистов, закладывает основы свободы массовой информации, устанавливает недопустимость цензуры.

4.9Законодательство о техническом регулировании

Закон – «О техническом регулировании» от 27.12.2002 № 184-ФЗ.

Технический регламент - документ, который устанавливает обязательные для применения и исполнения требования к объектам технического регулирования.

Сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров.

Техническое регулирование - правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, а также в области установления и применения на добровольной основе требований к продукции и правовое регулирование отношений в области оценки соответствия.

Оценка соответствия - прямое или косвенное определение соблюдения требований, предъявляемых к объекту.

Формы подтверждения соответствия

1. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации органом по сертификации.

2. Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом и осуществляется в формах:

- принятия декларации о соответствии (декларирование);
- обязательной сертификации.

Декларирование осуществляется по одной из следующих схем:

- на основании собственных доказательств;
- на основании собственных доказательств и доказательств, полученных с участием органа по сертификации.

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем.

4.10 Законодательство о техническом регулировании и стандартизации

Закон «О стандартизации в РФ» от 29.06.2015 № 162-ФЗ

Стандартизация в РФ основывается принципе добровольности применения документов по стандартизации.

Стандартизация - деятельность по разработке, утверждению, изменению, отмене, опубликованию и применению документов по стандартизации.

Стандарт организации - документ по стандартизации, утвержденный юридическим лицом.

Основополагающий национальный стандарт - национальный стан-

дарт, разработанный и утвержденный федеральным органом исполнительной власти в сфере стандартизации, устанавливающий общие положения, касающиеся выполнения работ по стандартизации, а также виды национальных стандартов.

Документ по стандартизации - документ, в котором для добровольного и многократного применения устанавливаются общие характеристики объекта стандартизации.

К документам по стандартизации относятся (162-ФЗ):

1) документы национальной системы стандартизации;

2) общероссийские классификаторы;

3) стандарты организаций, в том числе технические условия;

4) своды правил;

5) документы по стандартизации, которые устанавливают обязательные требования в отношении следующих объектов стандартизации:

- оборонной продукции;
- продукции, используемой в целях защиты гос. тайны или иной информации ограниченного доступа;
- продукции, сведения о которой составляют гос. тайну;
- продукции, для которой устанавливаются требования, связанные с
- обеспечением безопасности в области использования атомной энергии.

Исключено понятие «Государственный стандарт»!

Организацию работ по стандартизации осуществляет Федеральное агентство по техническому регулированию и метрологии (Росстандарт).

Оно выполняет функции:

- утверждение национальных стандартов;
- организацию экспертизы проектов национальных стандартов;
- обеспечение соответствия национальной системы стандартизации интересам национальной экономики;

- осуществление учета национальных стандартов, правил стандартизации;
- создание технических комитетов по стандартизации и координа цию их деятельности;
- организацию опубликования национальных стандартов;
- представление РФ в международных организациях, осуществляющих деятельность в области стандартизации.

Задание на практические занятия – изучить документы

ГОСТ Р 1.0-2012 Стандартизация в Российской Федерации. Основные положения.

ГОСТ Р 1.2-2014 Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления и отмены.

ГОСТ Р 1.4-2004 Стандарты организаций. Общие положения.

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

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

5 Законодательство о лицензировании деятельности

Согласно ГОСТ 50922-2006 «Защита информации. Основные термины и определения» вводятся следующие определения.

Лицензирование в области защиты информации – деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

Лицензия - документ, дающий право на осуществление указанного видадеятельности в течение определенного времени.

Сертификация на соответствие требованиям по безопасности информации – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Сертификат - документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Требование по защите информации – установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов (ГОСТ Р 53114-2008)

В статье 12 ФЗ № 99 от 4.05.2011 «О лицензировании отдельных видов деятельности» приведён Перечень видов деятельности, на которые требуются лицензии:

1) разработка, производство, распространение криптографических средств, информационных систем и телекоммуникационных систем, защи-

щенных с использованием криптографических средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание криптографических средств, информационных систем и телекоммуникационных систем, защищенных с использованием криптографических средств;

2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации;

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации.

Постановление Правительства РФ от 21.11.2011 № 957 (ред. от 28.10.2013) «Об организации лицензирования отдельных видов деятельности» **ФСБ России.**

Разработка, производство, распространение шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенныхс использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.

Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если

указанная деятельность осуществляется для обеспечения собственных нужд).

5.1 Нормативные документы по лицензированию

1. Пост. Правительства РФ от 21.11.2011 № 957 (ред. от 28.10.2013) "Об организации лицензирования отдельных видов деятельности».

2. Пост. Правительства РФ от 03.02.2012 № 79 «О лицензиировании деятельности по технической защите конфиденциальной информации».

3. Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Постановлением № 79.

4. Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Постановлением № 79.

5. Пост. Правительства РФ от 3.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

6. Пост. Правительства РФ от 12.04.2012 № 287 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации».

7. Пост. Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информацион-

ных систем и телекоммуникационных систем, защищенных с использованием шифровальных средств».

8. Пост. Правительства РФ от 15.04.1995 № 333 (ред. от 05.05.2012) «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих гос. тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

9. Пост. Правительства РФ от 16.04.2012 № 314 "Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)".

10. Приказ ФСБ России от 11.04.2014 № 202 «Об утверждении Административного регламента ФСБ РФ по предоставлению государственной услуги по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих гос. тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите гос. тайны».

11. Приказ ФСБ России от 30.08.2012 г. № 440 «Об утверждении Администр. регламента ФСБ РФ по предоставлению государственной услуги по лицензированию деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем…».

12. Приказ ФСБ России от 28.12.2012 № 683 «Об утверждении Административного регламента ФСБ РФ по предоставлению государственной

услуги по осуществлению лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации».

13. Приказ ФСТЭК России от 12.07.2012 № 84 (ред. от 10.10.2014) «Об утверждении Административного регламента ФСТЭК по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации».

14. Приказ ФСТЭК России от 12.07.2012 № 83 (ред. от 10.10.2014) «Об утверждении Административного регламента ФСТЭК по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

Постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» утверждено соответствующее «Положение».

Под технической защитой конфиденциальной информации понимается выполнение работ и (или) оказание услуг по ее защите от НСД, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа.

Лицензированию подлежат следующие виды работ и услуг:

а) контроль защищенности конфиденциальной информации от утечки по техническим каналам;

б) контроль защищенности конфиденциальной информации от НСД и ее модификации в средствах и системах информатизации;

в) сертификационные испытания на соответствие требованиям по безопасности продукции, используемой в целях защиты конфиденциальной информации;

г) проектирование в защищенном исполнении, а также аттестационные испытания и аттестация на соответствие требованиям по защите информации средств информатизации, помещений;

д) установка, монтаж, испытания, ремонт средств защиты информации.

5.2 Нормативные документы по сертификации

1. Постановление Правительства РФ от 26.06.1995 № 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».

2. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994).

3. Положение о сертификации средств защиты информации по требованиям безопасности информации" (утв. Прик. Гостехкомиссии от 27.10.1995 № 199).

4. Информационное сообщение ФСТЭК от 7 апреля 2014 г. № 240/24/1208 «О применении сертифицированной по требованиям безопасности информации операционной системы Windows XP в условиях прекращения поддержки разработчиком».

5. Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

6 Правовые основы организации защиты государственной тайны в Российской Федерации

Нормативно-правовую основу работы с государственной тайной составляет Федеральный закон «О государственной тайне» от 21.07.1993 № 5485-1 ФЗ (ред. от 08.03.2015).

6.1Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной власти, а также организациями, наделенными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности, органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

6.2 Основные понятия, термины и определения

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, состав-

ляющие 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 документ;

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.

Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

Палаты Федерального Собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны ;
- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.

Президент Российской Федерации:

- утверждает государственные программы в области защиты государственной тайны ;
- утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне, Перечень должностей, при замещении которых лица считаются допущенными к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации.

Правительство Российской Федерации:

- устанавливает порядок разработки Перечня сведений, отнесен-

ных к государственной тайне ;

- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;
- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам или международным организациям.

Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства Российской Федерации о государственной тайне
- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны
- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны ;
- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти .

Перечень сведений, составляющих государственную тайну:

- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых

программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке.

Сведения в области экономики, науки и техники:

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
- о достижениях науки и техники, о научно-исследовательских, об

опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

- о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации).

Сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;
- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства.

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:

- о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
- о методах и средствах защиты секретной информации;

- об организации и о фактическом состоянии защиты государственной тайны;
- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации.

Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном настоящим Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

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.

Постановление Правительства РФ от 04.09.1995 № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»

К сведениям **особой важности** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К **совершенно секретным** сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной

деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К **секретным** сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

6.3 Нормативные документы по тайнам

1. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 03.10.2014) «Об утверждении перечня сведений, отнесенных к государственной тайне».

2. Указ Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005) «Об утверждении перечня сведений конфиденциального характера».

3. Распоряжение Президента РФ от 16.04.2005 № 151-рп (ред. от 27.06.2014) «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».

4. Распоряжение Президента РФ от 15.01.2010 № 24-рп (ред. от 14.01.2011) «Об утверждении перечня должностей, при замещении которых лица считаются допущенными к государственной тайне».

5. Постановление Правительства РФ от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» (в ред. Пост. РФ от 03.10.2002 № 731).

6. Постановление Правительства РФ от 04.09.1995 № 870 (ред. от 22.05.2008) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

7. Постановление Правительства РФ от 22.08.1998 № 1003 (ред. от

27.05.2008) «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне».

8. Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 01.11.2012) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

9. Приказ ФСБ РФ от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» (Зарегистрировано в Минюсте РФ 27.12.1999 N 2028).

10. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»

Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»

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

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах гос. защиты, осуществляемой в соответствии с нормативными правовыми актами РФ.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»

Положение определяет общий порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения.

К **служебной информации** ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка **«Для служебного пользования».**

Задание на практические занятия – изучить документы:

Указ Президента РФ от 30.11.1995 № 1203 (ред. от 03.10.2014) «Об утверждении перечня сведений, отнесенных к государственной тайне».

Распоряжение Президента РФ от 16.04.2005 № 151-рп (ред. от 27.06.2014) «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».

Постановление Правительства РФ от 5 декабря 1991 г. № 35
«О перечне сведений, которые не могут составлять коммерческую тайну» (в ред. Пост. РФ от 03.10.2002 № 731)

Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 01.11.2012) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации

к государственной тайне»

ТЕСТ № 1 (нормативная база)

1. Структура нормативно-правовой базы РФ в области ИБ.

2. Какие международные конвенции и документы в области ИТ и защиты информации действуют в Российской Федерации?

3. Назовите основные законы РФ, регулирующие отношения в области информационных технологий и защиты информации.

4. Назовите виды деятельности в области ИТ, подлежащие лицензированию.

5. Какой орган государственной власти лицензирует деятельность по технической защите конфиденциальной информации?

ФСБ ФСТЭК Роскомнадзор ФСО СВР Минобороны МВД

6. В чем отличие стандарта РФ от технического регламента?

7. Какой орган государственной власти осуществляет деятельность по стандартизации и техническому регулированию?

ФСБ ФСТЭК Роскомнадзор Росстандарт Роспатент МВД Минобороны

8. Какие органы государственной власти осуществляет деятельность по сертификации средств защиты информации?

ФСБ ФСТЭК Роскомнадзор Росстандарт Роспатент МВД Минобороны

9. Какие степени секретности присваиваются сведениям, содержащим государственную тайну, каким законом РФ?

10. На какие категории подразделяется информация в зависимости от порядка доступа к ней?

11. На какие категории подразделяется информация в зависимости от порядка ее распространения?

12. На какие сведения не может быть установлен режим государственной тайны?

13. На какие сведения не может быть установлен режим коммерческой тайны?

14. До какой даты можно использовать для защиты информации сертифицированную ОС Windows XP?

7 Законодательство по защите интеллектуальной собственности в Российской Федерации

Гражданский Кодекс. Часть 4. (вступила в силу с 1.01.2008).Принята федеральным законом № 230-ФЗ от 18.12.2006.

Утратили силу:

«О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23.09.1992 № 3520-1.

«О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 № 3523-1.

«О правовой охране топологий интегральных микросхем» от 23.09. 1992 года № 3526-1.

«Об авторском праве и смежных правах» от 9.07.1993 № 5351-1.

«Патентный закон» от 23.09.1992 № 3517-1.

Права на результаты интеллектуальной деятельности и средства индивидуализации:

Статья 1225. «Результатами интеллектуальной деятельности, которым предоставляется правовая охрана (интеллектуальной собственностью), являются: произведения науки, литературы и искусства; программыдля ЭВМ; базы данных; фонограммы. . .»

Статья 1233. Правообладатель может предоставить другому лицу права использования результата интеллектуальной деятельности в установленных договором пределах (лицензионный договор).

Статья 1261. Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею

аудиовизуальные отображения**.**

Статья 1262. Правообладатель может по своему желанию зарегистрировать программу или базу данных в федеральном органе исполнительной власти по интеллектуальной собственности**.**

Статья 1274. Выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Статья 1281. Исключительное право на программу действует в течение всей жизни автора и 70 лет, считая с 1 января года, следующего за годом смерти автора.

Статья 1295. Авторские права на произведение науки, литературы или искусства, созданное в пределах установленных для работника (автора) трудовых обязанностей (служебное произведение), принадлежат автору.

Исключительное право на служебное произведение принадлежит работодателю, если трудовым или иным договором между работодателем и автором не предусмотрено иное.

Если работодатель в течение трех лет не начнет использование этого произведения, не передаст исключительное право на него другому лицу или не сообщит автору о сохранении произведения в тайне, исключительное право на служебное произведение возвращается автору.

Статья 1296. Исключительное право на программу для ЭВМ, базу данных или иное произведение, созданные по договору, предметом которого было создание такого произведения (по заказу), принадлежит заказчику, если договором между исполнителем и заказчиком не предусмотрено иное. Автор созданных по заказу программы для ЭВМ или базы данных, которому не принадлежит исключительное право, имеет право на возна-

граждение.

Статья 1297. Исключительное право на программу для ЭВМ, базу данных или иное произведение, созданные при выполнении договора подряда либо договора на выполнение научно-исследовательских, опытно-конструкторских или технологических работ, которые прямо не предусматривали создание такогопроизведения, принадлежит исполнителю, если договором между ним и заказчиком не предусмотрено иное.

Статья 1299. Техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

Статья 1301. В случаях нарушения исключительного права на произведение автор или иной правообладатель наряду с использованием других применимых способов защиты и мер ответственности, установленных Кодексом , вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

1) в размере от 10000 рублей до 5 млн. рублей, определяемом по усмотрению суда исходя из характера нарушения;

2) в двукратном размере стоимости контрафактных экземпляров произведения;

3) в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая обычно взимается за правомерное использование произведения тем способом, который использовал нарушитель.

Статья 1304. Объектами смежных прав являются: базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов.

Статья 1311. Ответственность за нарушение исключительного права

на объект смежных прав – аналогично ст. 1301.

Статья 1333. Изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При отсутствии доказательств иного изготовителем базы данных признается гражданин или юридическое лицо, имя или наименование которых указано обычным образом на экземпляре базы данных и (или) его упаковке.

Изготовителю базы данных принадлежат:

- исключительное право изготовителя базы данных;

- право на указание на экземплярах базы данных и (или) их упаковках своего имени или наименования;

- право на обнародование базы данных.

Статья 1334. Никто не вправе извлекать из базы данных материалы и осуществлять их последующее использование без разрешения правообладателя, кроме случаев, предусмотренных настоящим Кодексом.

При этом под извлечением материалов понимается перенос всего содержания базы данных или существенной части составляющих ее материалов на другой носитель с использованием любых технических средств и в любой форме.

Статья 1335. Срок действия исключительного права изготовителя базы данных.

1. Исключительное право изготовителя базы данных действует в течение 15 лет.

2. Сроки, предусмотренные п.1 настоящей статьи, возобновляются при каждом обновлении базы данных.

Статья 1335.1. Действия, не являющиеся нарушением исключительного права изготовителя базы данных (введена 12.03.2014 № 35-ФЗ)

1. Лицо, правомерно пользующееся обнародованной базой данных, вправе без разрешения изготовителя базы данных и в той мере, в которой

такие действия не нарушают авторские права изготовителя базы данных и других лиц, извлекать из базы данных материалы и осуществлять их последующее использование:

- в целях, для которых база данных ему предоставлена, в любом объеме, если иное не предусмотрено договором;

- в личных, научных, образовательных целях в объеме, оправданном указанными целями;

- в иных целях в объеме, составляющем несущественную часть базы данных.

Использование извлеченных материалов способом, предполагающим получение к ним доступа неограниченного круга лиц, должно сопровождаться указанием на базу данных, из которой эти материалы извлечены.

2. Совершение действий другим лицом не считается нарушением права, если это лицо докажет, что оно не могло установить личность изготовителя или оно обоснованно считало, что срок действия исключительного права на базу данных истек.

3. Не допускается неоднократное извлечение или использование материалов, составляющих несущественную часть базы данных, если такие действия противоречат нормальному использованию базы данных и ущемляют необоснованным образом законные интересы изготовителя базы данных.

4. Изготовитель базы данных не может запрещать использование отдельных материалов, хотя и содержащихся в базе данных, но правомерно полученных использующим их лицом из иных, чем эта база данных, источников.

ГОСТ Р 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» (введен в действие с 1.06.2016 г.).

Стандарт устанавливает единый понятийный аппарат и выделяет

специфические риски, относящиеся к использованию интеллектуальной собственности в сети Интернет.Все объекты интеллектуальной собственности подразделяются на 2 типа:

1. Созданные в сети Интернет.

2. Используемые в сети Интернет.

Основные субъекты отношений в сети Интернет:

1. Авторы.

2. Интернет-правообладатели (правообладатели объектов интеллектуальной собственности и информационных ресурсов, размещенных в сети Интернет).

3. Интернет-пользователи (лица, имеющие доступ к сети Интернет).

4. Информационные посредники (лица, оказывающие услуги по предоставлению доступа к сети Интернет и услуги, связанные с размещением информации в сети, в том числе организаторы распространения информации в сети Интернет как они определены в законе № 149-ФЗ).

Иск по делу о защите прав на объекты интеллектуальной собственности, размещенные в сети Интернет, по выбору истца может быть подан по месту нахождения:

- доменного имени, под которым создан сайт, содержащий результаты интеллектуальной деятельности (РИД);
- организации-администратора сайта;
- владельца сайта;
- информационных посредников владельца сайта;
- обладателя информационного ресурса, содержащего РИД;
- Интернет-пользователя, нарушившего интеллектуальные права.

8 Основные положения Федерального Закона «О персональных данных»

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

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных

Информационные системы персональных данных, созданные до дня вступления в силу закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года. Однако сроки переносились: № 363-ФЗ от 27.12.2009 – срок до 1.01.2011; № 359-ФЗ от 23.12.2010 – срок до 1.07.2011.

В настоящее время существует около 30 нормативных документов (Указы Президента РФ, Постановления Правительства РФ, документы ФСТЭК, ФСБ, Роскомнадзора). Более 20 Федеральных Законов РФ, затрагивающих вопросы обработки ПД.

8.1 Основные понятия № 152-ФЗ

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу(субъекту персональных данных);

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПД, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с ПД;

Обработка ПД – любое действие или совокупность действий, совер шаемыхс использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПД.

Распространение ПД – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направлены на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование ПД – временное прекращение обработки персональных данных.

Уничтожение ПД - действия, в результате которых невозможно восстановить содержание ПД в информационной системе ПД или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание ПД - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту персональных данных;

Информационная система ПД – совокупность содержащихся в базах данных ПД и обеспечивающих их обработку информационных технологий и технических средств.

Автоматизированная обработка персональных данных – обработка ПД с помощью средств вычислительной техники.

Трансграничная передача ПД – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

8.2 Нормативные документы, затрагивающие вопросы обработки ПД

Согласие в письменной форме субъекта ПД на обработку его ПД должно содержать:

1) ФИО, адрес субъекта, данные основного документа (паспорта);

2) ФИО, адрес представителя субъекта ПД, данные паспорта, реквизиты доверенности или иного документа, подтверждающего его полномочия;

3) наименование и адрес оператора, получающего согласие субъекта ПД;

4) цель обработки персональных данных;

5) перечень ПД, на обработку которых дается согласие субъекта;

6) наименование и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;

8) срок, в течение которого действует согласие субъекта , а также способ его отзыва;

9) подпись субъекта персональных данных.

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим ФЗ (Ст. 18.1):

1) назначение ответственного за организацию обработки ПД;

2) издание документов, определяющих политику оператора в отно шении обработки ПД, локальных актов по вопросам обработки ПД;

3) применение правовых, организационных и технических мер по обеспечению безопасности ПД;

4) осуществление внутреннего контроля соответствия обработки ПД закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПД;

5) оценка вреда, который может быть причинен субъектам ПД в случае нарушения закона;

6) ознакомление работников оператора, непосредственно осуществляющих обработку ПД, с положениями законодательства РФ о персональных данных, в том числе локальными актами оператора по вопросам обработки ПД и обучение указанных работников.

Меры по обеспечению безопасности ПД при их обработке (Ст. 19):

1) определение угроз безопасности ПД при их обработке в ИСПДн; (РД ФСТЭК «Методика определения актуальных угроз безопасности ПД при их обработке в информационных системах ПД»)

2) применение организационных и технических мер по обеспечению безо пасности ПД в ИСПДн;

3) применение прошедших процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности ПД;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к ПД и принятием мер;

7) восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к ПД, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПД;

9) контроль за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности информационных систем персональных данных.

Уведомление об обработке ПД должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки ПД;

3) категории ПД;

4) категории субъектов, ПД которых обрабатываются;

5) правовое основание обработки ПД;

6) перечень действий с ПД, описание используемых способов обработки ПД;

7) описание мер по обеспечению безопасности ПД;

8) дата начала обработки ПД;

9) срок или условие прекращения обработки ПД;

10) сведения о наличии или отсутствии трансграничной передачи ПД;

10.1) сведения о месте нахождения базы данных информации, содержащей ПД граждан РФ (введено с 1.09.2015);

11) сведения об обеспечении безопасности ПД данных в соответствии с требованиями к защите, установленными Правительством РФ (Пост. № 1119).

Орган по защите прав субъектов ПД (Роскомнадзор) имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий;

2) осуществлять проверку сведений, содержащихся в увед. об обработке ПД;

3)требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПД;

3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства РФ в области ПД **(введено с 1.09.2015);**

4) принимать меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПД;

6) направлять заявление в орган, осуществляющий лицензирование

деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии;

7) направлять в органы прокуратуры материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД;

8) привлекать к админ. ответственности лиц, виновных в нарушении закона.

Документы ФСТЭК с грифом «ДСП» февраль 2008 г.:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Гриф ДСП снят в ноябре 2009 года. Выписки из первого документа и тексты остальных документов опубликованы на сайте ФСТЭК.

Последние 2 отменены

Действующие документы:

Постановления Правительства РФ:

от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

от 1.11.2012 г. N 1119

«Об утверждении требований к защите персональных данныхпри их обработке в информационных системах персональных данных»

от 21.03.2012 г. N 211

«Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей , предусмотренных Федеральным Законом « О персональных данных» и принятыми в соответствии с нимнормативными правовыми актами операторами, являющимися государственными или муниципальными органами»;

от 6.07.2008 г. N 512

«Об утверждении требований к материальным носителям биометрическихперсональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Приказ ФСТЭК от 18 февраля 2013 г. N 21

«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК от 11.02.2013 № 17

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных ИС»

Методический документ ФСТЭК от 11.02.2014

«Меры защиты информации в государственных информационных системах».

Приказ ФСБ от 10 июля 2014 г. N 378

«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите ПД для каждого из уровней защищенности».

Приказ Роскомнадзора от 19.08.2011 № 706

"Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) ПД».

Приказ Роскомнадзора от 05.09.2013 № 996

«Об утверждении требований и методов по обезличиванию персональных данных».

Методические рекомендации по применению приказа Роскомнадзора от 5.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013)

Приказ Минкомсвязи РФ от 14.11.2011 № 312

«Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»

Приказ Минкомсвязи России от 21.12.2011 № 346

«Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных».

Стратегия институционального развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных на период до 2020 года. Роскомнадзор, **2016 г**.

Приказ Роскомнадзора от 30.05.2017 г. № 94

«Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее предоставленные сведения».

Рекомендации по составлению документа, определяющего политику оператора в отношении обработки ПД, в порядке, установленном

Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (2017 г.)

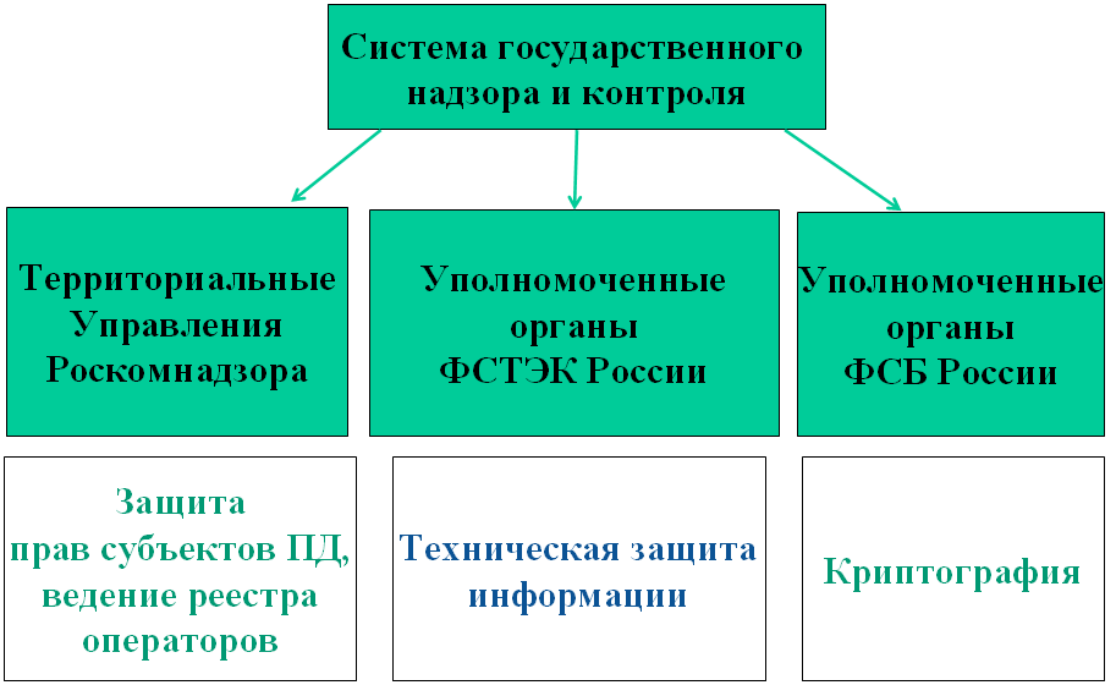

Рис.8.1-Государственный надзор и контроль за обработкой ПД

Рис.8.2-Организация взаимодействия при защите прав субъектов персональных данных

Постановление Правительства РФ от 21.03.2012 г. N 211

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»:

а) назначают ответственного за организацию обработки персональных данных;

б) утверждают актом руководителя следующие документы:

- Положение об обработке персональных данных;

- правила рассмотрения запросов субъектов ПД или их представителей;

- правила осуществления внутреннего контроля соответствия обработки ПД требованиям к защите персональных данных;

- перечень информационных систем персональных данных;

- перечни персональных данных, обрабатываемых в учреждении;

- перечень должностей сотрудников, замещение которых предусматривает осуществление обработки ПД либо осуществление доступа к ПД;

- должностная инструкция ответственного за организацию обработки ПД;

- типовое обязательство сотрудника, осуществляющего обработку ПД, в случае расторжения с ним контракта прекратить обработку ПД, ставших известными ему в связи с исполнением должностных обязанностей;

- типовая форма согласия на обработку ПД сотрудников и иных субъектов ПД;

- порядок доступа сотрудников в помещения, в которых ведется обработка ПД;

в) при эксплуатации информационных систем ПД принимают правовые, организационные и технические меры по обеспечению безопасности ПД, установленные постановлением Правительства РФ № 1119 от 1.11.2012 г.;

г) при обработке ПД, осуществляемой без использования средств автоматизации, выполняют требования, установленные постановлением Правительства РФ от 15 сентября 2008 г. № 687;

д) организуют проведение периодических проверок условий обработки ПД;

е) осуществляют ознакомление сотрудников, непосредственно осуществляющих обработку ПД, с положениями законодательства РФ, локальными актами по вопросам обработки ПД и (или) организуют обучение указанных сотрудников;

ж) уведомляют Роскомнадзор об обработке ПД.

Постановление Правительства РФ от 1.11.2012 г. N 1119

Документ устанавливает требования к защите ПД и уровни защищенности таких данных.

Безопасность ПД обеспечивается с помощью системы защиты, нейтрализующей актуальные угрозы, определенные в соответствии с документами ФСТЭК.

Под актуальными угрозами безопасности ПД понимается совокупность факторов, создающих актуальную опасность НСД к ПД при их обработке в ИС, результатом которых могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПД, а также иные неправомерные действия.

Вводится 3 типа актуальных угроз (1, 2, 3).

При обработке ПД в ИС устанавливаются 4 уровня защищенности ПД в зависимости от типа актуальных угроз, перечня обрабатываемых ПД и количества субъектов ПД.

Правовой акт, статья	Ответчик	Максимальная мера наказания
Кодекс об админ. правонарушениях		
5.27. Нарушение законодательства о труде	Должн.лицо Юрид. лицо	Штраф до 5 тыс. руб. Дисквалифик. до 3 лет Штраф до 50 тыс. руб. Приостан. деят. до 90 су
5.39. Отказ в предоставлении гражданину информации	Должностное лицо	Штраф до 1 тыс. руб.
13.11. Нарушение порядка сбора, хранения, использования или распространения перс. данных	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 500 руб. С 1.07.2017: 5000 руб. Штраф до 1000 руб. 10000 руб. Штраф до 10000 руб. 75000 руб.
13.12. Нарушение правил защиты информации	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 1 тыс. руб. Штраф до 4 тыс. руб. Штраф до 30 тыс. руб.
13.13. Незаконная деятельность по защите информации	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 1 тыс. руб. Штраф до 3 тыс. руб. Штраф до 20 тыс. руб.
13.14. Разглашение информации с ограниченным доступом	Физ. лицо Должн. лицо	Штраф до 1 тыс. руб. Штраф до 5 тыс. руб.
19.4. Неповиновение законному распоряжению органа, осуществляющего гос. надзор	Физ. лицо Должн. лицо	Штраф до 1 тыс. руб. Штраф до 2 тыс. руб.
19.5. Невыполнение в срок законного предписания органа, осуществляющего государственный надзор (Роскомнадзор)	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 500 руб. Штраф до 2 тыс. руб. Дисквалиф. до 3 лет Штраф до 20 тыс. руб.
19.6. Непринятие мер по устранению причин и условий правонарушения	Должностное лицо	Штраф до 500 руб.
19.7. Непредставление или несвоевременное представление сведений в гос. орган	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 300 руб. Штраф до 500 руб. Штраф до 5 тыс. руб.
19.20. Осуществление деятельности без лицензии или с нарушением ее условий	Предприним. Должн. лицо Юрид. лицо	Штраф до 1500 руб. Штраф до 2000 руб. Штраф до 20 тыс. руб.

8.3 Локальные нормативные акты по обработке ПД

habrahabr.ru/post/169527

САЙТЫ ПО ЗАЩИТЕ ПД

rkn.gov.ru

www.iso27000.ru

habrahabr.ru/post/169527

pdsec.ru

И вот, это случилось: начальник, не особо заморачиваясь подписал приказ:

«Системному администратору ООО «Рога и копыта» Иванову И. И. сделать так, чтобы защита персональных данных в нашей организации была по фен-шую».

Что делать в первую очередь?

1. Выяснить, есть ли в реестре Роскомнадзора ваша организация.

Если уведомления нет, то нужно его подать (но это уже повод для регулятора оштрафовать вашу организацию). Если уведомление есть, нужно уточнить его содержание.

2. Нужно издать и утвердить комплект документов (инструкции, положения, приказы, журналы и тд). Они должны регламентировать не только автоматизированную обработку но и «бумажную» тоже.Строго определенного перечня документов не существует, есть лишь перечень аспектов, которые вы должны описать в них.

Примерный перечень документов:

- приказ о назначении лиц, ответственных за организацию обработки ПД;
- перечень ПД, подлежащих защите;
- приказ об утверждении мест хранения ПД;
- инструкция пользователей ИСПДн;
- порядок резервирования и восстановления работоспособности технических средств и ПО, баз данных и средств защиты информации;
- план внутренних проверок режима защиты персональных данных;
- приказ о вводе в эксплуатацию ИСПДн;
- журнал учета носителей информации;
- журнал учета обращений граждан-субъектов ПД;
- правила обработки ПД без использования средств автоматизации;
- положение о разграничении прав доступа к обрабатываемым ПД;
- инструкция по проведения антивирусного контроля в ИСПДн;
- инструкция по организации парольной защиты;
- форма акта уничтожения документов, содержащих персональные данные;

- соглашение о неразглашении персональных данных;

- приказ о перечне лиц, допущенных к обработке персональных данных;

- положение об обработке и защите персональных данных;

- модель угроз безопасности в информационной системе персональных данных.

ВАЖНО:

Все лица, которых касаются эти документы должны расписаться в том, что они с ними **ознакомлены.**

В **должностные инструкции** всех лиц, допущенных к обработке ПД нужно вписать строку «При работе с персональными данными руководствоваться Положением об обработке и защите персональных данных».

«Положение…» должно вывешиваться на веб-сайте оператора, либо находиться в другом общедоступном месте.

Задание на практические занятия – изучить документы:

1 Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2 Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

3 Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработкев информационных системах пер-

сональных данных».

4 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК 15.02.2008 г.

5 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК 14.02.2008 г.

Литература

1 Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. Учебное пособие. – С.Петербург, «Питер», 2008.- 272с.

2 Галатенко В.А. Стандарты информационной безопасности: курс лекций : уч. пособие / Интернет-Университет Информационных Технологий, 2006.

3 Родичев Ю.А. Компьютерные сети. Нормативно-правовые аспекты информационной безопасности. Часть 1. Учеб. пособие для вузов. – Самара:изд-во «Универс-групп», 2007. – 344 с.

4 Курило А.П., и др. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2016. – 244 с.6 ил. – Серия «Вопросы управления ИБ. Выпуск 1.»

5 Моисеев А.И. Информационная безопасность распределённых информационных систем: учеб. / А.И. Моисеев, Д.Б. Жмуров. – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. – 180 с.

6 Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов; под ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.

7 Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. СПб.: Питер, 2017 г.-256 с.

8 Родичев Ю.А., Кубанков Ю.А., Симонов П.И. Безопасность инфокоммуникаций: стандартизация, измерения соответствия и подготовка кадров. Учебное пособие для вузов / Под ред. Родичева Ю.А. – М.: Горячая линия – телеком, 2018. – 160 с.: ил.

9 Электронные ресурсы на сервере Inf (\\ JUPITER4):tutorial\ Teachers\Yury A. Rodichev\нормативная база tutorial\Teachers\Yury A. Rodichev\методы и стандарты.

10 Правовая система «Консультант Плюс»

11 Сайты в сети Интернет: ФСТЭК, ФСБ, Минкомсвязи, Роскомнадзора,Росстандарта, Роспатента и др.