Тема 1.1 Информационные отношения, как объект правового регулирования; законодательство РФ в области информационной безопасности

1 Структура и состав информационного законодательства

В основе комплексной системы информационной безопасности любого объекта лежат следующие методы защиты:

1) Правовые (международные, государственные, местные, ведомственные и внутрифирменные правовые акты);

2) Организационные (создание служб безопасности и введение режима защиты информации, подготовка и переподготовка кадров, системы лицензирования и сертификации в области защиты информации);

3) Технические (программные, аппаратные, криптографические средства, физические ограждения и препятствия).

Применение каждого метода защиты информации регламентируется нормативно-правовыми документами, т.е. законами и подзаконными актами, которые в своей совокупности образуют правовую базу информационного права. Информационное право – относительно молодая отрасль права, которая начала формироваться в системе права Российской Федерации после принятия в 1994 г. 1-й части Гражданского кодекса и закона «Об информации, информатизации и защите информации» в 1995 г.

Информационное законодательство регулирует общественные отношения в области создания, использования и защиты информации. Применять средства и методы защиты можно только к материальным объектам, поэтому объектами защиты информации всегда являются физические носители информации, т.е. персонал, документы и технические средства.

Особенно актуальными в настоящее время являются вопросы защиты информации ограниченного доступа, к которой относится государственная тайна и информация конфиденциального характера. Правовое обеспечение за-

щиты информации зависит от вида и характера носителей информации. Наличие различных источников угроз, ведение бумажного и электронного делопроизводства конфиденциального характера требуют разграничения прав, обязанностей и компетенции коммерческих и некоммерческих структур, юридических и физических лиц, а также установления мер административной и уголовной ответственности.

Организационная структура, реализующая комплекс мер безопасности на предприятии – служба безопасности также базируется на правовых, методических и организационно-распорядительных документах, определяющих статус, права и обязанности этих органов защиты, порядок лицензирования их деятельности и сертификацию используемых ими технических средств защиты информации.

Информационное законодательство - это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предметом правового регулирования в информационной сфере являются: создание и распространение информации; формирование информационных ресурсов; реализация права на поиск, получение, передачу и потребление информации; создание и применение информационных систем и технологий; создание и применение средств информационной безопасности.

Формирование законодательства в области информационного права в Российской Федерации (РФ) началось, в основном, со времени появления «Концепции правовой информатизации России», утвержденной Указом Президента РФ от 28.06.93 г. № 966. В основе информационного законодательства находится свобода информации и запретительный принцип права (все, что не запрещено законом - разрешено). Это закреплено в основных международных и российских правовых документах, например, в ст. 3 Всеобщей декларация прав человека от 10.12.1948 г. и в ст. 29 Конституции РФ, принятой 12.12.1993 г. В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают гарантии, обязанности, механизмы защиты и ответственность.

Структура информационного законодательства строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов:

1) Конституция РФ.
2) Федеральные конституционные законы РФ
3) Федеральные законы РФ
4) Указы и распоряжения Президента РФ
5) Законодательные акты субъектов РФ
6) Постановления и распоряжения
7) Правительства РФ
8) Нормативные правовые акты высших органов исполнительной власти субъектов РФ
9) Нормативные правовые акты федеральных органов исполнительной власти
10) Нормативные правовые акты органов исполнительной власти субъектов РФ
11) Правовые акты органов местного самоуправления

Закон «Об информации, информационных технологиях и о защите информации» от 27.13.2006 г. № 149-ФЗ установил следующие принципы правового регулирования отношений, в информационной сфере (ст. 3):

– свобода поиска, получения, передачи, производства и распространения
– информации любым законным способом;
– установление ограничений доступа к информации только федеральными
– законами;

– открытость информации о деятельности государственных органов и органов

– местного самоуправления и свободный доступ к такой информации;

– обеспечение безопасности Российской Федерации при создании и эксплуатации информационных систем;

– достоверность информации и своевременность ее предоставления;

– неприкосновенность частной жизни, недопустимость сбора, хранения,

– использования и распространения информации о частной жизни лица без его согласия;

– недопустимость преимуществ применения одних информационных технологий перед другими, кроме государственных информационных систем, установленных в соответствии с федеральными законами.

Информационное законодательство имеет следующую структуру:

1) Международные акты информационного законодательства.

2) Конституция РФ, Гражданский кодекс РФ, Уголовный кодекс РФ и др.

3) Закон РФ «Об информации, …» и др. (всего около 80 законов).

4) Указы и распоряжения Президента РФ. Постановления Правительства РФ.

5) Местные, ведомственные и внутриорганизационные другие подзаконные акты.

Совокупность вышеперечисленных документов составляет правовую базу в информационной сфере.

2 Основные определения в области информационного права

Основной нормативно-правовой документ в сфере информационного права это закон «Об информации, информационных технологиях и о защите информации”, который регулирует отношения, связанные с:

– осуществлением права на поиск, получение, передачу, производство и

– распространение информации;

– применением информационных технологий;

– обеспечением защиты информации.

В законе даны основные понятия (ст. 2):

– информация – сведения (сообщения, данные) независимо от формы их

– представления;

– конфиденциальность информации – обязательное требование не передавать

– такую информацию третьим лицам без согласия ее обладателя;

– документированная информация – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Информация может являться объектом правовых отношений (ст. 5).

Электронное сообщение, подписанное электронной цифровой подписью, признается, равнозначным документу, подписанному собственноручной подписью (ст. 11).

3 Классификация и виды информационных ресурсов

Информационные ресурсы принято классифицировать по принадлежности и доступности.

По принадлежности информационные ресурсы подразделяются на государственные (принадлежащие органам государственной власти) и не государственные (принадлежащие юридическим и физическим лицам).

Обладателем информации (ст. 6) может быть физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

Обладатель информации вправе:

– разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

– использовать информацию, в том числе распространять ее, по своему усмотрению;

– передавать информацию другим лицам по договору или на ином установленном законом основании;

– защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Негосударственные информационные ресурсы, это ресурсы созданные, приобретенные за счет средств негосударственных учреждений, организаций, предприятий и физических лиц или полученные в результате дарения юридическими или физическими лицами.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и информацию ограниченного доступа.

Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Документированная информация с ограниченным доступом подразделяется на информацию, отнесенную к государственной тайне и конфиденциального характера.

К конфиденциальной информации относится коммерческая, служебная, профессиональная и др. тайны всего около 40 видов тайн, а также персональные данные (информация о гражданах).

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Законом РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ регулируются отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти, юридическими лицами и физическими лицами.

Персональные данные – любая информация, относящаяся к определенному физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

В законе дано определение общедоступных и конфиденциальных персональных данных (ст. 3):

– конфиденциальность персональных данных – обязательное требование не допускать их распространение без согласия субъекта персональных данных или законного основания;

– общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с федеральными законами.

В связи с этим положением закона, в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В которых с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением указанных в законе случаев (осуществление правосудия, угроза состоянию здоровья и т.п.).

Оператор при обработке персональных данных обязан принимать необходимые меры, в том криптографические средства, для защиты персональных данных от несанкционированного доступа (НСД), уничтожения, и иных неправомерных действий.

В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами

В зависимости от порядка распространения информация подразделяется на:

– свободно распространяемую;

– предоставляемую по соглашению;

– распространяемую в соответствии с федеральными законами;

– распространение которой в РФ ограничивается или запрещается.

Общедоступная информация – сведения, доступ к которым не ограничен (ст. 8):

– нормативные правовые акты, затрагивающие права, свободы и обязанности

– человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

– информация о состоянии окружающей среды;

– информация о деятельности государственных органов и органов местного самоуправления (за исключением сведений, составляющих государственную или служебную тайну);

– информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных для обеспечения граждан и организаций такой информацией;

– информация, недопустимость ограничения доступа к которой установлена федеральными законами.

4 Правовое регулирование информационного взаимодействия в компьютерных сетях

Право на информацию, выражено Конституцией «Каждый имеет право свободно искать, получать, передавать и распространять информацию любым законным способом» (ст. 29). Это право подтверждено также и в ст. 8 закона «Об информации…» от 2006г. В соответствии с законом (ст. 9) право на информацию может быть ограничено только федеральным законом, что отсекает ведомственный и региональный произвол.

Правовое регулирование информации в сети основывается на ст. 15 Закона «Об информации…», где сказано, что передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений только при условии соблюдения требований к распространению информации и охране объектов интеллектуальной собственности.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность (ст. 10).

Кроме этого, федеральными законами может быть предусмотрена обязательная идентификация лиц, использующих информационно-телекоммуникационную сеть. При этом получатель электронного сообщения вправе установить отправителя электронного сообщения.

При использовании почтовых отправлений и электронных сообщений (ст. 10), лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

Защита информации (ст. 16, 17) представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются уполномоченным федеральным органом исполнительной власти.

Органами, осуществляющими контроль за соблюдением требований к защите информации, являются: Федеральная служба безопасности (ФСБ), Министерство Обороны (МО), Служба внешней разведки (СВР), Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Правовое обеспечение защиты информации в компьютерных сетях представляет собой совокупность законодательных актов и нормативно-правовых документов, включающих нормы международного права (соглашения, договора, лицензии, патенты, авторские права) и национального права (конституция и законы РФ, постановления Правительства РФ, указы Президента РФ, руководящие документы ГТК, инструкции и др. нормативно-правовые акты).Для корпоративных сетей с большим количеством пользователей составляется документ, регламентирующий работу в сети – «Политика безопасности». Этот документ учитывает требования информационной безопасности и основан на стандарте ISO/IEC 17799 «Безопасность информационных систем».

«Политика безопасности» обеспечивает выполнение следующих правил безопасности информации:

1) Идентификация.
2) Разделение полномочий.
3) Регистрация и учет работы.
4) Шифрование.
5) Применение цифровой подписи.
6) Обеспечение антивирусной защитой.
7) Контроль целостности информации.

В общем случае система защиты информации в компьютерной сети реализуется в три этапа:

- анализ риска;
- реализация политики безопасности;
- поддержание политика безопасности.

Реализация требований политики безопасности обеспечивает выполнение трех основных функций системы: доступность, целостность, конфиденциальность.

Требования к безопасности компьютерных сетей в РФ разработаны Государственной технической комиссией РФ ныне ФСТЭК. Эти требования обязательны для государственных предприятий или для коммерческих предприятий, допущенных к сведениям составляющих ГТ. В остальных случаях они носят рекомендательный характер.

К таким документам относится, например, следующие РД ГТК:

1) «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30.03.1992 г.

2) «Средства ВТ. Защита от НСД. Показатели защищенности от НСД к информации» от 30.03.1992 г.

3) «Защита от НСД к информации. Термины и определения». Решение Председателя ГТК от 30.03.1992 г.

4) «Концепция защиты СВТ и АС от НСД к информации». Решение Председателя ГТК от 30.03.1992 г.

5) «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники». Решение Председателя ГТК от 30.03.1992 г.

6) «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа к информации». Решение Председателя ГТК от 25.07.1997 г.

7) «Специальные требования и рекомендации по технической защите конфиденциальной информации» от 2001г.

Эффективная борьба с компьютерными преступлениями в РФ ведется с 1997 г. после принятия УК РФ, в котором помещена глава 28 «Преступления в сфере компьютерной безопасности». Составы компьютерных преступлений даны в следующих статьях: «Неправомерный доступ к компьютерной информации» (ст. 272); «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273); «Нарушение правил эксплуатации ЭВМ» (ст. 274).

В соответствии с Указом Президента РФ от 12.05.2004 № 611 субъектам международного информационного обмена в РФ запрещается осуществлять включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в международную ассоциацию сетей «Интернет».

Тема 1.2 Правовой режим защиты государственной тайны

1 Правовое обеспечение защиты государственной тайны

Система защиты государственных секретов основывается на Законе РФ «О государственной тайне» от 21.07.93г. №5485-1 (ред. 11 ноября 2003г. №153) регулирующем отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах безопасности РФ.

С появлением данного Закона правоотношения в рассматриваемой сфере стали регулироваться открытыми законодательными актами, а не секретными нормативными документами государственных органов управления.

В настоящем Законе используются следующие основные понятия:

– государственная тайна (ГТ) – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

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

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

Субъектами правоотношений (в соответствии со ст.1 Закона) являются:

– органы государственного управления;

– юридические лица, независимо от их организационно-правовых форм деятельности и видов собственности;

– граждане и должностные лица, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной тайне.

В соответствии с этой нормой физическое лицо является субъектом

рассматриваемых правоотношений лишь в случае допуска к закрытым сведениям в добровольном порядке на договорной основе. В противном случае доступ к таким сведениям может быть квалифицирован как нарушение законодательства, а гражданин не может быть ограничен в своих правах, в частности, на выезд за границу и неприкосновенность частной жизни.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом о ГТ и другими нормативно-методическими документами, утвержденными в соответствии с введением в действие этого закона.

Перечень сведений, отнесенных к государственной тайне, утвержден Указом Президента РФ от 30.11.95г. №1203 (уточнен Указом Президента РФ от 11.02.2006 № 90).

К сведениям, представляющим государственную тайну, относят:

– информацию в военной области;

– информацию о внешнеполитической и внешнеэкономической деятельности;

– информацию в области экономики, науки и техники;

– сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

В частности, в сферах экономики, науки и техники к государственной тайне относятся сведения:

– о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение;

– о методах и средствах защиты секретной информации;

– о государственных программах и мероприятиях в области защиты государственной тайны.

Правила, по которым определяется степень секретности сведений, представляющих государственную тайну утверждены постановлением Правительства РФ №870 от 04.09.1995г.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается. Порядок засекречивания сведений, составляющих государственную тайну, основан на трех принципов: законности, обоснованности и своевременности. Принцип законности заключается в том, что засекречиванию не подлежат сведения, указанные в статье 7 закона о ГТ (которые раньше относились к ГТ):

– о чрезвычайных происшествиях и катастрофах;

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

– о привилегиях и льготах гражданам, должностным лицам, предприятиям;

– о фактах нарушения прав и свобод человека и гражданина;

– о размерах золотого запаса и государственных валютных резервах;

– о состоянии здоровья высших должностных лиц;

– о фактах нарушения законности органами государственной власти и их должностными лицами.

Виновные в нарушении требований закона должностные лица могут быть привлечены к уголовной, административной или дисциплинарной ответственности. Все граждане вправе обжаловать такие действия в суде.

Принцип обоснованности заключается в установлении целесообразности засекречивания сведений по экономическим или иным критериям.

Принцип своевременности заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью путем утверждения соответствующих перечней.

Право принятия решения по засекречиванию сведений принадлежит руководителю органа государственной власти, который утвердил тот или иной конкретный перечень (ст. 9).

В статье 10 Закона сказано об ограничении прав собственности юридических и физических лиц на информацию в связи с ее засекречиванием.

Должностные лица, наделенные полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся у собственника информации, если эта информация включает сведения, перечисленные в перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником.

При засекречивании сведений их носителям присваивается соответствующий гриф секретности.

Материальными носителями сведений, содержащих ГТ или другую информацию ограниченного доступа, являются: бумага, магнитная лента, физические поля, фото- и кинопленка, дискеты, лазерные диски и др. носители.

На носители сведений, составляющих государственную тайну, наносятся

– реквизиты, включающие следующие данные:

– о степени секретности сведений со ссылкой на соответствующий пункт перечня сведений, подлежащих засекречиванию;

– об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

– о регистрационном номере;

– о дате или условии рассекречивания сведений.

При невозможности нанесения таких реквизитов на носитель эти данные указываются в сопроводительной документации на этот носитель.

Не может быть ограничено право собственности на информацию иностранных юридических лиц и граждан, если она получена без нарушения законодательства РФ.

Постановлением Правительства РФ №170 от 20.02.95 г. установлен порядок рассекречивания и продления сроков засекречивания архивных документов.

Основаниями для рассекречивания сведений являются:

– взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;

– изменение обстоятельств, вследствие чего дальнейшая защита сведений является нецелесообразной.

Органы государственной власти обязаны не реже чем через каждые 5 лет пересматривать содержание действующих перечней.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании.

В статье 17 и 18 указан порядок передачи сведений, составляющих государственную тайну.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам осуществляется с разрешения органа государственной власти только при наличии у предприятия, лицензии на проведение работ с соответствующей степени секретности, а у граждан - соответствующего допуска.

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством РФ при наличии экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

Режим защиты государственных секретов обеспечивается уполномоченными органами. Эти органы организуют и обеспечивают защиту информации, содержащей государственную тайну, в соответствии с функциями, возложенными на них законодательством РФ.

К органам защиты государственной тайны относятся:

– межведомственная комиссия по защите государственной тайны;

– органы федеральной исполнительной власти: ФСБ, МО, СВР, ФСТЭК.

Лица, которые имеют право решать вопросы по отнесению сведений к ГТ, определены распоряжением Президента РФ от 30.05.97г. №226-рп «О перечне должностных лиц органов государственной власти, наделенных полномочиями по отнесению сведений к государственной тайне».

Допуск должностных лиц и граждан к государственной тайне предусматривает:

– принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;

– согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;

– письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

– определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;

– ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

– принятие решения руководителем органа государственной власти или

– предприятия, о допуске лица к сведениям, составляющим государственную тайну.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

– процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

– преимущественное право при прочих равных условиях на оставление на работе при проведении организационных или штатных мероприятий.

Постановлением Правительства РФ №573 от 18.09.2006г установлен размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке). Так за работу со сведениями, имеющими степень секретности «особой важности», надбавка составляет 50-75 процентов; имеющими степень секретности «совершенно секретно»: 30- 50 процентов; имеющими степень секретности «секретно» при оформлении допуска с проведением проверочных мероприятий: 10-15 процентов, без проведения проверочных мероприятий: 5 - 10 процентов.

Устанавливаются три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих ГТ.

Особый порядок допуска к ГТ.

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных статьей 21 настоящего Закона.

Должностное лицо или гражданин, допущенные, или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в следующих правах:

– права выезда за границу на срок, оговоренный в трудовом договоре при оформлении допуска к ГТ;

– права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

– права на неприкосновенность частной жизни при проведении проверочных мероприятий.

Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Допуск предприятий и организаций к проведению работ, связанных с использованием сведений, составляющих ГТ, созданием средств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите государственной тайны, осуществляется путем получения ими, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение работ с использованием сведений, составляющих ГТ, выдается предприятию, учреждению, организации при выполнении ими следующих условий (ст. 27):

– выполнение требований, утверждаемых Правительством РФ, по обеспечению защиты ГТ;

– наличие в их структуре подразделений по защите ГТ и специально

– подготовленных сотрудников для работы по защите информации;

– наличие у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на ФСБ, МО, СВР, ФСТЭК. Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

2 Контроль и надзор за обеспечением защиты государственной тайны

В соответствии со статьями 30 и 32 закона установлен ведомственный и межведомственный контроль и прокурорский надзор за обеспечением защиты государственной тайны.

Контроль за обеспечением защиты ГТ осуществляют Президент и Правительство РФ.

Межведомственный контроль осуществляют: ФСБ, МО, СВР, ФСТЭК.

Надзор за соблюдением законодательства осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

Уголовно-правовая ответственность за разглашение информации, содержащей государственную тайну, определяется Уголовным кодексом РФ: ст. 275, 276, 283, 284. В частности, статьей 283 определено, что разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены, наказывается арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. То же деяние, с тяжкими последствиями, наказываются лишением свободы от трех до семи лет с лишением права занимать определенные должности на срок до трех лет.

В законодательных актах установлены правовые нормы в отношении прав, обязанностей и ответственности субъектов, участвующих в информационном обмене.

Предметом правового регулирования в информационной сфере являются:

– создание и распространение информации;

– формирование и использование информационных ресурсов;

– реализация права на поиск, получение, передачу и потребление информации;

– создание и применение информационных систем и технологий;

– создание и применение средств информационной безопасности.

Ответственность, возлагаемая в случаях правонарушений в информационной сфере, формулируется в различных нормативных правовых актах. Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в основном в Уголовном и др. кодексах РФ.

Уголовное право регулирует отношения в области наиболее опасных правонарушений (преступлений).

Санкции за нарушение информационных правоотношений представлены в УК следующими статьями:

1) Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

2) Статья 140. Отказ в предоставлении гражданину информации.

3) Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

4) Статья 272. Неправомерный доступ к компьютерной информации.

5) Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

6) Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

7) Статья 275. Государственная измена.

8) Статья 276. Шпионаж.

9) Статья 283. Разглашение государственной тайны.

10) Статья 284. Утрата документов, содержащих государственную тайну.

Тема 1.3 Правовые режимы защиты информации конфиденциального характера

1 Правовая защита конфиденциальной информации.

В действующем законодательстве РФ упоминается более 40 видов тайн (банковская, налоговая, коммерческая, профессиональная и т.д.), требующих введения режима конфиденциальности, и их число постоянно увеличивается. Указом Президента РФ от 06.03.97 г. № 188 был утвержден Перечень сведений «конфиденциального характера», где указаны шесть видов такой информации:

- персональные данные;
- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них.

В соответствии с нормами международного права и Конституции РФ данный перечень должен быть в дальнейшем утвержден законом. Конфиденциальность сведений отражает гриф, устанавливаемый на материальном носителе информации. Для обозначения грифа конфиденциальности используются международные и национальные нормативные документы. Причем требования российского законодательства отличаются от утвержденных стандартов ISO 17799 «Безопасность информационных международных стандартов». Так в соответствии с ISO 17799 используются следующие обозначения:

- ОТ–открытая информация;
- КИ –конфиденциальная информация;
- СКИ – строго конфиденциальная информация.

В российском законодательстве используются следующие грифы конфиденциальности:

– ОТ – открытая информация;

– ДВИ – для внутреннего использования;

– КИ – конфиденциальная информация.

2 Нормативно-правовое регулирование профессиональной и служебной тайны

2.1 Нормативно-правовое регулирование профессиональной тайны

К числу тайн частной жизни относятся личные тайны, доверенные представителям определенных профессий (адвокату, врачу, священнику, психологу, нотариусу, банкиру, налоговому инспектору, депутату, журналисту и др.).

Профессиональная тайна – защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой и не являющаяся государственной или коммерческой тайной, распространение которой может нанести ущерб интересам лица, доверившего эти сведения.

В соответствии с данным определением можно выделить следующие объекты профессиональной тайны:

1) Врачебная тайна – информация содержащая: результаты обследования лица, вступающего в брак; сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья.

2) Тайна связи – тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

3) Нотариальная тайна – сведения, доверенные нотариусу в связи с совершением нотариальных действий.

4) Адвокатская тайна – сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи.

5) Тайна усыновления – сведения об усыновлении ребенка усыновителем.

6) Тайна страхования – сведения о страхователе, застрахованном лице и выгодоприобретателе.

7) Тайна исповеди – сведения, доверенные священнослужителю гражданином на исповеди.

К правовым документам о профессиональной тайне относятся:

1) Законы РФ – ГК РФ (ст. 964); ГПК РСФСР (ст.9); УК РФ (ст.155); УПК РСФСР (ст.51); Семейный кодекс РФ (ст.15, 139); ФЗ от 16.02.1995г. «О связи» (ст.32); «Основы законодательства РФ об охране здоровья граждан» от 22.07.1993г. (ст.30,31,35,49,61); закон РФ от 02.07.1992г. «О психиатрической помощи и гарантиях прав граждан при ее оказании» (ст.9,46); ФЗ от 25.07.2002г. №112 «О религиозных объединениях»; закон РСФСР от 20.11.1980г. «Об утверждении положения об адвокатуре РСФСР» (ст. 16); «Основы законодательства РФ о нотариате» от 10.02.1993г. (ст.5, 14,16,17,28,34); закон РФ от 22.12.1992г. «О трансплантации органов и (или) тканей человека» (ст.14); ФЗ «О социальном обслуживании граждан пожилого возраста и инвалидов» от 17.05.1995г. №122 – ФЗ (ст.11).

2) Подзаконные акты – постановления Правительства РФ №352 от 28.05.1992г. (в ред. Постановления №792 от 02.07.1997г.) «О заключении межправительственных соглашений об избежании двойного налогообложения доходов и имущества» (ст.23); №1235 от 26.09.1997г. «Об утверждении правил оказания услуг телефонной связи» (п.8); №1239 от 26.09.1997г. «Об утверждении правил оказания услуг почтовой связи (п.132,140); №1017 от 13.10.1995г.; №221 от 28.02.1996г. «Об утверждении правил обязательного медицинского освидетельствования на выявление ВИЧ-инфекции» и др.

3) Судебная практика – постановление Конституционного суда РФ №8-П от 27.03.1996г. (в части профессиональной тайны адвоката); постановления Пленума Верховного суда РФ №10 от 20.12.1994г. «Некоторые вопросы применения законодательства о компенсации морального вреда» и др.

4) Международные договоры и соглашения – более 30 двусторонних соглашений об избежание двойного налогообложения доходов и имущества и др.

В современном законодательстве РФ не дано чёткого определения профессиональной тайны, хотя она выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим федеральный закон «О профессиональной тайне».

В законодательстве не предусматривается сегодня возможность доступа к профессиональной тайне, со стороны государственных органов – только в двух случаях: в отношении адвокатской тайны и тайны исповеди.

В УК РФ прямо предусматривается уголовная ответственность лишь в случае разглашения двух видов профессиональной тайны – тайны усыновления (ст. 155 УК РФ) и тайны связи (глава 19, ст. 138 УК РФ).

2.2 Нормативно-правовое регулирование служебной тайны

Должностная служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления.

Доступ к профессиональным сведениям закрытого характера связан с

должностным статусом лица, которому эти сведения стали известны по службе. Поэтому при утечки этой секретной информации страдают интересы службы (в отличие от интересов клиентов в случае профессиональной тайны).

Примерами таких противоправных действий являются: разглашение судьями тайны совещания при вынесении приговора, должностными лицами Банка России банковской тайны, работниками налоговой инспекции налоговой тайны (сведения о налогоплательщике).

Определение понятия «служебная тайна» дано в ст.139 части первой ГК РФ, называющейся «Служебная и коммерческая тайна»: 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.

Нормативно-правовыми документами в отношении защиты служебной тайны являются:

1) Закон РФ от 31.07.95 №119-ФЗ «Об основах государственной службы РФ».

2) Закон РФ от 17.01.92 №2202-1 (ред. от 10.02.99) «О прокуратуре РФ».

3) Закон РФ от 02.12.90 №395-1 (ред. от 31.07.98 №151) «О банках и банковской деятельности».

4) Закон РФ от 18.04.91. №1026-1 (ред. от 15.06.96 № 73-ФЗ) «О милиции».

5) Закон РФ от 12.08.95г. №144-ФЗ «Об оперативно-розыскной деятельности».

6) Закон РФ от 16.02.95 №15-ФЗ (ред. от 06.01.99) «О связи».

7) Закон РФ от 29.07.2004г. №98-ФЗ «О коммерческой тайне».

8) Гражданский код кодекс РФ от 13.06.96 №63-ФЗ (ред. от 09.02.99).

9) Таможенный кодекс РФ утв. ВС РФ 18.06.1993 г. №5221-1 (ред. от 10.02.1999 г.).

В качестве примера рассмотрим правовую защиту налоговой и коммерческой тайны.

Понятие налоговой тайны введено Налоговым кодексом РФ. Согласно ст.102 НК РФ – это сведения о налогоплательщике, полученные налоговой инспекцией или таможенным органом при налоговом контроле.

Режим хранения сведений, составляющих НТ, и доступа к ним устанавливается ФНС РФ. Часть 4 ст.102 НК РФ определяет два вида нарушений в отношении НТ:

– разглашение НТ;

– утрата документов, содержащих налоговую тайну организации.

За эти нарушения виновные привлекаются к ответственности.

За утрату документов сотрудники налоговых органов несут дисциплинарную ответственность. Если же при этом по их вине разглашена не только налоговая, но и коммерческая или банковская тайна, то может наступить уголовная ответственность по ст.183 УК РФ.

Утрата документов и предметов, содержащих секретные сведения, не повлекшая за собой тяжких последствий – состава преступления не образует.

Материальные носители секретных сведений имеют регистрационный номер, гриф секретности, установленный порядок хранения, выдачи, размножения и уничтожения. Они могут быть официальными или неофициальными (черновики, наброски).

В условиях жесткой конкуренции фирмы прилагают значительные усилия для сбора информации о рынке, о партнерах и другой полезной информации. Как правило, эти действия носят разведывательный характер и нацелены, прежде всего, на получение коммерческой тайны (КТ) конкурента.

Принято различать конкурентную разведку («деловая разведка», «бизнес-разведка») и промышленный шпионаж:

1) Конкурентная разведка – это сбор и обработка информации законными способами.

2) Промышленный шпионаж - незаконный сбор сведений, составляющих коммерческую тайну, незаконное использование секретной информации лицом или предприятием, не уполномоченным на то ее владельцем.

Понятие «коммерческая тайна» в нашем законодательстве впервые появилось в 1990 году в тексте Закона о предприятиях и предпринимательской деятельности. Затем в Законе РФ «Об информации, информатизации и защите информации», от 25.01.95г., в Гражданском кодексе РФ, ч.1. и, наконец, в Законе «О коммерческой тайне», от 29.07.2004г. №98-ФЗ.

Закон «О коммерческой тайне» регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

Коммерческая тайна – конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (ст. 3).

Это – научно-техническая, технологическая, производственная, финансово-экономическая информация, в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Сведения, которые не могут составлять коммерческую тайну (ст. 5):

– учредительные документах юридического лица, документы, подтверждающие факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

– документы, дающие право на осуществление предпринимательской деятельности;

– о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

– о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической обстановке и других факторах;

– о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

– о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

– о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;

– об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

– о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

– о перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

Обладатель информации, составляющей коммерческую тайну, по требованию органа государственной власти предоставляет ее на безвозмездной основе (ст. 6). Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

3 Организационные меры по охране конфиденциальности информации

Организационные меры по охране конфиденциальности информации должны включать (ст. 10):

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

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

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

– нанесение на документы, содержащие коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Охрана конфиденциальности информации в рамках трудовых отношений (ст. 11).

Работодатель обязан:

– ознакомить под расписку работника с перечнем информации, составляющей коммерческую тайну;

– ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

– создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Причиненные ущерб не возмещается работником или прекратившим трудовые отношения лицом, если разглашение информации, составляющей коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанности по обеспечению режима коммерческой тайны.

Работник обязан не разглашать коммерческую тайну после прекращения трудового договора в течении 3-х лет даже, если соглашение о конфиденциальности не заключалось (ст. 11).

В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством РФ.

Ответственность за нарушение настоящего закона (ст. 14) влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Органы государственной власти, несут гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

Ответственность за разглашение сведений, составляющих коммерческую тайну, дана в УК РФ в статье 183: Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну:

1) Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного пользования этих сведений наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо лишением свободы на срок до двух лет.

2) Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

Согласно части 2 данной статьи субъектом преступления могут быть также любые лица, включая должностных лиц, имевших доступ к сведениям, составляющим коммерческую или банковскую тайну.

Для обозначения степени важности коммерческой информации предприятие может использовать следующие грифы конфиденциальности:

1) Коммерческая тайна – строго конфиденциально (КТ-СК).

2) Коммерческая тайна – конфиденциально (КТ-К).

3) Коммерческая тайна (КТ).

4) Промежуточный гриф рекомендуется использовать ДВИ – для внутреннего использования.

В законодательных актах установлены правовые нормы в отношении прав, обязанностей и ответственности субъектов, участвующих в информационном обмене.

Предметом правового регулирования в информационной сфере являются:

– создание и распространение информации;

– формирование и использование информационных ресурсов;

– реализация права на поиск, получение, передачу и потребление информации;

– создание и применение информационных систем и технологий;

– создание и применение средств информационной безопасности.

Ответственность, возлагаемая в случаях правонарушений в информационной сфере, формулируется в различных нормативных правовых актах. Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в основном в Уголовном и др. кодексах РФ.

Уголовное право регулирует отношения в области наиболее опасных правонарушений (преступлений).

Санкции за нарушение информационных правоотношений представлены в УК следующими статьями:

11) Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

12) Статья 140. Отказ в предоставлении гражданину информации.

13) Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

14) Статья 272. Неправомерный доступ к компьютерной информации.

15) Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

16) Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

17) Статья 275. Государственная измена.

18) Статья 276. Шпионаж.

19) Статья 283. Разглашение государственной тайны.

20) Статья 284. Утрата документов, содержащих государственную тайну.

Тема 1.4 Государственное регулирование деятельности в области защиты информации

1 Правовая основа системы лицензирования и сертификации в РФ

Лицензирование - это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ. Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования.

Лицензия – документ, дающий право на осуществление указанного вида деятельности в течение определенного времени.

Перечень видов деятельности в области ЗИ, на которые выдаются лицензии, определен Постановлением Правительства РФ – «О лицензировании отдельных видов деятельности» от 24.12.1994 №1418 к ним, в частности, относится разработка, производство, реализация и сервисное обслуживание:

- шифровальных средств;
- защищенных систем телекоммуникаций;
- программных средств;
- специальных технических средств ЗИ.

А также подготовка и переподготовка кадров.

Сертификация - это подтверждение соответствия продукции или услуг установленным требованиям или стандартам. Сертификат –документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Законодательной и нормативной базой лицензирования и сертификации в области ЗИ являются законы РФ:

1) «О государственной тайне» от 21.07.1993 №5485-1.
2) «О техническом регулировании» от 27.12. 2002 г. № 184-ФЗ.
3) «О лицензировании отдельных видов деятельности», от 8.08. 2001г. №128 (ред. от 11.03.2003г. №32).
4) «О защите прав потребителей» от 07.02.1992 №2300-1.

Постановления Правительства РФ:

1) «О лицензировании отдельных видов деятельности» от 24.12.1994 № 1418.
2) «О лицензировании деятельности предприятий...» от 15.04.95 №333.
3) «О сертификации средств ЗИ» от 26.06.95 №608.
4) «О лицензировании…» от 27.05.2002 №348.
5) «О лицензировании…» от 30.04.2002 №290, (ред. №64 от 6.02.2003).

А также Указы Президента РФ, и ряд подзаконных актов.

2 Лицензирование деятельности по защите государственной тайны

Общие нормы, устанавливающие порядок организации и осуществления этой деятельности, содержатся в статье 27 Закона «О государственной тайне».

Основные положений данной статьи:

– лицензия выдается только на основании результатов специальной экспертизы (проверки готовности организации к работе со сведениями, составляющими государственную тайну);

– в структуре организации должно быть подразделения по защите

– государственной тайны (ГТ) и специально подготовленные сотрудники;

– организация должна иметь сертифицированные средства защиты информации;

– необходима государственная аттестация руководителей организации, ответственных за защиту государственных секретов.

Постановлением Правительства РФ № 333 утверждено Положение о лицензировании деятельности предприятий, в котором установлено, что:

– лицензия разрешает осуществление конкретного вида деятельности в течение установленного срока на всей территории РФ, а также в учреждениях РФ, находящихся за границей;

– органами, уполномоченными на ведение лицензионной деятельности, являются:

1) По допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности РФ (ФСБ) и ее территориальные органы (на территории РФ), Служба внешней разведки РФ (СВР) (за рубежом).

2) На право проведения работ, связанных с созданием средств защиты информации – Федеральная служба технического и экспортного контроля (ФСТЭК), ФСБ.

3) На право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – ФСБ, ФСТЭК, СВР.

Лицензирование деятельности предприятий ФСБ, МО (министерства обороны), СВР и ФСТЭК по допуску к проведению работ, связанных с использованием сведений, составляющих государственную тайну, осуществляется руководителями министерств и ведомств РФ, которым подчинены указанные предприятия.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет. Продление срока действия лицензии производится в порядке, установленном для ее получения. На каждый вид деятельности выдается отдельная лицензия.

Основанием для отказа в выдаче лицензии является:

– наличие в представленных документах недостоверной или искаженной информации;

– отрицательное заключение экспертизы;

– отрицательное заключение по результатам государственной аттестации

– руководителя предприятия.

Специальные экспертизы предприятий выполняются по следующим направлениям:

– режим секретности;

– противодействие иностранной технической разведке;

– защита информации от утечки по техническим каналам.

Экспертные комиссии формируются при ФСБ, ФСТЭК и их органах на местах и аттестационных центрах.

Принципы лицензирования:

1) Лицензирование в области защиты ГТ является обязательным.

2) Деятельность в области ЗИ лиц, не прошедших лицензирование, запрещена (с применением соответствующих статей гражданского и уголовного кодексов к нарушителям).

3) Лицензии на право деятельности в области ЗИ выдаются только юридическим лицам независимо от организационно - правовой формы (физические лица не в состоянии удовлетворить указанным требованиям).

4) Лицензии выдаются только предприятиям, зарегистрированным на территории РФ на основании специальной экспертизы заявителя.

Для получения лицензии предприятие обязано предъявить следующий перечень документов:

– копия свидетельства о государственной регистрации предприятия;

– копии учредительных документов, заверенных нотариусом;

– копии документов на право собственности или аренды имущества, необходимого для ведения заявленной деятельности;

– справка налогового органа о постановке на учет;

– представление органов государственной власти РФ с ходатайством о выдаче лицензии;

– документ, подтверждающий оплату рассмотрения заявления.

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо аттестационными центрами. Например, коммерческому банку, претендующему на получение лицензии на эксплуатацию шифровальных средств для защиты конфиденциальной информации предъявляются требования по:

– наличию и составу необходимых аппаратно-программных средств и помещений;

– размещению, охране и специальному оборудованию помещений, в которых

– находятся средства криптографической ЗИ;

– обеспечению режима и порядка доступа к средствам криптографической ЗИ;

– обеспечению необходимой технической и эксплуатационной документацией;

– уровню квалификации и подготовленности специалистов в области защиты и эксплуатации АС;

– режиму эксплуатации и хранения средств криптографической ЗИ.

Государственная аттестация руководителей ответственных за ГТ. Основная цель государственной аттестации – повысить компетентность руководителей в части обеспечения сохранности сведений, составляющих государственную тайну.

Документом, по организации государственной аттестации руководителей является «Инструкция о порядке проведения государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну», утвержденная Председателем Гостехкомиссии России 17.10.1995 г.

Государственное аттестование проводится методом собеседования аттестационной комиссии с руководителем предприятия. К аттестуемому предъявляются следующие требования.

Должен знать:

– законодательные акты РФ по вопросам защиты государственной тайны;

– нормативные документы, утверждаемые Правительством РФ по обеспечению защиты сведений, составляющих государственную тайну;

– нормативно-методические документы по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, утверждаемые ФСБ и ГТК;

– перечень продукции предприятия, подлежащей защите от разведок, основные охраняемые сведения о предприятии и выпускаемой продукции;

– возможные каналы утечки информации по всему технологическому циклу разработки, изготовления и испытаний продукции предприятия;

– деловые и моральные качества сотрудников структурного подразделения предприятия по защите государственной тайны.

Должен уметь организовывать:

– разработку мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих государственную тайну, и оценку их достаточности;

– проведение анализа возможностей разведки по добыванию сведений,

– составляющих государственную тайну;

– аттестование рабочих мест по всему технологическому циклу разработки, изготовления и испытания продукции;

– комплексный контроль выполнения принимаемых мер по защите сведений, составляющих государственную тайну.

Быть ознакомленным:

– с государственной системой лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– с возможностями иностранных разведок по добыванию сведений, составляющих государственную тайну;

– с методиками контроля выполнения норм противодействия иностранным техническим разведкам.

От государственной аттестации освобождаются руководители предприятий, окончившие учебные заведения, готовящие специалистов по специальностям защиты информации.

3 Сертификация средств защиты информации

Национальный орган по сертификации определяется Правительством РФ. В настоящее время эти функции выполняет Федеральное агентство по техническому регулированию и метрологии.

Сертификация средств защиты информации, прежде всего, подразумевает проверку их качественных характеристик для реализации основной функции – защиты информации на основании государственных стандартов и требований по безопасности информации.

Общие принципы сертификации средств защиты ГТ определены нормами статьи 28 Закона «О государственной тайне» - средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством РФ. Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ. Положение о сертификации средств защиты информации, утверждено постановлением Правительства РФ от 25.06.95 г. № 608. Это положение зарегистрировано Госстандартом России в Государственном реестре 20 марта 1995 г. (Свидетельство № Р0СС RU. 0001. 01БИ00).

Принципы сертификации:

1) Сертификация изделий, обеспечивающих защиту ГТ, является обязательной.

2) Обязательность использования криптографических алгоритмов, являющихся стандартами.

3) Принятие на сертификацию изделий только от заявителей, имеющих лицензию.

В соответствии с вышеназванными документами, государственным организациям и предприятиям запрещено использование в информационных системах шифровальных средств, не имеющих сертификата.

Кроме этого в области информационных технологий действуют системы добровольной сертификации банковских технологий (МЕКАС) и средств связи.

Порядок сертификации:

1) В Центральный орган по сертификации подается заявление и полный комплект технической документации.

2) Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.

3) Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.

4) Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется Центральным органом.

Сертификат выдается на срок до 5 лет.

4 Лицензирование и сертификация в области защиты конфиденциальной информации

Лицензирование деятельности в области защиты конфиденциальной информации основано на Законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ (ред. от 11 марта 2003 г. № 32-ФЗ).

Действие данного закона не распространяется на следующие виды деятельности,

связанные с ЗИ:

– деятельность, связанная с защитой государственной тайны;

– деятельность в области связи;

– использование результатов интеллектуальной деятельности.

В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности в области ЗИ:

– разработка, производство, распространение, техническое обслуживание и предоставление услуг в области шифрования информации; шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– деятельность по выдаче сертификатов ключей электронных цифровых подписей,

– регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

– деятельность по выявлению электронных устройств, предназначенных для

– негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации;

– разработка, производство, реализация и приобретение в целях продажи

– специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Срок действия лицензии не может быть менее чем пять лет и может быть продлен по заявлению лицензиата.

Продление срока действия лицензии осуществляется в порядке переоформления документа, подтверждающего наличие лицензии.

В систему сертификации могут входить организации независимо от форм собственности, а также общественные объединения.

Постановление Правительства РФ от 23.04.96 № 509 устанавливает порядок сертификации средств защиты информации в РФ и ее учреждениях за

рубежом. Это 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.

Системы сертификации создаются ФСТЭК, ФСБ, Министерством обороны и СВР.

Система сертификации средств защиты информации в РФ осуществляется по требованиям безопасности информации, определенным ФСТЭК.

Положение о сертификации средств защиты информации по требованиям безопасности информации ведено в действие приказом Председателя Гостехкомиссии России от 27 октября 1995 г. № 199. В соответствии с которым обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом, а также средства, использующиеся в управлении экологически опасными объектами. В остальных случаях сертификация носит добровольный характер (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

Сертификационные испытания средств защиты в рамках данной системы сертификации предусматривают комплекс мероприятий по проверке соответствия этих средств формальным базовым требованиям по обеспечению безопасности информации, изложенным в нормативных документах ФСТЭК.

Тема 1.5 Правовая охрана результатов интеллектуальной деятельности

1 Объекты интеллектуальной собственности

Результатом интеллектуальной деятельности является информационный продукт, который представляется на рынке в виде информационных товаров и услуг.

Впервые же понятие «интеллектуальная собственность» прозвучало у нас в 1990 году в тексте Закона «О собственности в РСФСР».

Законодательными актами РФ регламентируется право собственности на информацию, полученную юридическими и физическими лицами в результате интеллектуальной деятельности. Это исключительное право представляет собой интеллектуальную собственность.

Определение «интеллектуальная собственность» дано в Конвенции, учреждающей Всемирную организацию интеллектуальной собственности (ВОИС), принятой на Стокгольмской конференции в 1967 году и ратифицированной в 1968 году СССР. В российском законодательстве вопросы защиты ИС рассмотрены в 1-й и 2-й частях ГК РФ.

Интеллектуальная собственность (ГК часть 1, ст.138) – исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполненных работ или услуг (фирменное наименование, товарный знак и т.п.). Использование результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

Уточнения даны в 4-й части ГК РФ, принятой 18.12.2006 г. № 230.

Результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

- произведения науки, литературы и искусства;
- программы для электронных вычислительных машин (ЭВМ);
- базы данных;
- исполнения;
- фонограммы;
- сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- изобретения;
- полезные модели;
- промышленные образцы;
- селекционные достижения;
- топологии интегральных микросхем;
- секреты производства (ноу-хау);
- фирменные наименования;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров;
- коммерческие обозначения.

На результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации) признаются интеллектуальные права, которые включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права и иные права (право следования, право доступа и другие).

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности: авторское право, патентное право, и секреты производства.

Авторское право – форма правовой защиты в отношении литературных, художественных и научных произведений.

Патентное право – форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

Секреты производства (ноу-хау) – форма правовой защиты любых полезных сведения (производственных, технических, экономических, организационных и других).

Историческая справка:

1) Первый закон об авторском праве был принят в Англии в 1710 году. Охрана личных прав давалась на 14 лет с продлением еще на 14 лет.

2) Первым патентным законом была Декларация Венецианской республики в 1474г. Изобретатель получал привилегию (патент) на 10 лет. В России выдача привилегий началась с 1748г. Общий закон «О привилегиях…» появился в 1812 г.

В РФ до недавнего времени действовали следующие законодательные акты, защищающие права граждан и юридических лиц на результаты своей интеллектуальной деятельности:

1) Закон РФ «Об авторском праве и смежных правах», от 9.07.93г. №5351-1 (редакция от 20.07.04г. №72).

2) Закон РФ «Патентный закон РФ», от 23.09.92г. № 3517-1.

3) Закон РФ «О правовой охране программ для ЭВМ и баз данных», от 23.09.92г. №3523-1.

4) Закон РФ «О правовой охране топологий интегральных микросхем», от 23.09.92г. №3526-1.

5) Закон РФ «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров», от 23.09.92г. № 3520-1.

6) Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках», от 22.03.91г. №948-1. (Ред. от 9 октября 2002 г №122-ФЗ).

7) Закон РФ «О защите конкуренции», от 26.07.2006г. N135-ФЗ.

После вступления в силу с 1 января 2008 г. 4-й части Гражданского кодекса РФ, которая посвящена нормированию прав на результаты интеллектуальной собственности, потеряло силу большинство указанных выше законов РФ, касающихся защиты ИС.

Заключены следующие международные конвенции и соглашения, связанные с охраной интеллектуальной собственности:

1) Конвенция по охране промышленной собственности от 20 марта 1883г. (редакция от 2 октября 1979г.), заключенная в Париже.

2) Конвенция по охране литературных и художественных произведений от 9 сентября 1886г., заключенная в Берне (последняя редакция 1971г.).

3) Конвенция о международной регистрации фабричных и товарных знаков от 14 апреля 1891г. (редакция от 2 октября 1979г.), заключенная в Мадриде.

4) Всемирная (Женевская) конвенция об авторском праве от 6 октября 1952г., заключенная в Женеве.

5) Конвенция по охране интересов производителей фонограмм от незаконного воспроизведения фонограмм от 29 октября 1971г., заключенная в Женеве.

6) Конвенция, учреждающая всемирную организацию интеллектуальной собственности от 14 июля 1967г. (редакция 2 октября 1979г.), заключенная в Стокгольме.

7) Брюссельская конвенция о распространение несущих сигналов, передаваемых через спутники от 21 мая 1974г.

8) Евразийская патентная конвенция 1994 г.

9) Гаагское соглашение по международному депонированию промышленных образцов от 28 ноября 1960г. (редакция от 2 октября 1979г.).

10) Международная конвенция об охране интересов исполнителей, производителей фонограмм и вещательных организаций, заключенной в Риме 26 октября 1961г. («Римская конвенция»).

2 Правовые нормы защиты интеллектуальной собственности

2.1 Правовая охрана авторских и смежных прав

Закон регулирует отношения, возникающие при создании и использовании произведений науки, литературы и искусства (авторское право), фонограмм исполнителей, постановок, передач организаций эфирно или кабельного вещания (смежные права).

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме:

- письменной;
- устной (выступление, исполнение и т.д.);
- звуко- или видеозаписи;
- изображения (рисунок, чертеж, теле-, фотокадр и т.д.);
- объемно-пространственной (скульптура, макет и т.д.);
- в других формах.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

Автор – физическое лицо, творческим трудом которого создано произведение.

Авторское право не распространяется на идеи, методы, процессы, системы, концепции, принципы, открытия, факты.

Не являются объектами авторского права:

– официальные документы (законы, судебные решения и т.п.);
– государственные символы и знаки (флаги, гербы, ордена и т.п.);
– произведения народного творчества;
– сообщения о событиях и фактах, имеющие информационный характер.

Авторское право на произведение возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения или соблюдения, каких – либо формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 настоящего Кодекса.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов:

– латинской буквы «С» в окружности;
– имени (наименования) обладателя исключительных прав;
– года первого опубликования произведения.

При опубликовании произведения анонимно или под псевдонимом представителем автора в соответствии с данным Законом является издатель, который имеет право защищать права автора пока автор не раскроет свою личность.

При соавторстве (произведение создано двумя и более лицами), авторское право принадлежит соавторам совместно, независимо от характера и структуры произведения (неразрывное целое или имеет отдельные самостоятельные части).

Если произведение создано в порядке выполнения служебных обязанностей, (служебное произведение) то авторское право на него принадлежит автору служебного произведения, а исключительные права на его использования – работодателю.

Авторское вознаграждение при этом определяется договором между автором и работодателем.

Автору в отношении его произведений принадлежат личные неимущественные права (право признаваться автором, право обнародовать или разрешать обнародовать произведения, право на защиту произведения от искажения и др. посягательств) и исключительные имущественные права (право на использование – воспроизводить, показывать, исполнять, распространять и т.д.).

Авторское право действует в течение всей жизни автора и 70 лет после его смерти.

В сфере авторского права до 70-х годов прошлого века в России срок действия исключительных прав составлял 15 лет после смерти автора, с 1973 г. был увеличен до 25 лет.

В 1991 г. в «Основах гражданского законодательства Союза ССР» срок действия авторских прав составил 50 лет.

В 2004 г. были приняты поправки к Закону РФ «Об авторском праве и смежных правах» где действие авторского права установлено с учетом действующих международных норм в течение всей жизни автора и 70 лет после его смерти.

Поправки, вступившие в силу с 1 сентября 2006 г., означают, что размещенные в сети, например, тексты книг или музыкальные файлы в формате mp3 охраняются авторским правом так же, как обычные книги или компакт-диски. Они подпадают под действие ст. 146 Уголовного кодекса РФ («Нарушение авторских и смежных прав»), предусматривающей наказание для пиратов в виде

лишения свободы на срок до пяти лет. Теперь владельцы mp3-сайтов, например, должны подписать лицензионные соглашения со всеми поставщиками музыки. Истечение срока действия авторского права на произведения означает их переход в общественное достояние. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Знак охраны смежных прав – буква «Р» в окружности, имя обладателя прав и год первого опубликования фонограммы.

Исключительное право на исполнение действует в течение всей жизни исполнителя, но не менее пятидесяти лет, считая с 1 января года, следующего за годом, в котором осуществлены исполнение, либо запись исполнения, либо сообщение исполнения в эфир или по кабелю. По истечении срока действия исключительного права на исполнение это право переходит в общественное достояние.

Исключительное право на фонограмму действует в течение пятидесяти лет, считая с 1 января года, следующего за годом, в котором была осуществлена запись. В соответствии с законом запрещается импортировать экземпляры фонограмм в целях распространения, переделывать, продавать и воспроизводить без разрешения их правообладателей.

2.2 Правовая охрана программ для ЭВМ и баз данных

Программы для ЭВМ и базы данных относятся Законом к объектам авторского права. Программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных – как сборникам.

Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Правообладатель в течение срока действия исключительного права на программу для ЭВМ или на базу данных может по своему желанию зарегистрировать такую программу или такую базу данных в федеральном органе исполнительной власти по интеллектуальной собственности.

Исключительное право изготовителя базы данных возникает в момент завершения ее создания и действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее создания. Исключительное право изготовителя базы данных, обнародованной в указанный период, действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее обнародования.

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

Импорт, тиражирование, продажа, а также иное введение в гражданский оборот экземпляров программ без разрешения их правообладателей является нарушителем авторского права.

Суд может наложить арест на все экземпляры произведения, в отношении которых предполагается, что они являются контрафактными, а также на материалы и оборудование, используемые или предназначенные для их изготовления или воспроизведения.

Контрафактными признаются экземпляры программы, изготовление или использование которых влечет за собой нарушения авторского права.

Свободное воспроизведение произведения в личных целях (статья 1273) допускается без согласия автора или иного правообладателя и без выплаты вознаграждения за воспроизведение гражданином исключительно в личных целях, за исключением:

– воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;

– воспроизведения баз данных или их существенных частей;

– воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса (например, для архивных целей);

– репродуцирования книг (полностью) и нотных текстов;

– видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;

– воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.

2.3 Технические средства защиты авторских прав

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.

В отношении произведений не допускается:

– осуществление без разрешения автора или иного правообладателя действий, направленных на то, чтобы устранить ограничения использования произведения, установленные путем применения технических средств защиты авторских прав;

– изготовление, распространение, сдача в прокат, предоставление во временное безвозмездное пользование, импорт, реклама любой технологии, любого технического устройства или их компонентов, использование таких технических средств в целях получения прибыли либо оказание соответствующих услуг, если в результате таких действий становится невозможным использование технических средств защиты авторских прав либо эти технические средства не смогут обеспечить надлежащую защиту указанных прав.

В случаях нарушения исключительного права на произведение или на объект смежных прав правообладатель вправе требовать по своему выбору от нарушителя возмещения убытков либо выплаты компенсации:

– в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда;

– в двукратном размере стоимости экземпляров произведения или в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения.

Предусмотрена также уголовная ответственность за нарушение авторских и смежных прав (Уголовный кодекс РФ статья 146):

– незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, – наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

– те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, – наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

2.4 Охрана типологии интегральных микросхем

Топология: это зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними.

Автору топологии интегральной микросхемы, принадлежат следующие интеллектуальные права:

– исключительное право;

– право авторства.

Предоставляемая правовая охрана распространяется только на оригинальную топологию. Оригинальной является топология, созданная в результате творческой деятельности автора.

Автором топологии признается физическое лицо, в результате творческой деятельности которого эта топология была создана.

Право автора на топологию является неотъемлемым личным правом и охраняется законом бессрочно.

Правообладатель в течение срока действия исключительного права на топологию интегральной микросхемы может по своему желанию зарегистрировать топологию в федеральном органе исполнительной власти по интеллектуальной собственности.

Топология, содержащая сведения, составляющие государственную тайну, государственной регистрации не подлежит.

Автору принадлежит исключительное право использовать эту топологию по своему усмотрению, в частности путем изготовления и распространения ИМС с такой топологией, включая право запрещать использование этой топологии другим лицам без соответствующего разрешения.

Нарушением исключительного права на использование топологии признается совершение следующих действий без разрешения автора или иного правообладателя:

– воспроизведение топологии в целом или частично, за исключением копирования только той ее части, которая не является оригинальной;

– ввоз на территорию Российской Федерации, продажа и иное введение в гражданский оборот топологии, или интегральной микросхемы, в которую включена эта топология, или изделия, включающего в себя такую интегральную микросхему.

Имущественные права на топологию, созданную в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю, если договором не предусмотрено иное.

Правообладатель для оповещения о своем исключительном праве на топологию вправе использовать знак охраны, который помещается на топологии, а также на изделиях, содержащих такую топологию, и состоит из выделенной прописной буквы «Т» («Т», [Т], Т*, буквы «Т» в окружности, или буквы «Т» в квадрате), даты начала срока действия исключительного права на топологию и информации, позволяющей идентифицировать правообладателя.

Исключительное право на использование топологии действует в течение десяти лет. Автор топологии и иной правообладатель вправе требовать:

– признания прав;

– возмещения причиненных убытков.

За защитой своего права автор может обратиться в суд (арбитражный или третейский).

Автор может требовать правовую охрану топологии в зарубежных странах. Если международным договором РФ установлены иные правила, чем те, которые содержатся в настоящем Законе, то применяются правила международного договора.

Тема 1.6 Преступления в сфере компьютерной информации

1 Классификация компьютерных преступлений

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. По кодификатору Интерпола (в 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен в более чем 100 странах) все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q.

Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

1) QA – Несанкционированный доступ и перехват.
2) QD – Изменение компьютерных данных.
3) QF – Компьютерное мошенничество.
4) QR – Незаконное копирование.
5) QS – Компьютерный саботаж.
6) QZ – Прочие компьютерные преступления.

Например, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:

1) QAH – «Компьютерный абордаж» (хакинг - hacking): неправомерный доступ в компьютер или сеть. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

2) QAI – перехват (interception): перехват при помощи технических средств, без правана то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновыесистемы, системы спутниковой связи, а

также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup).

Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

3) QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая терминология:

1) «Жучок» (bugging) – характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала.

2) «Откачивание данных» (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе.

3) «Уборка мусора» (scavening) – характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д.; электронный вариант требует исследования данных, оставленных в памяти машины.

4) Метод следования «За дураком» (piggbackiiig), характеризующий несанкционированное проникновение, как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним.

5) Метод «За хвост» (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.

6) Метод «Неспешного выбора» (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

7) Метод «Поиск бреши» (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно.

8) Метод «Люк» (trapdoor), являющийся развитием предыдущего. В найденной «бреши» программа «разрывается» и туда вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу.

9) Метод «Маскарад» (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.

10) Метод «Мистификация» (spoofing), который используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например, коды пользователя.

Анализ компьютерных преступлений. С целью совершенствования методов расследования, правоохранительные органы проводят анализ компьютерных преступлений. Разрабатываются системы адаптации «традиционных» методов расследования преступлений с использованием компьютерных средств.

Диапазон компьютерных преступлений в настоящее время расширился и включает кроме традиционного мошенничества также киберслежку, мошенничество с инвестициями, сексуальные домогательства, кражу информации, внутригосударственный и международный терроризм, нарушение авторских прав, фальсификацию систем, насильственные преступления, жестокое обращение с пожилыми.

По мере развития электронной коммерции число компьютерных преступлений будет соответствующим образом расти. Для анализа преступлений теперь требуются не только региональные, но и международных средств анализа. Эти системы могут объединять преступления по местоположению, времени и методу действий, что может помочь прогнозировать потенциальные будущие угрозы.

В университете Карнеги-Меллона создана группа «скорой компьютерной помощи» Computer Emergency Response Team (CERT), которая ставит своей целью анализ и разработку мер противодействия компьютерным преступлениям. Проделанная этой группой работа показывает, насколько важно понять мотивы преступника. Понимание целей, которые ставит перед собой злоумышленник, позволяет определять его будущие поступки.

Для выявления нарушений системной защиты используются методы активной добычи данных. Такой подход предполагает анализ поступков, которые приводят к нарушениям, и сравнивает их с поведением при нормальной работе. Добывается информация о часто встречающейся последовательности действий. Эти сведения используются для создания автоматического классификатора, который способен различать агрессивное и нормальное поведение.

2 Криминалистические особенности расследования компьютерных преступлений.

Главная проблема при расследовании преступлений в компьютерных системах заключается в установлении самого факта совершения преступления. Особенность состоит в том, что для того, чтобы утверждать, что было совершено преступление с использованием компьютера, необходимо доказать:

– факт, что компьютерная информация, к которой произведен несанкционированный доступ, охраняется законами РФ;

– факт, что злоумышленником были осуществлены определенные неправомерные действия;

– факт, что самими несанкционированными действиями нарушены права собственника информации;

– факт несанкционированного доступа к средствам компьютерной техники либо попытка получения такого доступа;

– факт использования злоумышленником полученных в результате неправомерных действий денежных средств в своих целях.

Например, необходимо доказать, что доступ был несанкционированным с целью совершения преступления. Тогда установлению и доказыванию подлежит:

– факт, что действительно были совершены несанкционированные манипуляции, например, с программным обеспечением;

– факт, что, эти манипуляции были недозволенными;

– факт, что лицо, совершавшее их, знало об этом и осуществляло их с целью преступного умысла.

Комплекс следственных действий обязательных для первоначального этапа расследования должен включать:

1) Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей машинной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному отношению программного обеспечения или носящих иные следы подготовки к хищению денежных средств.

2) Исследование: журналов сбойных ситуаций, рабочего времени ЭВМ, по передачи смен операторами; средств защиты и контроля банковских компьютерных систем, регистрирующих пользователей, моменты включения (активации) системы либо подключение к ним абонентов с определенным индексом или без такового; протоколов вечернего решения, представляющих собой копию действий операторов, отображенную на бумажном носителе в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня; контрольных чисел файлов; всего программного обеспечения ЭВМ; «прошитых» микросхем постоянно запоминающих устройств, микропроцессоров и их схемного исследования.

3) Получение и анализ технических указаний по обработке ежедневной бухгалтерской информации с перечнем выходящих форм.

4) Допрос лиц из числа инженеров - программистов, занимавшихся разработкой программного обеспечения и его сопровождением, специалистов, отвечающих за защиту информации и специалистов электронщиков, занимающихся эксплуатацией и ремонтом вычислительной техники.

5) Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах.

В ходе судебно-бухгалтерской экспертизы устанавливаются нарушения требований положений о документообороте, их причины (с целью совершения

преступления, злоупотребления или ошибки) и ответственные лица за эти нарушения.

Результаты программно-технической экспертизы, как заключение экспертов, играют роль доказательств в процессе суда. С помощью таких экспертиз могут решаться следующие задачи:

1) Воспроизведение информации, содержащейся на физических носителях.

2) Восстановление информации, ранее содержавшейся на физических носителях и в последствии стертой или измененной по различным причинам.

3) Установление времени ввода, изменение, уничтожение либо копирование той или иной информации.

4) Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.

5) Установление авторства, места, средства, подготовки и способа изготовления документов (файлов, программ).

6) Выяснения возможных каналов утечки информации из компьютерной сети и помещений.

7) Выяснение технического состояния, исправности программно-аппаратных комплексов, возможности их адаптации под конкретного пользователя.

8) Установления уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

3 Международные стандарты и соглашения в области безопасности информационных технологий.

Ключевым аспектом решения проблемы безопасности информационных технологий (ИТ) является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ. Необходимо было разработать эту систему в виде международного стандарта.

В 1990 г. Международной организацией по стандартизации (ISO) была начата разработка международного стандарта критериев оценки для общего использования. Версия 1.0 ОК была завершена ССЕВ в январе 1996 г. и одобрена ISO в апреле 1996 г. Бета-версия 2.0 ОК появилась в октябре 1997 г. В результате этих работ появился Международный стандарт ISO/IEC 15408-99 «Критерии оценки безопасности информационных технологий» или так называемые «Общие критерии».

В России аналогичный стандарт подготовлен в 2001г. Это ГОСТ Р ИСО/МЭК 15408-1-2001 «Критерии оценки безопасности информационных технологий».

Данный стандарт содержит общие критерии (ОК) оценки безопасности информационных технологий и предназначен в качестве руководства при разработке и при приобретении коммерческих продуктов или систем с функциями безопасности ИТ.

ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами.

Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК.

ОК безопасности продуктов и систем ИТ предназначены в основном для потребителей, разработчиков и оценщиков.

ОК предоставляют потребителям, независимую от реализации структуру, называемую профилем защиты (ПЗ), для выражения их специфических требований к мерам безопасности ИТ в объекте оценки.

Кроме указанного выше используется также ГОСТ Р50922-96 «Защита информации. Основные термины и определения».

В настоящее время разработан и действует еще один международный стандарт ISO/IEC 17799 «Безопасность информационных систем».

Представители 26 европейских стран, а также Канады, США, ЮАР и Японии подписали 23 ноября 2001 г. в Будапеште конвенцию по борьбе с киберпреступностью. Конвенция разрабатывалась специальным комитетом Совета Европы при участии юристов США и других стран в течение четырех лет. Семнадцатью государствами, включая Россию, документ не подписан, считая, что она нарушает права человека.