Вопросы к экзамену

МОДУЛЬ 1: **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (НЕКРАСОВ А.В.)**

Содержание

1. Нормативно-правовое регулирование общественных отношений.

Нормативно-правовое регулирование отношений в области защиты информации осуществляется *информационным правом*, которое является одним из составляющих существующей *системы права*.

В юриспруденции представлены много таких составляющих, которых объединяет одна общая научная дисциплина - *теория государства и права*. Она изучает закономерности возникновения, развития, назначения и функционирования государства и права.

Основы этих знаний обычно рассматриваются в курсе «Правоведение».

Классификация нормативно-правовых актов.

- По юридической силе.
- По субъектам, их издающим.

По субъектам их издающим правовые акты подразделяются на

- акты законодательной власти (законы);
- акты исполнительной власти (подзаконные акты);
- акты судебной власти (юрисдикционные акты общего характера).

По юридической силе все нормативно-правовые акты подразделяются на

- *законы,*
- *подзаконные акты*.

Признаки закона:

- законы принимаются высшими законодательными органами государства (Федеральное собрание – Государственная Дума и Совет Федерации) ;

- принятие закона включает в себя четыре обязательные стадии:

• внесение законопроекта в законодательный орган;

• обсуждение законопроекта;

• принятие закона;

• его опубликование в течении 7 дней после подписания Президентом.

Законы вступают в силу по истечении 10 дней после их опубликования,

- законы не подлежат контролю или утверждению со стороны какого-либо другого органа государства. Они могут быть отменены или изменены только законодательной властью. Конституционный или другой аналогичный суд может признать закон, принятый парламентом, неконституционным, однако отменить его может только законодательный орган.

Подзаконные нормативно-правовые акты подразделяются на:

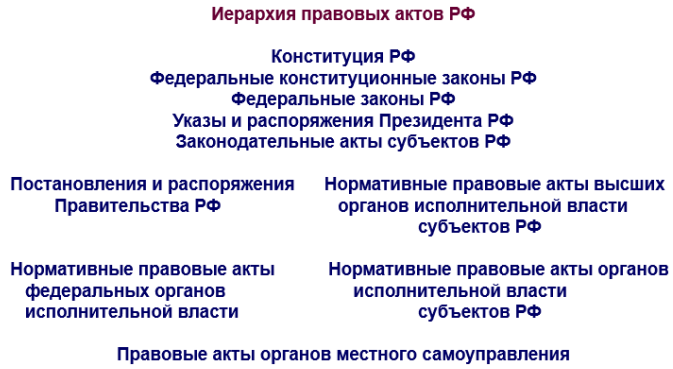
• Указы президента. В системе подзаконных актов они обладают высшей юридической силой и издаются на основе и в развитие законов (вступают в силу по истечении 7 дней после их опубликования).

• Постановления правительства. Это подзаконные нормативные акты, принимаемые в контексте с указами президента (вступают в силу по истечении 7 дней после их опубликования).

• Местные акты. Это нормативно-правовые акты органов законодательной и исполнительной власти на местах. Действие этих актов ограничено подвластной им территорией.

• Ведомственные (приказы, инструкции). Это нормативно-правовые акты общего действия, однако они распространяются лишь на ограниченную сферу общественных отношений (таможенные, банковские, транспортные, государственно-кредитные и другие).

• Внутриорганизационные. Это такие нормативно-правовые акты, которые издаются различными организациями для регламентации своих внутренних вопросов и распространяются на членов этих организаций.



Юридическая ответственность подразделяется по отраслевому признаку:

Уголовная ответственность наступает за совершение преступлений и устанавливается только уголовным законом.

Административно-правовая ответственность наступает за совершение административных проступков. Меры административного принуждения - предупреждение, штраф, лишение специального права (на ношение оружия, управление транспортным средством и т.д.), административный арест.

Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. (Возмещение убытков, выплата неустойки).

Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Меры дисциплинарной ответственности - выговор, строгий выговор, отстранение от занимаемой должности и т.п.

Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

2. Система и строение права.

Система права — это совокупность всех нормативно-правовых актов.

Внутреннее строение права можно представить по вертикали и горизонтали. Вертикальное строение права - это совокупность следующих элементов:

• Отрасль права - охватывает сферу общественных отношений. Например, имущественные отношения - гражданское право, управленческие отношения - административное право, и т.п.

• Подотрасль права - охватывает область общественных отношений. Многие отрасли права имеют подотрасли. Например, в гражданском праве выделяются подотрасли - авторское и наследственное право.

• Институт права - охватывает вид общественных отношений. В трудовом праве - институт трудового договора.

• Субинститут права - охватывает разновидность общественных отношений. Институт преступлений против жизни, здоровья, достоинства личности делится на субинституты преступлений против жизни, против здоровья и преступлений против достоинства личности.

• Норма права - это обязательное правило поведения, охраняемое силой государственного принуждения.

• Правовое предписание - это часть нормы права, логически завершенная и обособленная.

Горизонтальное строение права показывает все составляющие его отрасли. Выделяют две группы отраслей регулятивные и охранительные.

Регулятивные отрасли устанавливают права и обязанности участников правоотношений. Это следующие отрасли:

• конституционное право закрепляет основы государственного и общественного строя страны. Главным нормативным актом отрасли является Конституция;

• административное право регулирует общественные отношения, возникающие в процессе исполнительно-распорядительной деятельности органов государства;

• гражданское право регулирует различные имущественные отношения. Основной нормативный акт - Гражданский кодекс (ГК);

• финансовое право регулирует доходы и расходы государства.

• предпринимательское право регулирует экономические рыночные отношения. Основные нормативные акты – ГК, Законы об АО и ООО;

• трудовое право регулирует общественные отношения, связанные с применением труда. Основной нормативный акт – Трудовой Кодекс (ТК);

• природоресурсное право определяет порядок владения, пользования и распоряжения природными ресурсами: землей (Земельный кодекс), недрами (Закон о недрах), водой (Водный кодекс), воздушным пространством (Воздушный кодекс), лесными богатствами (Лесной кодекс);

• экологическое право регулирует защиту природных объектов и всей окружающей среды. Нормы экологического права рассредоточены по многим нормативным актам (УК, КоАП, ГК и др.);

• информационное право регулирует комплекс общественных отношений, связанных с информацией, защитой информации, защитой прав собственников информационных ресурсов, формирования различных институтов тайн (государственной, служебной, банковской, коммерческой, личной и т.п.).

Охранительные отрасли права (защита правоотношений):

• уголовное право – устанавливает общественно опасные деяния (преступления) и наказание за их совершение. Основной нормативный документ - Уголовный кодекс (УК);

• уголовно-процессуальное право объединяет нормы, определяющие порядок проведения предварительного следствия, дознания, порядок ведения

судебного разбирательства, назначения наказания. Основной нормативный акт - Уголовно-процессуальный кодекс (УПК);

• уголовно-исполнительное право регулирует процесс исполнения мер уголовного наказания. Основной нормативный акт - Уголовно-исполнительный кодекс (УИК);

• гражданско-процессуальное право регулирует порядок рассмотрения споров (трудовые, жилищные, наследственные и др.), в которых хотя бы одной из сторон выступает гражданин. Основной нормативный акт - Гражданский процессуальный кодекс;

• арбитражно-процессуальное право регулирует порядок рассмотрения гражданско-правовых споров между юридическими лицами. Основной нормативный акт - Арбитражно-процессуальный кодекс.

• Международное право – система юридических принципов и норм, регулирующих отношения между государствами.

В широком смысле выделяются 3 основных направления:

- международное публичное право - особая правовая система, регулирующая отношения между государствами, созданными ими международными организациями и некоторыми другими субъектами международного общения.

- международное частное право - совокупность норм внутригосударственного законодательства, международных договоров и обычаев, которые регулируют гражданско-правовые, трудовые и иные отношения, осложнённые иностранным элементом.

- наднациональное право - форма международного права, при которой государства идут на сознательное ограничение некоторых своих прав и делегирование некоторых полномочий наднациональным органам.

3. Структура информационного законодательства.

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 10.12.48 г. и в ст. 29 Конституции РФ, принятой

12.12.93 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 (рис 1.1).

<table>
<tr><td colspan="2">Конституция РФ</td></tr>
<tr><td colspan="2">Федеральные конституционные законы РФ</td></tr>
<tr><td colspan="2">Федеральные законы РФ</td></tr>
<tr><td colspan="2">Указы и распоряжения Президента РФ</td></tr>
<tr><td colspan="2">Законодательные акты субъектов РФ</td></tr>
<tr><td>Постановления и распоряжения Правительства РФ</td><td>Нормативные правовые акты высших органов исполнительной власти субъектов РФ</td></tr>
<tr><td>Нормативные правовые акты федеральных органов исполнительной власти</td><td>Нормативные правовые акты органов исполнительной власти субъектов РФ</td></tr>
<tr><td colspan="2">Правовые акты органов местного самоуправления</td></tr>
</table>

Рис. 1.1. Иерархия правовых актов РФ.

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

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации;

4) обеспечение безопасности Российской Федерации при создании и эксплуатации информационных систем;

5) достоверность информации и своевременность ее предоставления;

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

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

Информационное законодательство имеет следующую структуру:

• Международные акты информационного законодательства.

• Конституция РФ, Гражданский кодекс РФ, Уголовный кодекс РФ и др.

• Закон РФ “Об информации, …” и др. (всего около 80 законов).

• Указы и распоряжения Президента РФ. Постановления Правительства РФ.

• Местные, ведомственные и внутриорганизационные другие подзаконные акты.

Совокупность вышеперечисленных документов составляет правовую базу в информационной сфере.

4. Основные определения в области информационного права.

Основной нормативно-правовой документ в сфере информационного права это закон “Об информации, информационных технологиях и о защите информации” от 27.07.2006г №149-ФЗ, который регулирует отношения, связанные с:

• осуществлением права на поиск, получение, передачу, производство и распространение информации;

• ограничение доступа к информации;

• обеспечением защиты информации.

В законе раскрыты следующие важные вопросы:

1. Основные понятия в области информации, и ее защиты.
2. Права обладателя информации.
3. Право на доступ и ограничения доступа к информации.
4. Использование информационно - телекоммуникационных сетей и государственное регулирование в этой сфере.
5. Защита информации, в том числе использование электронной подписи (ЭП; ранее – электронная цифровая подпись, ЭЦП).

Электронная подпись – собственноручная подпись в электронном виде, которой можно подписывать документы.

В законе даны основные понятия (ст. 2):

• информация - сведения (сообщения, данные) независимо от формы их представления (может являться объектом правовых отношений и свободно использоваться любым лицом за исключением ограничений, введенных законом);

• информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

• информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

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

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

• доступ к информации – возможность получения информации и ее использования;

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

• предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

• распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

• электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

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

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

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

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

Электронное сообщение, подписанное электронной подписью, признается, равнозначным документу, подписанному собственноручной подписью.

Защита информации 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;

• соблюдение конфиденциальности информации ограниченного доступа;

• реализацию права на доступ к информации.

5. Права обладателя и режимы доступа к информации.

Обладателем информации 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 (в зависимости от порядка ее распространения) подразделяется на:

- свободно распространяемую;
- предоставляемую по соглашению;
- распространяемую в соответствии с федеральными законами;
- распространение которой в РФ ограничивается или запрещается.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

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.

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.

В законе определены режимы информации свободного и ограниченного доступа.

Режим доступа	Вид режима	Состав сведений
Свободный доступ	Общественного достояния	Научные открытия, рукописи и т.п.
	Массовой информации	Информация в СМИ, различные публикации и т.д.
	Исключительных прав	Результаты интеллектуальной деятельности
Ограниченный доступ	Конфиденциальности	Коммерческая, служебная и профессиональная тайны. Персональные данные. Тайна следствия и судопроизводства. Сведения о сущности неопубликованных изобретений
	Государственной тайны	Секретно, совершенно секретно и особой важности

Режим исключительных прав

(защита объектов интеллектуальной собственности)

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности:

- авторское право,
- патентное право,
- секреты производства - «ноу-хау».

Режим исключительных прав определен Гражданским кодексом РФ, часть 4, от 18.12.2006 г. № 230.

Режим общественного достояния

Создает условия для беспрепятственного ознакомления и использования соответствующих сведений. Так истечение срока действия исключительных прав на объекты интеллектуальной собственности (например, авторское право действует в течении всей жизни автора и 70 лет после его смерти) означает переход их в общественное достояние

Произведение, перешедшее в общественное достояние, может свободно использоваться любым лицом без чьего-либо согласия или разрешения и без выплаты авторского вознаграждения.

При этом охраняются авторство, имя автора и неприкосновенность произведения. (ГК РФ часть 4, ст. 1282).

Режим массовой информации

Распространяется на информацию в СМИ и различные публикации и отражает гарантируемую Конституцией РФ свободу массовой информации (ст. 29).

Ограничения на публикуемые в СМИ сообщения даны в Конституции РФ, Законе РФ «О средствах массовой информации» от 27.12.1991 г. № 2124-1.

Режим ограниченного доступа

Включает режим государственной тайны и режим конфиденциальности

Режим государственной тайны

Устанавливается в соответствии с законом РФ “О государственной тайне”.

Режим конфиденциальности

Устанавливается в отношении сведений, перечисленных в Указе Президента РФ "Об утверждении перечня сведений конфиденциального характера" № 188 от 06.03.1997 г. и регулируется законами “О коммерческой тайне”, “О персональных данных”, “О вязи”, “О банках и банковской деятельности”, “О полиции” и др.

Режим конфиденциальной информации по данным законодательных и подзаконных актов в настоящее время включает более 50 видов тайн. Указом Президента РФ "Об утверждении перечня сведений конфиденциального характера" от 06.03.1997 г. № 188 утвержден перечень сведений конфиденциального характера:

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

• Служебная тайна – служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством. Это информация о деятельности государственных органов власти и органов местного самоуправления, доступ к которой ограничен нормативно-правовыми актами государства, а также это сведения, которые поступают в вышеупомянутые органы на законном основании для исполнения служебных обязанностей.

• Профессиональная тайна

• Персональные данные

• Тайна следствия и судопроизводства

• Сведения о защищаемых лицах и мерах государственной защиты

• Сведения о сущности неопубликованных изобретений

В отношении профессиональной тайны действуют нормы Закона “Об информации, информационных технологиях и о защите информации” (статья 9)

Профессиональная тайна – информация, полученная лицами при исполнении ими профессиональных обязанностей, подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Профессиональная тайна может быть предоставлена третьим лицам в соответствии с федеральными законами или по решению суда.

Срок сохранения профессиональной тайны, может быть ограничен только с согласия гражданина, предоставившего такую информацию о себе.

6. Сведения, составляющие государственную тайну.

Система защиты государственных секретов основывается на Законе РФ «О государственной тайне» от 21.07.1993 г. № 5485-1.

Закон регулирует отношения, связанные с:

• отнесением сведений к государственной тайне (ГТ),

• их рассекречиванием,

• защитой в интересах безопасности РФ.

В законе даны следующие определения:

• государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

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

• система защиты государственной тайны – совокупность органов защиты ГТ, используемых средств и методов защиты сведений, составляющих ГТ, и их носителей, а также мероприятий, проводимых в этих целях

Субъекты правоотношений:

• 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 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 ГТ утверждены Постановлением Правительства РФ «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» № 870 от 04.09.1995 г.

Степень секретности сведений, составляющих ГТ, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих ГТ, и соответствующие грифы секретности для носителей указанных сведений:

• "особой важности" (ОВ),

• "совершенно секретно" (СС),

• "секретно" (С).

ОВ – если при разглашении наносится ущерб интересам РФ;

СС – если при разглашении наносится ущерб интересам отрасли или министерства;

С – если при разглашении наносится ущерб интересам предприятия.

При засекречивании сведений их носителям присваивается соответствующий гриф секретности.

Существует также промежуточный гриф для документов, которые не являются тайной предприятия, но не предназначены для открытого использования:

ДСП – для служебного пользования.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию.

На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

• об органе государственной власти,

• о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

• о регистрационном номере.

На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

• о дате или условии рассекречивания сведений.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих ГТ, эти данные указываются в сопроводительной документации на этот носитель.

Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах:

• законности,

• обоснованности

• своевременности.

Принцип законности заключается в том, что засекречиванию не подлежат сведения, указанные в статье 7 «Сведения, не подлежащие отнесению к государственной тайне и засекречиванию» закона о ГТ (которые раньше относились к ГТ).

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

Не подлежат отнесению к государственной тайне и засекречиванию сведения (Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию):

• 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.

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

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

Обоснование необходимости отнесения сведений к ГТ в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Межведомственная комиссия по защите ГТ формирует, Перечень сведений, отнесенных к ГТ.

В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями.

Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

Перечень должностных лиц, наделенных полномочиями по отнесению сведений к ГТ, утвержден распоряжением Президента РФ «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» от 16.05.2005 г. № 151-рп.

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 ГТ.

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 соответствии с договором между органом государственной власти и ее собственником информации.

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

Основания для рассекречивания сведений устанавливает статья 13 Закона РФ «О государственной тайне». К ним относятся:

• взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими ГТ;

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

Под рассекречиванием сведений и их носителей в названном Законе понимается: «снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих ГТ, и на доступ к их носителям».

Порядок рассекречивания носителя сведений, составляющих ГТ, определяет статья 14 Закона РФ «О государственной тайне». Она устанавливает, что «носители сведений, составляющих ГТ, рассекречиваются не позднее сроков, установленных при их засекречивании». До истечения сроков засекречивания носители сведений, составляющих ГТ, подлежат рассекречиванию при изменении действующего в данном органе государственной власти, на предприятии, в учреждении и в организации развернутого перечня сведений, подлежащих засекречиванию, на основании которого они были засекречены.

Кроме того, руководители органов государственной власти, предприятий, учреждений и организаций имеют право осуществлять рассекречивание носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

Органы государственной власти обязаны каждые 5 лет пересматривать содержание действующих перечней.

Срок засекречивания сведений, составляющих ГТ, не должен превышать 30 лет.

В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите ГТ.

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

В статье 17 и 18 закона указан порядок передачи сведений, составляющих ГТ.

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

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

Режим защиты государственных секретов обеспечивается уполномоченными органами.

Эти органы организуют и обеспечивают защиту информации, содержащей ГТ в соответствии с функциями, возложенными на них законодательством РФ.

Органы защиты государственной тайны:

• межведомственная комиссия по защите ГТ;

• ФСБ,

• Министерство обороны (МО),

• Служба внешней разведки (СВР),

• ФСТЭК.

Допуск должностных лиц и граждан к ГТ предусматривает:

• принятие на себя обязательств перед государством по нераспространению сведений, составляющих ГТ;

• 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 РФ о ГТ, предусматривающими ответственность за его нарушение;

• принятие решения руководителем органа государственной власти или предприятия, о допуске лица к сведениям, составляющим ГТ.

Для должностных лиц и граждан, допущенных к ГТ 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.

Особый порядок допуска к ГТ имеют, например:

• Члены Совета Федерации,
• депутаты Государственной Думы,
• судьи на период исполнения ими своих полномочий,
• адвокаты, участвующие в уголовном судопроизводстве по делам, связанным со сведениями, составляющими ГТ.

Эти лица допускаются к сведениям, составляющим ГТ, без проведения проверочных мероприятий, предусмотренных статьей 21.1. Закона «О государственной тайне», которая определяет круг должностей, занимая которые лицо автоматически считается допущенным к гостайне без проведения проверочных мероприятий со стороны ФСБ, если по роду деятельности им требуется разрешение на работу с гостайной.

Указанные лица предупреждаются о неразглашении ГТ, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

Сохранность ГТ в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Должностное лицо или гражданин, допущенные к ГТ, 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 ГТ, и на использование открытий и изобретений, содержащих такие сведения;
• права на неприкосновенность частной жизни при проведении проверочных мероприятий.

Допуск должностного лица или гражданина к ГТ может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

• расторжения с ним трудового договора в связи с проведением организационных и (или) штатных мероприятий;
• однократного нарушения им взятых на себя предусмотренных трудовым договором обязательств, связанных с защитой ГТ
• возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к ГТ;
• прекращения допуска должностного лица или гражданина к ГТ является дополнительным основанием для расторжения с ним трудового договора, если такие условия предусмотрены в трудовом договоре.

7. Ответственность за разглашение государственной тайны.

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

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

Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется Уголовным кодексом РФ - ст. 275, 276, 283, 284.

Статья 275. Государственная измена

Государственная измена, то есть совершенные гражданином РФ шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством РФ, переход на сторону противника либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности РФ, - наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет или пожизненным лишением свободы.

Примечание 1. Под переходом на сторону противника в настоящей статье понимается участие лица в составе непосредственно противостоящих Российской Федерации сил (войск) иностранного государства, международной либо иностранной организации в вооруженном конфликте, военных действиях или иных действиях с применением вооружения и военной техники.

Примечание 2. Лицо, совершившее преступления, предусмотренные настоящей статьей, а также статьями 276 и 278 настоящего Кодекса, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления.

Статья 276. Шпионаж

Передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности Российской Федерации либо передача, собирание, похищение или хранение в целях передачи противнику сведений, которые могут быть использованы против Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов Российской Федерации, совершенные в условиях вооруженного конфликта, военных действий или иных действий с применением вооружения и военной техники с участием Российской Федерации, то есть шпионаж, если эти деяния совершены иностранным гражданином или

лицом без гражданства, - наказываются лишением свободы на срок от десяти до двадцати лет.

При установлении нарушений норм защиты информации используется понятие "утраты документа".

Утрата документов – это выход (в т.ч. и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.

За обеспечением защиты ГТ установлен (ст. 30 и 32 закона) ведомственный контроль, который осуществляют

Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями, составляющими ГТ. Они обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Межведомственный контроль осуществляют:

• федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности,

• федеральный орган исполнительной власти, уполномоченный в области обороны,

• федеральный орган исполнительной власти, уполномоченный в области внешней разведки,

• федеральный орган исполнительной власти, уполномоченный в области противодействия

• техническим разведкам и технической защиты информации, и их территориальные органы, на которые эта функция возложена законодательством РФ.

За обеспечением защиты ГТ установлен контроль, который осуществляют Президент и Правительство РФ. Надзор за соблюдением законодательства осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

• Меры предупреждения нарушений режима секретности:

• Правильный профотбор кадров.

• Ограничение доступа к секретам. (Каждый сотрудник должен иметь доступ только к той информации, которая ему необходима в процессе выполнения прямых служебных обязанностей).

• Проведение воспитательной работы. (Стимулирование за поддержание режима секретности и строгие наказания за нарушения).

• Подписание соглашений с работниками о неразглашении.

• Политика «чистых столов». (По окончании рабочего дня, перед уходом, нужно убрать все с вашего рабочего места, а именно со стола (или другой поверхности).

• Создание службы безопасности фирмы.

• Использование технических средств защиты.

• Применение сертифицированных программных и аппаратных средств защиты информации (ЗИ) в информационных системах.

8. Сведения, составляющие коммерческую тайну.

В условиях жесткой конкуренции сбор информации фирмой о рынке, о партнерах и другой полезной информации, как правило, носит разведывательный характер. Главным предметом разведки является КОММЕРЧЕСКАЯ ТАЙНА (КТ).

Принято различать:

• конкурентную разведку (синонимы: бизнес-разведка, деловая разведка, аналитическая разведка, экономическая разведка, маркетинговая разведка, коммерческая разведка) и

• промышленный шпионаж.

Отличие в первом случае заключается в соблюдении закона, а во втором – в нарушениях уголовного, авторского или любого другого права.

Конкурентная разведка – это сбор и обработка информации законными способами.

На данный момент в нашей стране под конкурентной разведкой подразумеваются четыре вида сбора информации:

• Сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны.

• Информация о потенциальных партнерах и сотрудниках. Обычно этим занимаются отделы безопасности компаний или частные детективные агентства.

• Выполнение услуг охраны и сыска, предусмотренных Законом "О частной детективной и охранной деятельности" от 11.03.1992 г. № 2487-1.

• Сбор информации маркетингового характера.

Именно это направление понимается на Западе под конкурентной разведкой.

Виды конкурентной разведки (сбор информации маркетингового характера):

• наблюдение;

• отчеты торговых работников;

• поиск информации в открытых базах данных (БД);

• анализ годовых отчетов предприятий;

• обратный инжиниринг - исследование некоторого готового устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности (в том числе программные закладки), сделать изменение или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без прямого копирования. Обычно применяется, когда создатель оригинального объекта не предоставил информации о структуре и способе создания (производства) объекта. Правообладатели таких объектов могут заявить, что проведение обратной разработки или использование ее результатов нарушает их исключительное право по закону об авторском праве и патентному законодательству.

В настоящее время широко используется конкурентная разведка через Интернет.

Выделяют три режима такой разведки:

• оперативный (сбор и предоставление информации за 10 мин.)

• ситуационный центр (подготовка информации руководству с выводом на экран за 3-4 часа) и

• оперативные исследования (проведение исследований и подготовка отчета за 1-2 дня).

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" (утратил силу).

Затем в Законе РФ "Об информации, информатизации и защите информации" от 25.01.1995 г. (утратил силу, заменен Законом РФ "Об информации, информационных технологиях и о защите информации" от 27.06.2006 г. № 149-ФЗ), в Гражданском кодексе РФ, в 1994 г. ч.1. и в Законе РФ "О коммерческой тайне", от 29.07.2004 г. № 98-ФЗ

К КТ относят следующие три группы сведений:

1. Деловая информация (о сферах деятельности):

• финансовые сведения;

• данные о себестоимости продукции и услуг;

• деловые планы и планы производства и развития;

• информация о маркетинге;

• соглашения, предложения, контракты;

• организационные схемы.

2. Техническая информация:

• научно-исследовательские проекты;

• конструкторская документация на продукцию;

• заявки на патенты;

• дизайн, передовые технологии и оборудование;

• программное обеспечение ЭВМ и информационный процесс (Информационный процесс - процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.);

• химические формулы.

3. Информация о клиентах и конкурентах

На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, интересы в личной жизни, о представляемых ему фирмой привилегиях и т.п.

Аналогичные базы данных составляют и на своих конкурентов.

Таким образом, формируются «профиль клиента» (портрет клиента или аватар – усредненное описание человека, который будет покупать продукт) и «профиль конкурента».

Существует три основных направления сбора информации, представляющей коммерческий интерес.

1. Информация о рынке (издается и публикуется):

• цены, условия договоров, скидки;
• объем, тенденции и прогнозы сбыта продуктов;
• доля на рынке и тенденция ее изменения;
• рыночная политика и планы;
• отношения с потребителями и репутация;
• численность и расстановка торговых агентов;
• каналы, политика и методы сбыта;
• постановка целей рекламы.

2. Информация о производстве продукции (закупки, наблюдение, опрос):
• оценка качества и эффективности;
• номенклатура изделий;
• технология и оборудование;
• уровень издержек;
• производственные мощности;
• способ упаковки;
• доставка;
• размещение и размер производственных подразделений и складов;
• результаты НИОКР (научно-исследовательские и опытно-конструкторские работы – совокупность работ, направленных на получение новых знаний и их практическое применение при создании нового изделия или технологии.

Научно-исследовательские работы (НИР) – работы поискового, теоретического и экспериментального характера, выполняемые с целью определения технической возможности создания новой техники в определенные сроки, подразделяются на фундаментальные (получение новых знаний) и прикладные (применение новых знаний для решения конкретных задач) исследования.

Опытно-конструкторские работы (ОКР) и Технологические работы (ТР) – комплекс работ по разработке конструкторской и технологической документации на опытный образец изделия, изготовлению и испытаниям опытного образца изделия, выполняемых по техническому заданию.).

3. Информация об организационных особенностях и планах развития:
• выявление лиц, принимающих ключевые решения (ЛПР);
• программы развития фирмы;
• главные проблемы и возможности их решения;
• программы проведения научно-исследовательских работ.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выписывают у биржевиков, покупают у частных детективов, а также с помощью конкурентной разведки через Интернет.

В настоящее время существуют аналитические структуры, учрежденные крупнейшими финансово-промышленными группами, задачи которых заключаются в сборе данных на все фирмы, зарегистрированные в данном регионе: их оборот, уставной капитал, принадлежащая им недвижимость, точность в расчетах, отношения с налоговыми, административными, судебными инстанциями.

9. Защита коммерческой тайны.

Отличие коммерческой тайны от государственной:

1. Сведения, составляющие ГТ, установлены соответствующим перечнем, а КТ этим перечнем не определена и определяется руководителем предприятия.

2. ГТ охраняется силой государства в лице соответствующих органов, а коммерческая информация – службой безопасности предприятия

Основное отличие связано с тем, чьи интересы страдают в случае ее разглашения в одном случае – государства, в другом – коммерческой фирмы. Соответственно и методы, используемые в одном случае, могут использоваться и в другом.

По аналогии с ГТ коммерческая информация может быть ранжирована по степени ее важности для предприятия с тем, чтобы регулировать ее распространение среди работающих на предприятии, указывать пользователей этой информации, уровень ее защиты и т.д.

Для обозначения степени важности коммерческой информации для предприятия может быть предложена трехуровневая система обозначения степени ее секретности:

• Коммерческая тайна – строго конфиденциально (КТ-СК)
• Коммерческая тайна – конфиденциально (КТ-К)
• Коммерческая тайна (КТ)
• Промежуточный гриф рекомендуется использовать
• Для внутреннего использования (ДВИ).

Закон "О коммерческой тайне" от 29.07.2004 г. № 98-ФЗ регулирует отношения, связанные с отнесением информации к КТ, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять КТ.

КТ - конфиденциальность информации, 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)

КТ – 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 меры по охране ее конфиденциальности.

Не могут составлять КТ (ст. 5) сведения:

1) содержащие в учредительных документах юридического лица, и индивидуальных предпринимателях;

2) дающие право на осуществление предпринимательской деятельности;

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

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

5) 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;

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

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

8) 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;

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

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) сведения, недопустимость ограничения доступа к которым установлена иными федеральными законами.

Обладатель информации, составляющей КТ, 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 КТ, и срок предоставления этой информации. (мотивированное – значит обоснованное).

Режим коммерческой тайны является обязательным условием охраны конфиденциальности информации

Законом о КТ установлены требования, предъявляемые к режиму коммерческой тайны

Режим КТ считается установленным, после принятия обладателем информации следующих мер (ст. 10 и 11):

1) определение перечня информации, составляющей КТ;

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

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

4) регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров (контрагент - лицо или учреждение, берущее на себя известные обязательства по договору);

5) нанесение на документы, содержащие КТ, грифа "Коммерческая тайна" и обладателя этой информации для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.

6) ознакомить под расписку работника с перечнем информации, составляющей КТ;

7) создать работнику необходимые условия для соблюдения им установленного работодателем режима КТ;

8) ознакомить под расписку работника с установленным работодателем режимом КТ и с мерами ответственности за его нарушение.

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

В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством РФ (ст. 13).

Ответственность за нарушение настоящего закона (ст. 14).

Нарушение закона влечет за собой

• дисциплинарную,
• гражданско-правовую,
• административную или
• уголовную ответственность

Органы государственной власти, несут гражданско-правовую ответственность за разглашение или незаконное использование КТ их должностными лицами, которым она стала известна в связи с выполнением ими должностных обязанностей (ст. 14).

Лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, (получило доступ к ней в результате случайности или ошибки), не может быть привлечено к ответственности (ст. 14).

Невыполнение обладателем информации, составляющей КТ, законных требований органов государственной власти о предоставлении им информации, составляющей КТ, влечет за собой ответственность в соответствии с законодательством РФ (ст. 15).

Ответственность за разглашение КТ, дана в УК РФ

ст. 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода, осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе -

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо лишением свободы на срок до 3-х лет.

10. Правовое регулирование отношений по защите коммерческой тайны на предприятии.

В соответствии с установленными законом о КТ на предприятии используются правовые нормы внутрифирменных документов для регулирования правовых отношений по защите КТ.

Такими документами являются:

• Устав предприятия;

• Коллективный договор предприятия;

• Трудовые и гражданско-правовые договоры;

• Правила внутреннего трудового распорядка рабочих и служащих предприятия;

• Должностные обязанности руководителей, специалистов, рабочих и служащих предприятия, и другие документы.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо:

1. Ввести в Устав предприятия в раздел “Права и обязанности предприятия”:

“Предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих КТ, требовать от сотрудников предприятия обеспечения ее сохранности”.

“Предприятие обязано обеспечить сохранность КТ”.

Внесение этих требований дает право администрации предприятия:

• создавать организационные структуры по защите КТ;

• издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих КТ, и механизмы ее защиты;

• включать требования по защите КТ в договоры по всем видам хозяйственной деятельности;

• требовать защиту интересов предприятия перед государственными и судебными органами.

2. Разработать “Перечень сведений, составляющих КТ предприятия” и довести его под роспись до всех сотрудников.

3. Дополнить “Коллективный договор” следующими требованиями:

В раздел “Предмет договора” Администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по введению режима и защите КТ.

Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите КТ.

В раздел “Кадры” Администрация обязуется привлекать нарушителей требований по защите КТ к административной и уголовной ответственности в соответствии с действующим законодательством.

4.Дополнить правила внутреннего распорядка дня работников требованиями о неразглашении КТ.

При поступлении рабочего или служащего на работу, переходе его на другую работу а также при увольнении, администрация обязана проинструктировать работника по правилам сохранения КТ с оформлением письменного обязательства о ее неразглашении.

5. Ввести в текст трудового договора требования по защите КТ.

Независимо от формы заключения договора (устная или письменная) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.

Если договор заключается в устной форме, то действует требование по защите КТ, вытекающее из правил внутреннего трудового распорядка.

6. В должностные обязанности руководителей, специалистов, рабочих и служащих записать, что сотрудники должны знать относящиеся к их деятельности сведения, являющиеся КТ, выполнять лично требования по ее защите и принимать меры по предупреждению нарушений установленных норм сохранности КТ.

Включение этих требований дает право администрации предприятия применять к нарушителям меры дисциплинарного воздействия в соответствии с Трудовым кодексом РФ.

Руководителю предприятия, при создании системы безопасности на нем, необходимо определить следующее:

• какая информация нуждается в защите;
• кого она может заинтересовать;
• каков “срок жизни” этих секретов;
• во что обойдется их защита.

В рамках режима КТ на предприятии вводятся система закрытого делопроизводства, которая включает:

1. Создание отдела защищенного делопроизводства (ОЗД).

2. Проведение документирования:

• определение перечня документов, содержащих секреты предприятия;
• контроль за содержанием документов и степени секретности;
• контроль за размножением и рассылкой документов;
• учет документов с грифом “КТ” (производится отдельно от несекретных документов и документов ДВИ) включает:
• регистрация каждого входящего и исходящего документа;
• инвентарный учет;
• номенклатуру дел, журналов и карточек;
• контроль за местоположением документов.

Корреспонденция с грифом “КТ” поступает в ОЗД, где она проверяется на наличие недостачи и регистрируется на корточках или в журнале.

Листы журналов нумеруются, прошиваются и опечатываются.

На первом листе зарегистрированного входящего документа с грифом “КТ” ставится штамп

Наименование предприятия		
Входящий № и дата	Количество листов	
	основных	приложений

Исходящие документы с грифом “КТ” печатаются в машбюро ОЗД или с учтенных носителей с помощью средств вычислительной техники (ВТ).

На последнем листе каждого экземпляра проставляется количество отпечатанных экземпляров, фамилия исполнителя, машинистки (которая печатала документ) и дата.

Отпечатанный документ регистрируется в журнале.

Все черновики выполняются на предварительно учтенных в ОЗД листах, сдаются после окончания работы и уничтожаются в ОЗД.

Отправка документов с грифом “КТ” производится заказными письмами или бандеролями.

При этом рекомендуется использовать двойной конверт, причем, на внешнем пишется адрес, а на внутреннем ставится гриф.

Проверка наличия документов проводится

• ежеквартально – для документов, находящихся на исполнении;

• ежегодно – для всех зарегистрированных документов.

Режимные документы, находящихся у сотрудников на исполнении, хранятся на предприятии в опечатанных папках или чемоданах.

3. Организацию документооборота:

• установление разрешительной системы доступа исполнителей к документам;

• установление грифа секретности (степени секретности);

• установление порядка приема-передачи документов между сотрудниками;

• контроль за порядком работы с документами;

• установление порядка хранения и уничтожения документов;

• установление порядка обращения с документами.

Порядок хранения и уничтожения документов включает:

• выделение специально оборудованных помещений;

• установление порядка доступа к делам;

• контроль за своевременностью и правильностью формирования дел;

• установление порядка подготовки документов для уничтожения;

• обеспечение необходимых условий уничтожения;

• контроль за правильностью и своевременностью уничтожения документов.

Порядок обращения с документами

1.Выдача документов с грифом КТ сотрудникам производится по разрешению руководителя предприятия на основании служебной записки от начальника подразделения исполнителя.

2.Передача документов с грифом “КТ” между сотрудниками осуществляется под расписку и в пределах круга лиц, допущенных к данному документу.

3. После окончания рабочего дня помещения ОЗД передаются под охрану.

4.Разрешение на уничтожение документа дает руководитель подразделения, к деятельности которого относится документ, путем записи в журнал учета «Уничтожить», подпись, дата.

5.Уничтожение документов производится путем их сожжения или измельчения.

11. Защита коммерческой информации в договорной документации.

Правовая защита коммерческих секретов, основывается на использовании таких внутрифирменных нормативных документов как трудовой договор (контракт) и должностные инструкции.

Трудовой договор – это соглашение между работодателем и работником, в котором определены права и взаимные обязанности сторон. Содержанием трудового договора являются взаимные права и обязанности и установлена ответственность при исполнении должностных инструкций.

Должностная инструкция – это внутренний организационно-распорядительный документ, содержащий конкретный перечень должностных обязанностей работника с учетом особенностей организации производства, труда и управления, а также его прав и ответственности.

В трудовом договоре принято различать основные (законодательно определенные) и дополнительные (факультативные) условия.

Вопросы защиты информации закрепляются в трудовом договоре в виде дополнительных условий.

В обязанности работника включают условие о неразглашении служебной (коммерческой) тайны, к которой он будет допущен в силу его должностных обязанностей.

Кроме трудового договора данное условие может быть также включено и в другие виды договоров:

• договор поручительства (По договору поручительства поручитель обязывается перед кредитором другого лица отвечать за исполнение последним его обязательства полностью или в части. Договор поручительства может быть заключен в обеспечение как денежных, так и неденежных обязательств, а также в обеспечение обязательства, которое возникнет в будущем.);

• договор коммерческого представительства (Коммерческим представителем является лицо, постоянно и самостоятельно представительствующее от имени предпринимателей при заключении ими договоров в сфере предпринимательской деятельности);

• агентский договор (По агентскому договору одна сторона (агент) обязуется за вознаграждение совершать по поручению другой стороны

(принципала) юридические и иные действия от своего имени, но за счет принципала либо от имени и за счет принципала.);

• договор поручения или доверенности (По договору поручения одна сторона (поверенный) обязуется совершить от имени и за счет другой стороны (доверителя) определенные юридические действия, может быть, как бессрочным, так и срочным. Права и обязанности по сделке, совершенной поверенным, возникают непосредственно у доверителя. Полномочия поверенного в отношениях с третьими лицами оформляются с помощью особенного документа – доверенности, которую ему выдаёт доверитель. Доверенность – представляет собой, письменно оформленное и заверенное поручительство, которое одно лицо выдает другому для представительства и взаимодействия с другими физическими и юридическими лицами.);

• договор о рекламных услугах (представляет собой соглашение, по которому одна сторона по поручению другой стороны осуществляет рекламную кампанию какого-либо продукта.);

• другие информационные услуги.

В этих документах включаются следующие обязательства:

• не разглашать КТ организации третьим лицам или публично без согласия администрации;

• сохранять КТ тех организаций, с которыми имеются деловые связи;

• выполнять требования приказов и инструкций по защите КТ предприятия;

• не использовать секретные сведения организации, занимаясь другой деятельностью (ущерб от конкурентного действия);

• незамедлительно извещать службу безопасности (СБ) о попытках посторонних лиц получить закрытую информацию;

• незамедлительно извещать об утрате носителей секретной информации и другие факты нарушения режима ее защиты;

• при увольнении все носители КТ с которыми работал сотрудник передаются соответствующему должностному лицу;

• предупреждение работника о наступлении гражданской, административной или уголовной ответственности в случае нарушения взятых обязательств.

Обязанности по сохранению КТ возлагаются и на руководителя организации. Для этого в контракт, заключаемый с руководителем, вводятся соответствующие положения:

• обязательство руководителя хранить КТ и не использовать ее в ущерб организации;

• о персональной ответственности за создание необходимых условий для сохранности КТ;

• об ответственности руководителя за нарушения режима защиты КТ и возможных последствиях.

(ГК РФ ст. 12, 15).

Убыток – это выраженный в денежной форме ущерб, который состоит из затрат, связанных с созданием этих документов (например, стоимость бумаги) и

упущенной выгоды, т.е. из доходов, которые могло бы получить предприятие в случае сохранения тайны.

12. Правовая защита от компьютерных преступлений.

Средства автоматизированной обработки информации с использованием ЭВМ имеют ряд особенностей, дающих широкие возможности для злоумышленных действий.

Потери от компьютерных преступлений (КП) во всем мире составляют миллиарды долларов в год. Особенно страдают кредитно-финансовые учреждения.

Кроме этих действий значительные потери возникают в результате распространения вредоносных программ - компьютерных вирусов, появившиеся начиная с 1987 г.

Особенностью компьютерных преступлений является то, что их жертвы не всегда обращаются за защитой в правоохранительные органы (по коммерческим соображениям).

Можно выделить следующие виды угроз информации в автоматизированных системах (АС).

1. Перехват информации:

• по электромагнитному излучению (излучения электронно-лучевые трубки (ЭЛТ) можно принимать на расстояниях до 1000 м.);

• по виброакустическому каналу (таблетки, клопы, жучки, через несущие конструкции и проемы здания, стетоскоп);

• видеоперехват (бинокль, фото- и видеокамеры);

• использование отходов информационного процесса (физические - диски, пленки и “мусор” в памяти компьютера).

2. Несанкционированный доступ (НСД) к информации:

• физическое проникновение;

• установка шлейфов;

• подключение к линии связи законного пользователя;

• подбор кода доступа в т.ч. с помощью программ- “взломщиков”, вручную с помощью «интеллектуального» перебора - вскрывается 42% паролей из 8 символов.

3. Манипуляция данными и управляющими командами:

• умышленное изменение данных;

• изменение логических связей в электронных цепях и топологии микросхем.

4. Вредоносные программы

Вредоносная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.

Вредоносные программы могут быт классифицированы по:

• по вредоносной нагрузке;

• по методу размножения.

По методу размножения вредоносное ПО подразделяется на:

• Эксплойт – теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Здесь вред наносит не сам файл, а неадекватное поведение ПО с ошибкой, приводящее к уязвимости. Также эксплойтом называют программу для генерации подобных «отравленных» данных.

• Логическая бомба – вредоносная часть компьютерной программы (полезной или нет), срабатывающая при определённом условии.

• Троянская программа не имеет собственного механизма размножения и устанавливается «в придачу» к полезной или под видом полезной. Часто «в придачу» ставят ПО, которое не является истинно вредоносным, но является нежелательным – например, рекламным.

Компьютерный вирус размножается в пределах компьютера и через сменные диски. Размножение через сеть возможно, если пользователь сам выложит заражённый файл в сеть. Вирусы, в свою очередь, делятся:

• по типу заражаемых файлов (файловые, загрузочные, макро-, автозапускающиеся);

• по способу прикрепления к файлам (паразитирующие, «спутники» и перезаписывающие) и т.д.

Сетевой червь способен самостоятельно размножаться по сети. Делятся на IRC-черви (распространяются через IRC-каналы (чат-каналы, Internet Relay Chat), почтовые, размножающиеся с помощью эксплойтов) и т.д.

Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта на компьютере жертвы развертывается загрузчик, устанавливающий из интернета червя-вирус с логическими бомбами.

5. Использование специальных программных средств:

• “моделирование” процессов и способов преступления путем создания игровой программы защита-преодоление.

6. Комплексные методы

Использование двух и более способов и их комбинации.

Эффективная борьба с КП в РФ ведется с 1996 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).

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати

месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности -наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Те же деяния, если они повлекли тяжкие последствия или создали угрозу их наступления - наказываются лишением свободы на срок до семи лет.

Примечание 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Примечание 2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Целям защиты информации, обрабатываемой в АС служит Закон РФ "Об электронной подписи" от 06.04.2011 г. № 63-ФЗ

• ЭП – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

• ЭП – собственноручная подпись в электронном виде, которой можно подписывать документы.

• ЭП признается равнозначной собственноручной подписи лица на бумажном носителе, заверенном печатью.

13. Правовые основы деятельности службы безопасности.

Служба безопасности (СБ) фирмы – это самостоятельное структурное подразделение, которое решает задачи обеспечения защиты жизненно важных интересов фирмы в условиях коммерческого риска и конкурентной борьбы.

Деятельность СБ должна быть основана на государственных и внутрифирменных нормативных документах.

Законы РФ:

• «О частной детективной и охранной деятельности» от 11.03.1992 г. № 2487-1,

• «О безопасности» от 28.12.2010 г. № 390-ФЗ,

• «Об оружии» от 13.12.1996 г. № 150-ФЗ,

• «Об информации, информационных технологиях и о защите информации» от 27.13.2006 г. № 149-ФЗ,

• «О ведомственной охране» от 14.04.1999 г. № 77-ФЗ,

• ГК РФ и Трудовой Кодекс.

Постановления Правительства РФ:

• «Вопросы частной детективной (сыскной) и частной охранной деятельности» от 14.08.1992 г. № 587,

• «Об организации ведомственной охраны» от 12.07.2000 г. № 514.

Внутренние документы:

• устав фирмы, трудовые договоры, правила внутреннего трудового распорядка, должностные обязанности руководителей, специалистов, рабочих и служащих, положение о СБ;

• инструкция по организации режима и охраны;

• инструкция по защите КТ;

• перечень сведений, составляющих КТ;

• инструкция по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

• инструкция по хранению документов, содержащих КТ в архиве;

• инструкция по инженерно-технической защите информации;

• инструкция о порядке работы с иностранными представителями.

Основным документом, регулирующим вопросы создания и деятельности СБ, является Закон РФ «О частной детективной и охранной деятельности», от 11.03.92 г. № 2487-1

Основные положения:

Частная детективная и охранная деятельность осуществляется физическими и юридическими лицами, имеющими специальное разрешение (лицензию) (ст. 1), которая выдается органом внутренних дел (лица, занимающиеся частной детективной деятельностью, не вправе осуществлять оперативно–розыскные действия).

Согласно Постановлению Правительства РФ “О лицензировании отдельных видов деятельности” от 04.05.2011 г. № 99-ФЗ подлежат лицензированию (ст. 12):

32) частная охранная деятельность;

33) частная детективная (сыскная) деятельность.

Частная детективная и охранная деятельность осуществляется для сыска и охраны.

В целях сыска разрешается предоставление следующих 8 видов услуг (ст. 3):

1)сбор сведений по гражданским делам на договорной основе с участниками процесса;

2) изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

3)установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований,

недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

4) выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;

5) поиск без вести пропавших граждан;

6) поиск утраченного имущества гражданами или предприятиями, учреждениями, организациями;

7) сбор сведений по уголовным делам на договорной основе с участниками процесса. В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом лицо, производящее дознание, следователя или суд, в чьем производстве находится уголовное дело;

8) поиск лица, являющегося должником в соответствии с исполнительным документом, его имущества, а также поиск ребенка по исполнительному документу, содержащему требование об отобрании или о передаче ребенка, порядке общения с ребенком, требование о возвращении незаконно перемещенного в РФ или удерживаемого в РФ ребенка или об осуществлении в отношении такого ребенка прав доступа на основании международного договора РФ, на договорной основе с взыскателем.

В целях охраны разрешается предоставление следующих 7 видов услуг:

1) защита жизни и здоровья граждан;

2) охрана объектов и (или) имущества (в том числе при его транспортировке), находящихся в собственности, во владении, в пользовании, хозяйственном ведении, оперативном управлении или доверительном управлении, за исключением объектов и (или) имущества, предусмотренных пунктом 7 настоящей части;

3) охрана объектов и (или) имущества на объектах с осуществлением работ по проектированию, монтажу и эксплуатационному обслуживанию технических средств охраны, перечень видов которых устанавливается Правительством РФ, и (или) с принятием соответствующих мер реагирования на их сигнальную информацию;

4) консультирование и подготовка рекомендаций клиентам по вопросам правомерной защиты от противоправных посягательств;

5) обеспечение порядка в местах проведения массовых мероприятий;

6) обеспечение внутриобъектового и пропускного режимов на объектах, за исключением объектов, предусмотренных пунктом 7 настоящей части;

7) охрана объектов и (или) имущества, а также обеспечение внутриобъектового и пропускного режимов на объектах, в отношении которых установлены обязательные для выполнения требования к антитеррористической защищенности, за исключением объектов, предусмотренных частью третьей статьи 11 настоящего Закона.

Организации, осуществляющие частную охранную деятельность, оказывают содействие правоохранительным органам в обеспечении правопорядка, в том числе в местах оказания охранных услуг и на прилегающих к ним территориях, а

частные детективы оказывают содействие правоохранительным органам в предупреждении и раскрытии преступлений, предупреждении и пресечении административных правонарушений в порядке, установленном Правительством РФ.

В ходе частной сыскной деятельности допускаются устный опрос граждан и должностных лиц (с их согласия), наведение справок, изучение предметов и документов (с письменного согласия их владельцев), внешний осмотр строений, помещений и других объектов, наблюдение для получения необходимой информации в целях оказания услуг, перечисленных в части первой статьи 3 настоящего Закона.

При осуществлении частной сыскной деятельности допускается использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда жизни и здоровью граждан, и окружающей среде, в соответствии с законодательством РФ.

В ходе осуществления своей деятельности частный детектив обязан соблюдать законодательство РФ в части защиты информации, затрагивающей личную жизнь и имущество граждан.

Частным детективам запрещается (ст. 7):

1) скрывать от правоохранительных органов ставшие им известными факты готовящихся, совершаемых или совершенных преступлений;

2) выдавать себя за сотрудников правоохранительных органов;

3) собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;

4) осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;

5) прибегать к действиям, посягающим на права и свободы граждан;

6) совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;

7) фальсифицировать материалы или вводить в заблуждение клиента;

8) разглашать собранные в ходе выполнения договорных обязательств сведения о заказчике, в том числе сведения, касающиеся вопросов обеспечения защиты жизни и здоровья граждан и (или) охраны имущества заказчика, использовать их в каких-либо целях вопреки интересам заказчика или в интересах третьих лиц, кроме как на основаниях, предусмотренных законодательством РФ;

9) передавать свою лицензию для использования ее другими лицами;

10) использовать документы и иные сведения, полученные в результате осуществления оперативно-розыскной деятельности органами, уполномоченными в данной сфере деятельности;

11) получать и использовать информацию, содержащуюся в специальных и информационно-аналитических базах данных органов, осуществляющих оперативно-розыскную деятельность, в нарушение порядка, установленного законодательством РФ.

Лицензия частным детективам не предоставляется (ст. 6):

1) гражданам, не достигшим двадцати одного года;

2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;

3) гражданам, имеющим судимость за совершение умышленного преступления;

4) гражданам, которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);

5) гражданам, уволенным с государственной службы, из судебных, прокурорских и иных правоохранительных органов по компрометирующим их основаниям;

6) бывшим работникам правоохранительных органов, осуществлявшим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год;

7) гражданам, не представившим документы, перечисленные в части второй настоящей статьи.

Удостоверение частного охранника выдается сроком на пять лет. Срок действия удостоверения частного охранника может продлеваться в порядке, установленном Правительством РФ. Продление срока действия удостоверения частного охранника осуществляется только после прохождения профессионального обучения по программе повышения квалификации частных охранников в организациях, указанных в статье 15_2 настоящего Закона (ст. 11).

Частная охранная организация может быть создана только в форме общества с ограниченной ответственностью и не может осуществлять иную деятельность, кроме охранной (ст. 15).

Руководитель частной охранной организации должен иметь высшее образование и получить дополнительное профессиональное образование по программе повышения квалификации руководителей частных охранных организаций. Обязательным требованием является наличие у руководителя частной охранной организации удостоверения частного охранника. (ст. 15).

В ходе осуществления частной детективной деятельности разрешается применять

• специальные средства, а при осуществлении частной охраной деятельности

• специальные средства и огнестрельное оружие только в случаях и в порядке, предусмотренных настоящим Законом. Охранник при применении специальных средств или огнестрельного оружия обязан:

• предупредить о намерении их использовать, предоставив при этом достаточно времени для выполнения своих требований, за исключением тех случаев, когда промедление в применении физической силы, специальных средств или огнестрельного оружия создает непосредственную опасность его жизни и здоровью или может повлечь за собой иные тяжкие последствия;

• стремиться в зависимости от характера и степени опасности правонарушения и лиц, его совершивших, а также силы оказываемого противодействия к тому, чтобы любой ущерб, причиненный при устранении опасности, был минимальным;

• обеспечить лицам, получившим телесные повреждения, первую помощь и уведомить о происшедшем в возможно короткий срок органы здравоохранения и внутренних дел, территориальный орган федерального органа исполнительной власти, уполномоченного в сфере частной охранной деятельности;

• немедленно уведомить прокурора о всех случаях смерти или причинения телесных повреждений.

Перечень видов специальных средств, используемых в частной охранной деятельности в соответствии с Постановлением Правительства «Вопросы частной детективной (сыскной) и частной охранной деятельности» от 14.08.1992 г. № 587:

1) Шлем защитный 1-3 классов защиты отечественного производства;

2) Жилет защитный 1-5 классов защиты отечественного производства;

3) Наручники отечественного производства "БР-С", "БР-С2", "БКС-1", "БОС";

4) Палка резиновая отечественного производства "ПР-73М", "ПР-К", "ПР-Т", "ПУС-1", "ПУС-2", "ПУС-3".

Виды вооружения охранников (порядок приобретения, учета, хранения и ношения оружия регламентируются данным постановлением):

1. Сертифицированные в установленном порядке в качестве служебного оружия:

а) огнестрельное гладкоствольное и нарезное короткоствольное оружие отечественного производства;

б) огнестрельное гладкоствольное длинноствольное оружие отечественного производства;

в) огнестрельное оружие ограниченного поражения отечественного производства.

2. Сертифицированные в установленном порядке в качестве гражданского оружия:

а) огнестрельное оружие ограниченного поражения отечественного производства;

б) газовые пистолеты и револьверы отечественного производства;

в) механические распылители, аэрозольные и другие устройства, снаряженные слезоточивыми веществами, разрешенными к применению компетентным федеральным органом исполнительной власти;

г) электрошоковые устройства и искровые разрядники отечественного производства, имеющие выходные параметры, соответствующие требованиям государственных стандартов РФ и нормам Минздрава России

3. Сертифицированные в установленном порядке:

а) патроны к служебному оружию отечественного производства;

б) патроны к гражданскому оружию травматического, газового и светозвукового действия, соответствующие нормам Минздрава России.

Частные охранники обязаны проходить периодические проверки на пригодность к действиям в условиях, связанных с применением огнестрельного оружия и (или) специальных средств. Содержание периодических проверок, порядок и сроки их проведения определяются федеральным органом

исполнительной власти, уполномоченным в сфере частной охранной деятельности.

Частные охранники имеют право применять физическую силу в случаях, если настоящим Законом им разрешено применение специальных средств или огнестрельного оружия.

Охранники имеют право применять огнестрельное оружие в следующих случаях (ст. 18):

1) для отражения нападения, когда его собственная жизнь подвергается непосредственной опасности;

2) для отражения группового или вооруженного нападения на охраняемое имущество;

3) для предупреждения (выстрелом в воздух) о намерении применить оружие, а также для подачи сигнала тревоги или вызова помощи;

4) для пресечения функционирования беспилотных аппаратов в целях, предусмотренных частью десятой статьи 12 настоящего Закона.

Запрещается применять огнестрельное оружие в отношении женщин, лиц с явными признаками инвалидности и несовершеннолетних, когда их возраст очевиден или известен охраннику, кроме случаев оказания ими вооруженного сопротивления, совершения вооруженного либо группового нападения, угрожающего жизни охранника или охраняемому имуществу, а также при значительном скоплении людей, когда от применения оружия могут пострадать посторонние лица.

Федеральный государственный контроль (надзор) за соблюдением законодательства РФ в области частной детективной деятельности и федеральный государственный контроль (надзор) за соблюдением законодательства РФ в области частной охранной деятельности осуществляют федеральный орган исполнительной власти, уполномоченный в сфере частной охранной деятельности, и его территориальные органы в пределах, установленных настоящим Законом, другими законами и иными нормативными правовыми актами РФ. Контроль за частной детективной деятельностью и частной охранной деятельностью на территории РФ осуществляют иные уполномоченные федеральные органы исполнительной власти и подчиненные им органы и подразделения в пределах, установленных настоящим Законом, другими законами и иными нормативными правовыми актами РФ.

Надзор за исполнением настоящего Закона осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Задачи службы безопасности:

1. Определение сведений, составляющих КТ; лиц, имеющих к ним доступ; предприятий-партнеров на которых возможна утечка общих секретов.

2. Выявление лиц и предприятий, проявляющих интерес к КТ предприятия.

3. Разработка системы защиты документов с грифом КТ.

4. Определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон предприятию.

5. Планирование, обоснование и организация мероприятий по защите экономической информации (техническое оснащение, подготовка кадров).

6. Взаимодействие с органами внутренних дел (ОВД).

СБ для сохранения КТ принимает меры по

• максимальному ограничению круга лиц, допускаемых к КТ;

• физической сохранности документов, содержащих такие сведения;

• обработке информации с грифом «КТ» на защищенных ЭВМ;

• внесению требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами, а также проводит другие мероприятия по решению руководства.

Служба безопасности должна быть готова к возникновению кризисных ситуаций

Кризисная группа создается в структуре системы безопасности фирмы для быстрого преодоления чрезвычайных ситуаций.

В состав группы входят ключевые фигуры фирмы: директор, руководители подразделений, филиалов, служб, главный бухгалтер, юрист и др.

Деятельность этой группы тщательно планируется, а вся информация о ней должна быть конфиденциальной и максимально защищена.

Кризисной группой разрабатываются следующие виды планов действий:

• при угрозе взрыва;

• при захвате заложников или похищения сотрудников фирмы;

• при вымогательстве;

• при нападении на сотрудников и помещения фирмы;

• при природных и техногенных катастрофах и т.п.

Кризисные планы составляются не более чем в 2-3 экз. и хранятся у руководителя и начальника СБ.

Частным детективам запрещается проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных для негласного получения информации.

Перечень специальных технических средств (СТС), утвержденных Постановлением Правительства РФ от 01.07.1996 г. № 770:

1. СТС для негласного получения и регистрации акустической информации.
2. СТС для негласного визуального наблюдения и документирования.
3. СТС для негласного прослушивания телефонных переговоров.
4. СТС для негласного перехвата и регистрации информации с технических каналов связи.
5. СТС для негласного контроля почтовых сообщений и отправлений.
6. СТС для негласного исследования предметов и документов.
7. СТС для негласного проникновения и обследования помещений, транспортных средств и других объектов.
8. СТС для негласного контроля за перемещением транспортных средств и других объектов.
9. СТС для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.
10. СТС для негласной идентификации личности.

Ответственность за данные нарушения указана в статьях УК РФ.

УК РФ. Статья 203. Превышение полномочий частным детективом или работником частной охранной организации, имеющим удостоверение частного охранника, при выполнении ими своих должностных обязанностей

1. Совершение частным детективом или работником частной охранной организации, имеющим удостоверение частного охранника, действий, выходящих за пределы полномочий, установленных законодательством РФ, регламентирующим осуществление частной охранной и детективной деятельности, и повлекших существенное нарушение прав и законных интересов граждан и (или) организаций либо охраняемых законом интересов общества или государства - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное с применением насилия или с угрозой его применения либо с использованием оружия или специальных средств и повлекшее тяжкие последствия, - наказывается лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

14. Правовые основы использования технических средств сбора и защиты информации.

К техническим средствам сбора информации относятся:

1. Основные технические средства:

• телефоны городской, внутренней и сотовой связи;

• селекторная связь;

• ПК и сети ПЭВМ;

• копировальная техника.

Способы сбора информации с использованием телефона (ТЛФ) и линий связи (ЛС)

Переизлучение самой конструкции аппарата.

Старые кнопочные аппараты переизлучали информацию в радиусе до 200 м в диапазонах радиоволн СВ, КВ и УКВ. Средние волны (СВ) – длина волны 1000 – 100 м (частота 300 кГц – 3 МГц). Короткие волны (КВ) – длина волны 100 – 10 м (частота 3 – 30 МГц). Ультракороткие волны (УКВ) – длина волны 10 м – 0,1 мм (частота 30 МГц – 3000 ГГц).

Утечка по звонковой цепи ТЛФ при электроакустическом преобразовании при неснятой трубке (микрофонный эффект).

Подача ВЧ колебаний (от 150 кГц) на один провод, а с другого снятие модулированных речью колебаний (трубка не снята). Дальность съема информации этими способами – несколько десятков метров. Высокие частоты (ВЧ) – частота 3 – 30 МГц (длина волны 100 – 10 м).

За счет наводки в проводе, параллельном телефонному аппарату. Датчик может быть на расстоянии до 20 см от самого провода. Способ трудно обнаружить.

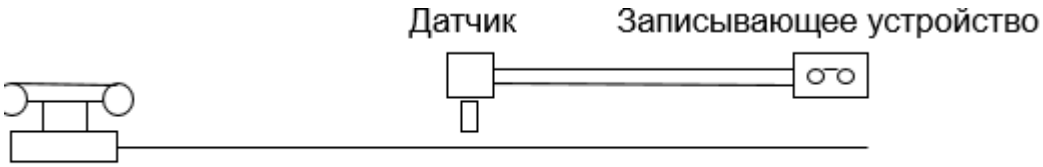


Схема снятия информации с телефонной линии

2. Вспомогательные технические средства и системы

• телевизор, магнитофон и другие виды бытовой радиоэлектроники;

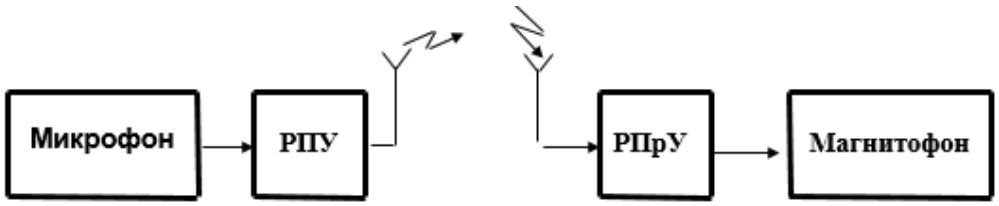
• датчики охраной и пожарной сигнализации;

• кондиционер;

• штатное электрооборудование и сети газификации помещения.

3. Специальные технические средства сбора информации

Радиомикрофон (жучок)

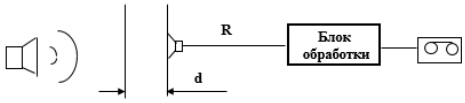


Структурная схема подслушивающего устройства

РПУ – радиопередающее устройство; РПрУ – радиоприемное устройство.

Стетоскоп

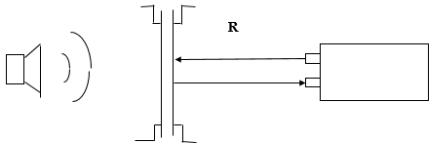
Прослушивание через резонирующие перегородки - стены, стекла, батареи отопления.



Структурная схема использования стетоскопа

При d до 1 м и R до 25 м.
d - толщина стены или балки.

Лазерный локатор



Структурная схема использования лазерного локатора.
При R до 600 м.

• Направленный микрофон - Информация по звуковому каналу считывается на расстоянии до 150 м.

• Миниатюрные видео- и фотокамеры – Миниатюрные телекамеры, размещенные в корпусе наручных часов, замаскированые под винт, авторучку и т.п.

• Оборудование для приема побочного электромагнитного (ЭМ) излучения элементов персонального компьютера (ПК) - Излучение исходит от монитора, центрального процессора, клавиатуры, принтера, цепи питания. Диапазон излучения от десятков кГц до сотен мГц и R до 1000 м от ПК.

• Оборудование для прослушивания каналов мобильной связи

Технические средства защиты и противодействия

Средства для «контршпионажа» помогают «очистить» помещения и телефоны от всевозможных закладок или их нейтрализовать.

К таким средствам относятся:

1. Устройства поиска и обнаружения активных технических устройств и побочных электромагнитных излучений, и наводок (ПЭМИН) (детекторы, сканеры-приемники, детекторы магнитофонов, анализаторы спектра).

Детекторы «жучков» и видеокамер изготавливаются в виде авторучки, пачки сигарет со светодиодным индикатором. Радиус действия - несколько метров.

Карманный детектор подслушивающих "жучков" и скрытых видеокамер определяет точное местонахождения средств нелегального съема аудио и видео информации с передачей данных по радиоканалу.

Индикаторы радиоизлучения в виде широкополосных приемников или сканирующих детекторов (0,5 – 3000 МГц).

Нелинейные локаторы – находят пассивные и активные устройства, содержащие полупроводниковые и другие нелинейные элементы.

2. Средства обеспечения скрытности информационного обмена

Скремблер – шифровальное средство, предназначенное для защиты информации от непосредственного прослушивания за счет преобразования аналоговых параметров речи (временная или частотная перестановка сигнала) или цифрового шифрования.

3. Устройства нейтрализации средств съема информации

• Передатчики активных помех (в т.ч. прицельных)

• Генераторы шумов

• Устройства защиты от подслушивания через телефонную сеть

• Индикаторы субъектов и системы ограничения доступа с использованием паролей, ключей, биометрических систем (по отпечаткам пальцев, по голосу, по сетчатке глаз).

4. Программные и криптографические средства защиты

Программные средства защиты реализуются путем применения специальных программ, включенных в состав программного обеспечения АС и реализующих защиту баз данных и программ обработки конфиденциальной информации.

Используются: пароли, антивирусные программы, электронная подпись, защищенные документы.

Криптографические средства основаны на преобразовании математическими методами какого-либо сообщения.

5. Новые средства:

• устройства, реагирующие на свет (подающие сигнал при открытии ящика стола), светочувствительные покрытия, наносимые на документы;

• маркеры-красители не смывающиеся в течение недели, защищающие от ксерокопирования, дурнопахнущие;

• вязкая пена;

• лазерные ослепители (фонари).

Детекторы лжи для мобильных телефонов

Устройство может подключаться к сотовому телефону и оценивать правдивость собеседника, отличает различные типы состояния и определяет, говорит ли человек правду, сильно возбужден, пытается слегка хитрить или просто врет. Разработчики заявляют, что точность мобильного полиграфа составляет около 85%.

Для этого могут использоваться, например, технологии многослойного анализа голоса Sence и Layered Voice Analysis (LVA) израильской фирмы Nemesysco. Человеческая речь проходит через датчики, определяющие ее эмоциональную насыщенность. В конце разговора обладатель детектора лжи получает график, демонстрирующий сомнительные моменты беседы и делает соответствующие выводы.

Правовая защита информации, циркулирующей в телефонных и других линиях связи

Конституция РФ (ст. 23, 24) - Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Ограничение этого права допускается только на основании судебного решения (ст. 23).

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается (ст. 24).

УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, -

наказываются штрафом до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до четырех лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до четырех лет.

3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, 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.

Примечание 1. Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя.

Примечание 2. К специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном

обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, с открыто расположенными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно путем специальной технической доработки, программирования или иным способом не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя.

Регулирование деятельности, связанной со специальными техническими средствами

Указ Президента РФ «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» от 09.01.1996 г. № 21 постановляет возложить на ФСБ:

- лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц (далее именуются - неуполномоченные лица), связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в Российскую Федерацию и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также, регистрацию и учет таких специальных технических средств;

- выявление и пресечение случаев проведения оперативно-розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами;

15. Правовая основа системы лицензирования и сертификации в РФ.

Для обеспечения защиты ГТ и СТ (в важных для страны областях) действует Государственная система защиты информации в РФ (ГСЗИ).

ГСЗИ представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Так же является составной частью системы обеспечения национальной безопасности РФ и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере.

Организацию деятельности государственной системы защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной Государственной системой осуществляет ФСТЭК России.

ГСЗИ как система более сложная, включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

ГСЗИ включает:

• совокупность органов (ФСБ, ФСТЭК, СБ), сил и средств, осуществляющих деятельность в области защиты информации (ЗИ);

• систему лицензирования деятельности в области ЗИ;

• систему сертификации средств ЗИ;

• систему подготовки и переподготовки специалистов в области ЗИ.

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 течении определенного времени.

Перечень видов деятельности в области ЗИ, на которые выдаются лицензии, определен Постановлением

Правительства РФ “Об организации лицензирования отдельных видов деятельности” от 04.05.2011 № 99-ФЗ.

К ним, в частности, относятся (ст. 12):

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

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

3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации.

Положениями о лицензировании конкретных видов деятельности устанавливаются исчерпывающие перечни выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности, в случае, если указанные перечни не установлены федеральными законами.

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:

• “О государственной тайне” от 21.07.1993 г. № 5485-1;

• “О техническом регулировании” от 27.12.2002 г. № 184-ФЗ;

• “О лицензировании отдельных видов деятельности” от 04.05.2011 г. № 99-ФЗ;

• “О защите прав потребителей” от 07.02.1992 г. № 2300-1.

16. Лицензирование деятельности по защите государственной тайны.

Общие нормы, устанавливающие порядок организации и осуществления этой деятельности, содержатся в ст. 27 "Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну" Закона "О государственной тайне".

Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

• выполнение требований нормативных документов, утверждаемых Правительством РФ, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

• наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

• наличие у них сертифицированных средств защиты информации.

В периоды мобилизации, действия чрезвычайного или военного положения Президентом РФ может быть установлен иной порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Постановлением Правительства РФ № 333 от 15.04.1995 г. утверждено Положение о лицензировании 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.

В постановлении 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:

по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих ГТ - ФСБ, СВР(за рубежом);

на право проведения работ, связанных с созданием средств защиты информации - ФСТЭК, МО, ФСБ (в пределах их компетенции);

на право осуществления мероприятий и (или) оказания услуг в области защиты ГТ - ФСБ и ее территориальные органы, ФСТЭК, СВР (в пределах их компетенции).

Лицензирование деятельности предприятий ФСБ, МО, Федеральной пограничной службы РФ, СВР и ФСТЭК по допуску к проведению работ, связанных с использованием сведений, составляющих ГТ, а также с осуществлением мероприятий и (или) оказанием услуг по защите ГТ, осуществляется руководителями министерств и ведомств РФ, которым подчинены указанные предприятия.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не более чем на 5 лет. По просьбе заявителя лицензия может выдаваться на срок менее 5 лет. Срок действия лицензии, выданной предприятию, не может превышать срока действия лицензии предприятия, структурное подразделение по защите ГТ которого оказывает услуги по защите ГТ.

Продление срока действия лицензии производится в порядке, установленном для ее получения.

Предприятие может иметь несколько лицензий.

Основанием для отказа в выдаче лицензии является:

• наличие в документах, представленных заявителем, недостоверной или искаженной информации;

• отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям, указанным в пункте 7 настоящего Положения;

• отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Специальные экспертизы проводятся на основе договора между предприятием и органом, проводящим специальную экспертизу. Расходы по проведению специальных экспертиз относятся на счет 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 ГК и УК к нарушителям).

3. Лицензии на право деятельности в области защиты ГТ 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 заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности, следующие документы:

а) заявление о выдаче лицензии с указанием:

• наименования, организационно-правовой формы и местонахождения предприятия;

• идентификационного номера налогоплательщика;

• даты уплаты предприятием государственной пошлины за предоставление лицензии;

• сведений о наличии допуска к ГТ у руководителя предприятия;

• адресов мест осуществления лицензируемого вида деятельности;

• реквизитов правоустанавливающих документов на объекты недвижимости,

необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

• вида деятельности, на осуществление которого должна быть выдана лицензия;

• срока действия лицензии;

• подтвержденной в установленном порядке степени секретности сведений, составляющих ГТ, с которыми заявитель предполагает проводить работы;

• формы предоставления лицензии (на бумажном носителе или в электронной форме (в форме электронного документа, подписанного электронной подписью));

б) копии учредительных документов юридического лица;

в) копии правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

г) копия договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите ГТ другой организации).

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо Аттестационными центрами.

Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.

В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в 15-дневный срок после получения заключения экспертизы, но не позднее чем через 60 дней со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

В зависимости от сложности и объема подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до 30 дней.

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.

Система лицензирования обеспечивает в отношении АС выполнение 3 основных требований к защищаемой информации:

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Целостность информации – термин в информатике (криптографии, теории телекоммуникаций, теории информационной безопасности), означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

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

Государственная аттестация руководителей ответственных за защиту ГТ

Основная цель государственной аттестации – повысить компетентность руководителей в части обеспечения сохранности сведений, составляющих ГТ.

Решением от 13.03.1996 г. № 3 Межведомственная комиссия по защите государственной тайны утвердила и ввела в действие "Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну".

Государственное аттестование проводится методом собеседования аттестационной комиссии с руководителем предприятия.

К аттестуемому предъявляются следующие требования.

Должен знать:

• законодательные акты РФ по вопросам защиты ГТ;

• нормативные документы, утверждаемые Правительством РФ, по обеспечению защиты сведений, составляющих ГТ;

• нормативно-методические документы по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам;

• 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 ГТ.

Должен уметь организовывать:

• разработку мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих ГТ, и оценку их достаточности;

• проведение анализа возможностей разведки по добыванию сведений, составляющих ГТ;

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

• комплексный контроль выполнения принимаемых мер по защите сведений, составляющих ГТ.

Быть ознакомленным:

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

• с возможностями иностранных разведок по добыванию сведений, составляющих ГТ;

• с методиками контроля выполнения норм противодействия иностранным техническим разведкам.

17. Сертификация средств защиты информации.

Системы сертификации – это системы норм, правил, критериев качества продукции, методов их выявлений и оценки соответствия необходимым параметрам.

Системы сертификации могут быть международными, национальными и региональными. Национальный орган по сертификации определяется Правительством РФ.

В настоящее время национальным органом сертификации в РФ является Росстандарт - Федеральное агентство по техническому регулированию и метрологии (ФАТРиМ).

На данный момент в России выделяется более 100 различных систем сертификации, которые в свою очередь подразделяются на обязательные и добровольные системы сертификации.

Обязательная система сертификации подразумевает, что проверка соответствия качества товара или услуги в этой системе установлена законодательно как обязательная, и реализация данного товара невозможна без оформления соответствующих документов в данной системе. Можно сказать, что самыми важными системами обязательной сертификации в России являются:

• Система сертификации ГОСТ Р;

• Система гигиенической (или санитарно-эпидемиологической) сертификации;

• Система пожарной сертификации.

Добровольные системы сертификации отличаются от обязательных только тем, что добровольный сертификат никто не может требовать. Однако, любая добровольная сертификация – это подтверждение качества товара или услуги, ответственности производителя.

Целями сертификации являются:

• создание условий для деятельности предприятий и предпринимателей на товарном рынке РФ и участия в международной торговле;

• содействие потребителям в компетентном выборе продукции;

• содействие экспорту и повышение конкурентоспособности продукции;

• защита потребителя от недобросовестности изготовителя (продавца, исполнителя);

• контроль безопасности продукции для окружающей среды, жизни и имущества;

• подтверждение показателей качества продукции, заявленных изготовителями.

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну также входит в перечень систем обязательной сертификации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности (ст. 28. Порядок сертификации средств защиты информации Закона о государственной тайне).

Организация сертификации средств ЗИ возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством РФ.

Координация работ по организации сертификации средств ЗИ возлагается на межведомственную комиссию по защите ГТ.

Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

Положение о системе сертификации средств ЗИ утверждено Приказом ФСТЭК России 03.04.2018 г. № 55 и зарегистрировано в Министерстве юстиции РФ 11.05.2018 г., регистрационный № 51063.

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.

Сертификации в системе сертификации ФСТЭК России подлежат:

• средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

• средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

• средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Сертификация средств защиты информации иностранного производства, в отношении которых нормативными правовыми актами Российской Федерации установлены ограничения или запреты на их использование в Российской Федерации, в системе сертификации ФСТЭК России не осуществляется.

Сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России (т.е. требованиями по безопасности информации).

Участниками системы сертификации ФСТЭК России являются:

• федеральный орган по сертификации;

• организации, аккредитованные ФСТЭК России в качестве органа по сертификации (далее – органы по сертификации);

• организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории (далее – испытательные лаборатории);

• изготовители средств защиты информации.

ФСТЭК России в соответствии с подпунктами 13 и 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 г. № 1085, организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации, а также в соответствии с Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26.06.1995 г. № 608, выполняет функции федерального органа по сертификации.

Органы по сертификации осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации (сертификат соответствия).

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов.

Изготовители разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации.

Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну.

Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.

Сертификация средств защиты информации осуществляется по следующим схемам:

• для единичного образца средства защиты информации – проведение испытаний образца средства защиты информации и проверки организации его технической поддержки;

• для партии средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его технической поддержки;

• для серийного производства средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его производства и технической поддержки.

Сертификация единичного образца или партии средства защиты информации организуется заявителем, планирующим применять средство защиты

информации, в случае, если отсутствуют идентичные серийно производимые сертифицированные средства защиты информации.

Сертификация серийного производства средства защиты информации организуется заявителем, осуществляющим разработку и (или) производство средства защиты информации.

Сертификационные испытания средств защиты информации проводятся на материально-технической базе испытательной лаборатории, а также на материально-технических базах заявителя и (или) изготовителя, расположенных на территории РФ.

Срок действия сертификата соответствия не может превышать 5 лет.

Сертификат соответствия выдается на срок, указанный в заявке на сертификацию.

Серийно производимое средство защиты информации считается сертифицированным, если оно произведено в период срока действия сертификата соответствия на его серийное производство, соответствует требованиям по безопасности информации и изготовитель и (или) заявитель осуществляют его техническую поддержку.

Для единичного образца или партии средства защиты информации срок действия сертификата соответствия не устанавливается.

Сертификация средства защиты информации включает следующие процедуры:

- подача заявки на сертификацию;
- принятие решения о проведении сертификации средства защиты информации;
- сертификационные испытания средства защиты информации;
- оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия;
- выдача (или отказ в выдаче) сертификата соответствия;
- предоставление дубликата сертификата соответствия;
- маркирование средств защиты информации;
- внесение изменений в сертифицированное средство защиты информации;
- переоформление сертификата соответствия;
- продление срока действия сертификата соответствия;
- приостановление действия сертификата соответствия;
- прекращение действия сертификата соответствия.

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.

Помимо этого, в области ИТ действуют системы добровольной сертификации. Например, Система сертификации банковских технологий МЕКАС (ССБТ МЕКАС); Система добровольной сертификации услуг связи, средств связи и систем менеджмента качества организаций связи "Связь-Качество"; Система добровольной сертификации "Связь-Эффективность".

Преимуществами наличия такого добровольного сертификата является повышение в разы конкурентоспособности компании на рынке и предоставляет ряд определенных выгод для бизнеса:

• повышение шансов на участие в конкурсных процедурах по выбору поставщика, проводимых в рамках государственных или коммерческих закупок;
• рост доверия заказчиков к предприятию;
• стимулирование спроса на услуги и расширение клиентской базы;
• формирование положительного имиджа фирмы;
• укрепление деловой репутации;
• рост эффективности маркетинговых кампаний;
• улучшение узнаваемости бренда;
• повышение инвестиционной привлекательности и капитализации бизнеса;
• выход на новые рынки и пр.

18. Аттестация объектов информатизации по требованиям безопасности информации.

Аттестация объектов информатизации по требованиям безопасности информации осуществляется системой аттестации объектов информатизации по требованиям безопасности информации, являющейся составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации, созданной Гостехкомиссией России и возглавляемой ею до 2005 г. С 2005 г. эту систему возглавляет ФСТЭК России.

Деятельность по аттестации объектов информатизации в названной системе осуществляется в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Государственной технической комиссии при Президенте РФ 25.11.1994 г.

Оно устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

В соответствии с п. 1.5 названного Положения обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей ГТ, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит

добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизациимер и средств защиты информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

Организационная структура системы аттестации объектов информатизации:

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

Порядок проведения аттестации объектов информатизации и осуществления государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации определяет раздел 3 названного Положения.

Проведение аттестации объектов информатизации по требованиям безопасности информации в соответствии с п. 3.1 раздела 3 названного Положения включает в себя следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработку программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрацию и выдачу "Аттестата соответствия";

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

- рассмотрение апелляций.

Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи «Аттестата соответствия» и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Если объект информатизации отвечает (соответствует) требованиям по безопасности информации, органом по аттестации выдается «Аттестат соответствия» на этот объект заявителю.

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

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

19. 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 04.05.2011 г. № 99-ФЗ.

Лицензирование – деятельность лицензирующих органов по предоставлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, оценке соблюдения соискателем лицензии, лицензиатом лицензионных требований, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по

предоставлению в установленном порядке информации по вопросам лицензирования.

Лицензия – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается записью в реестре лицензий.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории РФ и на иных территориях, над которыми РФ осуществляет юрисдикцию в соответствии с законодательством РФ и нормами международного права, требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами, указанными в части 3 статьи 1 настоящего Федерального закона и регулирующими отношения в соответствующих сферах деятельности.

Лицензирующие органы – уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, органы исполнительной власти субъектов РФ, осуществляющие лицензирования в рамках полномочий субъектов РФ по предметам совместного ведения РФ и субъектов РФ, либо в случае передачи осуществления полномочий РФ в области лицензирования органам государственной власти субъектов РФ, а также Государственная корпорация по космической деятельности "Роскосмос".

Соискатель лицензии – юридическое лицо (в том числе иностранное юридическое лицо, если возможность осуществления лицензируемого вида деятельности иностранным юридическим лицом установлена в соответствии с частью 4 статьи 12 настоящего Федерального закона) или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии.

Лицензиат – юридическое лицо (в том числе иностранное юридическое лицо, если возможность осуществления лицензируемого вида деятельности иностранным юридическим лицом установлена в соответствии с частью 4 статьи 12 настоящего Федерального закона) или индивидуальный предприниматель, имеющие лицензию.

Лицензионные требования – обязательные требования, которые связаны с осуществлением лицензируемых видов деятельности, установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства РФ и (или) положениях международных договоров РФ, не требующих издания внутригосударственных актов для их применения и действующих в РФ, направлены на обеспечение достижения целей лицензирования и оценка соблюдения которых осуществляется в порядке, предусмотренном настоящим Федеральным законом.

Место осуществления отдельного вида деятельности, подлежащего лицензированию (место осуществления лицензируемого вида деятельности) – производственный объект (здание, помещение, сооружение, линейный объект, территория, в том числе водные, земельные и лесные участки, транспортное средство и другой объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении,

соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо ином законном основании, а также территория, которая предназначена для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении. Место осуществления лицензируемого вида деятельности имеет почтовый адрес и (или) другие данные, позволяющие его идентифицировать. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата. Положением о лицензировании конкретного вида деятельности может быть предусмотрено, что местом осуществления лицензируемого вида деятельности не могут являться помещения, здания, сооружения жилого назначения.

Уполномоченное должностное лицо лицензирующего органа – руководитель лицензирующего органа, иное должностное лицо лицензирующего органа, уполномоченное на принятие решения, осуществление иного действия в сфере лицензирования.

В соответствии с законом лицензированию подлежат следующие виды деятельности в области ЗИ (ст. 12):

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

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

3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации;

6) частная охранная деятельность;

7) частная детективная (сыскная) деятельность.

Заявление о предоставлении лицензии и прилагаемые к нему документы соискатель лицензии вправе направить в лицензирующий орган как почтовым отправлением, так и в форме электронного документа, подписанного ЭП.

В этом случае лицензирующий орган направляет соискателю лицензии в форме электронного документа, подписанного ЭП.

На каждый вид деятельности предоставляется лицензия, которая действует бессрочно.

Особенности лицензирования, в том числе в части, касающейся порядка принятия решения о предоставлении лицензии, срока действия лицензии и порядка продления срока ее действия, приостановления, возобновления и аннулирования действия лицензии, могут устанавливаться федеральными законами, регулирующими осуществление, например, следующих видов деятельности:

• оказание услуг связи, телевизионное вещание и (или) радиовещание;

• частная детективная (сыскная) деятельность и частная охранная деятельность.

Постановление Правительства РФ от 03.02.2012 г. № 79 утвердило "Положение о лицензировании деятельности по технической защите конфиденциальной информации.

Положение определяет порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством РФ), осуществляемой юридическими лицами и индивидуальными предпринимателями.

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

Лицензирование работ по ТЗКИ осуществляет ФСТЭК.

При осуществлении лицензируемого вида деятельности лицензированию подлежат:

а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

• в средствах и системах информатизации;

• в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

• в помещениях со средствами (системами), подлежащими защите;

• в помещениях, предназначенных для ведения конфиденциальных переговоров (защищаемые помещения);

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по ЗИ:

• средств и систем информатизации;

• помещений со средствами (системами) информатизации, подлежащими защите;

• защищаемых помещений;

д) работы и услуги по проектированию в защищенном исполнении:

• средств и систем информатизации;

• помещений со средствами (системами) информатизации, подлежащими защите;

• защищаемых помещений;

е) услуги по установке, монтажу, наладке, испытаниям, ремонту СЗИ (технических СЗИ, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) СЗИ, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Лицензионными требованиями, предъявляемыми к соискателю лицензии на осуществление лицензируемого вида деятельности (лицензия), являются:

а) наличие у соискателя лицензии:

• юридического лица - в штате по основному месту работы в соответствии со штатным расписанием руководителя и (или) уполномоченного руководить работами по лицензируемому виду деятельности лица, имеющих высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов), а также инженерно-технических работников (не менее 2 человек), имеющих высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов);

• индивидуального предпринимателя - высшего образования по направлению подготовки (специальности) в области ИБ и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, или высшего образования по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и

технических наук и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или иного высшего образования и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, а также дополнительного профессионального образования по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

б) наличие по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, в которых созданы необходимые условия для размещения работников, производственного и испытательного оборудования для осуществления лицензируемого вида деятельности, обсуждения информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

в) наличие принадлежащего соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, оборудования, необходимого для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем, в том числе:

• измерительных приборов, прошедших в установленном законодательством РФ порядке метрологическую поверку (калибровку);

• программных (программно-технических) средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации, а также средств контроля (анализа) исходных текстов программного обеспечения;

г) наличие по месту осуществления лицензируемого вида деятельности принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, автоматизированных систем, предназначенных для обработки конфиденциальной информации, средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством РФ;

д) наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем. Документы, содержащие информацию ограниченного доступа, должны быть получены в установленном законодательством РФ порядке.

Для получения лицензии соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:

а) заявление о предоставлении лицензии с описью прилагаемых документов;

б) копии документов, подтверждающих наличие в штате соискателя лицензии руководителя и (или) уполномоченного руководить работами по лицензируемому виду деятельности лица, инженерно-технических работников и их квалификацию (приказов о назначении или выписок из трудовых книжек, дипломов, удостоверений, свидетельств), и (или) сведения о трудовой деятельности, предусмотренные ст. 66_1 ТК РФ;

в) копии документов, подтверждающих наличие у соискателя лицензии по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, необходимых для осуществления лицензируемого вида деятельности и принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях (зданиях, сооружениях);

г) копии технических паспортов и аттестатов соответствия защищаемых помещений, находящихся по месту осуществления лицензируемого вида деятельности, требованиям безопасности информации;

д) документы на автоматизированные системы, находящиеся в защищаемых помещениях по месту осуществления лицензируемого вида деятельности, предназначенные для обработки конфиденциальной информации, и средства защиты такой информации:

• копии технических паспортов автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации, планов размещения основных и вспомогательных технических средств, и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации;

• перечень защищаемых в автоматизированных системах ресурсов;

• описание технологического процесса обработки информации в автоматизированных системах;

е) копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;

ж) документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;

з) документы, содержащие сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством РФ порядке;

и) копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами (при выполнении работ, указанных в подпункте "в" пункта 4 настоящего Положения).

При осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:

а) разработка средств защиты конфиденциальной информации, в том числе:

• технических средств защиты информации;

• защищенных технических средств обработки информации;

• технических средств контроля эффективности мер защиты информации;

• программных (программно-технических) средств защиты информации;

• защищенных программных (программно-технических) средств обработки информации;

• программных (программно-технических) средств контроля защищенности информации;

б) производство средств защиты конфиденциальной информации, в том числе:

• технических средств защиты информации;

• защищенных технических средств обработки информации;

• технических средств контроля эффективности мер защиты информации;

• программных (программно-технических) средств защиты информации;

• защищенных программных (программно-технических) средств обработки информации;

• программных (программно-технических) средств контроля защищенности информации;

Если в качестве лицензирующего органа выступает ФСТЭК, лицензионными требованиями, предъявляемыми к соискателю лицензии на осуществление лицензируемого вида деятельности (далее - лицензия), являются:

а) наличие в штате у соискателя лицензии по основному месту работы в соответствии со штатным расписанием следующего квалифицированного персонала:

• руководитель и (или) уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому

виду деятельности не менее 7 лет, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов);

• инженерно-технические работники (не менее 2 человек), имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

б) наличие по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, в которых созданы необходимые условия для размещения работников, производственного и испытательного оборудования, необходимого для осуществления лицензируемого вида деятельности, обсуждения информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

в) наличие принадлежащего соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, оборудования, необходимого для выполнения работ и (или) оказания услуг, предусмотренных пунктом 3 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем, в том числе:

• производственного и испытательного оборудования;

• измерительных приборов, прошедших в установленном законодательством РФ порядке метрологическую поверку (калибровку);

• программных (программно-технических) средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации, а также средств контроля (анализа) исходных текстов программного обеспечения;

г) наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 3 настоящего Положения, в соответствии с определяемым ФСТЭК перечнем. Документы, содержащие информацию ограниченного доступа, должны быть получены в установленном законодательством РФ порядке;

д) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при

выполнении работ, предусмотренных подпунктом "а" п. 3 настоящего Положения);

е) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

Если в качестве лицензирующего органа выступает ФСБ России, лицензионными требованиями, предъявляемыми к соискателю лицензии, являются:

а) наличие в штате у соискателя лицензии на основной работе согласно штатному расписанию следующего квалифицированного персонала:

• руководитель и (или) уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области проводимых работ по лицензируемому виду деятельности не менее 5 лет;

• инженерно-технические работники (не менее 2 человек), имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по этой специальности (нормативный срок - свыше 100 аудиторных часов);

б) наличие помещений для осуществления лицензируемого вида деятельности, соответствующих требованиям технической и технологической документации, национальных стандартов и методических документов в области защиты информации и принадлежащих соискателю лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования;

в) наличие у соискателя лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования, контрольно-измерительного оборудования (прошедшего в соответствии с законодательством РФ метрологическую поверку (калибровку) и маркирование), производственного, испытательного оборудования и иных объектов, необходимых для осуществления лицензируемого вида деятельности;

г) наличие предназначенных для осуществления лицензируемого вида деятельности программ (в том числе программных средств разработки средств защиты конфиденциальной информации) для электронно-вычислительных машин и баз данных, принадлежащих соискателю лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования;

д) наличие аттестованных по требованиям безопасности информации средств обработки информации, используемых для разработки и производства средств защиты конфиденциальной информации, в соответствии с требованиями по защите информации;

е) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при выполнении работ, предусмотренных подпунктом "а" пункта 3 настоящего Положения);

ж) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

Для получения лицензии соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:

а) заявление о предоставлении лицензии с описью прилагаемых документов;

б) копии документов, подтверждающих наличие в штате соискателя лицензии специалистов по защите информации и их квалификацию (приказов о назначении или выписок из трудовых книжек, дипломов, удостоверений, свидетельств) и (или) сведения о трудовой деятельности, предусмотренные ст. 66_1 ТК РФ;

в) копии правоустанавливающих документов на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);

г) копии аттестатов соответствия защищаемых помещений требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;

д) копии аттестатов соответствия средств обработки информации требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;

е) копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;

ж) сведения о наличии производственного, испытательного и контрольно-измерительного оборудования, средств защиты информации, средств разработки и производства средств защиты конфиденциальной информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного

оборудования, а также документов, подтверждающих право соискателя лицензии на использование указанных оборудования и средств;

з) сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных п. 3 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством Российской Федерации порядке (в случае, если в качестве лицензирующего органа выступает Федеральная служба по техническому и экспортному контролю);

и) копии документов, подтверждающих наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при выполнении работ, предусмотренных подпунктом "а" п. 3 настоящего Положения);

к) копии документов, подтверждающих наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий 45 дней с даты поступления в лицензирующий орган заявления.

Схема последовательности действий при лицензировании

1. Прием лицензирующим органом заявления о предоставлении (продлении срока действия, переоформлении документа, подтверждающего наличие) лицензии

2. Проверка лицензирующим органом полноты и достоверности сведений о соискателе лицензии и возможности выполнения соискателем лицензии лицензионных требований и условий

3. Принятие лицензирующим органом решения о предоставлении или об отказе в предоставлении лицензии

4. Уведомление лицензирующим органом соискателя лицензии о предоставлении или об отказе в выдаче лицензии

5. Выдача лицензирующим органом соискателю лицензии документа, подтверждающего наличие лицензии (в случае принятия решения о предоставлении лицензии)

6. Занесение сведений о лицензиате в реестр лицензий

Грубыми нарушениями лицензионных требований и условий являются:

- невыполнение лицензиатом режима конфиденциальности при обращении со сведениями, которые ему доверены или стали известны в ходе служебной деятельности;

- отсутствие у руководителя лицензиата документа о высшем профессиональном образовании в области технической защиты информации, а также производственного стажа в области лицензируемой деятельности не менее 5 лет;

- отсутствие у инженерно-технического персонала, осуществляющего работы в области лицензируемой деятельности, документа о высшем образовании или профессиональной подготовке со специализацией, соответствующей выполняемым работам.

20. Нормы ответственности за правонарушения в информационной сфере.

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 представлены в Уголовном, Гражданском, Административном кодексах и других правовых актах.

Уголовное право регулирует отношения в области наиболее опасных правонарушений – преступлений.

Санкции за нарушение информационных правоотношений представлены в УК следующими статьями.

Статья 128_1. Клевета

т.е. клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет", либо в отношении нескольких лиц, в том числе индивидуально не определенных.

Статья 137. Нарушение неприкосновенности частной жизни

т.е. действия направленные на незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой

информации, включая те же деяния, совершенные лицом с использованием своего служебного положения.

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

Статья 140. Отказ в предоставлении гражданину информации

Статья 141. Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий

Статья 142. Фальсификация избирательных документов, документов референдума, документов общероссийского голосования

Статья 144. Воспрепятствование законной профессиональной деятельности журналистов

т.е. путем принуждения их к распространению либо к отказу от распространения информации.

Статья 146. Нарушение авторских и смежных прав

Статья 147. Нарушение изобретательских и патентных прав

Статья 180. Незаконное использование средств индивидуализации товаров (работ, услуг)

т.е. незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров.

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

т.е. собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом, а также без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Статья 204. Коммерческий подкуп

Статья 205_2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма

Статья 207. Заведомо ложное сообщение об акте терроризма

Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей

Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов

в т.ч. с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет".

Статья 242_1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних

в т.ч. с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет".

Статья 272. Неправомерный доступ к компьютерной информации

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

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

Статья 275. Государственная измена

Статья 276. Шпионаж

Статья 280. Публичные призывы к осуществлению экстремистской деятельности

Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства

Статья 283. Разглашение государственной тайны

Статья 283_1. Незаконное получение сведений, составляющих государственную тайну

Статья 283_2. Нарушение требований по защите государственной тайны

Статья 284. Утрата документов, содержащих государственную тайну

Статья 287. Отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации

Статья 298_1. Клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения Российской Федерации

Статья 354. Публичные призывы к развязыванию агрессивной войны

21. Защита информации от неправомерных действий органов, занимающихся оперативно-розыскной деятельностью.

Деятельность этих органов основывается на Законе РФ “Об оперативно-розыскной деятельности”, от 12.08.1995 г. № 144-ФЗ.

Оперативно-розыскная деятельность (ОРД) – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим ФЗ (далее – органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств (ст. 1).

Задачи ОРД (ст. 2):

• выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших;

• осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших;

• добывание информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации;

• установление имущества, необходимого для обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий, или имущества, подлежащего конфискации.

Принципы ОРД. ОРД основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина, а также на принципах конспирации, сочетания гласных и негласных методов и средств (ст. 3).

Сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-розыскных мероприятий составляют государственную тайну и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность (ст. 12, ст. 12_1). В связи с этим в открытой литературе подобные сведения практически отсутствуют.

Оперативно-розыскными мероприятиями (ОРМ) предусматривается (ст. 6):

1. Опрос.
2. Наведение справок.
3. Сбор образцов для сравнительного исследования.
4. Проверочная закупка.
5. Исследование предметов и документов.
6. Наблюдение.
7. Отождествление личности.
8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
9. Контроль почтовых отправлений, телеграфных и иных сообщений.
10. Прослушивание телефонных переговоров.
11. Снятие информации с технических каналов связи.
12. Оперативное внедрение.
13. Контролируемая поставка.
14. Оперативный эксперимент.
15. Получение компьютерной информации.

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

ОРМ, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов ФСБ, ОВД в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность.

Ввоз в РФ и вывоз за ее пределы специальных технических средств (СТС), предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-розыскной деятельности физическими и юридическими лицами подлежат лицензированию в порядке, устанавливаемом Правительством РФ.

Перечень видов СТС, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством РФ.

Разработка, производство, реализация и приобретение в целях продажи СТС, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность, подлежат лицензированию в соответствии с законодательством РФ.

Запрещается проведение ОРМ и использование СТС, не уполномоченными на то физическими и юридическими лицами.

Органам (должностным лицам), осуществляющим ОРД, запрещается:

• проводить оперативно-розыскные мероприятия в интересах какой-либо политической партии, общественного и религиозного объединения;

• принимать негласное участие в работе федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, а также в деятельности зарегистрированных в установленном порядке и незапрещенных политических партий, общественных и религиозных объединений в целях оказания влияния на характер их деятельности;

• разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали известными в процессе проведения оперативно-розыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами;

• подстрекать, склонять, побуждать в прямой или косвенной форме к совершению противоправных действий (провокация);

• фальсифицировать результаты оперативно-розыскной деятельности (ст. 5).

В России применяется Система технических средств для обеспечения функций оперативно-разыскных мероприятий (СОРМ). СОРМ – это комплекс технических средств и мер, предназначенных для проведения оперативно-разыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи.

СОРМ обеспечивает два режима передачи информации:

• передача статистической информации;

• передача полной информации.

Различают 3 вида СОРМ:

СОРМ-1 – система прослушивания телефонных переговоров, организованная в 1996 г.;

СОРМ-2 – система протоколирования обращений к сети Интернет, организованная в 2000 г.

СОРМ-3 – обеспечивает сбор информации со всех видов связи и ее долговременное хранение. Она обеспечивает объединение всех вышеуказанных систем и дополнительно контролирует часть VPN серверов, прослушивает в прямом эфире Skype, ICQ, спутниковую связь и ряд других нововведений. Ключевой фактор СОРМ 3 – это единая глобальная база данных которая взаимно связанна с различными направлениями СОРМ. Она сохраняет полную статистику о пользователе, анализируя все виды трафика: мобильный, интернет-трафик, переписку в мессенджерах и т.д. Система позволяет сохранять полный объем данных за конкретный период (до трех лет) или анализировать их в реальном времени.

При проведении ОРМ должны соблюдаться права человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции (ст. 5).

Полученные в результате ОРД материалы в отношении лиц, виновность которых не доказана, хранятся 1 год, а затем уничтожаются.

Фонограммы и другие материалы, полученные в результате прослушивания телефонных и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, уничтожаются в течение шести месяцев с момента прекращения прослушивания. Об этом уведомляется соответствующий судья.

Основания для проведения ОРМ (ст. 7):

1. Наличие возбужденного уголовного дела.

2. Ставшие известными органам, осуществляющим ОРД, сведения о:

• признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;

• событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности РФ;

• лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания;

• лицах, без вести пропавших, и об обнаружении неопознанных трупов.

3. Поручения следователя, руководителя следственного органа, дознавателя, органа дознания или определения суда по уголовным делам и материалам проверки сообщений о преступлении, находящимся в их производстве.

4. Запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье.

5. Постановление о применении мер безопасности в отношении защищаемых лиц, осуществляемых уполномоченными на то государственными органами в порядке, предусмотренном законодательством РФ.

6. Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами РФ.

Органы, осуществляющие оперативно-розыскную деятельность, в пределах своих полномочий вправе также собирать данные, необходимые для принятия решений:

1. О допуске к сведениям, составляющим ГТ.

2. О допуске к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья людей, а также для окружающей среды.

3. О допуске к участию в ОРД или о доступе к материалам, полученным в результате ее осуществления.

4. Об установлении или о поддержании с лицом отношений сотрудничества при подготовке и проведении оперативно-розыскных мероприятий.

5. По обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность.

6. О предоставлении либо об аннулировании лицензии на осуществление частной детективной или охранной деятельности, о переоформлении документов, подтверждающих наличие лицензии, о выдаче (о продлении срока действия, об аннулировании) удостоверения частного охранника.

6_1. О выдаче (предоставлении), переоформлении, об изъятии и (или) аннулировании лицензий на приобретение, экспонирование или коллекционирование оружия, разрешения на ношение и использование охотничьего оружия, разрешений на хранение, хранение и ношение, хранение и использование оружия и патронов к нему, их ввоз в Российскую Федерацию либо вывоз из Российской Федерации, а также о внесении изменений в реестры указанных лицензий и разрешений.

8. О достоверности сведений о законности происхождения денег, ценностей, иного имущества и доходов от них у близких родственников, родственников и близких лиц лица, совершившего террористический акт, при наличии достаточных оснований полагать, что деньги, ценности и иное имущество получены в результате террористической деятельности, но не ранее установленного факта начала участия лица, совершившего террористический акт, в террористической деятельности и (или) являются доходом от такого имущества.

Проведение ОРМ (включая получение компьютерной информации), которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации:

1. О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.

2. О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно.

3. О событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ.

В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности РФ, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение ОРМ, предусмотренных частью второй настоящей статьи, с обязательным уведомлением суда (судьи) в течение 24 часов.

В течение 48 часов с момента начала проведения ОРМ орган, его осуществляющий, обязан получить судебное решение о проведении такого ОРМ либо прекратить его проведение.

Прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях.

Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами.

В случае возбуждения уголовного дела в отношении лица, телефонные и иные переговоры которого прослушиваются, фонограмма и бумажный носитель записи переговоров передаются следователю для приобщения к уголовному делу в качестве вещественных доказательств.

Дальнейший порядок их использования определяется уголовно-процессуальным законодательством РФ.

В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) в течение 48 часов.

Исключение составляет только радиосвязь, осуществляемая с помощью радиостанций, для прослушивания которой судебного решения не требуется.

Срок действия, вынесенного судьей постановления, исчисляется в сутках со дня его вынесения и не может превышать 6 месяцев.

Право осуществлять ОРД (ст. 13) на территории РФ предоставляется оперативным подразделениям:

1. Органов внутренних дел РФ.

2. Органов ФСБ.

4. Федерального органа исполнительной власти в области государственной охраны.

6. Таможенных органов РФ.

7. Службы внешней разведки РФ.

8. Федеральной службы исполнения наказаний.

Оперативное подразделение органа внешней разведки Министерства обороны Российской Федерации проводит оперативно-розыскные мероприятия только в целях обеспечения безопасности указанного органа внешней разведки и

в случае, если проведение этих мероприятий не затрагивает полномочий органов, указанных в пунктах 1, 2, 4, 6-8 части первой настоящей статьи.

Контроль за ОРД

Контроль за ОРД осуществляют Президент, Федеральное Собрание РФ и Правительство РФ в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами. (ст. 20).

В соответствии со ст. 21 предусмотрен прокурорский надзор за ОРД. Прокурорский надзор за исполнением настоящего ФЗ закона осуществляют Генеральный прокурор РФ и уполномоченные им прокуроры.

Руководители органов, осуществляющих ОРД, несут персональную ответственность за соблюдение законности при организации и проведении ОРМ.

Отдельным законом регулируется деятельность ФСБ - “О федеральной службе безопасности” от 03.04.1995 г. № 40-ФЗ.

ФСБ – единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности РФ.

Правовую основу деятельности федеральной службы безопасности составляют Конституция РФ, настоящий ФЗ, другие федеральные законы и иные нормативные правовые акты РФ.

Деятельность ФСБ осуществляется также в соответствии с международными договорами РФ.

На ФСБ возложены функции по организации системы защиты государственных секретов и ее методического обеспечения, а также оказание содействия негосударственным учреждениям, организациям и предприятиям в вопросах защиты коммерческой тайны и другой приоритетной информации.

Это дает основания всем заинтересованным субъектам соответствующих правовых отношений обращаться к органам ФСБ за содействием в обеспечении защиты коммерческой информации. Такое содействие может выражаться в консультировании, оказании технической и организационной помощи.

Полученные в процессе деятельности органов ФСБ сведения о частной жизни, затрагивающие честь и достоинство гражданина или способные причинить вред его законным интересам, не могут сообщаться органами ФСБ кому бы то ни было без добровольного согласия гражданина, за исключением случаев, предусмотренных федеральными законами.

В случае нарушения сотрудниками органов ФСБ прав и свобод человека и гражданина руководитель соответствующего органа ФСБ, прокурор или судья обязаны принять меры по восстановлению этих прав и свобод, возмещению причиненного ущерба и привлечению виновных к ответственности, предусмотренной законодательством РФ.

Должностные лица органов ФСБ, допустившие злоупотребление властью или превышение служебных полномочий, несут ответственность, предусмотренную законодательством РФ.

Для осуществления своей деятельности органы ФСБ могут без лицензирования разрабатывать, создавать и эксплуатировать информационные

системы, системы связи и системы передачи данных, а также средства защиты информации, включая средства криптографической защиты (ст. 20).

Наличие в информационных системах сведений о физических и юридических лицах не является основанием для принятия органами ФСБ мер, ограничивающих права указанных лиц.

Контроль за деятельностью органов ФСБ осуществляют Президент РФ, Федеральное Собрание РФ, Правительство РФ и судебные органы в пределах полномочий, определяемых Конституцией РФ, федеральными конституционными законами и федеральными законами (ст. 23).

Надзор за исполнением органами ФСБ законов РФ осуществляют Генеральный прокурор Российской Федерации и уполномоченные им прокуроры (ст. 24).

Сведения о лицах, оказывающих или оказывавших органам федеральной службы безопасности содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления деятельности органов федеральной службы безопасности в предмет прокурорского надзора не входят.

Имеются и другие правовые акты, регламентирующие деятельность этих органов. В ФЗ “О государственной гражданской службе РФ” от 27.07.2004 г. № 79-ФЗ указано, что государственный служащий обязан не разглашать сведения, составляющие государственную и иную охраняемую федеральным законом тайну, а также сведения, ставшие ему известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство (ст. 15).

22. Защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов.

Законодательной базой, регулирующей правовые отношения с контролирующими и правоохранительными органами, являются следующие документы:

1. Закон РФ “О защите конкуренции” от 26.07.2006 г. № 135-ФЗ.
2. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, от 22.03.1991 г. № 948-1.
3. Закон РФ “О полиции” от 07.02.2011 г. № 3-ФЗ.
4. Закона РФ “О санитарно-эпидемиологическом благополучии населения” от 30.03.1999 г. № 52-ФЗ.
5. Закон РФ “О банках и банковской деятельности” от 01.12.1990 г. № 395-1 (в ред. ФЗ от 03.02.1996 г. № 17-ФЗ).

Одной из форм недобросовестной конкуренции согласно закону “О защите конкуренции” является недобросовестная конкуренция, связанная с незаконным получением, использованием или разглашением информации, составляющей коммерческую или иную охраняемую законом тайну (ст. 14_7).

К числу контролирующих органов относится федеральный антимонопольный орган, который имеет свои территориальные управления.

В настоящее время функции федерального антимонопольного органа осуществляет Федеральная антимонопольная служба (ФАС) России. Положение о

Федеральной антимонопольной службе утверждено Постановлением Правительства РФ от 29.07.2004 г. № 331.

ФАС является уполномоченным федеральным органом исполнительной власти, осуществляющим функции по принятию нормативных правовых актов и контролю за соблюдением антимонопольного законодательства, законодательства в сфере деятельности субъектов естественных монополий, в сфере государственного регулирования цен (тарифов) на товары (услуги), рекламы, контролю за осуществлением иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства, контролю (надзору) в сфере государственного оборонного заказа, в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд и в сфере закупок товаров, работ, услуг отдельными видами юридических лиц, а также по согласованию применения закрытых способов определения поставщиков (подрядчиков, исполнителей).

Антимонопольный орган располагает для выполнения возложенных функций значительными полномочиями (беспрепятственный доступ в органы управления, на предприятия, право на ознакомление со всеми необходимыми документами и др.). Одна из его обязанностей - соблюдение КТ.

Сведения о ней, полученные в порядке выполнения возложенных обязанностей, не подлежат разглашению.

В случае разглашения сотрудниками ФАС сведений, составляющих КТ, причиненные убытки подлежат возмещению в соответствии с гражданским законодательством.

1. Информация, составляющая коммерческую, служебную, иную охраняемую законом тайну и полученная антимонопольным органом при осуществлении своих полномочий, не подлежит разглашению, за исключением случаев, установленных федеральными законами.

2. За разглашение информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, работники антимонопольного органа несут гражданско-правовую, административную и уголовную ответственность.

3. Вред, причиненный физическому или юридическому лицу в результате разглашения антимонопольным органом либо его должностными лицами информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, подлежит возмещению за счет казны РФ (ст. 26 ФЗ “О защите конкуренции”).

Вопросы, связанные с полномочиями органов МВД отражены в ФЗ “О полиции” от 07.02.2011 г. № 3-ФЗ.

Сотрудники полиции вправе беспрепятственно входить в помещения, занимаемые предприятиями, учреждениями, организациями, независимо от подчиненности и форм собственности, только при наличии данных о влекущем уголовную или административную ответственность нарушении законодательства, и производить осмотр в присутствии не менее двух понятых и представителя юридического лица.

Поэтому собственник или его представитель вправе потребовать от работника полиции сведений, объясняющих необходимость вхождения на

предприятие (или иной объект, например, факт возбуждения уголовного дела либо получения сведений при расследовании иного дела, его номер и орган, осуществляющий расследование).

Осмотр производственных, складских, торговых и иных служебных помещений, транспортных средств, других мест хранения и использования имущества производится только с участием собственника либо его представителей или уполномоченных им лиц.

Государственный контроль за деятельностью полиции осуществляют Президент РФ, палаты Федерального Собрания РФ, Правительство РФ в пределах полномочий, определяемых Конституцией РФ, федеральными конституционными законами и федеральными законами (ст. 49).

Прокурорский надзор за исполнением полицией законов осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры в соответствии с полномочиями, предоставленными федеральным законодательством (ст. 52).

Вред, причиненный гражданам и организациям противоправными действиями (бездействием) сотрудника полиции при выполнении им служебных обязанностей, подлежит возмещению в порядке, установленном законодательством РФ (ст. 33).

Значительными полномочиями по проверке соблюдения на предприятиях санитарных правил, норм и гигиенических нормативов обладают должностные лица и специалисты Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор) (ранее эту роль выполняла Государственная санитарно-эпидемиологическая служба РФ).

Роспотребнадзор является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере защиты прав потребителей, здорового питания, в области организации питания, обеспечения качества и безопасности пищевых продуктов, материалов и изделий, контактирующих с пищевыми продуктами, разработке и утверждению государственных санитарно-эпидемиологических правил и гигиенических нормативов, а также по организации и осуществлению федерального государственного санитарно-эпидемиологического контроля (надзора), федерального государственного контроля (надзора) в области защиты прав потребителей и федерального государственного контроля (надзора) за соблюдением законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию, федерального государственного лицензионного контроля (надзора) за деятельностью в области использования возбудителей инфекционных заболеваний человека и животных (за исключением случая, если указанная деятельность осуществляется в медицинских целях) и генно-инженерно-модифицированных организмов III и IV степеней потенциальной опасности, осуществляемой в замкнутых системах, федерального государственного лицензионного контроля (надзора) за деятельностью в области использования источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности) (ст. 1 «Положения о Федеральной службе по надзору в сфере защиты прав

потребителей и благополучия человека», утвержденного постановлением Правительства РФ от 30.06.2004 г. № 322).

Должностные лица, осуществляющие государственный санитарно-эпидемиологический надзор, обязаны соблюдать государственную, врачебную и иную охраняемую законом тайну в отношении информации, ставшей им известной при выполнении своих служебных обязанностей, и несут ответственность за ненадлежащее исполнение своих служебных обязанностей.

23. Сведения конфиденциального характера.

В действующем законодательстве РФ упоминается более 40 видов тайн (банковская, налоговая, коммерческая, профессиональная и т.д.), а с учетом законодательства Союзного государства (Республика Беларусь и РФ) таких тайн более 50.

В законе «Об информации, информационных технологиях и о защите информации» нет термина «конфиденциальная информация», но дается определение понятия «конфиденциальность информации».

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

Указом Президента Российской Федерации "Об утверждении перечня сведений конфиденциального характера" от 06.03.1997 г. № 188 был утвержден «Перечень сведений конфиденциального характера», где указаны:

- Коммерческая тайна
- Служебная тайна
- Профессиональная тайна
- Персональные данные
- Тайна следствия и судопроизводства
- Сведения о защищаемых лицах и мерах государственной защиты
- Сведения о сущности неопубликованных изобретений

Однако, данный перечень может быть утвержден только законом в соответствии с нормами международного права и Конституции РФ.

Отсутствие в законах четких определений видов информации с ограниченным доступом (за исключением государственной тайны) приводит к противоречиям между данным указом и существующими законодательными актами, что затрудняет их исполнение.

Например, в действующих кодексах есть такие понятия как личная, семейная тайны и неприкосновенность частной жизни, а в других законах - персональные данные.

В действующих законах нет понятия «тайна следствия и судопроизводства», но есть понятия «данные предварительного расследования», «данные предварительного следствия», «тайна совещания судей», «тайна совещания присяжных заседателей».

В законах не дается понятия служебной тайны и в то же время применяется понятие «служебная информация». Соотношение между ними не установлено, а в указе вводится категория только служебной тайны.

В действующем законодательстве наименее разработанными являются профессиональная тайна и служебная тайна.

Для обозначения грифа конфиденциальности используются международные и национальные нормативные документы. Причем требования российского законодательства отличаются от международных стандартов.

Так, в соответствии с международными стандартами в западных странах чаще используются следующиая классификация:

• открытая информация (ОИ) – Public;

• для внутреннего использования (ДВИ) – Internal;

• конфиденциальная информация (КИ) – Confidential;

• строго конфиденциальная информация (СКИ) – Strictly Confidential.

На основе российского законодательства предпочтительнее применять следующее разграничение информации по грифу конфиденциальности:

• открытая информация (ОИ);

• для внутреннего использования (ДВИ);

• конфиденциальная информация (КИ).

24. Нормативно-правовое регулирование профессиональной тайны.

В современном законодательстве РФ не принят закон «О профессиональной тайне» и нет чёткого определения профессиональной тайны.

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 определением профессиональной тайны выделяются следующие объекты профессиональной тайны:

Врачебная тайна – информация содержащая:

• результаты обследования лица, вступающего в брак;

• сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья.

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

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

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

Тайна усыновления – сведения об усыновлении ребенка усыновителем.

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

Тайна исповеди – сведения, доверенные священнослужителю гражданином на исповеди.

Журналистская тайна – сведения, сообщенные журналисту.

Правовые документы, включающие в себя и профессиональную тайну:

1. Законы РФ :

• ГК РФ (ст. 152.2. Охрана частной жизни гражданина);

• УК РФ (ст. 155. Разглашение тайны усыновления (удочерения));

• ГПК РФ (ст. 10. Гласность судебного разбирательства);

• УПК РФ (ст. 53. Полномочия защитника);

• Семейный кодекс РФ (ст. 15. Медицинское обследование лиц, вступающих в брак, ст. 139. Тайна усыновления ребенка);

• ФЗ «О связи» (ст. 63. Тайна связи) от 07.07.2003 г. № 126-ФЗ;

• ФЗ «Об основах охраны здоровья граждан в РФ» от 21.11.2011 г. № 323-ФЗ (ст. 13. Соблюдение врачебной тайны, ст. 73. Обязанности медицинских работников и фармацевтических работников);

• Закон «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 02.07.1992 г. (ст. 9. Сохранение врачебной тайны при оказании психиатрической помощи, ст. 46. Контроль общественных объединений за соблюдением прав и законных интересов граждан при оказании психиатрической помощи);

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 (ст. 138 УК РФ).

25. Нормативно-правовое регулирование служебной тайны.

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

Доступ к служебным сведениям закрытого характера связан с должностным статусом лиц, которым эти сведения стали известны по службе.

Поэтому при утечке этой информации страдают интересы службы (а не клиентов, как в случае профессиональной тайны).

До 2008 года в Гражданском кодексе РФ существовало понятие служебной тайны. Статья 139 ГК РФ закрепила, что информация является служебной тайной, когда она имеет коммерческую ценность в силу ее неизвестности третьим лицам. С принятием Федерального закона от 18.12.2006 г. № 231-ФЗ указанная статья ГК утратила силу. На охрану коммерческой тайны встал закон «О коммерческой тайне», а вот понятие служебной тайны осталось в подзаконных актах.

Ни федеральный закон, никакой-либо кодекс не содержат прямого определения служебной тайны, но сам термин остается в действующем ТК, КоАП и других актах. Исходя из действующих нормативных актов, понятие служебной тайны можно определить следующим образом:

Служебная тайна – это защищаемая конфиденциальная информация, доступ к которой ограничен законом, ставшая известной сотрудникам организаций при исполнении ими служебных обязанностей.

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

Служебная тайна не относится к коммерческой тайне. Служебная тайна – это служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (Указ Президента РФ от 06.03.1997 г. № 188). А коммерческая тайна – это информация, которая имеет действительную или потенциальную коммерческую ценность в силу того, что она неизвестна третьим лицам и охраняется обладателем.

То есть служебная тайна – это сведения конфиденциального характера о деятельности органов государственной, региональной или муниципальной власти. В это понятие также входят сведения ограниченного характера, в отношении которых предпринимаются действия по защите конфиденциальности и которые были получены законным путем в процессе исполнения должностных обязанностей госслужащими и сотрудниками перечисленных органов власти. Таким образом, отличительная особенность информации, относящейся к служебной тайне, заключается в том, что ее носителем является какой-либо государственный орган. То есть в коммерческой организации или у работодателя-физического лица не возникает необходимости охранять служебную тайну.

Обязанность работника не разглашать коммерческую или служебную тайну может быть установлена в трудовом договоре, должностной инструкции или в отдельном положении о служебной тайне.

Понятие служебной и профессиональной тайны также отличаются. Профессиональная тайна – это сведения, которые стали известны при выполнении профессиональной деятельности. В качестве примеров профессиональной тайны упоминается врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.п.

Служебная тайна регулируется актами специального назначения, которые направлены на деятельность работников государственного аппарата. Профессиональная тайна, в свою очередь, направлена на широкий круг специалистов и регулируется отдельным профильными законами.

В состав профессиональной тайны входят перечень сведений, которые относятся к той или иной профессии. Например, тайна журналиста, тайна исповеди и пр. Состав же служебной тайны определяется внутренними регламентами работы государственных и муниципальных органов. Например, следователь в ходе расследования уголовного дела будет опираться на внутренний регламент для защиты служебной тайны следственного отдела.

Есть сведения, которые нельзя однозначно отнести к профессиональной или служебной тайне. Например, персональные данные гражданина могут составить служебную тайну для прокурора, который рассматривает дело и является госслужащим. А для работника кадровой службы эти персональные данные будут являться профессиональной тайной.

Перечень сведений, которые составляют служебную тайну, можно выделить из определения служебной тайны (Положение о порядке обращения со служебной информацией ограниченного распространения, утв. Постановлением Правительства РФ от 03.11.1994 г. № 1233). Так, к служебной тайне относятся:

• сведения, которые касаются работы государственных органов или подведомственных организаций;

• сведения, которые получили работники этих учреждений в рамках исполнения своих должностных обязанностей о других лицах и структурах. (Это может быть личная, профессиональная, коммерческая информация, которая не подлежит разглашению.);

• тайна предварительного следствия и судебная тайна, включающая в себя тайну работы судей и присяжных;

• сведения, доступ к которым ограничил федеральный закон с целью защиты интересов государства.

Есть и другая классификация, которая поможет раскрыть сведения, которые относятся к служебной тайне. Так, к служебной тайне относятся:

• следственная;

• налоговая;

• судебная;

• военная тайна;

• конфиденциальная информация, которая составляет коммерческую, банковскую, профессиональную тайну или тайну личной жизни, которую служащий получил в ходе исполнения своих обязанностей.

Таким образом, условия отнесения информации к служебной тайне определяет закон. Можно выделить три критерия, по которым информация может быть отнесена к служебной тайне:

• она не составляет государственную тайну;

• она не является общедоступной;

• обеспечить ее сохранность и ограничить несанкционированный доступ можно в режиме профессиональной или служебной тайны.

Некоторые специалисты считают, что адвокатская и врачебная тайна относятся к служебной. Но врачи и адвокаты не являются государственными или муниципальными служащими и сведения, которые они получили в ходе работы, относятся к профессиональной тайне, а не к служебной.

Федеральный закон «Об информации, информационных технологиях и о защите информации» (от 27.07.2006 г. № 149-ФЗ), а также «Положение о порядке обращения со служебной информацией ограниченного распространения» содержит перечень сведений, которые не могут составлять служебную тайну:

1. Нормативно-правовые акты, которые затрагивают права, обязанности, свободы граждан.

2. Информация о состоянии окружающей среды (о чрезвычайных ситуациях, опасных природных явлениях), и необходимая для обеспечения безопасного существования населенных пунктов, производственных объектов, граждан и населения в целом.

3. Информация о деятельности государственных органов и органов местного самоуправления.

4. Порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц в органы государственной власти.

5. Сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения.

6. Информация в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах.

Служебная тайна относится к конфиденциальной информации. Поэтому закон предъявляет к ней особые меры защиты. Так, в целях защиты служебной информации необходимо принять меры, которые должны обеспечить:

• защиту от несанкционированного доступа, копирования, уничтожения, внесения изменений, блокирования и тиражирования сведений, составляющих служебную тайну;

• сохранение конфиденциальности;

• реализацию права на доступ только ограниченному кругу лиц, имеющих официальное разрешение.

Необходимые меры по защите служебной тайны – разработка локальных нормативных актов, напр., «Положение о порядке обращения со служебной информацией ограниченного пользования». Этим регламентом определяют категории должностей, которым в силу служебной необходимости будет открыт доступ к такого рода сведениям, а также порядок обращения с ними и передачи по запросам в другие органы государственной власти. Положением необходимо установить порядок присвоения и снятия статуса «Для служебного пользования» документам в организации, а также меры, направленные на защиту такой информации и документов.

Положение о защите служебной тайны не относится к тем, что в соответствии с ТК должны согласовываться с представительным органом работников. Работодатель вправе разработать и утвердить его самостоятельно.

Доступ к документам, которые содержат служебную тайну, работникам учреждения производится только под расписку. При необходимости передать сведения в другие органы или организации используется защищенный канал связи или пересылка заказными, или ценными отправлениями. Копии со служебных документов разрешается делать только по распоряжению руководителя. Все бумаги, составляющие служебную тайну, должны храниться в запираемых хранилищах.

Работники, которые имеют доступ к служебной тайне, должны подписать отдельный договор или соглашение о неразглашении служебной тайны. Условие о запрете распространять эту тайну можно также закрепить в его трудовом договоре.

Если государственный или муниципальный служащий разгласит служебную тайну, его можно уволить по инициативе работодателя по п. 6 ст. 81 ТК. В этом случае работодатель должен зафиксировать нарушение, далее запросить у работника письменные объяснения по факту разглашения коммерческой тайны (ч. 1 ст. 193 ТК). Уволить работника можно будет не позднее месяца со дня обнаружения проступка (ч. 3 ст. 193 ТК).

Все документы, которые содержат конфиденциальные сведения, должны иметь соответствующую пометку: «для служебного пользования». Право присваивать определенным документам такой статус есть у должностных лиц,

уполномоченных на это руководителем федерального органа исполнительной власти. Он же организует порядок:

• передачи сведений, составляющих служебную тайну, другим государственным органам или организациям;

• снятия отметки «для служебного пользования» с документов (информационных носителей и других источников);

• защиты служебной информации от распространения третьим лицам.

В свою очередь, сотрудники госорганов, которые имеют право присваивать сведениям и информации статус служебной тайны, несут ответственность за обоснованность своих действий. То есть для установления пометки «для служебного пользования» должны быть весомые основания. Кроме того, ответственный за защиту служебной тайны ведет обязательный учет документов и своевременно уничтожает документы с конфиденциальными сведениями.

За разглашение служебной тайны для должностных лиц предусмотрена различная ответственность. В первую очередь, Трудовым кодексом установлено право работодателя применить в случае разглашения работником охраняемой тайны дисциплинарное взыскание вплоть до увольнения (п. 6 ст. 81 ТК РФ). В этом случае в трудовой книжке указывается причина увольнения со ссылкой на статью ТК РФ.

В ст. 13.14 КоАП также предусмотрено наказание за разглашение информации с ограниченным доступом:

• для граждан штраф составляет от 500 руб. до 1000 руб.;

• для должностных лиц — от 4000 руб. до 5000 руб.

1. ФЗ “О государственной гражданской службе РФ” от 27.07.2004 г. № 79-ФЗ.

2. ФЗ “О прокуратуре РФ” от 17.01.1992 г. № 2202-1.

3. ФЗ “О банках и банковской деятельности” от 02.12.1990 г. № 395-1.

4. ФЗ “О полиции” от 07.02.2011 г. № 3-ФЗ.

5. ФЗ “Об оперативно-розыскной деятельности” от 12.08.1995 г. № 144-ФЗ.

6. ФЗ “О связи” от 07.07.2003 г. № 126-ФЗ.

7. ФЗ РФ "О коммерческой тайне" от 29.07.2004 г. № 98-ФЗ.

8. Уголовный кодекс РФ от 13.06.1996 г. № 63-ФЗ.

9. Таможенный кодекс Евразийского экономического союза (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза, ратифицирован ФЗ от 14.11.2017 г. № 317-ФЗ).

10. "Правила обращения со сведениями, составляющими служебную тайну в области обороны" утв. ПП РФ от 26.11.2021 г. № 2052.

26. Правовое обеспечение защиты персональных данных.

Под персональными данными (ПД) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ "О персональных данных" от 27.07.2006 г. № 152-ФЗ. По сути, это всевозможные сведения, с помощью которых можно определить (идентифицировать) субъекта персональных данных, что в полной мере согласуется с положениями ст. 2 «Конвенции о защите физических лиц при автоматизированной обработке

персональных данных», принятой Советом Европы 28 января 1981 г. Правовой защите подлежит лишь та информация о человеке, которая позволяет его персонифицировать. Схожее определение персональных данных приводится и в Регламенте Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR) То есть и ФЗ "О персональных данных" и европейский Регламент определяют персональные данные достаточно широко, поэтому какого-либо перечня сведений, относящихся к персональным данным субъекта, не существует.

К инсайдерам относят:

• сотрудников, сознательно работающих на конкурентов (нанятых или предварительно трудоустроенных ими);

• сотрудников, прямо или косвенно связанных с криминальными структурами;

• просто недобросовестных сотрудников, ставящих свои интересы заведомо выше интересов фирмы;

• сотрудников, обиженных на начальство и по этой причине скрытно вредящих, не получая от этого какой-либо выгоды.

Не соответствие правовых норм защиты ПД в российском законодательстве требованиям указанной Конвенции, к которой присоединилась Россия (конвенция ратифицирована ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 г. № 160-ФЗ), тормозило обмен сведениями с европейскими госучреждениями и компаниями, делая невозможными многие коммерчески перспективные проекты.

ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ устранил указанные препятствия, во многом повторив основные положения европейского законодательства в данной сфере.

Конвенция и последовавшие за ней Директивы Евросоюза сформулировали следующие задачи, которые должно регулировать национальное законодательство в отношении ПД:

• защита ПД от НСД к ним со стороны других лиц, в том числе представителей государственных органов и служб, не имеющих на то необходимых полномочий;

• обеспечение сохранности, целостности и достоверности данных в процессе работы с ними, в том числе при передаче по каналам связи;

• обеспечение надлежащего правового режима этих данных при работе с ними для различных категорий ПД;

• обеспечение контроля над использованием ПД со стороны самого гражданина;

• создание специальной независимой структуры, обеспечивающей эффективный контроль за соблюдением прав гражданина на защиту его ПД

(например, создание должности Уполномоченного по защите ПД). Таковым в настоящее время органом является Роскомнадзор.

Для выполнения требований закона, существенно изменилась работа с документами, содержащими ПД.

1. Во всех организациях появился новый, объемный пакет документов. Это документы, связанные с получением согласия физических лиц на обработку их ПД, с регистрацией баз данных в уполномоченном органе, с документированием всех операций с ПД и т.д.

2. Возникла необходимость выделения содержащих ПД документов и информации; их особой маркировки как на бумажных, так и на электронных носителях; ведения отдельного учета и отслеживания доступа к ним.

3. Установлен норматив сроков хранения документов и информации и максимальный срок хранения, который необходимо соблюдать и отслеживать.

4. При работе с ПД необходимо заранее продумать и зафиксировать в нормативных документах все, что связано с их обработкой. В противном случае организация может быть привлечена к ответственности в том числе по искам от самих субъектов персональных данных.

5. Законом вводятся жесткие сроки исполнения всех обращений граждан, связанных с обработкой ПД.

В целях настоящего ФЗ используются следующие основные понятия (ст. 3):

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

1_1) персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

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

3) обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Принципы обработки персональных данных (ст. 5).

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных

данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Выделяется 2 способа обработки ПД:

• с использованием средств автоматизации;

• без использования средств автоматизации.

Под автоматизированным способом обработки ПД законодатель и ведомство понимают совершение любых действий с персональными данными, которые связаны с использованием средств вычислительной техники. Закон не раскрывает термин «средства вычислительной техники» конкретно, но очевидно, что под ними понимаются информационные системы. Для способа обработки персональных данных средствами автоматизации есть одно серьезное ограничение. Ни одно решение, на основании которого могут быть изменены права или обязанности гражданина, не может быть принято только исходя из результатов обработки сведений средствами вычислительной техники.

Ручной (не автоматизированный) способ обработки ПД – это занесение их на материальные носители вручную и дальнейшая работа с такими носителями.

Закон «О персональных данных» называет несколько видов действий, которые могут производиться с поступившими в распоряжение организации персональными данными. Этот перечень ограничен и расширительному толкованию не подлежит. Таким образом, оператор ПД может производить с ними следующие действия:

• сбор – это фактическая передача ПД от их субъекта оператору;

• запись – может происходить и ручным, и машинным способом;

• систематизация – техническое действие, облегчающее обработку ПД для оператора;

• накопление – термин не имеет самостоятельного значения и предполагает хранение информационных массивов на материальных носителях или с использованием средств автоматизации до момента их уничтожения;

• хранение – законодатель устанавливает множество требований к способам физической и технической защиты ПД;

• уточнение – под этим термином могут подразумеваться или обновление, или изменение информации;

• извлечение – здесь предполагается перенос ПД из памяти средств автоматизации на материальные носители;

• использование – действия (операции) с ПД, совершаемые оператором в определенных целях;

• передача – термин рассматривает такие способы предоставления к данным доступа третьим лицам, как распространение, предоставление. Распространение предполагает, что сведения становятся доступными неограниченному кругу лиц, которые могут получить их, зайдя на открытый сайт, купив газету или компакт-диск с информацией. Для предоставления характерно совершение тех же

действий, но в отношении нескольких субъектов, определенных соглашением или иным способом;

• обезличивание – действия, в результате которых невозможно определить принадлежность ПД конкретному субъекту. Обезличивание может происходить только в условиях применения способа обработки данных при помощи средств автоматизации. Если оно используется, выделение данных одного субъекта из массива возможно только при применении специальных средств;

• блокирование – временное прекращение любых действий с ПД. Блокировка производится по заявлению субъекта персональных данных или по требованию регулятора. Если она необходима, обработка сведений возможна только в целях их уточнения;

• удаление – отличается от уничтожения, так как производится в целях коррекции ПД или для решения иных технических задач;

• уничтожение – действия, которые не только уничтожают ПД, обрабатываемые ручным или автоматизированным способом, но и полностью исключают их восстановление. Если данные находились на материальных носителях, вместе с ними уничтожаются и сами носители. Уничтожение происходит по требованию субъекта ПД или по истечении срока их обработки.

27. Международные стандарты и соглашения в области безопасности информационных технологий.

Важным элементом решения проблемы безопасности ИТ является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ в виде международного стандарта. За общими критериями оценки безопасности информационных технологий закрепилось название Общие критерии (ОК).

Главная тенденция, которая прослеживается при анализе современных стандартов в области информационной безопасности, состоит в отказе от жесткой универсальной шкалы классов безопасности и обеспечении гибкости в подходе к оценке безопасности различных типов изделий ИТ.

В начале 80-х годов в США были разработаны "Критерии оценки доверенных компьютерных систем" (TCSEC – Trusted Computer System Evaluation Criteria) – стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации.

В Европе в 1991 г. были разработаны "Критерии оценки безопасности информационных технологий" (ITSEC – Information Technology Security Evaluation Criteria) совместно Францией, Германией, Нидерландами и Великобританией.

В Канаде в начале 1993 г. были созданы "Канадские критерии оценки доверенных компьютерных продуктов" (CTCPEC - Canadian Trusted Computer Product Evaluation Criteria).

В США в это же время был издан проект стандарта "Федеральные критерии безопасности информационных технологий" (FC - Federal Criteria for Information

Technology Security), использовавший другой подход к объединению североамериканской и европейской концепций критериев оценки.

В 1990 г. Международная организация по стандартизации (ISO) начала разработку международного стандарта критериев оценки для общего использования. В результате появился Международный стандарт ISO/IEC 15408-99 "Критерии оценки безопасности информационных технологий" или так называемые "Общие критерии" (ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security).

Появление «Общих критериев» оценки безопасности информационных технологий и соответствующих им международных стандартов явилось новым этапом в развитии нормативной базы оценки информационной безопасности.

Рис. 1. Предыстория «Общих критериев»

Аналогичный национарный стандарт был принят в России ГОСТ Р ИСО/МЭК 15408-1-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (принят постановлением Госстандарта РФ от 4 апреля 2002 г. № 133-ст) (отменен).

Действующим национальным стандартом является ГОСТ Р ИСО/МЭК 15408-1-2012 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст).

Стандарт содержит общие критерии (ОК) оценки безопасности информационных технологий. 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.

В настоящее время действуют также и другие международные и российские стандарты

ISO/IEC 17799 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры обеспечения информационной безопасности» (ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls)

ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий«

ГОСТ Р ИСО/МЭК 19794-2-2005 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки»

В Будапеште 23 ноября 2001 г. подписана Конвенция по борьбе с киберпреступностью. (26 европейских стран, а также Канады, США, ЮАР и Японии)

В конвенции представлена классификация киберпреступлений.

• Противозаконный доступ
• Неправомерный перехват
• Воздействие на данные
• Воздействие на функционирование системы
• Противозаконное использование устройств
• Подлог с использованием компьютерных технологий
• Мошенничество с использованием компьютерных технологий
• Правонарушения, связанные с детской порнографией
• Правонарушения, связанные с нарушением авторского права и смежных прав
• Покушение, соучастие или подстрекательство к совершению преступления

28. Особенности и классификация компьютерных преступлений.

Проблема: при расследовании многих преступлений в компьютерных системах заключается в установлении самого факта совершения преступления.

Особенность: чтобы утверждать, что было совершено преступление с использованием компьютера, необходимо доказать следующие факты:

• компьютерная информация, к которой произведен несанкционированный доступ, охраняется законами РФ;

• злоумышленником были осуществлены определенные неправомерные действия;

• этими несанкционированными действиями нарушены права собственника информации;

• несанкционированный доступ к средствам компьютерной техники либо попытка доступа;

• использование информации в преступных целях. Например, с целью совершения преступления. Тогда доказыванию подлежит:

• совершение несанкционированных манипуляций с программным обеспечением (ПО), что лицо совершало их с преступной целью.

Комплекс следственных действий включает:

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого и изъятие физических носителей информации и других документов.

2. Исследование журнала рабочего времени ЭВМ, средств защиты и контроля регистрирующих систем пользователей, всего ПО ЭВМ, "прошитых" микросхем ПЗУ, микропроцессоров и т.п.

3. Анализ указаний по обработке ежедневной бухгалтерской информации.

4. Допрос инженеров, программистов и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.

5. Проведение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением соответствующих специалистов правоохранительных органов.

Судебно-бухгалтерская экспертиза устанавливает нарушения в документообороте, их причины и ответственные лица за эти нарушения.

Результаты программно-технической экспертизы играют роль доказательств в процессе суда.

С помощью таких экспертиз решаются 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.

Классификация способов совершения КП

По кодификатору Интерпола с 1991 г. все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q.

QA - Несанкционированный доступ и перехват

QD - Изменение компьютерных данных

QF - Компьютерное мошенничество

QR - Незаконное копирование

QS - Компьютерный саботаж

QZ - Прочие компьютерные преступления

В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время используется в более чем 100 странах.

Для характеристики преступления могут использоваться до пяти кодов. Например, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды КП:

QAH – "Компьютерный абордаж" (хакинг – hacking): неправомерный доступ в компьютер или сеть.

QAI – перехват (interception): перехват при помощи технических средств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду КП также относится электромагнитный перехват (electromagnetic pickup).

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

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

• "Жучок" (bugging) – установка микрофона в компьютере;

• "Откачивание данных" (data leakage) – возможность сбора информации, для получения данных, о технологии ее прохождения в системе;

• "Уборка мусора" (scavening) – поиск данных, оставленных пользователем после работы на компьютере (в мусорных корзинах, в памяти машины);

• метод следования "За дураком" (piggybackig), характеризующий несанкционированное проникновение как в закрытые зоны. Его суть: дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

• метод "За хвост" (between the lines entry). Подключаются к линии связи законного пользователя, когда последний заканчивает активный режим, и осуществляют доступ к системе;

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.

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

Для предупреждения преступлений используются региональные и международные средства анализа. Эти системы могут объединять преступления по местоположению, времени и методу действий, что может помочь прогнозировать потенциальные будущие угрозы.

Например, в университете Карнеги-Меллона создана Компьютерная группа реагирования на чрезвычайные ситуации Computer Emergency Response Team

(CERT), которая ставит своей целью анализ и разработку мер противодействия компьютерным преступлениям.

Проделанная этой группой работа показывает, что понимание целей, которые ставит перед собой злоумышленник, позволяет определять его будущие поступки.

Для выявления нарушений системной защиты используются методы активной добычи данных.

При этом проводят анализ поступков, которые приводят к нарушениям, и сравнивают их с поведением при нормальной работе.

Собирается информация о часто встречающейся последовательности действий.

Эти сведения используются для создания автоматического классификатора, который способен различать агрессивное и нормальное поведение.

29. Требования к безопасности компьютерных сетей в РФ.

Эти требования были разработаны бывшей ГТК РФ и обязательны для государственных предприятий или для коммерческих предприятий, допущенных к сведениям составляющих ГТ. В остальных случаях они носят рекомендательный характер.

Например, РД ГТК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.) устанавливает классификацию АС, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

• наличие в АС информации различного уровня конфиденциальности;

• уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

• режим обработки данных в АС – коллективный или индивидуальный.

Требования к безопасности АС устанавливаются в соответствии с классом защищенности. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Т.е. установлено 9 классов защищенности в трех группах:

3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А.

3-я группа - в АС работает 1 пользователь, допущенный к информации одного уровня конфиденциальности;

2-я группа – в АС пользователи имеют одинаковые права к информации различного уровня конфиденциальности;

1-я группа – многопользовательские системы с доступом к информации разного уровня.

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»

1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»

1 А - в случае обработки секретной информации с грифом «особая важность»

1 Г - АС, в которых циркулирует служебная тайна

1 Д - АС, в которых циркулируют персональные данные

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;

• обеспечения целостности.

Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Применение в комплекте СВТ средств криптографической защиты информации может быть использовано для повышения гарантий качества защиты.

Для присвоения класса защищенности АС должна иметь:

• руководство администратора по системе;

• руководство пользователя;

• тестовую и конструкторскую документацию.

«Политика безопасности» обеспечивает выполнение следующих правил безопасности информации:

• идентификация;

• разделение полномочий;

• регистрация и учет работы;

• шифрование;

• применение цифровой подписи;

• обеспечение антивирусной защитой;

• контроль целостности информации.

При этом обеспечивается выполнение трех основных функций системы:

• доступность;

• целостность;

• конфиденциальность.

Политика безопасности имеет два-три уровня

Верхний уровень политики безопасности определяет политику организации в целом.

На указанном уровне формулируются главные цели информационной безопасности (определяемые сферой деятельности предприятия): обеспечение конфиденциальности, целостности и доступности.

Средний уровень политики безопасности выделяют в случае структурной сложности организации или наличии специфичные подсистемы организации.

Например, наличие подразделений обрабатывающих секретную информацию.

Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации.

На нижнем уровне описываются механизмы защиты информации и программно-технические средства для их реализации.

За политику безопасности нижнего уровня отвечают системные администраторы (администраторы безопасности).

30. Объекты интеллектуальной собственности.

П. 1 ст. 44 Конституции РФ устанавливает гарантии свободы творчества и охраны интеллектуальной собственности:

1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

Термин интеллектуальная собственность в широком понимании означает закрепленное законом временное исключительное право, а также личные неимущественные права авторов на результат интеллектуальной деятельности или средства индивидуализации.

Законодательство, определяющее права на интеллектуальную собственность, устанавливает монополию авторов на определенные формы использования результатов своей интеллектуальной, творческой деятельности, которые, таким образом, могут использоваться другими лицами лишь с разрешения первых.

В ст. 1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» дается определение результатов интеллектуальной деятельности.

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

1) произведения науки, литературы и искусства;

2) программы для электронных вычислительных машин (программы для ЭВМ);

3) базы данных;

4) исполнения;

5) фонограммы;

6) сообщение в эфир или по кабелю, радио- или телепередач (вещание организаций эфирного или кабельного вещания);

7) изобретения;

8) полезные модели;

9) промышленные образцы;

10) селекционные достижения;

11) топологии интегральных микросхем;

12) секреты производства (ноу-хау);

13) фирменные наименования;

14) товарные знаки и знаки обслуживания;

14.1) географические указания;

15) наименования мест происхождения товаров;

16) коммерческие обозначения.

2. Интеллектуальная собственность охраняется законом.

Ст. 1226 ГК РФ Интеллектуальные права

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 объектов интеллектуальной собственности (ОИС):

• авторское право;

• патентное право;

• 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 сведений (производственных, технических, экономических, организационных и других).

31. Правовая охрана авторских и смежных прав.

Правовая охрана авторских и смежных прав регулируется Разделом VII. Права на результаты интеллектуальной деятельности и средства индивидуализации Части 4 ГК РФ.

Статья 1226 ГК РФ. Интеллектуальные права

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).

Авторские права регулируются Главой 70. Авторское право Части 4 ГК РФ.

Статья 1255 ГК РФ. Авторские права

1. Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами.

2. Автору произведения принадлежат следующие права:

1) исключительное право на произведение;

2) право авторства;

3) право автора на имя;

4) право на неприкосновенность произведения;

5) право на обнародование произведения.

3. В случаях, предусмотренных настоящим Кодексом, автору произведения наряду с правами, указанными в п. 2 настоящей статьи, принадлежат другие права, в том числе право на вознаграждение за служебное произведение, право на отзыв, право следования, право доступа к произведениям изобразительного искусства.

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 ст. 1262 Гражданского 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 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.).

Для включения механизма защиты смежных прав необходимо заявление обладателя прав о нарушении его прав (т.к. многие фирмы этого не делали, то до недавнего времени около 90% пиратской продукции на рынке считалось законной).

Обладатели исключительных или смежных прав вправе требовать от нарушителя: признания своих прав, возмещения убытков, взыскание полученного дохода, выплаты компенсации в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда.

32. Правовая охрана программ для ЭВМ и баз данных.

Впервые программы для ЭВМ и базы данных стали объектами авторского права в 1991 г., когда были приняты Основы гражданского законодательства СССР и союзных республик.

Закон “О правовой охране программ для ЭВМ и баз данных” от 23.09.1992 г. № 3523 регулировал до 2008 г. отношения, связанные с созданием, правовой охраной и использованием программ ЭВМ и баз данных.

Программы для ЭВМ и базы данных были отнесены Законом к объектам авторского права.

Статья 1261 ГК РФ. Программы для ЭВМ

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы или базы данных, использовать знак охраны авторского права, состоящий из трех элементов:

• буквы С в окружности или в круглых скобках ©;

• наименования (имени) правообладателя;

• года первого выпуска программы в свет.

Авторские права на все виды программ для ЭВМ охраняются так же, как авторские права на произведения литературы.

Личные права автора на программу или базу данных охраняются бессрочно.

33. Технические средства защиты авторских прав.

Статья 1299 ГК РФ. Технические средства защиты авторских прав

1. 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.

2. В отношении произведений не допускается:

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

2) 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.

3. В случае нарушения положений, предусмотренных пунктом 2 настоящей статьи, автор или иной правообладатель вправе требовать по своему выбору от нарушителя возмещения убытков или выплаты компенсации в соответствии со статьей 1301 настоящего Кодекса.

4. В случае, если пунктами 1-3 статьи 1274 и статьей 1278 настоящего Кодекса разрешено использование произведения без согласия автора или иного правообладателя и такое использование невозможно осуществить в силу наличия технических средств защиты авторских прав, лицо, правомерно претендующее на осуществление такого использования, может требовать от автора или иного правообладателя снять ограничения использования произведения, установленные путем применения технических средств защиты авторских прав, либо предоставить возможность такого использования по выбору правообладателя при условии, что это технически возможно и не требует существенных затрат.

34. Охрана топологии интегральных микросхем.

Статья 1448 ГК РФ. Топология интегральной микросхемы

1. Топологией интегральной микросхемы является зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними. При этом интегральной микросхемой является микроэлектронное изделие окончательной или промежуточной формы, которое предназначено для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено такое изделие.

2. Правовая охрана, предоставляемая настоящим Кодексом, распространяется только на оригинальную топологию интегральной микросхемы, созданную в результате творческой деятельности автора и неизвестную автору и (или) специалистам в области разработки топологий интегральных микросхем на дату ее создания. Топология интегральной микросхемы признается оригинальной, пока не доказано обратное.

Топологии интегральной микросхемы, состоящей из элементов, которые известны специалистам в области разработки топологий интегральных микросхем на дату ее создания, предоставляется правовая охрана, если пространственно-

геометрическое расположение совокупности таких элементов и связей между ними в целом отвечает требованию оригинальности.

3. Правовая охрана, предоставляемая настоящим Кодексом, не распространяется на идеи, способы, системы, технологию или закодированную информацию, которые могут быть воплощены в топологии интегральной микросхемы.

Статья 1449 ГК РФ. Права на топологию интегральной микросхемы

1. Автору топологии интегральной микросхемы, отвечающей условиям предоставления правовой охраны, предусмотренным настоящим Кодексом (топологии), принадлежат следующие интеллектуальные права:

1) исключительное право;

2) право авторства.

2. В случаях, предусмотренных настоящим Кодексом, автору топологии интегральной микросхемы принадлежат также другие права, в том числе право на вознаграждение за служебную топологию.

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

Исключительное право на использование топологии действует в течении 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.

35. Охрана патентных прав.

Изобретение – техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств), в том числе к применению продукта или способа по определенному назначению. Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо (ст. 1350 ГК РФ).

Полезная модель – техническое решение, относящееся к устройству. Полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой (ст. 1351 ГК РФ).

Промышленный образец – решение внешнего вида изделия промышленного или кустарно-ремесленного производства. Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным. (ст. 1352 ГК РФ).

Уровень техники для изобретения включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

При установлении новизны изобретения в уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патентов на изобретения, полезные модели и промышленные образцы, с документами которых вправе ознакомиться любое лицо в соответствии с пунктами 2 и 4 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения, полезные модели и промышленные образцы.

Не являются изобретениями, в частности:

1) открытия;

2) научные теории и математические методы;

3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;

4) правила и методы игр, интеллектуальной или хозяйственной деятельности;

5) программы для ЭВМ;

6) решения, заключающиеся только в представлении информации.

В соответствии с настоящим пунктом исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

6. Не предоставляется правовая охрана в качестве изобретения:

1) сортам растений, породам животных и биологическим способам их получения, то есть способам, полностью состоящим из скрещивания и отбора, за исключением микробиологических способов и полученных такими способами продуктов;

2) топологиям интегральных микросхем.

Срок действия исключительного права на изобретение, полезную модель, промышленный образец и удостоверяющего это право патента исчисляется со дня подачи заявки на выдачу патента и составляет:

• двадцать лет - для изобретений;

• десять лет - для полезных моделей;

• пятнадцать лет - для промышленных образцов.

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Право на получение патента, созданного работником в связи с выполнением им своих служебных обязанностей или полученным от работодателя заданием, принадлежит работодателю.

При этом автор имеет право на вознаграждение, соразмерное выгоде, которая получена работодателем или могла бы быть им получена.

Вознаграждение выплачивается в размере и на условиях, определяемых на основе соглашения между ними.

Патентообладателю принадлежит исключительное право на использование охраняемых патентом изобретения, полезной модели или промышленного образца по своему усмотрению.

Нарушением исключительного права патентообладателя признается несанкционированное изготовление, применение, ввоз, предложение к продаже,

продажа, иное введение в хозяйственный оборот продукта, содержащего запатентованное изобретение.

Правительство РФ имеет право в интересах обороны и безопасности разрешить использование изобретения, полезной модели или промышленного образца без согласия патентообладателя с уведомлением его об этом в кратчайший срок и с выплатой ему соразмерной компенсации.

На изобретения, содержащие сведения, составляющие ГТ распространяются положения раздела «Особенности правовой охраны и использования секретных изобретений» настоящего Кодекса.

Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана не предоставляется.

В качестве полезной модели охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой.

В качестве промышленного образца охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным.

Заявка на изобретение должна содержать:

1) заявление о выдаче патента с указанием автора изобретения и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;

2) описание изобретения, раскрывающее его с полнотой, достаточной для осуществления изобретения специалистом в данной области техники;

3) формулу изобретения, выражающую его сущность и полностью основанную на его описании;

4) чертежи и иные материалы, если они необходимы для понимания сущности изобретения;

5) реферат.

Заявка на полезную модель должна содержать:

1) заявление о выдаче патента с указанием автора полезной модели и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;

2) описание полезной модели, раскрывающее ее с полнотой, достаточной для осуществления полезной модели специалистом в данной области техники;

3) формулу полезной модели, выражающую ее сущность и полностью основанную на ее описании;

4) чертежи, если они необходимы для понимания сущности полезной модели;

5) реферат.

Заявка на промышленный образец должна содержать:

1) заявление о выдаче патента с указанием автора промышленного образца и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;

2) комплект изображений изделия, дающих полное детальное представление о внешнем виде изделия;

3) чертеж общего вида изделия, эргономическую схему, конфекционную карту (карту изготовления), если они необходимы для раскрытия сущности промышленного образца;

4) описание промышленного образца;

5) перечень существенных признаков промышленного образца.

Экспертиза заявки на изобретение по существу включает:

• информационный поиск в отношении заявленного изобретения для определения уровня техники, по сравнению с которым будет осуществляться оценка новизны и изобретательского уровня изобретения;

• проверку соответствия заявленного изобретения условиям патентоспособности.

По истечении шести месяцев со дня начала экспертизы федеральный орган исполнительной власти по интеллектуальной собственности направляет заявителю отчет об информационном поиске.

На основании решения о выдаче патента на изобретение, полезную модель или промышленный образец федеральный орган вносит изобретение, полезную модель или промышленный образец в соответствующий государственный реестр:

• Государственный реестр изобретений РФ,

• Государственный реестр полезных моделей РФ,

• Государственный реестр промышленных образцов РФ

• и выдает патент на изобретение, полезную модель или промышленный образец.