МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ
(РГГМУ)

П.Ю. Богданов, Н.В. Яготинцева

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные системы, геоинформационные системы

ООО «Андреевский издательский дом»
Санкт-Петербург, 2015

УДК681.3.06:800.92

Богданов П.Ю., Яготинцева Н.В.

Организационно-правовое обеспечение информационной безопасности: Учебное пособие. СПБ.: ООО «Андреевский издательский дом», 2015 г. - 169 стр.

Учебное пособие предназначено для студентов специальности 10.05.02 информационная безопасность телекоммуникационных систем. В настоящем учебном пособии собран материал, необходимый для самостоятельно освоения тем учебного курса «Организационно-правовое обеспечение информационной безопасности», связанных с нормативно-правовыми аспектами деятельности по защите информации.

Изложенный материал снабжен ссылками на используемые источники и нормативно-правовые акты.

Богданов П.Ю., Яготинцева Н.В.
Организационно-правовое обеспечение информационной безопасности:
Учебное пособие
Редактор: Новожилова Е.С.
Верстка: Истомин Д.Е.
ООО «Андреевский издательский дом»
197738, Санкт-Петербург, пос. Репино, Приморское шоссе, д. 394
E-mail: biom@nm.ru
Подписано в печать: 10.11.2015 г.
Печатных листов: 6,57. Тираж: 200 экз.
Отпечатано с готовых диапозитивов в ООО «Андреевский издательский дом»

ВВЕДЕНИЕ

Основная цель данного учебного пособия – изложение учебного материала, необходимого для освоения следующих тем курса «Организационно-правовое обеспечение информации»:

— Структура органов государственной власти РФ

— Классификация защищаемой законом информации.

— Нормативно-правовое обеспечение защиты информации.

— Регуляторы в области защиты информации.

— Ответственность за нарушения законодательства РФ в сфере ИТ.

В настоящее время появилось много книг, посвященных рассматриваемой тематике. В ряде работ Парошина А.А., Загинайлова Ю.Н., Казанцева С.Я., Терехова А.В., Бурцевой Е.В., Родичева Ю.А., Кулишкина В.А. и других авторов достаточно точно, конкретно и правильно представлены понятия, определения и положения в области организационно-правового обеспечения информационной безопасности. Многие из них использованы в учебном пособии.

В пособии представлены ссылки на некоторые законодательные акты, которые могут использоваться студентами в качестве правовой базы обеспечения информационной безопасности. Ссылки на нормативно—правовые и методические документы приводятся по состоянию на 22.06.2015

ТЕМА 1. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Под информационной безопасностью объектов понимается состояние защищенности интересов их собственников в информационной сфере, обеспечивающей защиту информации от разглашения, утечки и несанкционированного доступа к ней, а также безопасность информационных и телекоммуникационных систем.

В этих целях необходимо:

— повысить безопасность информационных систем, включая сети связи;

— развивать аппаратные и программные средства защиты информации и методы контроля за их эффективностью;

— обеспечить защиту конфиденциальных сведений и сведений, составляющих государственную тайну;

9 сентября 2000 года Президентом РФ утверждена Доктрина информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и направления обеспечения информационной безопасности, основными из которых являются:

— предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

— исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

— предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств её обработки, хранения и передачи;

— предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

— выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения её целостности, доступности и конфиденциальности.

Целостность информации заключается в её существовании в неискаженном виде, неизменном по отношению к некоторому её исходному состоянию.

Доступность информации – это свойство, характеризующее её способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность информации – это свойство, указывающее на необходимость введения ограничения на доступ к ней определенного круга пользователей.

Все известные меры защиты информации можно разделить на следующие виды:

— правовые - включают в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов, а также надзор и контроль за их исполнением;

— технические заключаются в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

— криптографические - защита данных при помощи криптографического преобразования, т.е. при помощи шифрования и (или) выработки имитовставки;

— организационные — предусматривают установление режимных, временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режим работы объекта информатизации;

— физические — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

1.1 Информация как объект права

Информация может быть как в материальном, так и не в материальном виде. Поэтому без определения границ сферы информации как объекта права применение любых законодательных норм по отношению к ней весьма проблематично.

Федеральный закон «Об информации, информационных технологиях и о защите информации», направленный на регулирование взаимоотношений в информационной сфере, раскрывает понятие информации: «Информация – сведения (сообщения, данные) независимо от формы их представления».

Этим законом определено, что информация является объектом отношений физических, юридических лиц и государства, подлежит обязательному учету и защите, как всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно, в пределах своей компетенции, устанавливать режим защиты информации и доступа к ним. Физические и юридические лица являются собственниками тех документов,

массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

Информация в зависимости от порядка её предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В зависимости от категории доступа, информация подразделяется на общедоступную информацию и информацию ограниченного доступа (государственная тайна и конфиденциальная информация) (рис 1.1).

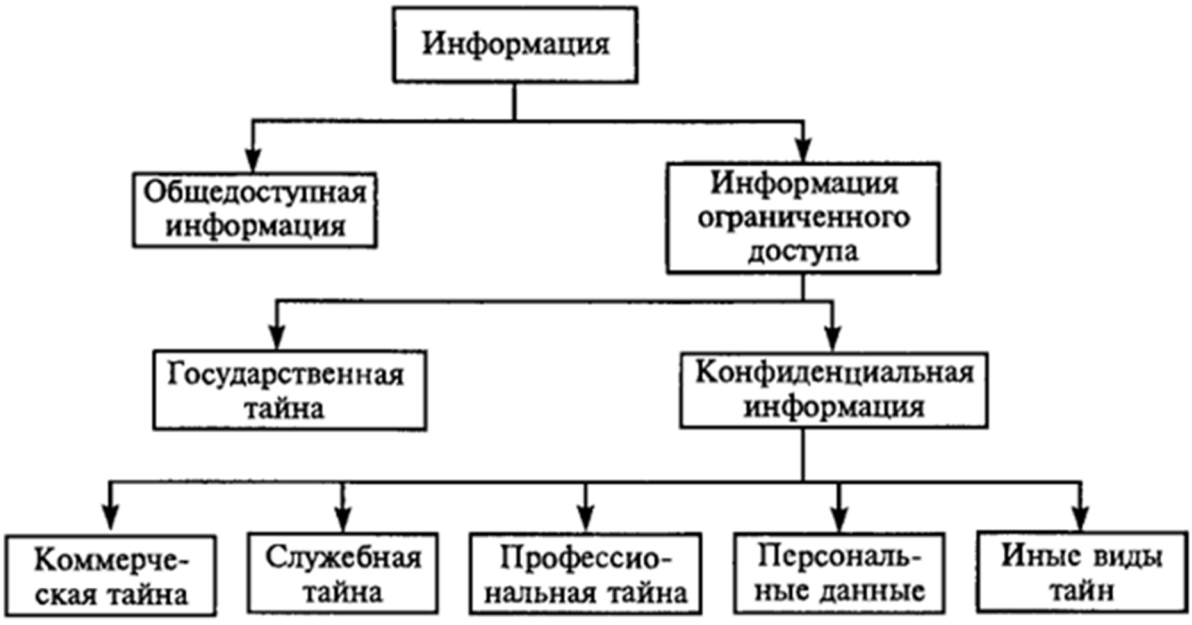

Рис. 1.1 Классификация информации по категориям доступа

Указом Президента Российской Федерации № 188 от 6 марта 1997 года утвержден перечень сведений конфиденциального характера. В него входят:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные

данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.

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

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

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

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

Ограничение доступа к информации возможно только в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства и устанавливается Федеральными законами. В Приложении 1 дана классификация информации ограниченного доступа с указанием правовой основы ограничения доступа.

Федеральный закон «Об информации, информационных технологиях и о защите информации» в ст. 8 ч. 4 определяет перечень сведений, доступ к которым не может быть ограничен:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

1.2 Основные правовые аспекты защиты информации.

Информация, являясь продуктом деятельности, выступает как собственность государства, предприятий, учреждений, организаций, граждан, и, как объект собственности, требует защищенности. Однако проблема защиты информации, не сводится только к защите прав ее собственников, но и содержит в себе такой важный аспект как защита прав граждан на свободный доступ к сведениям, гарантированный конституцией. Основы защиты информации разрабатываются органами государственной власти исходя из условий обеспечения информационной безопасности в частности и национальной безопасности России в целом.

Важнейшим гарантом прав и свобод граждан является Конституция Российской Федерации. В ней есть несколько статей, имеющих отношение к данному вопросу.

Статья 2. Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства.

Статья 15

1. Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации.

Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.

2. Органы государственной власти, органы местного самоуправления, должностные лица, граждане и их объединения обязаны соблюдать Конституцию Российской Федерации и законы.

3. Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

4. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

Положения Конституции нашли подкрепление и развитие в других законодательных актах.

Основой законодательства в сфере информационных правоотношений является Федеральный закон «Об информации, информационных технологиях и о защите информации». Он содержит массу ссылок на другие законы и отрасли права, в которых конкретизированы его положения. Закон регулирует отношения, возникающие:

— при осуществлении права на получение, поиск, передачу, производство и распространение информации;

— применении информационных технологий;

— обеспечении защиты информации.

Указанный закон не затрагивает отношений, регулируемых законодательством об интеллектуальной собственности, устанавливает права и обязанности субъектов информационных отношений, определяет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

С вопросами обеспечения информационной безопасности тесно увязаны вопросы правового регулирования информационных технологий, которые можно разделить по сферам деятельности:

1) Обеспечение связи и коммуникаций;

2) Использование криптографических средств, в т.ч. шифрования и ЭЦП;

3) Лицензирование, сертификация и аттестация объектов и средств защиты информации.

Все информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации. Информационные системы органов государственной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности.

Любая правовая норма, устанавливающая ограничения на какие-либо действия, должна содержать санкцию, предусматривающую юридическую ответственность за её нарушение. Так как наиболее действенным средством предупреждения преступлений является возможность привлечения к уголовной ответственности, обратимся к Уголовному кодексу.

Статья 137. Нарушение неприкосновенности частной жизни. Данная статья запрещает незаконный сбор 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.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, влечет за собой более суровое наказание. Также определен размер ответственности за незаконное производство, сбыт и приобретение специальных технических средств для негласного получения информации.

Статья 139. Нарушение неприкосновенности жилища. Согласно данной статье запрещается незаконное проникновение в жилище, совершенное против воли проживающего в нём лица. То же деяние, совершенное с применением насилия или с угрозой его применения, влечет более суровое наказание.

Статья 140. Отказ в предоставлении гражданину информации. Данная статья устанавливает ответственность за неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.

Статья 146. Нарушение авторских и смежных прав. Вводит ответственность за присвоение авторства (плагиат) и незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта.

Статья 147. Нарушение изобретательских и патентных прав. Данная статья вводит ответственность за незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству.

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Незаконное разглашение или использование таких сведений наказывается более сурово, чем незаконный сбор.

В связи с бурным развитием информационных технологий и их широким внедрением в деятельность различных предприятий, учреждений и организаций, возникновением такого нового вида преступлений как компьютерные преступления, появилась необходимость правового регулирования вопросов защиты компьютерной информации. Глава 28 УК РФ содержит три статьи,

определяющие меру ответственности за преступления в сфере компьютерной информации.

Таким образом, мы видим, что информационные отношения получили и уголовно-правовую защиту. Из этого следует, что безопасность информации стала новым объектом преступления, а информация вообще и охраняемая законом в частности – предметом преступления.

1.3. Преступления в сфере компьютерной информации

Под компьютерным преступлением следует понимать предусмотренное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного её собственником или государством порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба владельцу информации или автоматизированной системы, в которой эта информация генерируется (создаётся), обрабатывается, передаётся или уничтожается, или повлекло иные тяжкие последствия.

Компьютерные преступления имеют свои отличительные особенности:

— высокая скрытность, сложность сбора улик по установленным фактам;

— сложность доказательства в суде подобных дел;

— «интернациональность» компьютерных преступлений;

— высокий ущерб даже от единичного преступления;

— вполне определенный контингент лиц, совершающих правонарушения в сфере компьютерной информации: это, как правило, высококвалифицированные программисты, специалисты в области телекоммуникационных систем, системные и банковские программисты и т.д.

Специалисты выделяют четыре основные группы правонарушителей в данной сфере:

1) Пользователи информационных систем, занимающиеся поиском незаконных способов получения доступа к защищенным данным (хакеры). Они представляют собой многочисленную группу, включающую обычно программистов, имеющих фанатичное стремление преодолеть защиту какой-либо системы.

2) Преступники, преследующие цели обогащения путем непосредственного внедрения в финансовые системы для получения коммерческой и другой информации для организации действий уголовного характера. Она формируется в основном из тех хакеров, которые пришли к выводу о возможности заработать на своём «хобби».

3) Террористы и другие экстремистские группы, использующие внедрение в информационные системы для совершения устрашающих действий, шантажа и в других целях.

4) Различные коммерческие организации и структуры, стремящиеся вести промышленный шпионаж и борьбу с конкурентами путем добычи или искажения конфиденциальной финансовой, технологической, проектной, рекламной и другой информации. Рыночные отношения стимулируют совершенствование методов скрытого проникновения в файлы данных конкурирующих фирм.

Составы компьютерных преступлений приведены в 28 главе УК РФ.

Статья 272. Неправомерный доступ к компьютерной информации. Предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

Преступное деяние должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы

защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Неправомерным признается доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление либо относится к ним безразлично. Статья 272 УК не регулирует ситуацию, когда неправомерный доступ осуществляется в результате неосторожных действий, что, в принципе, отсекает огромный пласт возможных посягательств и даже те действия, которые действительно совершались умышленно, т.к., при расследовании обстоятельств доступа будет крайне трудно доказать умысел компьютерного преступника.

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

Статья предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами.

Под вредоносными программами в смысле ст. 273 УК РФ понимаются программы, специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу.

Наиболее распространенными видами вредоносных программ являются широко известные компьютерные вирусы и логические бомбы.

Для привлечения к ответственности по 273 ст. необязательно наступление каких-либо отрицательных последствий для владельца информации, достаточен сам факт создания программ или внесение изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье. Наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию.

Статья 274. Статья устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для Интернет, ее действие распространяется только на локальные сети организаций.

1.4 Компетенция органов государственной власти в области информационной безопасности.

Система обеспечения информационной безопасности Российской Федерации является частью системы безопасности страны. Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и

судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

В таблице 1.1 указаны основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Таблица 1.1 Основные элементы организационной основы системы обеспечения ИБ РФ

Орган государственной власти	Компетенция в области ИБ
Президент РФ	В пределах своих конституционных полномочий и в соответствии с законодательством руководит органами и силами по обеспечению ИБ РФ; санкционирует действия по обеспечению ИБ РФ; формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению ИБ РФ, определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения ИБ РФ, а также меры по реализации Доктрины ИБ
Палаты Федерального Собрания РФ	На основе Конституции по представлению Президента и Правительства формируют законодательную базу в области обеспечения ИБ РФ
Правительство РФ	В пределах своих полномочии и с учетом сформулированных в ежегодных посланиях Президента Федеральному Собранию приоритетных направлений в области обеспечения ИБ РФ координирует деятельность федеральных органов исполнительной власти, а также

	предусматривает выделение средств, необходимых для реализации федеральных программ в области ИБ РФ
Совет Безопасности РФ	Проводит работу по выявлению и оценке угроз ИБ РФ, оперативно подготавливает проекты решений Президента по предотвращению таких угроз, разрабатывает предложения в области обеспечения ИБ РФ, а также предложения по уточнению отдельных положений Доктрины ИБ, координирует деятельность органов и сил по обеспечению ИБ РФ, контролирует реализацию федеральными органами исполнительной власти решений Президента в области ИБ РФ.
Федеральные органы исполнительной власти	Обеспечивают исполнение законодательства, решений Президента и Правительства в области обеспечения ИБ РФ; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и предоставляют их в установленном порядке Президенту и в Правительство
Межведомственные и государственные комиссии	Решают в соответствии с предоставленными им полномочиями задачи обеспечения ИБ РФ
Органы исполнительной власти субъектов РФ	Взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства, решений Президента и Правительства в области обеспечения ИБ РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения ИБ РФ; вносят в федеральные органы исполнительной власти

	предложения по совершенствованию системы обеспечения ИБ РФ
Органы местного самоуправления	Обеспечивают соблюдение законодательства в области обеспечения ИБ РФ
Органы судебной власти	Осуществляют правосудие по делам о преступления, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению ИБ РФ

Нормативно-правовые документы

Конституция Российской Федерации

Уголовный Кодекс Российской Федерации

ФЗ от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»

ФЗ «Об электронной цифровой подписи»

Указ Президента РФ №188 от 6 марта 1997 г. "Об утверждении перечня сведений конфиденциального характера"

Вопросы для самоконтроля

1. Что понимается под "информационной безопасностью", каково ее место в системе национальной безопасности РФ?
2. Раскройте понятия информация, целостность, конфиденциальность и доступность информации.
3. Важнейшие задачи в области информационной безопасности?
4. Приведите классификацию информации в зависимости от порядка её представления или распространения.
5. Приведите классификацию информации в зависимости от категории доступа.

6. Перечислите сведения конфиденциального характера утвержденные Указом Президента РФ №188.

7. Перечислите сведения, доступ к которым не может быть ограничен.

8. Перечислите меры защиты информации.

9. Какие нормативные правовые акты составляют Законодательство в области защиты информации?

10. Какие отношения регулирует ФЗ "Об информации, информационных технологиях и о защите информации"

11. Перечислите компьютерные преступления указанные в 28 главе УК РФ.

12. Основные группы правонарушителей в компьютерной сфере.

13. Какие ведомства регулируют правовые отношения в области защиты информации?

ТЕМА 2 ПРАВОВОЙ РЕЖИМ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ.

В современном мире информация является одним из наиболее ценных продуктов человеческой жизнедеятельности, а информационные ресурсы и технологии, которыми обладает государство, определяют его стратегический потенциал и влияние в мире. Важным элементом информационных ресурсов является государственная тайна, отнесенная по условиям правового режима к документированной информации ограниченного распространения.

Сведения, составляющие государственную тайну, имеют особую важность для общества и государства. Поскольку информация, с одной стороны – объект отношений людей, а с другой стороны – ресурс управления и принятия решений. Из-за величины возможного ущерба от её разглашения государственная тайна занимает приоритетное место в системе социального института тайн.

2.1 Законодательство РФ о государственной тайне и основные понятия, используемые в нем.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законах Российской Федерации «О безопасности» и «О государственной тайне», а также положениях других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны. Кроме того, правоотношения в этой области регулируют нормативные акты, издаваемые Президентом РФ и Правительством, Федеральной службой технической и экспертной комиссии.

Основные понятия, используемые в законодательстве.

Государственная тайна — защищаемые государством сведения в области его военной, внешне политической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ;

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

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

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

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

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

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

Перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Правовой институт государственной тайны имеет три составляющие:

1) Сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);

2) Режим секретности (конфиденциальности) – механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты;

3) Санкции за неправомерное получение и (или) распространение этих сведений.

2.2 Сведения, относимые к государственной тайне. Засекречивание сведений и их носителей.

Отнесение сведений к государственной тайне — прерогатива высших органов государственной власти. Какие сведения могут быть отнесены к государственной тайне, определено в Законе "О государственной тайне", ст.5. Он описывает довольно широкие группы сведений, объединенных одним или несколькими признаками в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью. К таким группам относятся:

1) Сведения в военной области;
2) Сведения в области экономики, науки и техники;
3) Сведения в области внешней политики и экономики;
4) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму;

Однако при засекречивании сведений учреждения, организации, предприятия, органы государственной власти обязаны руководствоваться перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента РФ №1203 от 30.10.95г. Данный перечень содержит достаточно большой объем сведений (118 наименований на 2015 год), структурированных по областям деятельности. В Указе определены конкретные органы государственной власти, наделенные полномочиями по распоряжению соответствующими сведениями.

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

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 закона «О государственной тайне» и законодательству Российской Федерации о государственной тайне.

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

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

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

— о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

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

— о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

— о фактах нарушения прав и свобод человека и гражданина;

— о размерах золотого запаса и государственных валютных резервах Российской Федерации;

— о состоянии здоровья высших должностных лиц Российской Федерации;

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

Важным признаком государственной тайны является степень секретности сведений, отнесенных к ней. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений. Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные. Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается. Эти грифы проставляются на документах или изделиях (их упаковках или сопроводительных документах).

Какие критерии используются для отнесения сведений к той или иной степени секретности? Ответ на этот вопрос дает постановление Правительства РФ от 4 сентября 1995 №870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности»

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

К совершенно секретным сведениям следует относить сведения в областях военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической,

экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной области деятельности.

Из этих определений видно высокую степень неопределенности признаков, характеризующих ту или иную степень секретности сведений, составляющих государственную тайну. Эти качественные признаки – критерии степени секретности сведений, содержащих государственную тайну, всегда оставляют место для субъективного фактора в процессе засекречивания информации.

Тенденция увеличения степени открытости государства перед обществом диктует необходимость максимально возможного сокращения числа сведений, относимых к государственной тайне, открытости общего перечня относимых к ней категорий сведений, механизмов засекречивания и условий рассекречивания. Обязанность государства – взять на себя формирование взвешенного механизма защиты различных видов информации и установления рамок действия институтов тайн. Такие требования исходят, с одной стороны, из потребности современного общества быть более открытым и доступным, а с другой – диктуются необходимостью обеспечения безопасности личности, общества и государства.

При засекречивании сведений, относимых к государственной тайне, их носителям присваивается соответствующий гриф секретности и наносятся реквизиты:

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

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

— о регистрационном номере;

— о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

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

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

В связи с засекречиванием информации могут наступить ограничения прав собственности предприятий, учреждений, организаций и граждан РФ. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжении которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по её нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну, в соответствии с законодательством. Закон "О государственной тайне" не лишает собственника его собственности, а лишь временно ограничивает его право распоряжаться ею. Распоряжение сведениями, составляющими государственную тайну, как то: передача или взаимная передача, осуществляется в соответствии со ст. 16-18 Закона "О государственной тайне". Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством РФ в каждом отдельном случае при наличии экспертного заключения Межведомственной комиссии по защите государственной тайны о такой возможности.

2.3 Рассекречивание сведений и их носителей

Рассекречивание сведений и их носителей – снятие ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основанием для рассекречивания сведений являются:

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

— изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

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

Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.

В исключительных случаях право продления первоначально установленных сроков засекречивания носителей сведений, составляющих

государственную тайну, предоставляется руководителям государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.

Руководители органов государственной власти, предприятий, учреждений и организаций наделяются полномочиями по рассекречиванию носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

2.4 Система защиты государственной тайны.

Вопросы защиты государственной тайны приобрели особую значимость в последние годы, в период глубоких социально-экономических преобразований в РФ, когда, с одной стороны, появляются новые угрозы безопасности государства, а, с другой стороны, сложившиеся режимы защиты государственной тайны перестают срабатывать должным образом.

В общем смысле защита информации – комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и её носителям.

Защита информации разбивается на решение двух основных групп задач:

1) Своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, т.е. обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информацией;

2) Ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

При решении первой группы задач, всегда учитывается, что специалисты могут использовать как открытую, так и засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме ее фактического наличия. При снабжении специалиста засекреченной информацией действуют ограничения: наличие соответствующего допуска и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной информации всегда существуют противоречия: необходимо, с одной стороны, максимально ограничить его доступ к засекреченной информации и, тем самым, уменьшить вероятность утечки этой информации, а с другой наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной, для обоснованного решения им служебных задач.

Вторая группа задач включает такие условия, как:

1) Защита информационного суверенитета страны и расширение возможностей государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала;

2) Создание условий эффективного использования информационных ресурсов общества;

3) Обеспечение безопасности защищаемой информации: предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы;

4) Сохранение секретности информации в соответствии с установленными правилами ее защиты, в том числе, предупреждение ее утечки и НСД к её носителям;

5) Сохранение полноты, достоверности, целостности информации и ее массивов и программ обработки;

6) Недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству.

Режим секретности это реализация действующих норм и правил защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы. Основное назначение режима секретности – обеспечить соответствующий уровень защиты информации, т.к. чем выше степень ее секретности, тем более высокий уровень ее защиты устанавливается, соответственно изменяется и режим секретности.

Режим секретности включает следующие основные группы мер:

Во-первых, разрешительную системы, определяющую порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где ведутся конфиденциальные или секретные работы;

Во-вторых, порядок и правила делопроизводства с секретными или конфиденциальными документами и иными носителями защищаемой информации;

В-третьих, установление пропускного и внутриобъектового режима, соответствующего степени секретности информации, имеющейся на объекте;

В-четвертых, воспитательно-профилактическую работу с целью предотвратить или значительно уменьшить риск утечки засекреченной информации через сотрудников, работающих с такой информацией.

В рамках установленного на объекте режима секретности проводятся все остальные мероприятия по защите сведений, составляющих государственную тайну.

Таким образом, система защиты сведений, отнесенных к государственной тайне, и их носителей складывается из:

— органов защиты государственной тайны;

— средств и методов защиты государственной тайны;

— проводимых мероприятий.

Главным субъектом, осуществляющим защиту сведений, составляющих государственную тайну, является государство в лице его высших органов власти и управления, которое располагает всей полнотой властных полномочий по

решению задач защиты государственной тайны. Однако существует целая иерархия органов, учреждений, организаций, предприятий и других структурных подразделений, должностных лиц и исполнителей, которые наделены соответствующим объемом прав и обязанностей по эффективной защите сведений, составляющих государственную тайну.

Высшие органы государственной власти и управления создают нормативно-правовую базу, регламентирующую деятельность по защите сведений, отнесенных к государственной тайне. Координация деятельности по разработке и выполнению государственных программ, по подготовке нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне, возложена на Межведомственную комиссию. ФСБ, СВР, ФСТЭК, Минобороны и их территориальные органы организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ. Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции.

В систему защиты государственной тайны включаются кроме мер, осуществляемых непосредственно в местах сосредоточения и обращения сведений, составляющих эту тайну, также проводимые государством мероприятия и устанавливаемые административно-правовые режимы:

— борьба со шпионажем и разглашением государственной тайны;

— охрана государственных тайн в печати;

— пограничный режим;

— режим въезда и передвижения иностранцев;

— режим выезда специалистов в служебные командировки за границу.

Защита информации призвана обеспечить нормальное и эффективное функционирование вышестоящей системы, в которую она «встроена» и которой она создана: например, обеспечивать деятельность отрасли, предприятия и т.д. Цель режимной деятельности на любом предприятии состоит в том, чтобы

обеспечить научно-производственную, управленческую и другую деятельность секретной и другой защищаемой информации.

Любая система защиты информации имеет свои особенности и в то же время должна отвечать общим требованиям. Общими требованиями к системе защиты информации являются:

1) СЗИ должна быть представлена как нечто целое. Целостность системы будет выражаться в наличии единой цели её функционирования, информационных связей между элементами системы, иерархичности построения подсистемы управления системой защиты информации.

2) СЗИ должна обеспечивать безопасность информации, средств информации и защиту интересов участников информационных отношений.

3) СЗИ в целом, методы и средства защиты должны быть по возможности «прозрачными» для законного пользователя, не создавать ему больших дополнительных неудобств, связанных с процедурами доступа к информации, и в то же время быть непреодолимыми для НСД злоумышленника к защищаемой информации

4) СЗИ должны обеспечивать информационные связи внутри системы между её элементами для согласованного их функционирования и связи с внешней средой, перед которой система проявляет свою целостность и выступает как единое целое.

Система защиты информации включает в себя совокупность элементов, её составляющих, и их свойства. Внутренние связи системы и их свойства составляют архитектуру системы, её структуру и внутреннюю организацию. Одновременно элементы системы имеют и внешние связи, которые целенаправленно воздействуют на внешнюю среду и решают поставленные перед системой задачи, - это функциональная часть системы. Структурная и функциональная части системы не отделены друг от друга, это как бы две стороны одних и тех же элементов, составляющих систему защиты информации.

Структурная часть системы защиты информации составляет её внутреннюю организацию, которая позволяет системе нормально

функционировать, создает условия для обеспечения безопасности засекреченной информации, её обращения только по каналам, контролируемым данной системой.

Структурная часть системы защиты информации включает в себя:

1) систему законов и других нормативных актов, устанавливающих :

— порядок и правила защиты информации, а также ответственность за покушение на защищаемую информацию или на установленный порядок её защиты;

— защиту прав граждан, связанных по службе со сведениями, отнесенными к охраняемой тайне;

— права и обязанности государственных органов, предприятий и должностных лиц в области защиты информации;

2) систему засекречивания информации, в которую входят:

— законодательное определение категорий сведений, которые могут быть отнесены к государственной тайне;

— законодательное и иное правовое определение категорий сведений, которые не могут быть отнесены к государственной тайне;

— наделение полномочиями органов государственной власти и должностных лиц в области отнесения сведений к охраняемой законом тайне;

— составление перечня сведений, отнесенных к государственной тайне;

3) систему режимных служб и служб безопасности с их собственной структурой, штатным расписанием, обеспечивающих функционирование всей системы защиты информации.

Функциональная часть системы защиты информации решает задачи обеспечения засекреченной информацией деятельности вышестоящей системы, в которую данная система защиты информации «встроена». В эту деятельность вовлекается широкий круг работников объекта: сотрудники службы безопасности, связанные с обработкой, хранением, выдачей и учетом засекреченной информации; руководители объекта и структурных

подразделений; исполнители, т.е. все работники объекта, которые являются потребителями защищаемой информации.

Основные элементы функциональной части системы:

— порядок и правила определения степени секретности сведений и проставления грифа секретности на работах, документах, изделиях, а также рассекречивания информации или снижения степени её секретности;

— установленные на объекте режим секретности, внутриобъектовый режим и режим охраны, соответствующие важности накапливаемой и используемой на объекте информации;

— система обработки, хранения, учета и выдачи носителей защищаемой информации с использованием принятой системы накопления и обработки информации: автоматизированная, ручная, смешанная, иная, в том числе делопроизводство с секретными и конфиденциальными документами;

— разрешительная система, регламентирующая порядок доступа потребителей к носителям защищаемой информации, а также на предприятие и в его отдельные помещения;

— система выявления возможных каналов утечки информации и поиск решений по их перекрытию, включая воспитательно-профилактическую работу на объекте и в его структурных подразделениях;

— система контроля наличия носителей защищаемой информации и состояния на объекте установленных режимов: секретности, внутриобъектового, охраны объекта и его важнейших подразделений.

Таким образом, можно сказать, что структурная и функциональная части системы защиты информации существуют и работают в неразрывном единстве.

2.5 Допуск и доступ к государственной тайне.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

— принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

— согласие на частичные, временные ограничения их прав в соответствии со статьей 24 закона «О государственной тайне»;

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

— определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных законом;

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

— принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Допуск осуществляется в соответствии с Инструкцией о порядке допуска должностных лиц и граждан РФ к государственной тайне, утвержденной постановлением Правительства РФ от 6.02.10 №63. Инструкцией предусмотрена форма типового договора, заключаемого с должностными лицами и гражданами при оформлении допуска к государственной тайне.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации. Целью проведения проверочных мероприятий является выявление оснований для отказа должностному лицу или гражданину в допуске к государственной тайне.

Установлены три формы допуска к государственной тайне, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным, секретным. Наличие у должностных лиц и граждан допуска к сведениям более

высокой степени секретности является основанием для доступа к сведениям более низкой степени секретности.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается ряд льгот:

1) процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ: «особой важности» —50-75%, «совершенно секретным» — 30-50%, «секретным» — 10-15% при проведении проверочных мероприятий, 5-10% без проведения проверочных мероприятий. Данная норма реализована постановлением Правительства РФ от 18.0906 №573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны». При определении размера процентной надбавки учитывается объем сведений, к которым указанные граждане имеют доступ, а также продолжительность срока, в течении которого сохраняется актуальность засекречивания этих сведений.

2) преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Для сотрудников структурных подразделений по защите государственной тайны дополнительно к социальным гарантиям, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

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

Указанные лица предупреждаются о неразглашении государственной тайны, 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.

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

— расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

— однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;

— возникновения обстоятельств, являющихся согласно статье 22 закона «о государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

Прекращение допуска должностного лица или гражданина к государственной тайне является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте).

Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:

— права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска;

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

— права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны. Порядок доступа устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации (как правило это секретный Приказ Министра). Руководители несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

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 Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Порядок лицензирования установлен в Положении «О лицензировании деятельности предприятий, организаций и учреждений по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите государственной тайны" утвержденном Постановлением Правительства РФ № 333 от 15.04.95г. 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.

Лицензия выдается предприятию, учреждению, организации при выполнении ими следующих условий:

— выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, 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.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на ФСТЭК, ФСБ,

Минобороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

2.6 Контроль и надзор за обеспечением защиты государственной тайны.

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Федеральный государственный контроль за обеспечением федерального государственного контроля за обеспечением защиты государственной тайны осуществляется уполномоченными федеральными органами исполнительной власти согласно их компетенции в порядке, установленном Правительством РФ.

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют органы федеральной исполнительной власти (ФСБ РФ, МО РФ, СВР РФ, ФСТЭК РФ), и их органы на местах, на которые эта функция возложена законодательством Российской Федерации.

Органы государственной власти, наделенные полномочиями по распоряжению сведениями, составляющими государственную тайну, 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.

Контроль за обеспечением защиты государственной тайны в Администрации Президента Российской Федерации, в аппаратах палат Федерального Собрания, Правительства Российской Федерации организуется их руководителями.

Контроль за обеспечением защиты государственной тайны в судебных органах и органах прокуратуры организуется руководителями этих органов.
Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

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

2.7 Организационные и технические способы защиты государственной тайны.

Основными организационно-техническими способами, используемыми в защите государственной тайны, являются: скрытие, ранжирование, дробление,

учет, дезинформация, морально-нравственные меры, кодирование и шифрование.

Скрытие является реализацией на практике одного из основных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Обычно это достигается путем:

— засекречивания информации, т.е. отнесения её к секретной или конфиденциальной информации различной степени секретности и ограничения в связи с этим доступа к этой информации в зависимости её важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности

— устранения или ослабления технических демаскирующих признаков объекта защиты и технических каналов утечки сведений о них.

Скрытие один из наиболее общих и широко применяемых методов защиты информации.

Ранжирование – предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа. Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных лиц.

Дезинформация – заключается в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности.

Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по

внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Дробление информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину в целом. Применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления.

Морально-нравственные способы защиты информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам нередко становится источником утечки этой информации или по его вине соперник получает возможность НСД к носителям защищаемой информации. Морально-нравственные методы защиты информации предполагают прежде всего воспитание сотрудника, допущенного к секретам, т.е. проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений, и обучение сотрудника правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учет обеспечивает возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные о всех пользователях этой информации.

Принципы учета засекреченной информации:

— обязательность регистрации всех носителей защищаемой информации;

— однократность регистрации конкретного носителя такой информации;

— указание в учетах адреса, где находится в данное время данный носитель засекреченной информации;

— единоличная ответственность за сохранность каждого носителя защищаемой информации и отражение в учетах пользователя данной информации в настоящее время, а также всех предыдущих пользователей данной информации.

Кодирование – метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании открытого текста в условный сигнал для передачи информации по каналам связи, а также при обработке и хранении информации в средствах вычислительной техники.

Для кодирования используется обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть преобразована таким образом, что прочесть её можно будет только если потребитель имеет соответствующий ключ (код) для её раскодирования.
Шифрование применяется когда есть опасность перехвата сообщений соперником. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет ключа для раскрытия шифра.

Шифрование может быть предварительное (шифруется текст документа) и линейное (шифруется разговор) Для шифрования информации может использоваться специальная аппаратура.

Знание возможностей приведенных методов позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты секретной информации.

2.8 Виды посягательств на государственную тайну.

За посягательства на государственную тайну установлена уголовная ответственность. Виды посягательств определены в 29 главе УК РФ. "Преступления против основ конституционного строя и безопасности государства".

Определены следующие виды посягательств на государственную тайну :

Шпионаж. Это либо одна из форм государственной измены (ст. 275) если оно совершено гражданином России, либо специальный состав преступления

при совершении иностранцем или лицом без гражданства (ст. 276). При любой форме шпионаж может быть двух видов.

Шпионаж первого вида состоит в передаче, а равно собирании, похищении или хранении в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну.

Шпионаж второго вида представляет собой передачу или собирание по заданию иностранной разведки иных (т.е. не составляющих государственную тайну) сведений для использования их в ущерб внешней безопасности Российской Федерации.

Лицо, совершившее преступления, статьей 275 или 276 УК РФ, 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

Разглашение государственной тайны (ст. 283 УК России), состоит в предании ее гласности лицом, которому она была доверена или стала известна по службе или работе, если составляющие тайну сведения стали достоянием других лиц, при отсутствии признаков государственной измены. Это преступление может совершить лишь лицо, которому сведения, составляющие государственную тайну, стали известны по службе или работе, либо были доверены при тех или иных обстоятельствах, например, в ходе предварительного следствия, судебного процесса и т.п.

Утрата документов, содержащих государственную тайну (ст. 284 УК России). Под утратой понимается нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий.

Совершение всех перечисленных преступлений может быть сопряжено с другими общественно опасными деяниями, например, с контрабандой; незаконным экспортом технологий, научно-технической информации и услуг, используемых при создании оружия массового уничтожения, вооружений и военной техники; преступлениями в сфере компьютерной информации; разглашением данных предварительного расследования; разглашением сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса, либо в отношении должностного лица правоохранительного или контролирующего органа; похищением или повреждением документов, штампов, печатей и т.п. В таких случаях действия виновного квалифицируются по признаку совокупности преступлении.

Нормативно-правовые документы:

Конституция РФ.

ФЗ РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»

ФЗ от 28 декабря 2010 г. №390-ФЗ «О безопасности»

Указ Президента РФ от 30 ноября 1995 г. № 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне

Указ Президента РФ от 6 октября 2004 г. №1286 «Положение о Межведомственной комиссии по защите государственной тайны»

Постановление Правительства РФ от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

Постановление Правительства РФ от 6 февраля 2010 г. №63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»

Постановление Правительства РФ от 18 сентября 2006 № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны»

Постановление Правительства РФ от 15.04.1995 N 333 "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"

Вопросы для самоконтроля:

1. Какие нормативные правовые акты включает законодательство о ГТ?
2. Что понимается под "государственной тайной" и "средствами защиты информации"?
3. Сведения в каких областях относят к ГТ?
4. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?
5. Принципы отнесения сведений к ГТ и их засекречивания.
6. Понятие "засекречивание сведений" и степени секретности документов.
7. Какие данные содержат реквизиты, наносимые на носители секретных сведений?
8. Основные группы задач защиты информации.
9. Общие требования к системе защиты информации.
10. Перечислите органы защиты ГТ.
11. Что предусматривает допуск должностных лиц и граждан к ГТ?
12. Какие льготы устанавливаются для лиц допущенных к ГТ?
13. Какие ограничения прав граждан и должностных лиц могут наступить в связи с допуском к ГТ.?
14. Каким путем осуществляется допуск предприятий, организаций и учреждений к проведению работ связанных с использованием сведений, составляющих ГТ?
15. Какими органами осуществляется контроль и надзор за обеспечением защиты ГТ?

16. Основные организационно-технические способы используемые в защите государственной тайны.

17. Перечислите виды посягательств на государственную тайну.

18. Дайте характеристику понятию "шпионаж".

19. Что понимается под выдачей государственной тайны иностранному государству?

20. Что означает разглашение государственной тайны?

21. Что понимается под утратой документов, содержащих ГТ?

ТЕМА 3. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.

Широкое внедрение современных информационных технологий создает благоприятную обстановку для злоумышленников в плане доступа к конфиденциальной информации или её незаконного распространения, несанкционированного вмешательства в управление производственными процессами принятия решений. В этих условиях незаконное распространение конфиденциальных сведений может нанести значительный ущерб как государству и обществу в целом, так и отдельным его членам.

По своему содержанию конфиденциальная информация включает все виды существующих тайн определенных Законодательством РФ, за исключением государственной тайны. Однако отсутствие отдельного закона определяющего правовые основы защиты конфиденциальной информации усложняет задачу изучения этой проблемы и вызывает необходимость анализа и оценки достаточно большого перечня актов законодательства.

Согласно закону "Об информации, информатизации и защите информации", конфиденциальная информация - информация ограниченного доступа и она защищается законодательством. Поэтому важно определить структуру законодательства, которое регулирует правоотношения связанные с конфиденциальной информацией, а также правовой режим сохранения конфиденциальности и правовой ответственности за ее нарушение.

В качестве нормативной правовой базы, регулирующей отношения в области защиты конфиденциальной информации, следует рассматривать законодательные акты устанавливающие перечни сведений конфиденциального характера и ограничения по доступу к ним, а также определяющие ответственность за нарушения установленных норм права в этой области.

Основными нормативно-правовыми актами в области защиты конфиденциальной информации и прав субъектов информационных правоотношений являются:

Конституция РФ;

Гражданский кодекс РФ;

Уголовный кодекс РФ;

ФЗ «Об информации, информационных технологиях и о защите информации»;

Указ Президента РФ от 6 марта 1997 г. №188 «об утверждении перечня сведений конфиденциального характера»;

Кроме этого к законодательству в области защиты конфиденциальной информации относятся законодательные и нормативные акты регулирующие правоотношения в таможенных органах, пенсионных фондах, банковской сфере, коммерческой деятельности, в органах налоговой полиции и страхования, в сфере отдельных видов профессиональной деятельности. Перечень таких документов приводится в Приложении 1

Данные нормативные правовые акты определяют:

— перечни сведений конфиденциального характера (виды тайн);

— ограничение доступа к конфиденциальной информации и её защиту;

— гражданскую, уголовную и другие виды ответственности за правонарушения при обращении с конфиденциальной информацией.

В Приложении 2 приведен примерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации

3.1 Служебная тайна

Существуют следующие признаки отнесения сведений к служебной тайне:

1) Сведения, содержащие служебную информацию о деятельности государственных органов или подведомственных им предприятий, организаций, запрет на распространение которых установлен законом или диктуется служебной необходимостью;

2) Сведения, являющиеся конфиденциальной информацией для других лиц, но ставшие известными представителям государственных органов в силу исполнения ими служебных обязанностей.

Служебная тайна — защищаемая законом конфиденциальная информация, ставшая известной в государственных органах или органах местного самоуправления на законных основаниях, в силу исполнения ими служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен законом или в силу служебной необходимости.

Категории информации, составляющей служебную тайну:

1) Информация, составляющая собственную служебную информацию о деятельности самого органа власти;

2) Конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну – «чужая тайна»

3) Сведения, не являющиеся государственной тайной и не попадающие под перечень сведений, доступ к которым не может быть ограничен;

4) Информация, полученная в силу исполнения служебных обязанностей.

В постановлении Правительства РФ от 3 ноября 1994 г. №1233 приводится перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения. К таким сведениям относятся:

1) акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

2) сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

3) описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

4) порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

5) решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

6) сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

7) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Объекты служебной тайны:

1) Военная тайна.
2) Тайна следствия.
3) Судебная тайна.
4) Налоговая тайна.
5) Таможенная тайна.

На документы, содержащие служебную тайну, наносится гриф «для служебного пользования» (ДСП).

3.2 Коммерческая тайна

Коммерческая деятельность организации тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразной информации. В связи с этим возникают следующие вопросы:

— вся ли информация подлежит защите или следует выделять отдельные её группы?

— если для защиты выделяется определенная группа информации, то какие критерии для этого существуют?

Отвечая на поставленные вопросы, подчеркнём, что защите подлежит не вся информация, а только та, которая представляет ценность для организации. При определении ценности коммерческой информации необходимо руководствоваться такими её свойствами, как *полезность, своевременность* и *достоверность.*

Полезность информации состоит в том, что она создаёт обладателю выгодные условия для принятия оперативного решения и эффективного результата. В свою очередь полезность зависит от своевременного её получения и доведения до исполнителя. Из-за несвоевременного поступления важных по своему содержанию сведений часто упускается возможность заключить торговую или иную сделку.

Критерии полезности и своевременности тесно связаны и взаимозависимы с критерием достоверности информации. Причины возникновения недостоверных сведений различны: неправильное восприятие фактов или умышленное их искажение. Поэтому сведения, представляющие коммерческий интерес, а также источник их поступления должны подвергаться перепроверке.

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

В зарубежной экономической литературе коммерческая информация рассматривается не в качестве средства извлечения прибыли, а прежде всего как условие, способствующее или препятствующее прибыли. Особо подчеркивается наличие стоимостного фактора коммерческой информации, т.е. возможность выступать в качестве предмета купли-продажи. Поэтому важное значение имеет вопрос об определении принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге – о наличии у него прав на её защиту.

В совокупности под коммерческой тайной негосударственной организации следует понимать сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.

Закон РФ, регламентирующий коммерческую деятельность, предусматривает, что собственниками коммерческой информации могут быть граждане России, граждане иностранных государств, а также объединения граждан – коллективных предпринимателей.

Обширны и направления коммерческой деятельности. Это внутренние и внешние экономические сферы производственной, посреднической, коммерческой, научно-технической, инвестиционной, сервисной деятельности. Обеспечение защиты государственной тайны не имеет прямого отношения к защите коммерческой тайны. Однако, под защиту государства может быть взята коммерческая информация, оцененная как особо важная не только для её собственника, но и для государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимателем и органом федеральной безопасности, с обозначением пределов и функций профессиональной деятельности последних.

Основой для разработки положений ФЗ «О коммерческой тайне» послужили положения ст. 139 ГК РФ (утратила силу с 1 января 2008г), содержащие впервые сформулированные признаки информации, которая может составлять коммерческую тайну. ФЗ «О коммерческой тайне» выделяет следующие признаки относимости информации к коммерческой тайне:

— Информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;

— Отсутствует свободный доступ к информации на законном основании;

— Обладатель информации принимает меры к охране её конфиденциальности.

Первый признак информации как коммерческой тайны подчеркивает её зависимость от неизвестности третьим лицам. Из этого признака следует второй признак информации – отсутствие свободного доступа на законном основании, что означает следующее:

— посторонние лица могут получить указанную информацию либо незаконным путем, либо в результате небрежности её обладателя;

— не может быть ограничен доступ к сведениям, которые не могут составлять коммерческую тайну.

Третий признак информации, составляющей коммерческую тайну, означает что в отношении её необходимо устанавливать режим коммерческой тайны, что, однако, не имеет юридической силы в случае, если информация не содержит в себе первые два признака.

Коммерческая информация, циркулирующая в организации, подразделяется на техническую, организационную, финансовую, рекламную, информацию о спросе– предложении, конкурентах, криминальной обстановке и т.д.

Прежде чем принимать меры к защите определенной информации, необходимо ответить на следующие вопросы:

1) Какие сведения не могут составлять коммерческую тайну предприятия и предпринимателя?

2) Какие сведения невыгодно скрывать?

3) Какие сведения подлежат защите?

Ответ на первый вопрос содержится в ст.5 ФЗ «О коммерческой тайне», согласно которой к коммерческой тайне не могут быть отнесены следующие сведения:

1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащиеся в документах, дающих 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 и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

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

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

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

9) 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;

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

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Юридические лица и предприниматели обязаны на безвозмездной основе предоставлять информацию, составляющую коммерческую тайну, государственным органам и органам местного самоуправления по их мотивированному требованию. Согласно ст. 6 ФЗ «О коммерческой тайне» такое требование должно содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну и срок предоставления этой информации, если иное не установлено федеральными

законами. Мотивированное требование должно быть подписано уполномоченным должностным лицом. Информация, составляющая коммерческую тайну, предоставляется государственным органам в документированной форме с обязательным проставлением на материальных носителях грифа «Коммерческая тайна». Этот гриф включает в себя сведения об обладателе информации, составляющей коммерческую тайну: полное наименование и нахождение для юридического лица и Ф.И.О. и место жительства для индивидуального предпринимателя.

Статья 13 указанного закона устанавливает обязанность государственных органов и органов местного самоуправления сохранять конфиденциальность сведений, составляющих «чужую» коммерческую тайну. Дальнейшая передача такой информации возможна только с согласия её обладателя.

Обладатель информации, составляющей коммерческую тайну, устанавливает режим коммерческой тайны, и с этого момента возникают его права на эту информацию. Перечень мер по охране конфиденциальности информации, содержащийся в ст.10 указанного закона, носит исчерпывающий характер.

Меры по охране конфиденциальности информации должны включать в себя:

1) Определение перечня информации, составляющей коммерческую тайну;

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

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

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

5) Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая информация» с указанием обладателя этой информации.

Особое внимание в данном законе уделяется охране конфиденциальности информации в рамках трудовых отношений. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями. Если работник виновен в разглашении такой информации, то он обязан возместить причинённый работодателю. Однократное грубое нарушение работником трудовых обязанностей в виде разглашения конфиденциальной информации является основанием для расторжения трудового договора по инициативе работодателя, а также одним из случаев, когда на работника может быть возложена материальная ответственность в полном размере причиненного ущерба.

Ответ на вопрос, о том какие сведения невыгодно скрывать, касается коммерческой информации, которую невыгодно скрывать самой организации или предпринимателю. Это, прежде всего, рекламная информация. Без рекламы трудно добиться эффективного результата в хозяйственной деятельности, особенно в условиях жесткой конкуренции. Однако широкое распространение рекламы имеет как положительную, так и отрицательную стороны. Коммерческая информация, содержащаяся в рекламе, помогает преступникам определить объект будущего посягательства, изучить его слабые стороны.

К группе коммерческой сведений, подлежащих защите, относятся те, которые представляют хозяйственную ценность для предпринимателя и на которые не распространяется законный доступ третьих лиц, т.е. прежде всего сведения, составляющие коммерческую тайну.

Следует отметить, что ограничения, вводимые на использование коммерческой тайны, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при формировании трудовой деятельности организации, персонала её

подразделений, а также при их сотрудничестве с работникам других организаций.

Целью таких ограничений является предотвращение разглашения, утечки или несанкционированного доступа к конфиденциальной информации. Ограничения должны быть целесообразными и обоснованными с точки зрения необходимости обеспечения информационной безопасности. Не допускается использование ограничений для сокрытия ошибок и некомпетентности руководства организации, бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений в деятельности организации, а также для уклонения от выполнения договорных обязательств и уплаты налогов.

Коммерческая тайна может категоризироваться локальными нормативными актами организации. Соответственно могут использоваться несколько грифов, например «Конфиденциально», «Строго конфиденциально».

3.3 Профессиональная тайна

Согласно ст.9 ФЗ «Об информации, информационных технологиях и о защите информации» к профессиональной тайне отнесена информация, удовлетворяющая следующим требованиям:

• доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;

• лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной) (например, вызов ветеринара на дом относится к служебной тайной);

• запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;

• информация не относится к сведениям, составляющим государственную и коммерческую тайну.

Профессиональная тайна — защищаемая законом информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация, составляющая профессиональную тайну, может быть представлена третьим лицам в соответствии с федеральными законами и (или) по решению суда. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе. Сохранение в тайне сведений, полученных в связи выполнением профессиональных функций, вызвано в первую очередь нормами профессиональной этики, а не собственными коммерческими интересами предпринимателя или организации.

Выделяют следующие объекты профессиональной тайны:

1) Врачебная тайна. Согласно ст.13 ФЗ «Об основах охраны здоровья граждан в Российской Федерации» сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений составляющих врачебную тайну, в том числе после смерти человека, за исключением случаев предусмотренных Федеральным Законом. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

2) Тайна связи. Федеральный закон «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами по средствам связи. При такой постановке вопроса тайна

связи становится инструментом обеспечения сохранности конфиденциальной информации.

Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, передаваемых по сетям связи, охраняется Конституцией Российской Федерации. Обязанность обеспечения соблюдения тайны связи возлагается на оператора связи, под которым понимается физическое или юридическое лицо, имеющее право на предоставление услуг связи. Также операторы связи обязаны соблюдать конфиденциальность сведений об абонентах и оказываемых им услугах связи, ставших известными операторам в силу выполнения профессиональных обязанностей.

3*) Нотариальная тайна.* Тайна является специфическим правилом нотариальных действий. В соответствии со ст.5 Основ законодательства Российской Федерации о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами. Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

4) Адвокатская тайна. В соответствии с Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать сведения, сообщенные доверителем в связи с оказанием ему юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в устном виде.

Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя.

5) Тайна усыновления. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления.

Согласно ст. 155 УК РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну. Второй – все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

6) Тайна страхования. В соответствии со ст. 946 ГК РФ, тайну страхования составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст.139 или ст.150 ГК РФ.

Согласно ст.8 Закона РФ «Об организации страхового дела в Российской Федерации» в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица — страховые агенты и страховые брокеры.

Кроме того, в соответствии со ст. 33 указанного Закона должностные лица органа страхового надзора не вправе разглашать в какой-либо форме сведения, составляющие коммерческую и иную охраняемую законом тайну субъекта страхового дела, за исключением случаев, предусмотренных законодательством Российской Федерации.

7) Тайна исповеди. Обеспечение тайны исповеди является внутренним делом священника; юридической ответственности за её разглашение он не несёт. Согласно ч.7 ст. 3 ФЗ «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечён к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

8) Аудиторская тайна — любые сведения и документы, полученные и (или) составленные аудиторской организацией и её работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании аудиторских услуг, за исключением:

• сведений, разглашенных самим лицом, которому оказывались услуги, либо с его согласия;

• сведений о заключении с аудируемым лицом договора о проведении обязательного аудита;

• сведений о величине оплаты аудиторских услуг.

9) Журналистская тайна — главный редактор, журналист, сотрудник редакции обязаны сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом

10) Банковская тайна — информация об операциях, счетах и вкладах клиентов и корреспондентов. Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

Федеральный закон «О банках и банковской деятельности» определяет обязанности субъектов, категории информации и основания, по которым сведения предоставляются заинтересованным органам государственной власти, организациям и лицам. Кредитная организация, Банк России гарантирует тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах её клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных

и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к банковской тайне любые сведения, за исключением прямо указанных в Законе.

Информация некоторых из этих категорий носит двойственный характер и может быть отнесена также к служебной, коммерческой тайне и (или) персональным данным.

Законодательство обязует владельцев информации, относимой к профессиональной тайне, сохранять её конфиденциальность в интересах лиц, которым разглашением этой информации может быть причинен моральный или материальный ущерб.

3.4 Персональные данные

В России нормы, регулирующие вопросы защиты персональных данных, были впервые включены в Конституцию Российской Федерации 1993г. Согласно ст. 23 и 24 Конституции РФ каждый гражданин Российской Федерации имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Право на неприкосновенность частной жизни призвано защитить частную жизнь, личную и семейную тайну от какого бы то ни было проникновения в неё со стороны как государственных органов, органов местного самоуправления, так и негосударственных предприятий, учреждений, организаций, а также отдельных граждан.

Особое значение запрет собирать, хранить, использовать и распространять информацию о частной жизни лица приобретает в связи с созданием информационных систем на основе использования средств вычислительной техники и связи, позволяющих накапливать и определенным образом обрабатывать значительные массивы информации.

В январе 1981 г. государства — члены Совета Европы подписали Конвенцию о защите физических лиц при автоматизированной обработке персональных данных. Российская Федерация подписала этот международный акт 7 ноября 2001 г. и ратифицировала 19 декабря 2005 г. Одно из требований Конвенции — осуществить гармонизацию внутреннего законодательства Российской Федерации. Оно было выполнено путем принятия новых федеральных законов — «Об информации, информационных технологиях и о защите информации» и «О персональных данных».

Основные положения работы с информацией о гражданах и их частной жизни отражены в Федеральном законе «Об информации, информационных технологиях и о защите информации». Согласно ст. 9 этого закона «запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами. Порядок доступа к персональным данным граждан (физических лиц) устанавливается Федеральным законом «О персональных данных».

ФЗ «О персональных данных» регулирует отношения, связанные с обработкой персональных данных, осуществляемой с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации. Положения закона не распространяются на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов;

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

4) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации.

В указанном Законе даются следующие определения:

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

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

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;

Информационная система персональных данных (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Обязательным требованием к обработке персональных данных является соблюдение их конфиденциальности, за исключением тех случаев, когда распространение персональных данных осуществляется с согласия субъекта этих данных или на иных законных основаниях.

Реализуя основные положения Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, Федеральный Закон «О персональных данных» устанавливает, что обработка персональных данных должна осуществляться на следующих принципах:

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.

Субъект персональных данных принимает решение о предоставлении его персональных данных и даёт согласие на их обработку. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи (например, смс-спам), а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено. В таком случае, оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных.

Оператор персональных данных обязан выполнять требования на защиту персональных данных:

«Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Правительство РФ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Регуляторами в сфере защиты персональных данных являются следующие государственные органы:

Роскомнадзор (является основным проверяющим органом);

ФСТЭК России (привлекается к проверке систем защиты ПДн);

ФСБ России, 8-й Центр (привлекается к проверке в случае наличия в системе криптографических средств защиты информации и систем обнаружения атак).

Установлены 3 типа угроз для информационной системы обработки персональных данных:

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

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

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

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных:

Необходимость обеспечения 1-го уровня защищенности ПДн устанавливается при наличии хотя бы одного из следующих условий:

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

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем

100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности ПДн устанавливается при наличии хотя бы одного из следующих условий:

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

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

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

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

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

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

Необходимость обеспечения 3-го уровня защищенности ПДн устанавливается при наличии хотя бы одного из следующих условий:

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

100000 субъектов персональных данных, не являющихся сотрудниками оператора;

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

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

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

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

Для обеспечения 4-го уровня защищенности ПДн необходимо выполнение следующих требований:

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

б) обеспечение сохранности носителей персональных данных;

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

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

Для обеспечения 3-го уровня защищенности ПДн помимо требований для 4-го уровня защищенности необходимо, чтобы было назначено должностное лицо, ответственное за обеспечение безопасности персональных данных в информационной системе. Для обеспечения 2-го уровня защищенности ПДн добавляется требование, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходим для выполнения служебных обязанностей. Для обеспечения 1-го уровня защищенности дополнительно необходимо выполнение следующих требований:

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

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

3.5 Правовой режим персональных данных.

Правовой режим персональных данных складывается из норм:

— определяющих принципы и условия обработки персональных данных;

— устанавливающих порядок сбора и обработки персональных данных;

— государственного контроля за деятельностью по сбору и обработке персональных данных;

— устанавливающих ответственность за нарушение законодательства о персональных данных;

Основные принципы обработки персональных данных были изложены ранее.

Общим обязательным требованием к обработке персональных данных является согласие субъекта этих данных. Исключение составляют случаи обработки персональных данных, указанные в ч.2 ст.6 ФЗ «О персональных данных». К ним относится обработка персональных данных на основании федерального закона или обработка персональных данных, необходимая для доставки почтовых отправлений организациями почтовой связи.

В российском законодательстве персональные данные подразделяются на следующие виды:

1) *общедоступные персональные данные* — персональные данные, доступ к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

2) *специальные категории персональных данных* — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Обработка таких данных возможна только в случаях, прямо указанных в законе, в частности:

— если субъект персональных данных в письменной форме дал свое согласие;

— если обработка персональных данных необходима в связи с осуществлением правосудия;

— если обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

3) Биометрические персональные данные — сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. К таким персональным данным относится дактилоскопическая информация, порядок сбора, хранения и использования

которой регулируется Федеральным законом от 25 июля 1998 г. №128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

Частные виды персональных данных рассматриваются в отдельных специальных нормативных правовых актах. Например, регулированию вопросов, связанных с оборотом персональных данных работника, посвящена гл. 14 Трудового кодекса РФ, а персональных данных, полученных при Всероссийской переписи населения — соответствующий федеральный закон.

Права субъектов персональных данных вытекают из неотъемлемого права человека на неприкосновенность частной жизни. Право граждан Российской Федерации на неприкосновенность частной жизни, личной и семейной тайны, защиту своей чести и доброго имени гарантируется Конституцией РФ. Эти конституционные положения реализованы в гл.3 Федерального закона «О персональных данных»:

— обработка персональных данных осуществляется только с согласия субъекта таких данных;

— обязательное предоставление персональных данных осуществляется только в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Субъект персональных данных имеет право доступа:

— к своим персональным данным;

— к данным об операторе, целях, способах и сроках обработки своих персональных данных;

— к данным о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ.

Субъект персональных данных имеет право отозвать свое согласие на обработку своих персональных данных.

Ограничение указанных прав субъекта персональных данных возможно только в установленных законом случаях, в частности если предоставление таких данных нарушает конституционные права и свободы других лиц или

обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка.

Субъект персональных данных, полагающий, что оператор осуществляет обработку его персональных данных с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, имеет право обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. Субъект персональных данных имеет право на защиту своих прав и законных интересов.

Обязанности операторов (государственных органов, муниципальных органов, юридических или физических лиц, организующих и (или) осуществляющих обработку персональных данных) составляют следующий перечень:

1. При обработке персональных данных оператор *обязан принимать необходимые организационные и технические меры* по обеспечению безопасности персональных данных при их обработке, причем не только автоматизированной. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии её хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

2. В случаях, когда субъект персональных данных, реализуя свои права, обращается к оператору с запросом, оператор *обязан предоставить информацию*, запрашиваемую субъектом персональных данных. При отказе в предоставлении указанной информации оператор обязан в письменной форме дать мотивированный ответ, содержащий ссылку на положения федерального закона, являющиеся основаниями для такого отказа. Ознакомление субъекта персональных данных с собственными персональными данными осуществляется безвозмездно.

3. В случае если обнаружилось, что персональные данные, относящиеся к соответствующему субъекту, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор *обязан устранить допущенные нарушения*, незамедлительно прекратить обработку и уничтожить соответствующие персональные данные в случае достижения цели их обработки. О предпринятых мерах оператор обязан уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы.

Контроль и надзор за обработкой персональных данных осуществляет уполномоченный орган по защите прав субъектов персональных данных. В настоящее время соответствующими полномочиями обладает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Права и обязанности уполномоченного органа по защите прав субъектов персональных данных прописаны в ст. 23 Федерального закона «О персональных данных».

Нарушение законодательства о персональных данных влечет за собой юридическую ответственность, а именно:

— дисциплинарную;

— гражданскую;

— уголовную;

—административную.

Нормативно-правовые документы

ФЗ РФ от 29 июля 2004 г №98-ФЗ «О коммерческой тайне»

ФЗ от 27 июля 2004 г. №79-ФЗ «О государственной гражданской службе РФ»

ФЗ от 2 декабря 1990 г №395-1 «О банках и банковской деятельности»

ФЗ от 31 мая 2002 г. №63-ФЗ «Об адвокатской деятельности и адвокатуре в РФ»

ФЗ от 7 июля 2003 г. №126-ФЗ «О связи»

ФЗ от 30 декабря 2008 №307-ФЗ «Об аудиторской деятельности»

ФЗ от 27 июля 2006 г №152-ФЗ «О персональных данных»

ФЗ от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Закон РФ от 27 ноября 1992 № 4015-1 «Об организации страхового дела в Российской Федерации»

Указ Президента РФ от 6 марта 1997 №188 «Об утверждении Перечня сведений конфиденциального характера»

Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»

Постановление Правительства РФ от 1 ноября 2012 г № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

«Основы законодательства Российской Федерации о нотариате» утверждены Верховным Судом РФ от 11 февраля 1993 г. ; 4462-1

Вопросы для самоконтроля

1) Перечислите основные нормативно-правовые акты в области защиты конфиденциальной информации и прав субъектов информационных правоотношений.

2) Что понимается под конфиденциальной информацией?

3) Что такое служебная тайна?

4) Какие сведения не могут составлять служебную тайну?

5) Что такое коммерческая тайна?

6) Перечислите признаки относимости информации к коммерческой тайне

7) Какие сведения не могут составлять коммерческую тайну?

9) Перечислите меры по охране конфиденциальной информации

10) Что такое профессиональная тайна?

11) Перечислите объекты профессиональной тайны

12) Раскройте смысл понятий "Персональные данные" и "Информационная система персональных данных"

13) Перечислите принципы обработки персональных данных

14) Назовите регуляторы в сфере защиты персональных данных

15) Перечислите типы угроз для информационной системы обработки персональных данных

16) Перечислите категории персональных данных

17) Перечислите обязанности операторов осуществляющих обработку персональных данных

18) Какие виды правовой ответственности предусмотрены в России за нарушение конфиденциальности сведений и в чем их суть?

ТЕМА 4. ЛИЦЕНЗИРОВАНИЕ, СЕРТИФИКАЦИЯ И АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ.

Основными организационными методами регулирования в области информационной безопасности со стороны государства являются:

—лицензирование;

— техническое регулирование.

Лицензирование — мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании;

Техническое регулирование — правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия;

К лицензируемым видам деятельности относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам,

законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием.

Основными источниками технических требований, устанавливаемых в рамках технического регулирования, являются технические регламенты и стандарты:

Технический регламент — документ, который принят международным договором Российской Федерации, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации).

Стандарт — документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Технические регламенты принимаются только в форме ФЗ и исключительно в целях:

— Защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;

— Охраны окружающей среды, жизни или здоровья животных и растений;

— Предупреждения действий, вводящих в заблуждение приобретателей;

— Обеспечения энергетической эффективности.

Для оценки соответствия объектов защиты (продуктов, товаров, услуг) требованиям технических регламентов, положениям стандартов проводится подтверждение соответствия.

Подтверждение соответствия — документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Подтверждение соответствия может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации. Обязательное подтверждение соответствия осуществляется в формах:

— принятия декларации о соответствии;

— обязательной сертификации.

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Декларация о соответствии — документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

Основными регулирующими органами по лицензированию в области защиты информации являются ФСТЭК России, ФСБ России. Деятельность по предоставлению услуг в области ЭЦП лицензируется федеральным агентством Росинформтехнологии. Органом по стандартизации и техническому регулированию является Ростехрегулирование.

4.1 Лицензирование.

Лицензирование деятельности, связанной с государственной тайной и защитой информации, является составной частью политики государства по обеспечению информационной безопасности РФ, защите информационных интересов организаций и граждан. Оно осуществляется по двум направлениям.

Первое направление связано с защитой государственной тайны и созданием средств защиты информации. Лицензирование деятельности, в этом случае является допуском предприятия к проведению работ связанных с использованием сведений, составляющих государственную тайну. Второе направление связано с защитой всей информации с ограниченным доступом.

Суть лицензирования заключается в разрешении юридическим лицам или индивидуальным предпринимателям (лицензиатам) заниматься определенными видами деятельности только при соблюдении обязательных требований и условий. Такие требования и условия устанавливаются соответствующими положениями о лицензировании конкретных видов деятельности. Осуществляют лицензионную деятельность (первоначальную проверку наличия у лицензиата соответствующих условий, выдачу лицензий и ведение соответствующих реестров, последующий контроль за соблюдением установленных требований и условий) лицензирующие органы – федеральные органы исполнительной власти и органы исполнительной власти субъектов федерации. Перечень лицензирующих органов утвержден постановлением Правительства РФ от 21 ноября 2011 №957.

Лицензии выдаются на определенный срок и на каждый конкретный вид деятельности. В случае выявления неоднократных или грубых нарушений лицензионных требований и условий лицензирующие органы в праве наложить административное взыскание и приостановить действие лицензии, установив срок устранения лицензиатом нарушений. Если в установленный срок лицензиат не устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

Согласно ФЗ «О лицензировании отдельных видов деятельности» в области защиты информации обязательному лицензированию подлежат следующие виды деятельности:

1) Деятельность по распространению шифровальных (криптографических) средств;

2) Деятельность по техническому обслуживанию шифровальных (криптографических) средств;

3) Предоставление услуг в области шифрования информации;

4) Разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

5) Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случаев, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

6) Деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

7) Деятельность по технической защите конфиденциальной информации;

8) Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Полномочия государственных органов по лицензированию перечисленных выше видов деятельности распределены следующим образом:

1) Федеральная служба по техническому и экспертному контролю (ФСТЭК России) лицензирует:

— деятельность по технической защите конфиденциальной информации,

— разработку и производство средств защиты конфиденциальной информации.

2) Федеральная служба безопасности (ФСБ России) лицензирует:

— Разработку, 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);

— Разработку, производство, реализацию и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

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

— Разработку и производство средств защиты конфиденциальной информации.

Лицензированием деятельности по разработке и (или) производству средств защиты конфиденциальной информации занимается ФСТЭК России, а в части разработки и (или) производства таких средств, устанавливаемых на объектах высших органов государственно власти – ФСБ России.

Еще один вид деятельности, подлежащий обязательному лицензированию, это деятельность, связанная с использованием и защитой сведений, составляющих государственную тайну. В соответствии с ФЗ «О лицензировании отдельных видов деятельности» действие этого закона не распространяется на

такую деятельность. Обязательное требование лицензирования допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, содержится в Законе «О государственной тайне».

Для получения лицензии заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности:

а) заявление о выдаче лицензии с указанием:

—наименования и организационно-правовой формы, места нахождения предприятия, адресов мест осуществления лицензируемого вида деятельности, номера расчетного счета в банке и наименования банка;

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

— срока действия лицензии;

— степени секретности сведений, составляющих государственную тайну, с которыми заявитель предполагает осуществлять работы, подтвержденной органом государственной власти или организацией, наделенными полномочиями по распоряжению указанными сведениями;

б) копии учредительных документов (с предъявлением оригиналов, в случае если копии не заверены нотариусом);

в) копию документа, подтверждающего факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц;

г) копии документов, подтверждающих право собственности или иное законное основание на владение и использование имущества, необходимого для осуществления заявленного вида деятельности на срок действия лицензии;

д) копию свидетельства о постановке на налоговый учет в налоговом органе (с предъявлением оригинала свидетельства, если копия не заверена нотариусом);

е) документ, подтверждающий уплату государственной пошлины за предоставление лицензии;

ж) сведения о наличии допуска к государственной тайне у руководителя предприятия, а также сведения о наличии в уставном (складочном) капитале предприятия доли (долей) иностранных физических или юридических лиц;

з) копию договора об оказании услуг — в случае использования заявителем услуг структурного подразделения по защите государственной тайны другой организации.

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 может назначаться дополнительная экспертиза.

Лицензии выдаются после обязательного проведения следующих предварительных мероприятий.

1) Специальная экспертиза предприятия, организации или учреждения, целью которой является проверка выполнения ряда условий, таких как:

— соблюдение требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам;

— наличие в структуре предприятия подразделения по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

— наличие на предприятии сертифицированных средств защиты информации.

2) Государственная аттестация руководителей, ответственных за защиту сведений, составляющих государственную тайну.

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 государственной тайны которого оказывает услуги по защите государственной тайны.

Лицензия оформляется на бланке, имеющем степень защиты на уровне степени защиты ценной бумаги. Бланки лицензий являются документами строгой отчетности, имеют учетную серию и номер. Приобретение, учет и хранение таких бланков возлагается на органы, уполномоченные на ведение лицензионной деятельности.

Государственная аттестация руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами РФ и Государственной корпорацией по атомной энергии "Росатом", руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий. Расходы по государственной аттестации руководителей предприятий относятся на счет предприятий.

Аттестация проводится в соответствии с Методическими рекомендациями, утвержденными Решением Межведомственной комиссии по защите ГТ, методом собеседования.

От государственной аттестации освобождаются руководители предприятий, имеющие свидетельство об окончании учебных заведений, уполномоченных осуществлять подготовку специалистов по вопросам защиты информации, составляющей государственную тайну. Перечень указанных учебных заведений утверждается Межведомственной комиссией по представлению органов, уполномоченных на ведение лицензионной деятельности.

Аттестуемый обязан знать:

— основные требования нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам и условия выполнения этих требований;

— порядок организации защиты ГТ.

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 Положения «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»;

— отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Контроль за соблюдением лицензионных условий лицензиатами, осуществляют органы, уполномоченные на ведение лицензионной деятельности.

Органами, уполномоченными на ведение лицензионной деятельности по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайны, являются - Федеральная служба безопасности Российской Федерации и её территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом).

На орган, уполномоченный на ведение лицензионной деятельности, возлагается:

— организация лицензирования деятельности предприятий;

— организация и проведение специальных экспертиз предприятий;

— рассмотрение заявлений предприятий о выдаче лицензий;

— принятие решений о выдаче или об отказе в выдаче лицензий;

— выдача лицензий;

— принятие решений о приостановлении действия лицензии или о ее аннулировании;

— разработка нормативно-методических документов по вопросам лицензирования;

— привлечение в случае необходимости представителей министерств и ведомств Российской Федерации для проведения специальных экспертиз;

— ведение реестра выданных, приостановленных и аннулированных лицензий.

4.2 Сертификация.

Еще одним высокоэффективным средством государственного контроля в условиях рыночной экономики, когда большая часть предприятий практически не зависит от государства, является подтверждение соответствия продукции, процессов производства, эксплуатации, работ, услуг или иных объектов установленным требованиям (техническим регламентам, стандартам, или условиям договора).

Основным нормативным правовым актом в области подтверждения соответствия вообще и сертификации в частности является ФЗ от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании», который заменил собой прежний Закон РФ от 10 июня 1993 г. №5151-1 «О сертификации продукции и услуг».

В соответствии с ФЗ «О техническом регулировании» процедуру сертификации осуществляет независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация – орган по сертификации, т.е. юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации. Органы сертификации, осуществляющие обязательную сертификацию, должны быть аккредитованы в порядке, устанавливаемом Правительством Российской Федерации. Аккредитация органов по сертификации и испытательных лабораторий (центров) осуществляется в целях подтверждения компетентности органов по сертификации, обеспечения доверия изготовителей, продавцов и приобретателей к деятельности органов по сертификации и аккредитованных

испытательных лабораторий и создания условий для признания результатов деятельности органов по сертификации и аккредитованных испытательных лабораторий (центров).

Систему сертификации образует совокупность всех органов по сертификации, правил выполнения работ по сертификации и правил функционирования всей системы в целом. Все системы сертификации подлежат обязательной государственной регистрации в Федеральном агентстве по техническому регулированию и метрологии.

Документом, подтверждающем соответствие продукции установленным требованиям или условиям договора является сертификат соответствия, выдаваемый на срок, установленный соответствующим техническим регламентом.

В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства РФ о техническом регулировании.

ФЗ «О связи» устанавливает обязательную сертификацию средств связи. Сертификация средств связи требуется на оборудование, выполняющее функции коммутации и маршрутизации, радиопередающее оборудование, цифровые транспортные системы, оборудование используемое для учета объема оказанных услуг. Сертификация средств связи, как правило, требуется для оборудования, используемого провайдерами телекоммуникационных услуг.

Напомним, что одним из условий получения лицензии для осуществления работ со сведениями, составляющими государственную тайну, является наличие на предприятии сертифицированных средств защиты информации. К средствам защиты информации относятся технические, криптографические, программные и другие средства, в которых они реализованы, и средства контроля эффективности защиты информации. Указанные средства подлежат

обязательной сертификации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ РФ.

Организация сертификации средств защиты информации возлагается на ФСТЭК РФ, ФСБ РФ, Минобороны РФ в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утвержденных Правительством РФ и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

ФЗ «Об электронной цифровой подписи» устанавливает обязательность сертификации средств электронной цифровой подписи, используемых в открытых информационных системах, которую осуществляет ФСТЭК.

Кодекс Российской Федерации об административных правонарушениях содержит ряд соответствующих статей, устанавливающих ответственность за нарушение в области сертификации и лицензирования:

— ст. 13.6 Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи, если законом предусмотрена их обязательная сертификация;

— ст. 13.11 Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

— ст. 13.12. Нарушение правил защиты информации, а именно: нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации; использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации; нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну; грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну); нарушение требований о защите информации

4.3 Аттестация объектов информатизации.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России.

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

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

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

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

Аттестация является обязательной в следующих случаях:

— работа со сведениями, составляющими государственную тайну;

— при защите государственного информационного ресурса;

— при управление экологически опасными объектами;

— при ведение секретных переговоров.

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

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

— защита от НСД, в том числе компьютерных вирусов;

— защита от утечки через ПЭМИН;

— защита от утечки или воздействия на информацию за счет специальных устройств, встроенных в объект информатизации.

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

— анализ исходных данных по аттестуемому объекту информатизации;

— предварительное ознакомление с аттестуемым объектом информатизации;

— проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

— проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

— проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

— проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

— анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

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

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

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

В структуру системы аттестации входят:

— федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации — ФСТЭК России;

— органы по аттестации объектов информатизации по требованиям безопасности информации;

— испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

— заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

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

Органы по аттестации:

— аттестуют объекты информатизации и выдают "Аттестаты соответствия";

— осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

— отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

— формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

— ведут информационную базу аттестованных этим органом объектов информатизации;

— осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

— организует обязательную аттестацию объектов информатизации;

— создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

— устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

— организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

— аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

— осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

— рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;

— организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

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

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

Заявители:

— проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

— привлекают органы по аттестации для организации и проведения аттестации объекта информатизации (Приложение 3);

— предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

— привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

— осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия" (Приложение 4);

— извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");

— предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

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

— приемо-сдаточную документацию на объект информатизации;

— акты категорирования выделенных помещений и объектов информатизации;

— инструкции по эксплуатации средств защиты информации;

— технический паспорт на аттестуемый объект;

— документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;

— сертификаты соответствия требованиям безопасности информации на ВТСС;

— сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;

— акты на проведенные скрытых работ;

— протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);

— протоколы измерения величины сопротивления заземления;

— протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;

— данные по уровню подготовки кадров, обеспечивающих защиту информации;

— данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;

— нормативную и методическую документацию по защите информации и контролю эффективности защиты.

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

— пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;

— перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

— перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

— перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;

— перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;

— перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;

— схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;

— технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;

— планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;

— план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

— план-схему системы заземления объекта с указанием места расположения заземлителя;

— план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;

— план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;

— план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;

— схемы систем активной защиты (если они предусмотрены).

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

1) подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности" (Приложение 3). Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.

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

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

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

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

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

— анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и её соответствия требованиям нормативной документации по защите информации;

—определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

— проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

— проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

— проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

— оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

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

Протокол аттестационных испытаний должен включать:

— вид испытаний;

— объект испытаний;

— дату и время проведения испытаний;

— место проведения испытаний;

— перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);

— перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

— методику проведения испытания (краткое описание);

— результаты измерений;

— результаты расчетов;

— выводы по результатам испытаний.

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

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

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

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

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

Аттестат соответствия должен содержать:

— регистрационный номер;

— дату выдачи;

— срок действия;

— наименование, адрес и местоположение объекта информатизации;

— категорию объекта информатизации;

— класс защищенности автоматизированной системы;

— гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации;

— организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;

— номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;

— перечень руководящих документов, в соответствии с которыми проводилась аттестация;

— номер и дата утверждения заключения по результатам аттестационных испытаний;

— состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;

— организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;

— перечень действий, которые запрещаются при эксплуатации объекта информатизации;

— список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.

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

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

Нормативно-правовые документы.

ФЗ от 8 августа 2001 №128-ФЗ «О лицензировании отдельных видов деятельности»

ФЗ от 27 декабря 2002 №184-ФЗ «О техническом регулировании»

Указ Президента РФ от 9 января 1996 г. №21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ, вывоза за её пределы, а также использования специальных технических средств, предназначенных для негласного получения информации»

Постановление Правительства РФ от 15 апреля 1995 №333 «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»

Постановление Правительства РФ от 26 июня 1995 №608 «О сертификации средств защиты информации»

Постановление Правительства РФ от 21 ноября 2011 №957 «Об организации лицензирования отдельных видов деятельности»

Постановление Правительства РФ от 3 февраля 2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации»

Постановление Правительства РФ от 3 марта 2012 №171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»

Постановление Правительства РФ от 16 апреля 2012 №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, 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»

ФСТЭК от 25 ноября 1994г. «Положение по аттестации объектов информатизации по требованиям безопасности информации»

Вопросы для самоконтроля

1) Перечислите основные организационные методы регулирования в области информационной безопасности со стороны государства.

2) Что такое технический регламент и стандарт?

3) Что такое подтверждение соответствия?

4) Для каких видов деятельности в области защиты информации необходима лицензия?

5) Перечислите полномочия государственных органов по лицензированию в области защиты информации.

6) Перечислите необходимые мероприятия для получения лицензии предприятием на деятельность связанную с защитой государственной тайны.

7) Что такое аттестация руководителя предприятия?

8) Перечислите органы уполномоченные на ведение лицензионной деятельности по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

9) Что образует систему сертификации?

10) Что такое сертификат соответствия?

11) Перечислите органы по сертификации.

12) Что такое аттестация объектов информатизации?

13) В каких случаях необходима обязательная аттестация? Что такое добровольная аттестация?

14) Перечислите список работ для проведения аттестации объекта информатизации

15) Что входит в систему аттестации?

16) Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

17) Что содержит аттестат соответствия?

ТЕМА 5 ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ.

Движущей силой научно-технического прогресса является интеллектуальное творчество как одна из предпосылок социального, экономического и культурного развития общества. При надежной охране интеллектуальной собственности повышается уровень стимулирования авторов, что, в свою очередь, способствует увеличению количества творческих произведений и в целом ускоряет социально-экономическое развитие страны.

Высокая доходность и доступность интеллектуальной собственности стала особенно привлекательной для дельцов «теневой» экономики. Преступность в данной сфере приняла устойчивые организационные формы. Налажены нелегальные каналы получения, производства копий и распространения программных продуктов, аудио-видеопродукции. Простота производства нелегальных копий продуктов, низкий уровень правосознания общества способствуют получению крупной прибыли при минимальных издержках.

Введение в качестве объекта охраны программ для ЭВМ и баз данных явилось следствием изменения отношения к продуктам интеллектуальной деятельности человека, оно стало более «рыночным», а сами продукты интеллектуальной деятельности приобрели черты товара (продукта интеллектуального труда, созданного для функционирования его на рынке).

Результатами интеллектуальной деятельности и приравненным к ним средствам индивидуализации юридических лиц, товаров, работ, услуг и предприятий, 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;

15) наименования мест происхождения товаров;

16) коммерческие обозначения.

Интеллектуальная собственность – совокупность прав на продукт интеллектуального творчества. Владение, пользование, распоряжение плодами творчества носит такой же специфический характер, как и само понятие интеллектуальной собственности. С точки зрения права, к интеллектуальной собственности относится авторское право, которое и необходимо защищать. Применительно к области информатизации таким правом является авторское право на программы для ЭВМ и базы данных.

Понятие «право собственности» в объективном смысле представляет собой совокупность правовых норм, регулирующих отношения собственности в данном обществе и действительно для всех членов общества, а нарушение этих норм влечет за собой применение принудительных санкций государства.

Право интеллектуальной собственности не является разновидностью права собственности. Это два различных правовых института. Под интеллектуальной собственностью понимают исключительные права на нематериальные объекты, тогда как право собственности относится к вещным правам.

Конституцией РФ каждому гражданину гарантируется свобода литературного, художественного, научного, технического и других видов

творчества, преподавания. Интеллектуальная собственность охраняется законом.

Базовыми нормативными документами, регламентирующими общественные отношения, связанные результатами интеллектуальной деятельности и средствами индивидуализации, являются международные договоры, ратифицированные СССР и Россией, а так же Гражданский Кодекс РФ (часть 4).

Нарушение авторских прав подразумевает несанкционированное правообладателем распространение материала, защищенного авторским правом, такого как программное обеспечение, музыкальные композиции, фильмы, книги, компьютерные игры. Обладание правами на интеллектуальную собственность защищено законами большинства стран.

Под нарушением авторских прав обычно понимаются следующие действия:

— создание копии и ее продажа;

— создание копии и передача ее кому-либо еще;

— в некоторых случаях перепродажа легально приобретенной копии.

Незаконное использование произведений либо иное нарушение авторских прав влечет за собой гражданско-правовую, административную, уголовную ответственность в соответствии с законодательством Российской Федерации.

В частности обладатели исключительных авторских прав вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации.

Уголовный кодекс Российской Федерации в главе 19 «Преступления против конституционных прав и свобод человека и гражданина» предусматривает уголовную ответственность за нарушение авторских и смежных прав.

Статья 146 УК РФ определяет, что незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, наказываются штрафом в размере до 200 т.р

или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 480 часов, либо лишением свободы на срок до 2 лет.

5.1 Объекты и субъекты правовой охраны

Автором результата интеллектуальной деятельности признается физическое лицо, творческим трудом которого создан такой результат. Не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в создание такого результата, в том числе оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь либо только способствовавшие оформлению прав на такой результат или его использованию, а также граждане, осуществлявшие контроль за выполнением соответствующих работ.

Автору результата интеллектуальной деятельности принадлежит право авторства, а в случаях, предусмотренных Гражданским Кодексом РФ, право на имя и иные личные неимущественные права.

Право авторства, право на имя и иные личные неимущественные права автора неотчуждаемы и непередаваемы. Отказ от этих прав ничтожен.

Авторство и имя автора охраняются бессрочно. После смерти автора защиту его авторства и имени может осуществлять любое заинтересованное лицо, за исключением случаев, предусмотренных пунктом 2 статьи 1267 и пунктом 2 статьи 1316 ГК РФ.

Исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также может перейти к другим лицам по иным основаниям, установленным законом. Права на результат интеллектуальной деятельности, созданный совместным творческим трудом двух и более граждан (соавторство), принадлежат соавторам совместно.

Правообладатель — автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительными имущественными правами, полученными в силу закона или договора.

Авторское право охраняет произведение как систему идей, мыслей и образов именно в связи с возможностью его воспроизведения. Поэтому авторское право на произведение науки, литературы и искусства сохраняется даже в случае гибели того материального носителя, в котором оно было воплощено.

Однако не всякое произведение как результат мыслительной деятельности человека охраняется нормами авторского права. Объектами авторского права признаются лишь такие произведения, которые обладают предусмотренными законом признаками. Такими признаки являются творческий характер произведения и объективная форма его выражения.

Показателем творческого характера произведения, по мнению большинства российских ученых, является его новизна. Новизна в данном случае рассматривается как синоним оригинальности произведения. Она может выражаться в новом содержании, в новой форме произведения, в новой идее и т.п. Произведение как результат творческой деятельности автора становится объектом авторского права лишь при условии, что оно выражено в какой-либо объективной форме. Иными словами, произведение должно существовать в форме, которая отделена от личности автора и приобрела самостоятельное бытие.

Не являются объектами авторских прав:

1) официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы; Однако следует иметь в виду, что до тех пор, пока, например, закон не принят в качестве

официального нормативного документа, его проект практически представляет собой охраняемое литературное произведение

2) государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований;

3) произведения народного творчества (фольклор), не имеющие конкретных авторов; произведения народного творчества не могут выступать объектами авторских прав, так как в этом случае просто не представляется возможным установить их автора.

4) сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

Авторские правоотношения предполагают множество их участников. В них участвуют, с одной стороны, авторы произведений и их наследники, с другой стороны, организации, заинтересованные в их использовании (издательства, театры, киностудии и т.д.). Субъекты авторского права, в широком понимании, — это лица, участвующие в авторских правоотношениях. При таком определении субъектами авторского права будут являться лица, которым могут принадлежать авторские права, организации по защите авторских прав и другие субъекты. Субъекты авторского права, в узком понимании, — это авторы произведений, то есть обладатели личных авторских прав.

Субъекты авторских и смежных прав подразделяются на две группы:

1) субъекты с первоначальными правами (авторы, исполнители, производители фонограмм, организации вещания);

2) правопреемники (наследники, организации-правопреемники, государство);

Автор — главный субъект авторского права. Ни возраст, ни пол, ни раса (национальность) не имеют значение для признания лица автором. При этом авторская правоспособность возникает с момента рождения. Однако нужно учитывать, что право распоряжаться авторскими трудами тесно связано с понятием дееспособности. В соответствии ГК РФ без согласия родителей,

усыновителей и попечителей осуществлять права автора на произведение науки, литературы или искусства могут несовершеннолетние, достигшие возраста 14 лет.

Важно отметить, что для возникновения авторского права не имеет значение и дееспособность лица, т.е. автором может быть и лицо, признанное по действующему гражданскому законодательству недееспособным, но может быть ограничено его право распоряжаться результатами авторского труда (совершать сделки по отчуждению имущественных прав).

После смерти автора субъектами авторского права становятся его наследники, но наследуются не все права. По наследству не переходят: право авторства, право на авторское имя и право на защиту репутации автора.

Субъектом авторского права является также переводчик произведения на другой язык и автор другого производного произведения. Авторское право переводчика распространяется не на само произведение, которое он переводит, а только на созданный им перевод. При этом авторское право переводчика не препятствует другим лицам осуществлять свои собственные переводы. В данном случае имеется в виду не только перевод на другой язык отдельных слов или выражений, а перевод, соединенный с литературной обработкой текста с сохранением смыслового содержания произведения. Аналогичные права возникают и в отношении авторов других производных произведений (переделок, аранжировок или других переработок).

Информация, являющаяся результатом интеллектуальной деятельности, может охраняться и с позиции правового режима коммерческой или служебной тайны (например, сведения о технологии производства, внедрении изобретений). Служебная или коммерческая тайна обладает наибольшей универсальностью среди других объектов интеллектуальной собственности, поскольку под понятие служебной или коммерческой тайны могут быть подведены самые разнообразные сведения, связанные с производственной, управленческой, финансовой и другой деятельности.

Напомним, что информация составляет коммерческую или служебную тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране её конфиденциальности. Решение о наличии действительной или потенциальной коммерческой ценности информации, содержание и объем соответствующих сведений, а также срок её охраны определяются предпринимателем самостоятельно. Кроме того, коммерческая или служебная тайна как объект интеллектуальной собственности не требует официального признания её охраноспособности, выполнения каких-либо формальностей.

В целом, борьба с преступлениями в сфере интеллектуальной собственности в ближайшем будущем приобретет еще большую актуальность, так как с каждым днём возрастает значимость объектов интеллектуальной собственности, что обусловлено требованиями научно-технического прогресса, экономическим и социальным развитием России.

5.2 Неимущественные и имущественные права автора, авторский договор.

Содержанием любого авторского договора является передача имущественных прав, а объект (предмет) этого договора — имущественные авторские права. Личные неимущественные права принадлежат автору независимо от его имущественных прав и сохраняются за ним в случае уступки исключительных прав на использование произведения и не могут отчуждаться в пользу третьих лиц.

Автору в отношении его произведения принадлежат следующие личные *неимущественные права*:

— право признаваться автором произведения (право авторства);

— право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, то есть анонимно (право на имя);

— право обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;

— право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Имущественными правами именуются исключительные права автора на осуществление или разрешение действий по использованию произведения в любой форме и любым способом.

Исключительные права автора на использование произведения означают его право осуществлять или разрешать следующие действия:

— воспроизведение произведений;

— публичное исполнение и публичное оповещение произведений;

— публичную демонстрацию и публичный показ;

— любое повторное оповещение произведений, если оно осуществляется иной организацией, чем та, которая осуществила первое оповещение;

— переводы произведений;

— переработка, адаптация, аранжировка и иные изменения произведений;

— включение произведений как составных частей в сборники, антологии, энциклопедии и т.п.;

— распространение произведений путем первой продажи, отчуждение иным способом или путем сдачи в имущественный найм, в прокат или путем иной передачи в продажу экземпляров произведения;

— сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения путем передачи в эфир и (или) последующей передачи в эфир (право на передачу в эфир);

— сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения по кабелю, проводам или с помощью иных аналогичных средств (право на сообщение для всеобщего сведения по кабелю);

— сообщать произведение, таким образом, при котором любое лицо может иметь доступ к нему в интерактивном режиме из любого места и в любое время по своему выбору (право на доведение до всеобщего сведения);

— сдача в имущественный найм и (или) коммерческий прокат после первой продажи, отчуждение иным способом оригинала или экземпляров аудиовизуальных произведений, компьютерных программ, без данных, музыкальных произведений в нотной форме, а также произведений, зафиксированных в фонограмме или видеограмме или в форме, которую считывает компьютер;

— импорт экземпляров произведений.

Имущественные права на использование созданного произведения могут принадлежать как автору, так и другим лицам в зависимости от волеизъявления автора или правового статуса созданного произведения. Юридическому лицу (индивидуальному предпринимателю) могут принадлежать имущественные права на использование произведения, созданного в порядке выполнения работниками служебных обязанностей или служебного задания (служебное произведение).

Авторский договор – это двусторонняя сделка, в соответствии с которой автор передает или обязуется передать приобретателю свои права на использование произведения в пределах и на условиях, согласованных сторонами. Все права, прямо не переданные по авторскому договору, являются не переданными.

А вторский договор выступает основной правовой формой, в рамках которой автор имеет возможность трудиться над созданием произведений. Вместе с тем, автор может создавать то или иное произведение в рамках трудовых отношений с организацией, которая нуждается в использовании его произведений. В этих случаях правовой формой, опосредствующей использование произведений

автора, выступает трудовой договор. В связи с этим вполне закономерно возникает вопрос о разграничении этих договоров. Несмотря на то, что и по трудовому и по авторскому договору могут издаваться одни и те же произведения, содержание этих договоров различно: в одном случае отношения регулируются нормами трудового права, в другом – гражданского. Насколько позволяет характер творчества, автор сам избирает форму взаимоотношений с организацией.

Классификация авторских договоров:

— договор на создание и использование литературных, художественных, аудиовизуальных и иных произведений;

— договор на готовое произведение;

— договор на создание произведения. Одна сторона (автор – писатель, художник и т.п.) обязуется создать объект права интеллектуальной собственности в соответствии с требованиями второй стороны (заказчика) и в установленный срок. Договор о создании по заказу и использовании объекта права интеллектуальной собственности должен определять способы и условия использования этого объекта заказчиком. Оригинал произведения изобразительного искусства, созданного по заказу, переходит в собственность заказчика. При этом имущественные права на это произведение остаются за его автором, если иное не установлено договором. Условия договора о создании по заказу и использовании объекта права интеллектуальной собственности, ограничивающие права автора, являются недействительными;

— договор о передаче неисключительных прав. Права, приобретаемые в таком договоре покупателем, являются относительными: они действуют только по отношению к продавцу и не дают покупателю никаких прав по пресечению использования произведения третьими лицами. Поскольку авторский договор может предусматривать передачу разных видов имущественных прав, следует учитывать, что некоторые из них могут передаваться как исключительные, другие как неисключительные;

— договор о передаче исключительных прав. По договору одна сторона (лицо, имеющее исключительные имущественные права) передает второй стороне частично или в полном объеме эти права в соответствии с законом и на определенных договором условиях;

— издательский договор. В соответствии с ним стороны осуществляют издание и переиздание любых произведений, которые могут быть зафиксированы на бумаге, т.е. произведений литературы (научных, художественных, учебных и т.п.), драматических, сценарных, музыкальных произведений и т.д.;

— постановочный договор. Его предметом могут быть драматические произведения, музыка или либретто оперы, балета, оперетты и т.п., которые используются театрально-зрелищными организациями (театрами, филармониями, цирками и т.д.) путем постановки на сцене. Особый акцент следует сделать на том, что произведения, в отношении которых заключается постановочный договор, могут быть как необнародованными, так и уже известными публике;

— сценарный договор. Определяется тем, что отношения, которые он регламентирует, порождаются необходимостью использования текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие и т.д. Сценарный договор близок к постановочному, однако их главным отличием является то, что литературный сценарий дополняется, изменяется и перерабатывается для того, чтобы быть максимально приближенными к нуждам кинематографа. В то время как постановочный договор регулирует отношения, возникающие между сторонами при публичном исполнении произведения;

— договор о депонировании рукописи. Он заключается при передаче произведения на хранение в специальный информационный орган. Договором регулируются условия и порядок обнародования и дальнейшего использования произведения;

— договор художественного заказа. Он заключается с целью публичной демонстрации произведений изобразительного искусства, которые изготавливаются авторами по заказам организаций и частных лиц и переходят в собственность последних.

При защите интеллектуальных прав выделяют следующие институты гражданского права:

1) Авторское право;

2) Права, смежные с авторскими;

3) Патентное право;

4) Право на селекционное достижение;

5) Право на топологии интегральных микросхем;

6) Право на секрет производства (ноу-хау);

7) Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий;

8) Право на использование результатов интеллектуальной деятельности в составе единой технологии.

5.3 Защита программ и баз данных.

В настоящее время программы для компьютеров и базы данных превратились в универсальный инструмент для решения различных инженерно-технических, экономических, логических и информационно-поисковых задач. На первом этапе создания информационных систем техническое обеспечение (аппаратные средства) являлось приоритетным направлением их развития.

В связи с появлением и распространением персональных компьютеров, программное обеспечение стало пользоваться самостоятельным спросом. Появились программы, которые позволили применять компьютер для решения различного рода прикладных задач. Широкое распространение получили обучающие и игровые программы.

В условиях становления информационного общества программное обеспечение становится товаром, приносящим немалую прибыль. В развитых

странах пользователи информационных технологий вынуждены тратить значительную долю средств на покупку и обновление программного обеспечения. Разработка нового программного обеспечения – длительный и дорогостоящий процесс, требующий затрат на оплату высококвалифицированных специалистов. По ряду оценок, на разработку программного обеспечения приходится около 70% всех возможных производственных затрат в сфере информационных технологий.

В силу того что изготовление копий экземпляров программ – процесс технически несложный и постоянно совершенствующийся, он не поддается жесткому контролю. Незаконное же использование программного обеспечения наносит громадный ущерб разработчикам и поставщикам программного продукта. Поэтому фирмы – производители программного обеспечения объединяются в ассоциации и союзы, которые позволяют им более эффективно защищать свои права на интеллектуальный продукт.

В России алгоритмы и программы для компьютеров приобрели значение торговой продукции. Эта продукция соединяет в себе результаты интеллектуального творчества и индустриального труда большой сложности. Законодательство приравнивает компьютерные программы к произведениям науки, литературы и искусства.

На основании действующего законодательства объектами права являются программы для компьютера и базы данных. Предпосылкой охраноспособности является оригинальность программы и базы данных, т.е. они должны быть продуктом личного интеллектуального творчества автора. Творческий характер деятельности автора предполагается до тех пор, пока не доказано обратное.

Программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

База данных — это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Авторское право распространяется на любые программы для компьютеров и базы данных, как выпущенные, так и не впущенные в свет, представленные в объективной форме независимо от материального носителя. Любая передача прав на материальный носитель не влечет за собой передачи каких-либо авторских полномочий.

Базы данных охраняются независимо от того, являются ли данные, на которых они основаны или которые они включают, объектами авторского права. Охрана не распространяется на идеи и принципы, лежащие в основе программ и баз данных, в том числе на идеи и принципы организации интерфейса и алгоритма, а также на языки программирования.

Для признания авторского права на программу для ЭВМ или базу данных (БД) не требуется регистрации или соблюдения иных формальностей. Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, использовать знак охраны авторского права ©.

Авторское право действует с момента создания программы для ЭВМ или базы данных (БД) в течение всей жизни автора и 70 лет после его смерти. Правообладатель в течение срока действия авторского права может по своему желанию зарегистрировать программу для ЭВМ или базу данных (БД) в патентном ведомстве Российской Федерации. Смысл регистрации — показать, что на момент регистрации программный продукт существовал в объективном виде. Это может понадобиться при столкновении интересов или оспаривании авторства программного продукта.

Личные неимущественные права принадлежат только автору, к ним относятся:

1) Право авторства на программу и базу данных;
2) Право на имя, право определить форму указания имени автора;

3) Право на неприкосновенность (целостность) произведения и их названий от искажений и иных посягательств, способных нанести ущерб чести и достоинству (право на защиту репутации);

4) Право обнародовать или разрешать обнародование произведения, включая право на отзыв произведения. Обязательным условием отзыва произведения является возмещение пользователю причиненных таким решением убытков.

Исключительное право (т.е. имущественные права) может принадлежать как автору программы или базы данных, так и любому другому правообладателю. Им принадлежит исключительное право осуществлять и разрешать осуществление следующих действий:

1) Выпуск в свет программ для компьютера и баз данных;

2) Воспроизведение программ или базы данных в любой форме и любыми способами;

3) Распространение — предоставление доступа к программам или базам данных, воспроизведенным в любой форме, в том числе сетевыми или иными способами;

4) Модификация — переработка программы или базы, включающая в себя и перевод с одного языка на другой;

5) Публичный показ оригинала или экземпляра программы или базы данных;

6) Декомпилирование — технический приём, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы;

7) Распространение экземпляров программы или базы данных путем сдачи в прокат.

Особым образом регулируются отношения по поводу *служебных произведений* — произведений, которые создаются автором в порядке выполнения им служебных обязанностей или по заданию работодателя. Закон устанавливает, что исключительное право на служебное произведение принадлежит работодателю, если иное не оговорено в договоре между

сторонами. По российскому законодательству право авторства является неотъемлемым. Но у работодателя также возникает право указывать свое наименование при любом использовании произведения. На практике, в соответствии с договором, к работодателю может переходить право на неприкосновенность, обнародование и отзыв произведения.

Перепродажа или пересдача иным способом права собственности на экземпляр программы или базы данных после первой продажи или другой передачи права собственности допускается без согласия правообладателя и без выплаты ему дополнительного вознаграждения.

Имущественные права могут быть переданы автором полностью или частично любому физическому или юридическому лицу. Передача имущественных прав должна быть оформлена на основании договора или контракта, который заключается в письменном виде. В договоре должны быть обязательно оговорены следующие основные условия: объем и способы использования, порядок выплаты вознаграждения и срок действия договора, а также территория, на которой используется данный продукт.

Основополагающие принципы борьбы с пиратством:

— программы для ЭВМ и базы данных относятся к объектам авторского права;

— автору или иному правообладателю принадлежит исключительное право осуществлять и/или разрешать выпуск в свет, воспроизведение, распространение и иное использование программы для ЭВМ или базы данных;

— имущественные права на программные продукты могут быть переданы кому-либо только по договору;

— незаконное использование программ для ЭВМ либо иное нарушение авторских прав на программы для ЭВМ влечет за собой гражданско-правовую, административную, уголовную ответственность.

Таким образом, использование программы для ЭВМ кем бы то ни было (т.е. любым пользователем) в соответствии с законом должно осуществляться на основании договора с правообладателем. Лицо, правомерно владеющее

экземпляром программы для ЭВМ, вправе осуществлять ее запись в память одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем.

Использование программных продуктов без разрешения правообладателя нарушает имущественные права на интеллектуальную собственность и, следовательно, является правонарушением.

Наряду с охраной программ для ЭВМ в последние годы приобрел актуальность вопрос об охране произведений, создаваемых при помощи ЭВМ.

Если первоначально в юридической литературе господствовало мнение, согласно которому созданный ЭВМ продукт не может считаться творческим произведением, а значит, и объектом авторского права, то сейчас под влиянием достигнутого прогресса данная позиция разделяется далеко не всеми.

Заявка на официальную регистрацию программы для ЭВМ или базы данных, должна относиться к одной программе или одной базе данных. В ней должны содержаться следующие сведения:

— заявление на официальную регистрацию программы для ЭВМ или базы данных с указанием правообладателя, а также автора, если он не отказался быть упомянутым в качестве такового, и их местонахождения (местожительства);

— депонируемые материалы, идентифицирующие программу для ЭВМ или базу данных, включая реферат;

— документ, подтверждающий уплату государственной пошлины в установленном размере или основания для освобождения от уплаты государственной пошлины.

Охрана авторского права начинается с момента создания произведения в зафиксированной форме. Авторское право на авторское произведение немедленно становится собственностью лица, создавшего данное произведение. Только автор или те, кто приобретает свои права через автора, могут законно притязать на авторское право.

Регистрация авторского права — это юридическая формальность, служащая для создания публичного акта об основных фактах по конкретному

авторскому праву. Однако охрана авторского права не обусловливается регистрацией. Для охраны авторского права регистрация не требуется, в законодательстве об авторском праве предусмотрен ряд стимулов или выгод, которые могут побудить обладателей авторского права оформить регистрацию. Регистрация осуществляется только физическими лицами (независимо от того, кому принадлежат исключительные права на произведение — физическому или юридическому лицу). За регистрацию взимается плата. Автору произведения выдается свидетельство, которое может быть использовано в качестве доказательства при разбирательствах в судах. Но при этом следует иметь в виду, что сам факт регистрации не создает авторского права.

Нормативно-правовые документы

«Парижская конвенция по охране промышленной собственности» (Заключена в г. Париже 20.03.1883. Конвенция вступила в силу в 07.07.1884. СССР ратифицировал Конвенцию с оговоркой и заявлением). Конвенция вступила в силу для СССР 01.07.1965

«Бернская конвенция об охране литературных и художественных произведений» (Берн, 09.09.1886. Вступила в силу для России 13.03.1995)

Гражданский Кодекс РФ (часть четвертая) от 18.12.2006 №230-ФЗ

Указ Президента РФ от 7 октября 1993 №1607 «О государственной политике в области охраны авторского права и смежных прав»

Вопросы для самоконтроля.

1) Какие нормативно-правовые акты лежат в основе правовой охраны интеллектуальной собственности?
2) Что понимается под интеллектуальной собственностью?
3) Что означают понятия «база данных» и «программа для ЭВМ»?
4) Что является сферой деятельности авторского права?
5) Что является объектом авторского права? Какие произведения не являются объектами авторского права?

6) Приведите перечень субъектов, обладающих авторским правом.

7) Какие личные неимущественные права принадлежат автору в отношении его произведений?

8) Что означают исключительные права автора на использование произведения?

9) Какие личные права принадлежат автору программы для ЭВМ или базы данных?

10) Обязательна ли регистрация программы для ЭВМ или базы данных?

ТЕМА 6. КЛАССИФИКАЦИЯ УГРОЗ ОБЪЕКТОВ ЗАЩИТЫ

Информация может существовать в различных формах в виде совокупности некоторых символов (знаков) на носителях различных типов. В связи с бурным развитием информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи. В дальнейшем будут рассматриваться только те формы представления информации, которые используются при ее автоматизированной обработке.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Таким образом, АС представляет собой совокупность следующих компонентов:

— технических средств обработки и передачи информации;

— программного обеспечения;

— самой информации на различных носителях;

— обслуживающего персонала и пользователей системы.

Одним из основных аспектов проблемы обеспечения безопасности АС является определение, анализ и классификация возможных угроз конкретной АС. Перечень наиболее значимых угроз, оценка их вероятности и модель злоумышленника являются базовой информацией для построения оптимальной системы защиты.

6.1. Классификация угроз безопасности информации

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. *Угроза информационной безопасности АС* – это возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к нарушению конфиденциальности, целостности или доступности

этой информации, а также возможность воздействия на компоненты АС, приводящего к их утрате, уничтожению или сбою функционирования.

Источник угрозы безопасности информации – субъект, являющийся непосредственной причиной возникновения угрозы безопасности информации.

Основными источниками нарушения безопасности в АС являются:

— аварии и стихийные бедствия (пожар, землетрясение, ураган, наводнение и т.п.);

— сбои и отказы технических средств;

— ошибки проектирования и разработки компонентов АС (программных средств, технологий обработки данных, аппаратных средств и др.);

— ошибки эксплуатации;

— преднамеренные действия нарушителей.

Существует много критериев классификации угроз. Рассмотрим наиболее распространенные из них.

1) по природе возникновения: естественные и искусственные

Естественные угрозы - это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека. В свою очередь *искусственные угрозы* - это угрозы АС, вызванные деятельностью человека.

2) по степени мотивации: непреднамеренные (случайные) и преднамеренные. Первые связаны с разного рода ошибками – в проектировании АС, в программном обеспечении, ошибки персонала при работе с АС и т.п. Вторая группа связана с корыстными, идейными и другими целями людей, в данном случае, злоумышленников. Поводом может быть получение материальной выгоды, месть, моральные убеждения и пр.

К основным *случайным угрозам* можно отнести следующее:

— неумышленные действия, приводящие к нарушению нормального функционирования системы, либо ее полной остановке. В эту категорию также относится повреждение аппаратных, программных, информационных ресурсов

системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

— неумышленное отключение оборудования;

— неумышленная порча носителей информации;

— использование программного обеспечения, способного при неверном использовании привести к нарушению работоспособности системы (зависанию) или к необратимым изменениям в системе (удаление файлов, форматирование и т.п.);

— использование программ, которые не нужны для выполнения должностных обязанностей. К ним могут быть отнесены игровые, обучающие и др. программы, использование которых может привести к неумеренному расходу ресурсов системы, в частности, оперативной памяти и процессора;

непреднамеренное заражение компьютера вирусами;

— неосторожные действия, влекущие за собой разглашение конфиденциальной информации;

— ввод ошибочных данных;

— утрата, передача кому-то или разглашение идентификаторов, к которым относятся пароли, ключи шифрования, пропуски, идентификационные карточки;

— построение системы, технологии обработки данных, создание программ с уязвимостями;

— несоблюдение политики безопасности или других установленных правил работы с системой;

— отключение или некорректное использование средств защиты персоналом;

— пересылка данных по ошибочному адресу абонента (устройства).

К основным *преднамеренным угрозам* можно отнести следующее:

— физическое воздействие на систему или отдельные ее компоненты (устройства, носители, люди), приводящее к выходу из строя, разрушению, нарушению нормального функционирования;

— отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

— действия по нарушению нормальной работы системы (изменение режимов работы устройств или программ, создание активных радиопомех на частотах работы устройств системы и т.п.);

— подкуп, шантаж и другие пути воздействия на персонал или отдельных пользователей, имеющих определенные полномочия;

— применение подслушивающих устройств, дистанционная фото- и видео-съемка и т.п.;

— перехват ПЭМИН;

— перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

— хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

— несанкционированное копирование носителей информации;

— хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

— чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

— чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

— незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

— несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

— вскрытие шифров криптозащиты информации;

— внедрение аппаратных "спецвложений", программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему зашиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

— незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

— незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Рассмотрим другие критерии классификации угроз:

3) по положению относительно контролируемой зоны: внутренние и внешние угрозы. В качестве примера внешних угроз может быть перехват данных , передаваемых по сети или утечка через ПЭМИН. К внутренним угрозам можно отнести хищение носителей с конфиденциальной информацией, порчу оборудования, применение различного рода закладок.

4) по степени воздействия на АС: пассивные и активные. Пассивные угрозы – угрозы, не нарушающие состав и нормальную работу АС. Пример –

копирование конфиденциальной информации, утечка через технические каналы утечки, подслушивание и т.п. Активная угроза, соответственно, нарушает нормальное функционирование АС, ее структуру или состав.

5) по виду нарушаемого свойства информации - конфиденциальности, доступности, целостности.

К угрозам доступности можно отнести как искусственные, например, повреждение оборудования из-за грозы или короткого замыкания, так и естественные угрозы. В настоящее время широко распространены сетевые атаки на доступность информации – DDOS-атаки, которые мы рассмотрим в ходе данного курса более подробно.

В последнее время в специальной литературе всё чаще говорится о динамической и статической целостностях. К угрозам статической целостности относится незаконное изменение информации, подделка информации, а также отказ от авторства. Угрозами динамической целостности является нарушение атомарности транзакций, внедрение нелегальных пакетов в информационный поток и т.д.

Также важно отметить, что не только данные являются потенциально уязвимыми к нарушению целостности, но и программная среда. Заражение системы вирусом может стать примером реализации угрозы целостности.

К угрозам конфиденциальности можно отнести любые угрозы, связанные с незаконным доступом к информации, например, перехват передаваемых по сети данных с помощью специальной программы или неправомерный доступ с использованием подобранного пароля. Сюда можно отнести и "нетехнический" вид угрозы, так называемый, "маскарад" - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

6) по типу системы, на которую направлена угроза: системы на базе автономного рабочего места и система, имеющая подключение к сети общего пользования.

7) по способу реализации: несанкционированный доступ (в том числе случайный) к защищаемой информации, специальное воздействие на информацию, утечка информации через технические каналы утечки.

Наиболее распространенными являются классификации по способу реализации и по виду нарушаемого свойства информации.

Компании, занимающиеся разработками в области информационной безопасности, регулярно проводят аналитические исследования по утечкам информации. Результаты публикуются на их официальных сайтах. Приведем некоторую статистику из ежегодного аналитического отчета компании "InfoWath" за 2014 год. Согласно отчету, в 2014 году соотношение случайных и намеренных утечек составило 650/50 (рис. 6.1), что говорит о необходимости применения защитных мер не только от умышленных действий нарушителей, но и от случайных угроз.

Рис. 6.1. Соотношение случайных и умышленных утечек в 2014

Соотношение каналов утечки сильно зависит от типа носителя информации – рис 6.2.

Рис. 6.2. Распределение случайных и умышленных утечек по каналам.

В случае обработки защищаемой информации на компьютере преобладают умышленные утечки, а в случае использования бумажного носителя и доступа по сети – случайные. Неосторожная работа сотрудника с принтером зачастую приводит к утечке конфиденциальной информации: распечатал документ и забыл его, отправил не на тот сетевой принтер, проставил не тот адрес при автоматической распечатке и рассылке писем.

Для специалиста в области информационной безопасности важно знать критерии классификации угроз и их соотношение с целью систематизации своих знаний при построении системы защиты, в частности, проведения оценки рисков и выбора оптимальных средств защиты.

6.2 Методы оценки угроз

При определении угроз на конкретном объекте защиты важно понимать, что нельзя учесть абсолютно все угрозы, а тем более защититься от них. Здесь уместно говорить о принципе разумности и достаточности. При идентификации угрозы необходимо установить все возможные источники этой угрозы, так как зачастую угроза возникает вследствие наличия определенной уязвимости и может быть устранена с помощью механизма защиты (например, механизм

аутентификации). К идентификации угроз можно подходить двумя путями – по уязвимостям, повлекшим за собой появление угрозы, или по источникам угроз.

Опасность угрозы определяется риском в случае ее успешной реализации. Риск – потенциально возможный ущерб. Допустимость риска означает, что ущерб в случае реализации угрозы не приведет к серьезным негативным последствиям для владельца информации. Ущерб подразделяется на опосредованный и непосредственный. Непосредственный связан с причинением материального, морального, финансового , физического вреда владельцу информации. Опосредованный (косвенный) ущерб связан с причинением вреда государству или обществу, но не владельцу информации.

Для оценки рисков целесообразно привлекать экспертов - специалистов в области информационной безопасности, которые должны обладать:

— знаниями законодательства РФ, международных и национальных стандартов в области обеспечения информационной безопасности;

— знаниями нормативных актов и предписаний регулирующих и надзорных органов в области обеспечения информационной безопасности;

— знаниями внутренних документов организации, регламентирующих деятельность в области обеспечения информационной безопасности;

— знаниями о современных средствах вычислительной и телекоммуникационной техники, операционных системах, системах управления базами данных, а также о конкретных способах обеспечения информационной безопасности в них;

— знаниями о возможных источниках угроз ИБ, способах реализации угроз ИБ, частоте реализации угроз ИБ в прошлом;

— пониманием различных подходов к обеспечению информационной безопасности, знания защитных мер, свойственных им ограничений.

Существуют различные методы оценки риска, образующие два взаимодополняющих друг друга вида – количественный и качественный.

Целью *количественной оценки* риска является получение числовых значений потенциального ущерба для каждой конкретной угрозы и для

совокупности угроз на защищаемом объекте, а также выгоды от применения средств защиты. Основным недостатком данного подхода является невозможность получения конкретных значений в некоторых случаях. Например, если в результате реализации угрозы наносится ущерб имиджу организации, непонятно, как количественно оценить подобный ущерб.

Рассмотрим количественный подход боле подробно на примере метода оценки рисков, предлагаемого компанией Microsoft. При количественной оценке рисков необходимо определить характеристики и факторы, указанные ниже.

Стоимость активов. Для каждого актива организации, подлежащего защите, вычисляется его денежная стоимость. Активами считается все, что представляет ценность для организации, включая как материальные активы (например, физическую инфраструктуру), так и нематериальные (например, репутацию организации и цифровую информацию). Часто именно стоимость актива используется для того, чтобы определить меры безопасности для конкретного актива. Для назначения стоимости конкретному активу необходимо определить следующее:

— общая стоимость актива для организации. Например, веб-сервер, обрабатывающий заказы покупателей в Интернет-магазине. Пусть он при работе круглый год и круглосуточно приносит в среднем 2000 рублей в час, тогда в год - 17 520 000 рублей.

— ущерб в случае потери актива (в частности, выхода из строя). Допустим, рассматриваемый выше веб-сервер вышел из строя на 7 часов. При расчете делается допущение, что каждый час он приносит одинаковую прибыль, тогда за 7 часов простоя (например, в случае успешной DoS-атаки) убыток составит 7000 рублей.

— косвенный ущерб в случае потери актива. В описанном выше случае компания, которая владеет Интернет-магазином, может потерпеть убытки в результате негативного отношения покупателей к выходу из строя веб-сервера. Естественно, расчет косвенных убытков является наиболее трудной задачей и почти никогда не бывает точным. Допустим, чтобы восстановить репутацию,

компания должна потратить 100 000 на рекламу Интернет-магазина и ожидает, что годовой объем продаж упадет на 0.5 процентов, то есть на 87 600 рублей. Сложив две полученные величины, получим косвенный ущерб в виде 187 600 рублей.

Ожидаемый разовый ущерб – ущерб, полученный в результате разовой реализации одной угрозы. Другими словами, это денежная величина, сопоставленная одиночному событию и характеризующая потенциальный ущерб, который понесет компания, если конкретная угроза сможет использовать уязвимость. Вычисляется умножением стоимости актива на величину фактора подверженности воздействию. Последний выражает в процентах величину ущерба от реализации угрозы конкретному активу. Кажется сложным, но на примере всё более понятно. Допустим, стоимость актива 35 000 рублей и в результате пожара ущерб составит 25% от его стоимости, соответственно, ожидаемый разовый ущерб будет равен 8750рублей.

Ежегодная частота возникновения (по-простому вероятность) – ожидаемое число проявления угрозы в течение года. Понятно, что величина может меняться от 0 до 100 процентов и не может быть определена точно. В идеальном случае определяется на основе статистики.

Общий годовой ущерб – величина, характеризующая общие потенциальные потери организации в течение одного года. Это произведение ежегодной величины возникновения на ожидаемый разовый ущерб от реализации угрозы. Например, вероятность пожара статистически равна 0,1, тогда ущерб будет 0.1*8750 рублей=875 рублей. После расчета этого показателя организация может принять меры по уменьшению риска, то есть если речь идет о безопасности, использовать средства защиты информации. В частности от пожара можно применить резервное копирование информации и тогда потери в случае сгорания компьютера будут исчисляться только стоимостью оборудования.

Результатом проведения количественного анализа является:

1) перечень активов (ресурсов) организации, подлежащих защите;

2) перечень существующих угроз;

3) вероятность успешной реализации угроз;

4) потенциальный ущерб для организации от реализации угроз в годовой период.

Понятно, что рассмотренные выше показатели рассчитываются преимущественно на основе субъективных мнений экспертов в области безопасности, руководства организации или других лиц, выполняющих оценку, следовательно, несмотря на кажущуюся точность данного подхода он не менее "расплывчат", чем качественный анализ рисков.

Качественная оценка рисков оперирует не численными значениями, а качественными характеристиками угроз. Как правило, анализ рисков выполняется путем заполнения опросных листов и проведения совместных обсуждений с участием представителей различных групп организации, таких как эксперты по информационной безопасности, менеджеры и сотрудники ИТ-подразделений, владельцы и пользователи бизнес-активов.

В общем случае риск от реализации угрозы определяется на основании следующих качественных оценок:

вероятности реализации угрозы;

величины ущерба в случае реализации угрозы.

Каждой угрозе присваивается ранг, отображающий вероятность ее возникновения. Можно использовать трехбалльную шкалу (низкая=1, средняя=2, высокая=3 вероятность). Основными факторами при оценке вероятности являются:

— расположение источника угрозы;

— мотивация источника угрозы (если угроза не случайная);

— предположения о квалификации и (или) ресурсах источника угрозы;

— статистические данные о частоте реализации угрозы ее источником в прошлом;

— информация о способах реализации угроз ИБ;

— информация о сложности обнаружения реализации угрозы рассматриваемым источником;

— наличие контрмер.

Если для оценки угрозы привлекаются несколько экспертов и их оценки различаются, рекомендуется в качестве итоговой брать наибольшую оценку вероятности реализации угрозы.

Так как при оценке потенциального ущерба необходимо учитывать не только материальные факторы, но и такие, как потеря репутации, потеря конкурентоспособности, кража производственных идей и пр. Естественно, оценить ущерб точно в том или ином случае очень сложно, вот почему чаще всего потенциальный ущерб ранжируется по аналогии с вероятностью возникновения, например, по трехбалльной шкале. К основным факторам для оценки потенциального ущерба относятся:

степень влияния на непрерывность работы;

степень влияния на деловую репутацию;

объем финансовых и материальных потерь;

объем финансовых, людских и временных затрат на восстановление системы после атаки.

Для оценки риска можно применить банальное умножение вероятности угрозы на потенциальный ущерб. Если в обоих случаях использовалась трехбалльная шкала, то получится в итоге шесть значений: 1,2, 3,4,6,9. Первые два результата можно отнести к низкому риску, вторые два – к среднему, третий и четвертый – к высокому. Таким образом, получим опять трехбалльную шкалу, по которой можно оценить опасность той или иной угрозы.

Совокупный риск вычисляется по простой формуле:

$R=Сумма_i(B_i*Y_i)$, где:

i – порядковый номер угрозы;

В – вероятность реализации i-й угрозы;

У- потенциальный ущерб от i-й угрозы.

При этом можно пренебречь угрозами, вероятность которых очень мала. Например, землетрясение. Несмотря на то, что ущерб от него может быть очень велик, вероятность возникновения в рассматриваемый интервал времени стремится к нулю.

Подход по сути очень похож на количественный, за исключением того, что активам присваивается относительная стоимость и участникам оценки не приходится тратить много времени на расчет конкретных показателей. Следовательно, достоинством метода является быстрота расчета и, соответственно, принятия контрмер и снижения риска. Недостатком является неоднозначность получаемых результатов и сложность расчета эффективности и разумности применения тех или иных мер защиты.

Каждый из рассмотренных подходов имеет свои достоинства и недостатки. Сравнение двух подходов представлено в таблице 6.1.

Таблица 6.1. Сравнение качественного и количественного подхода оценки рисков

	Количественный	Качественный
Достоинство	— Приоритеты рисков определяются на основе финансового влияния; приоритеты активов определяются на основе финансовых стоимостей. —Результаты упрощают *управление рисками*, обеспечивая возврат инвестиций в безопасность. —Результаты могут быть сформулированы с использованием управленческой терминологии (например, с помощью финансовых показателей и вероятности, выраженной в процентах). —Точность результатов увеличивается по мере	—Обеспечивает наглядность и упрощает понимание процесса *ранжирования* ри сков. —Проще найти удовлетворяющее всех решение. —Не требуется количественная оценка частоты возникновения угроз. —Не нужно определять финансовые стоимости активов. —Упрощается вовлечение в процесс сотрудников, не имеющих подготовки в области безопасности или компьютеров.

	накопления организацией статистических данных в процессе работы.	
Недостатки	—Сопоставленные рискам величины влияния основываются на субъективном мнении участников. —Поиск решения, удовлетворяющего всех участников, и получение достоверных результатов занимают очень много времени. —Расчеты являются очень сложными и требуют значительных затрат времени. —Результаты представляются только в денежном выражении, а их интерпретация может вызывать трудности у сотрудников, не имеющих технической подготовки. —Процесс требует глубоких знаний, что затрудняет подготовку участников.	—Недостаточное различие между существенными рисками. —Трудности с определением размера инвестиций в реализацию контроля вследствие отсутствия данных для анализа выгод и затрат. —Результаты зависят от квалификации созданной группы управления рисками.

Проанализировав таблицу можно сделать вывод о том, что для маленьких организаций целесообразней использовать качественный подход, для больших – количественный. Оценка риска производится для какого-то заданного промежутка времени, что обусловлено динамичностью современных информационных систем. Рассматриваемый период должен быть достаточно велик для учета наиболее распространенных угроз и в то же время не превышать величину, по истечению которой система так меняется, что оценка теряет какой-либо смысл. Обычно интервал составляет 1-5 лет.

6.3 Особенности защиты информации в геоинформационных системах.

В последнее время значительный прогресс в области информационных систем и технологий позволил расширить возможности применения систем, выполняющих задачи моделирования окружающего мира, таких как геоинформационные системы (ГИС). Появились интерактивные модели местности, способные взять на себя интерфейсные функции управления банками данных для решения как отраслевых, так и межведомственных задач. Расширившийся спектр задач, которые стали подвластны современному ГИС-анализу, подтолкнул повышение интереса к ГИС. Это задачи управления бизнес-процессами, экологии, социальной сферы, медицины, промышленности и т.д.

Современные ГИС-технологии несут в себе системообразующую функцию в информационно-управляющих системах. Являясь информационных базисом центров ситуационного анализа поддержки лиц, принимающих решения, ГИС выходят за рамки ответственности классической науки. Системы с элементами искусственного интеллекта требуют особого подхода, особенно при решении неординарных задач, таких как реализация принципа системной безопасности, выражающегося в виде совокупности требований к качеству информационно-технологических процессов, реализуемых в ГИС, и к качеству функционирования программной среды.

Выполнение требований безопасности информации достигается архитектурными решениями, выбранными при построении системы, средствами администрирования системы, специально разработанными с учетом специфики геоинформатики, средствами операционной системы, функциональными возможностями СУБД, а также регламентацией назначения и аудита прав доступа с помощью организационных мер и технических средств, обеспечивающих требуемый уровень защиты от несанкционированного доступа.

В общем виде ГИС представляет собой совокупность объектов информатизации, состоящих из программно-технических комплексов, автоматизированных рабочих мест, объединенных средствами телекоммуникации.

Каждая ЛВС объединяет ряд взаимосвязанных и взаимодействующих автоматизированных подсистем, обеспечивающих решение отдельных задач пользователей. Программно-технические комплексы на объектах информатизации включают технические средства обработки данных, средства обмена данными в ЛВС с возможностью выхода в телекоммуникационные системы и сети, а также средства хранения.

Основными объектами защиты в ГИС являются:

— Тематические геопространственные данные с ограниченным доступом и сведения конфиденциального характера (служебная и коммерческая информация) и иные информационные ресурсы (в том числе открытая информация), представленные в виде документов, баз данных и т.п.;

— Система формирования, распространения и использования информации, информационные технологии, процедуры сбора, обработки, хранения и передачи информации, пользователи системы и ее обслуживающий персонал;

— Информационная инфраструктура, включающая центры обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, комплексные системы защиты информации от НСД, документация на них и другая, относящаяся к ним информация;

— Технологические процессы обработки, передачи и хранения информации в базах геоданных и базах тематической информации.

Информационная инфраструктура, включающая центры

ПРИЛОЖЕНИЕ 1

Перечень нормативных актов, относящих сведения к категории ограниченного доступа

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Статья 5 Закона РФ от 21.07.1993 N 5485-1 "О государственной тайне"
	Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне"
Коммерческая тайна	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
	Статья 12 Федерального закона от 28.11.2011 N 335-ФЗ "Об инвестиционном товариществе"
Конфиденциальность персональных данных (любой информации, относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных))	Статья 7 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Налоговая тайна	Статьи 102 и 313 Налогового кодекса РФ

Банковская тайна	Статья 857 Гражданского кодекса РФ (часть вторая)
	Статья 26 Федерального закона от 02.12.1990 N 395-1 "О банках и банковской деятельности"
	Статья 57 Федерального закона от 10.07.2002 N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)"
Врачебная тайна	Статьи 13, 92 Федерального закона от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации"
	Статья 15 Семейного кодекса РФ
	Статья 9 Закона РФ от 02.07.1992 N 3185-1 "О психиатрической помощи и гарантиях прав граждан при ее оказании"
	Статья 14 Закона РФ от 22.12.1992 N 4180-1 "О трансплантации органов и (или) тканей человека"
	Статья 13 Закона РФ от 20.07.2012 N 125-ФЗ "О донорстве крови и ее компонентов"

Нотариальная тайна	Статьи 16 и 28 Основ законодательства Российской Федерации о нотариате от 11.02.1993 N 4462-1
	Статья 26 Федерального закона от 05.07.2010 N 154-ФЗ "Консульский устав Российской Федерации"
Адвокатская тайна	Статья 8 Федерального закона от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации"
Аудиторская тайна	Статья 9 Федерального закона от 30.12.2008 N 307-ФЗ "Об аудиторской деятельности"
	Статья 10 Федеральный закон от 24.07.2008 N 161-ФЗ "О содействии развитию жилищного строительства"
Тайна страхования	Статья 946 Гражданского кодекса РФ (часть вторая)
	Статья 47 Федерального закона от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации"

	Статья 32 Федерального закона от 24.07.2009 N 212-ФЗ "О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования"
	Статья 18 Федерального закона от 24.07.1998 N 125-ФЗ "Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний"
Тайна ломбарда	Статья 3 Федерального закона от 19.07.2007 N 196-ФЗ "О ломбардах"
Тайна связи	Статьи 53 и 63 Федерального закона от 07.07.2003 N 126-ФЗ "О связи"
	Статья 15 Федерального закона от 17.07.1999 N 176-ФЗ "О почтовой связи"
Тайна завещания	Статья 1123 Гражданского кодекса РФ (часть третья)
Тайна усыновления	Статья 139 Семейного кодекса РФ

Тайна следствия	Статья 161 Уголовно-процессуального кодекса РФ
	Статья 20 Федерального закона от 10.06.2008 N 76-ФЗ "Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания"
Тайна судопроизводства	Статья 194 Гражданского процессуального кодекса РФ
	Статья 20 Арбитражного процессуального кодекса РФ
	Статьи 298 и 341 Уголовно-процессуального кодекса РФ
Конфиденциальность отдельных сведений при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд	Статьи 51, 60, 66, 68 Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"
Конфиденциальность сведений, ставших известными работнику органа записи актов гражданского состояния в связи с	Статья 12 Федерального закона от 15.11.1997

государственной регистрацией акта гражданского состояния	
Конфиденциальность сведений о защищаемых лицах	Статья 9 Федерального закона от 20.08.2004 N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства"
	Статья 9 Федерального закона от 20.04.1995 N 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов"
Конфиденциальность сведений, ставших известными гражданам в ходе оперативно-розыскной деятельности	Статья 17 Федерального закона от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности"
Конфиденциальность сведений, содержащихся в личном деле и документах учета сотрудника органов внутренних дел, в реестре сотрудников органов внутренних дел, а также сведений о гражданах, поступающих на службу в органы внутренних дел	Статьи 39 и 40 Федерального закона от 30.11.2011 N 342-ФЗ "О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации"

Ограничение доступа к сведениям о доходах, об имуществе и обязательствах имущественного характера, представляемых государственными и муниципальными служащими, а также иными лицами, указанными в части 1 статьи 8Федерального закона от 25.12.2008 N 273-ФЗ	Статья 8 Федерального закона от 25.12.2008 N 273-ФЗ "О противодействии коррупции"
	Статья 20 Федерального закона от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации"
Ограничение доступа к сведениям о расходах по приобретению земельного участка, другого объекта недвижимости, транспортного средства, ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций) и об источниках получения средств, за счет которых совершена сделка, представляемых лицами, замещающими (занимающими) одну из должностей, указанных в пункте 1 части 1 статьи 2Федерального закона от 03.12.2012 N 230-ФЗ	Статья 15 Федерального закона от 02.03.2007 N 25-ФЗ "О муниципальной службе в Российской Федерации"
	Статья 8 Федерального закона от 03.12.2012 N 230-ФЗ "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам"
Конфиденциальность информации, относящейся к процедуре медиации	Статья 5 Федерального закона от 27.07.2010 N 193-ФЗ "Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)"

Конфиденциальность третейского разбирательства	Статья 22 Федерального закона от 24.07.2002 N 102-ФЗ "О третейских судах в Российской Федерации"
Конфиденциальность информации о содержании корпоративного договора, заключенного участниками непубличного общества Конфиденциальность информации о новых решениях и технических знаниях, полученных сторонами по договору подряда Конфиденциальность сведений, касающихся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами Секрет производства (ноу-хау)	Статья 67.2 Гражданского кодекса РФ (часть первая)
	Статья 727 Гражданского кодекса РФ (часть вторая)
	Статья 771 Гражданского кодекса РФ (часть вторая)
	Статья 1465 Гражданского кодекса РФ (часть четвертая)
Запрет на распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях отдельных сведений Конфиденциальность информации, предоставляемой организациям (гражданам), осуществляющим	Статья 4 Закона РФ от 27.12.1991 N 2124-1 "О средствах массовой информации"
	Статья 41 Закона РФ от 27.12.1991 N 2124-1 "О средствах массовой информации"

производство и выпуск средств массовой информации	
Ограничение доступа к информации, входящей в состав кредитной истории, и (или) к коду субъекта кредитной истории	Статьи 6 и 7 Федерального закона от 30.12.2004 N 218-ФЗ "О кредитных историях"
Конфиденциальность информации, предоставляемой эмитентами, профессиональным участникам рынка ценных бумаг, саморегулируемыми организациям профессиональных участников рынка ценных бумаг федеральному органу исполнительной власти по рынку ценных бумаг. Конфиденциальность информации держателями реестра и депозитариями. Конфиденциальность информации, полученной в связи с осуществлением функций трансфер-агента. Конфиденциальность информации о счетах и об операциях клиентов центрального депозитария	Статья 8.1, 8.6, 44.1 Федерального закона от 22.04.1996 N 39-ФЗ "О рынке ценных бумаг"
	Статья 14 Федерального закона от 07.12.2011 N 414-ФЗ "О центральном депозитарии"
Конфиденциальность информации, предоставляемой клиринговым организациям и лицам, осуществляющим функции центрального контрагента	Статья 20 Федерального закона от 07.02.2011 N 7-ФЗ "О клиринге и клиринговой деятельности"

Конфиденциальность факта передачи в федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма информации, указанной впунктах 1 - 3 статьи 7.1-1 Федерального закона от 07.08.2001 N 115-ФЗ	Статья 7.1-1 Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"
Конфиденциальность инсайдерской информации	Статья 6 Федерального закона от 27.07.2010 N 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации"
Конфиденциальность сведений, предоставляемых участниками торгов в соответствии с правилами организованных торгов	Статья 23 Федерального закона от 21.11.2011 N 325-ФЗ "Об организованных торгах"
Конфиденциальность информации, полученной в связи с осуществлением деятельности по выдаче, погашению и обмену инвестиционных паев	Статья 28 Федерального закона от 29.11.2001 N 156-ФЗ "Об инвестиционных фондах"

Ограничение доступа к информации, полученной в ходе проведения проверок российских участников внешнеэкономической деятельности	Статья 17 Федерального закона от 18.07.1999 N 183-ФЗ "Об экспортном контроле"
Ограничение доступа к сведениям о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, к сведениям, содержащимся в планах обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств, к информационным ресурсам единой государственной информационной системы обеспечения транспортной безопасности	Статьи 5, 9, 11 Федерального закона от 09.02.2007 N 16-ФЗ "О транспортной безопасности"
Конфиденциальность сведений, составляющих дактилоскопическую информацию	Статья 12 Федерального закона от 25.07.1998 N 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации"
Ограничение доступа к информации, содержащейся в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации	Статья 59 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации"

Ограничение доступа к сведениям о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, поступающие в финансовые органы от органов Федерального казначейства	Статья 241 Бюджетного кодекса РФ
Конфиденциальность сведений, содержащихся в индивидуальных лицевых счетах застрахованных лиц в системе обязательного пенсионного страхования Конфиденциальность информации, полученной негосударственным пенсионным фондом при обработке сведений, содержащихся в пенсионных счетах негосударственного пенсионного обеспечения, пенсионных счетах накопительной части трудовой пенсии и др.	Статья 6 Федерального закона от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования"
	Статья 15 Федерального закона от 07.05.1998 N 75-ФЗ "О негосударственных пенсионных фондах"
Конфиденциальность информации о получателе социальных услуг	Статья 6 Федерального закона от 28.12.2013 N 442-ФЗ "Об основах социального обслуживания граждан в Российской Федерации"
Конфиденциальность сведений, содержащихся в Федеральной государственной информационной	Статья 18 Федерального закона от 28.12.2013 N 426-ФЗ "О специальной оценке условий труда"

системе учета результатов проведения специальной оценки условий труда	
Конфиденциальность сведений, ставших известными судебным приставам в связи с исполнением должностных обязанностей	Статья 4 Федерального закона от 21.07.1997 N 118-ФЗ "О судебных приставах"
Конфиденциальность информации, представляемой заинтересованным лицом в орган, проводящий расследования в целях принятия решения о целесообразности введения, применения, пересмотра или отмены специальной защитной меры, антидемпинговой меры или компенсационной меры	Статья 32 Федерального закона от 08.12.2003 N 165-ФЗ "О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров"
Конфиденциальность информации о членах политической партии, представляемой для сведения в уполномоченные органы	Статья 19 Федерального закона от 11.07.2001 N 95-ФЗ "О политических партиях"
Тайна исповеди	Статья 3 Федерального закона от 26.09.1997 N 125-ФЗ "О свободе совести и о религиозных объединениях"
Конфиденциальность сведений о населении, содержащихся в переписных листах	Статья 8 Федерального закона от 25.01.2002 N 8-ФЗ "О Всероссийской переписи населения"

Ограничение доступа к сведениям, содержащимся в переписных листах об объектах сельскохозяйственной переписи	Статья 12 Федерального закона от 21.07.2005 N 108-ФЗ О Всероссийской сельскохозяйственной переписи"
Ограничение доступа к первичным статистическим данным, содержащимся в формах федерального статистического наблюдения	Статья 9 Федерального закона от 29.11.2007 N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в Российской Федерации"
Ограничение доступа к информации, содержащейся в паспортах безопасности объектов топливно-энергетического комплекса	Статья 8 Федерального закона от 21.07.2011 N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса"
Конфиденциальность информации, полученной членами саморегулируемой организации в области энергетического обследования в ходе проведения энергетического обследования	Статья 18 Федерального закона от 23.11.2009 N 261-ФЗ"Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации"
Конфиденциальность сведений, содержащихся в заявках на участие в конкурсе на право заключить контракт на проведение лотерей	Статья 24.10 Федеральный закон от 11.11.2003 N 138-ФЗ "О лотереях

ПРИЛОЖЕНИЕ 2

Примерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации.

1.Производство

Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов и готовой продукции.

2.Управление

Сведения о применяемых оригинальных методах управления организацией. Сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, научно-техническим и иным вопросам.

3.Планы

Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. Также сведения инвестиций, закупок и продаж.

4. Совещания

Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

5. Финансы

Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредита организации (пассивы и активы). Главная книга организации.

6.Рынок

Сведения о применяемых организацией оригинальных методах изучения рынка (маркетинга). Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры. Сведения о рыночной стратегии организации, о применяемых организацией оригинальных

методах осуществления продаж, об эффективности служебной и коммерческой деятельности организации

7. Партнеры

Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

8. Конкуренты

Обобщенные сведения о внутренних и зарубежных предприятиях как о потенциальных конкурентах в деятельности организации, оценка качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

9. Переговоры

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами организации.

10. Контракты

Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами (клиентами, контрагентами).

11. Цены

Сведения о методах расчета, структуре, уровнях реальных цен на продукцию и размеры скидок.

12. Торги, аукционы

Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

13. Наука и техника

Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы,

конфигурация, процентное содержание компонентов, температура, давление, время и т.д.). Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условии экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект. Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

14. Технология

Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

15. Безопасность

Сведения о порядке и организации защиты служебной или коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме. Сведения, составляющие служебную или коммерческую тайну организации, предприятий-партнеров и передаваемые ими в пользование на доверительной основе.

ПРИЛОЖЕНИЕ 3

Заявка на проведение аттестации объекта информатизации

Кому: _____

(наименование органа по аттестации и его адрес)

ЗАЯВКА

на проведение аттестации объекта информатизации

1. (наименование заявителя) просит провести аттестацию (наименование объекта информатизации) на соответствие требованиям по безопасности информации: _____

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____

5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____

5.3. Испытания несертифицированных средств и систем информатизации (наименование средств и систем) предусмотрено провести в испытательных центрах (лабораториях) (наименование испытательных центров) в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____).

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

ПРИЛОЖЕНИЕ 4

Аттестат соответствия

"УТВЕРЖДАЮ"

(должность руководителя органа по аттестации)

м.п. Ф.И.О.

"__" _____ 20__ г.

АТТЕСТАТ СООТВЕТСТВИЯ

(указывается полное наименование объекта информатизации)

ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

N ____

Действителен до "__" _____ 20__ г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что: (приводится полное наименование объекта информатизации) _____ категории _____ класса соответствует требованиям нормативной и методической документации побезопасности информации.

Состав комплекса технических средств объекта информатизации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов), схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов) прилагаются.

2. Организационная структура, уровень подготовки специалистов, нормативное, методическое обеспечение и техническая оснащенность службы безопасности информации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищенности объекта информатизации в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация объекта информатизации выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными

"__" _____ 20__ г. N _____.

4. С учетом результатов аттестационных испытаний на объекте информатизации разрешается обработка (указывается высшая степень секретности, конфиденциальности) информации.

5. При эксплуатации объекта информатизации запрещается: (указываются ограничения, которые могут повлиять на эффективность мер и средств защиты информации).

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на службу безопасности информации.

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (N _____ "__" _____ 20__ г.) и протоколах испытаний.

8. "Аттестат соответствия" выдан на _____ года, в течение которых должна быть обеспечена неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, указанные в п. 9.

9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации.

9.1. _____

9.2. _____

Руководитель аттестационной комиссии
(должность с указанием наименования предприятия)
Ф.И.О.
"__" _____ 20__ г.

Отметки органа надзора: _____

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.

1) Нормативно-правовые аспекты защиты информации: Учебное пособие / А.А. Парошин. –Владивосток: Изд-во Дальневост. федер. Ун-та, 2010 – 116с.

2) Общие вопросы технической защиты информации [Электронный ресурс]: / Д.А. Скрипник. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012. -264 с.

3) Правовые основы защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Алтай: Изд-во Алтайск. гос. Технич. Ун-та, 2000 – 130 с.

4) Правовое обеспечение информационной безопасности: Учебное пособие / С.Я. Казанцев, О.Э. Згадзай, Р.М. Оболенский и д.р.

5) Правовое обеспечение информационной безопасности : методические указания / сост.: А.В. Терехов, Е.В. Бурцева. –Тамбов: Из-во ГОУ ВПО ТГТУ, 2010. -160 с.

6) Информационная безопасность: нормативно-правовые аспекты: Учебное пособие / Ю.А. Родичев, –СПб.: Питер, 2010 г. -272с. – Электронное издание.

7) Информационная безопасность и защита данных: Учебное пособие / Е.А. Степанов, -М.: ИНФРА-М, 2001

8) Организационно-правовое обеспечение информационной безопасности : Краткий курс лекций / В.А. Кулишкин, СПб.: РГГМУ, 2007 -149 с.

9) СПС «Консультант+»

10) СПС «Гарант»

11) Конституция Российской Федерации

12) Доктрина информационной безопасности Российской Федерации

13) Гражданский Кодекс Российской Федерации

14) Уголовный Кодекс Российской Федерации

15) ФЗ от 27.07.06 г №149-ФЗ «Об информации, информационных технологиях и о защите информации

16) ФЗ от 27.07.06 г. №152-ФЗ «О персональных данных»

17) ФЗ от 08.08.01 г №128-ФЗ «О лицензировании отдельных видов деятельности»

18) ФЗ от 06.04.11 г.№63-ФЗ «Об электронной цифровой подписи»

ОГЛАВЛЕНИЕ