АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. И.И.ПОЛЗУНОВА

КАФЕДРА ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ СВЯЗИ

Загинайлов Ю.Н.

Учебное пособие

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Утверждено и рекомендовано
к публикации на заседании кафедры ЗИРСС,
протокол № 12 от 26.12.2000г.

В пособии подробно рассмотрены вопросы, связанные с современным состоянием законо дательства, определяющего статус информации и информационного ресурса как объекта правовой за щиты. Основные нормативные акты, определяющие ключевые понятия, методы и средства юридической защиты, снабжены необходимыми пояснениями. Описаны механизмы правовой защиты конституционных прав и обязанностей граждан России, гарантирующие доступ к информации и защиту конфиденциаль ности информации на уровне государства, общества, личности.

Пособие предназначено для студентов, обучающихся по специальностям цикла информати ка и вычислительная техника и информационня безопасность.

ОГЛАВЛЕНИЕ

Введение

Стремительное развитие в последние годы средств вычислительной техники, связи и телекомму никаций создало новые уникальные возможности для включения информации в гражданский и иной обо роты, в том числе и распространения на нее статуса товара. Повсеместное внедрение информацион ных технологий и глобальной компьютерной сети привело к формированию глобального межгосударст венного информационного пространства, в котором информация обращается в непривычной для традици онного права электронной форме. В информационную сферу сегодня включена значительная часть сов ременного общества. Время в которое мы живем, все чаще называют "информационным веком".

Естественно, что отношения, возникающие между людьми и организациями, в процессе их дея тельности в информационной сфере должны быть законодательно урегулированы. Одним из важных воп

росов, подлежащих правовому регулированию, является вопрос о законодальной защите объектов и субъектов, действующих в информационной сфере.

Информационную сферу можно представить как совокупность информационных ресурсов, информа ционной инфраструктуры, системы формирования, распространения, использования информации и регу лирования возникающих при этом общественных отношений. Информационная сфера является системооб разующим фактором жизни общества, активно влияет на состояние политической, экономической, обо ронной и других составляющих безопасности государства.

Широкое распространение современных информационных технологий, в частности в банковской и экономической областях, привело к возникновению новых видов преступлений, основанных на несанкци онированном получении или искажении информации. С подобными преступлениями, как правило, соверша емыми с использованием современных ЭВМ и телекоммуникационных систем, ранее право не сталкива лось.

Надежное противодействие новому направлению криминальной деятельности требует выявления и осознания угроз информационной безопасности и изучение методов защиты от этих угроз. Важными элементами системы противодействия преступным посягательствам являются правовые меры защиты ин формации. Положения Гражданского и Уголовного кодексов, Законов Российской Федерации "Об инфор мации, информатизации и защите информации", "О правовой охране программ для электронных вычи слительных машин и баз данных", "О государственной тайне" и др. обеспечивают правовую основу для защиты объетов и субъектов, включенных в информационную сферу.

Наиболее сложными для правовой зашиты являются информационные ресурсы с ограниченным дос тупом, такие как государственная тайна и конфиденциальная информация. Поэтому правовым основам защиты государственной тайны и множеству других видов тайн, объединенных понятием конфиденциаль ная информация уделяется в пособии основное внимание.

Тема ╬1: 1 Политика информационной безопасности РФ и ее правовое обеспечение

Вопросы: 1.1 Информационная безопасность и ее место в системе национальной безопасности РФ.

1.2 Государственная политика информационной безопасности и ее реализация в Законодательстве РФ.

1.3 Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

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.

1.1 Информационная безопасность и ее место в системе национальной безопасности России.

Необходимым условием нормального существования и развития каждого общества является защищенность от внешних и внутренних угроз, устойчивость к попыткам внешнего давления, способность как парировать такие попытки и нейтрализовать возникающие угрозы, так и обеспечивать такие внутренние и внешние условия существования страны, которые гарантируют возможность стабильного и всестороннего прогресса общества и его граждан. Для характеристики этого состояния

используется понятие национальной безопасности.

Под национальной безопасностью следует понимать состояние защищенности жизненно важных на циональных интересов от внутренних и внешних угроз.

Система национальных интересов России определяется совокупностью основных интересов лич ности, общества, государства и охватывает все сферы их деятельности:политическую, экономичес кую, военную, экологическую, информационную, научно-техническую, социальную и другие.

Поэтому в содержании понятия "национальная безопасность" можно выделить различные струк турные элементы (компоненты), к основным из которых относятся политическая, экономи ческая, во енная, экологическая и информационная безопасность.

Сущность политической безопасности состоит в способности науки создать политическую сис тему, обеспечивающую баланс интересов различных социальных групп; самостоятельно решать воп росы государственного устройства;проводить независимую внутреннюю и внешнюю политику.

Под экономической безопасностью понимается состояние нации,при котором она может суверен но, без внешнего вмешательства определять пути и формы своего экономического развития.

Военная безопасность заключается в возможности обеспечения национальной безопасности средствами вооруженного насилия. В первую очередь военная безопасность характеризуется спо собностью нации сдерживать агрессию или противодействовать ей.

Экологическая безопасность состоит в наличии безопасной среды обитания, обеспечивающей нормальную жизнедеятельность человека. Баланс компонентов в системе "население -окружающая среда-природные ресурсы" является гарантом жизнеспособности человеческого общества.

Информационная безопасность - состояние защищенности информационных ресурсов от внутрен них и внешних угроз, способных нанести ущерб интересам личности, общества, государства (нацио нальным интересам).

Поскольку в условиях информатизации страны, развития информационных технологий, информа ционные ресурсы формируются во всех сферах деятельности, и в первую очередь в политической, военной, экономической, научно -технической, информационную безопасность следует рассматривать как комплексный показатель национальной безопасности. Этим определяется ее важное место и од на из ведущих ролей в системе национальной безопасности страны в современных условиях. Не да ром существует ряд пословиц и выражений характеризующих место информации в конкурентной борьбе

и в тактике военных действий: "Кто владеет информацией - тот владеет ситуацией", "побеждает тот, кто более информирован о противнике " и другие.

Основными угрозами информационной безопасности являются утечка информации и нарушение ее целостности.

Обеспечение информационной безопасности осуществляется в рамках обеспечения национальной безопасности.

Национальная безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства.

Политика России в области национальной безопасности строится на основе Концепции, утвержденной Указом Президента РФ ╬1300 от 17.12.97г.В настоящее время разработана новая концепция национальной безопасности, которая будет обсуждена и утверждена органами государственной власти.

Концепция национальной безопасности РФ определяет: место России в мировом сообществе на современном этапе развития государственности; национальные интересы России во всех сферах жизнедеятельности; угрозы национальной безопасности Российской Федерации; пути и силы обеспечения национальной безопасности.

В Концепции сделан акцент на национальные интересы России в информационной сфере, обусловливающие необходимость сосредоточения усилий общества и граждан на решении таких задач, как соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею, защита национальных духовных ценностей, пропаганда национального культурного наследия, норм морали и общественной нравственности, обеспечении права граждан на получение достоверной информации, развитие современных телекоммуникационных технологий. В то же время недопустимо использование информации для манипулирования массовым сознанием. Необходима защита государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

На основе анализа угроз национальной безопасности, сделан вывод о том, что главные из них в настоящее время и в обозримой перспективе не имеют военной направленности, носят преимущественно внутренний характер и содержаться во внутриполитической, экономической, социаль

ной, экологической и информационной безопасности.

В Концепции определены важнейшие задачи в области информатизации и защиты информации.

Законодательную основу обеспечения безопасности составляют:

* Конституция РФ;

* Закон РФ от 5.03.92г. ╬2446-1 "О безопасности";

* Законы и другие нормативные акты РФ, регулирующие отношения в области безопасности;

* Конституции, законы, нормативные акты республик;

* нормативные акты органов власти и управления краев, областей принятые в пределах их компе тенции;

* международные договоры и соглашения, заключенные или признанные РФ.

Основные положения и правовые основы обеспечения национальной безопасности закрепляет Закон РФ "О безопасности". Он также определяет систему безопасности и ее функции, объекты и субъекты безопасности.

Основным субъектом обеспечения безопасности является государство, осуществляющее фун кции в этой области через органы законодательной, исполнительной и судебной властей.

К основным объектам безопасности относятся: личность - ее права и свободы; общество - его материальные и духовные ценности; государство - его конституционный строй, суверенитет и тер риториальная целостность.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности.

Принципы обеспечения безопасности.

Основными принципами обеспечения безопасности являются:

- законность;

- соблюдение баланса жизненно важных интересов личности, общества и государства;

- взаимная ответственность личности, общества и государства по обеспечению безопасности;

- интеграция с международными системами безопасности.

Система безопасности Российской Федерации.

Систему национальной безопасности образуют:

* органы законодательной, исполнительной и судебной властей;

* государственные, общественные и иные организации и объединения;

* граждане, принимающие участие в обеспечении безопасности в соответствии с законом;

* законодательство, регламентирующее отношения в сфере безопасности.

Силы обеспечения безопасности.

Силы обеспечения безопасности включают в себя:

* Вооруженные Силы (ВС РФ);

* федеральные органы безопасности (ФСБ РФ);

* органы внутренних дел (МВД РФ);

* органы внешней разведки (СВР РФ);

* органы обеспечения безопасности органов законодательной, исполнительной, судебной властей и их высших должностных лиц,

* налоговой службы;

* службы ликвидации последствий чрезвычайных ситуаций (МЧС РФ);

* формирования гражданской обороны;

* пограничные войска,

* внутренние войска;

* органы, обеспечивающие безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве;

* службы обеспечения безопасности средств связи и информации (ФАПСИ);

* таможни, природоохранительные органы,органы охраны здоровья населения и другие государственные органы обеспечения безопасности.

Для рассмотрения вопросов внутренней и внешней политики РФ в области обеспечения безопасности, стабильности и правопорядка создан Совет безопасности РФ при Президенте. Он ответственен за состояние защищенности национальных интересов от внешних и внутренних угроз.

Совет безопасности РФ в соответствии с основными задачами его деятельности образует постоянные межведомственные комиссии, которые могут создаваться на функциональной или региональной основе.В частности, межведомственная комиссия по защите государственной тайны разрабаты

вает и координирует федеральные программы по защите информации составляющей государственную тайну.

Обеспечение информационной безопасности осуществляется в рамках обеспечения национальной безопасности России. Оно предусматривает наличие государственной системы защиты информации и законодательства в этой области.

1.2 Государственная политика информационной безопасности и ее реализация в Законодательстве РФ.

Государственная политика информационной безопасности реализуется в рамках политики национальной безопасности и политики информатизации всех сфер деятельности государства и общества. Она осуществляется на основе Указа Президента РФ ╬170 от 20.01.94г "Об основах государственной политики в сфере информатизации" и "Концепции национальной безопасности России" и "Доктрины информационной безопасности РФ" принятой в 2000 году.

Основными направлениями этой политики являются:

* обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
* формирование и защита государственных информационных ресурсов;
* создание и развитие федеральных и региональных информационных систем и сетей;
* обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;
* развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

В соответствии с этими направлениями в Концепции национальной безопасности определены задачи в области информационной безопасности.

Важнейшими задачами являются:

* установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
* совершенствование информационной структуры, ускорение развития новых информационных техноло

гий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и ана лиза информации с учетом вхождения России в глобальную информационную инфраструктуру;

* разработка соответствующей нормативной правовой базы и координация, при ведущей роли Феде рального агентства правительственной связи и информации при Президенте Российской Федерации, деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;

* развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритет ное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

* защита государственного информационного ресурса, и прежде всего в федеральных органах госу дарственной власти и на предприятиях оборонного комплекса.

Все направления политики защиты информации и информационных ресурсов реализованы в За конодательстве РФ.

Законодательство в области защиты информации включает:

* Закон РФ от 20.02.95г. ╬24-ФЗ "Об информации, информатизации и защите информации";

* Закон РФ от 21.09.93г. ╬182 "О государственной тайне".

* Закон РФ от 4.07.96г.╬85-ФЗ "Об участии России в международном информационном обмене";

* Закон РФ от19.07.95г. ╬110-ФЗ"Об авторском праве и смежных правах";

* Закон РФ от 23.09.92г. ╬3523-1"О правовой охране программ для электронных вычислительных машин и баз данных";

* Закон РФ от 27.12.91г. "О средствах массовой информации"

* Гражданский кодекс РФ (ч1 и 2);

* Уголовный кодекс РФ;

В целом развитие законодательной базы в области информационной безопасности идет по четырем основным направлениям:

* защита сведений составляющих государственную тайну;

* защита конфиденциальной информации;

* защита авторского права в сфере информатизации;

* защита права на доступ к информации.

Основу законодательства составляет закон "Об информации, информатизации и защите ин

формации", который выражает основные направления политики информационной безопасности,суть которой в своей основе сводится к защите государственных информационных ресурсов, регулирует отношения, возникающие при формировании и использовании информационных ресурсов, создании и использовании информационных технологий, защите информации, прав субъектов,участвующих в ин формационных процессах, а также определяет основные понятия используемые в законодательстве.

1.3 Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

Органы обеспечения информационной безопасности в совокупности с законодательством об разуют государственную систему информационной безопасности и защиты информации.

Государственная система защиты информации включает:

* органы законодательной, исполнительной и судебной властей;
* законодательство регулирующее отношения в области защиты информации и информационных ресурсов;
* нормативную правовую базу по защите информации;
* службы (органы) защиты информации предприятий, организаций, учреждений.

Органы законодательной власти (Государственная дума) издают законы регулирующие отно шения в области защиты информации.

Законодательство включает в себя законы. Их перечень будет рассмотрен в ходе изучения тем дисциплины.

Нормативная база формируется на основе нормативных правовых актов в области защиты ин формации, издаваемых органами различных ветвей власти, министерствами, ведомствами.

Основу нормативной базы составляют руководящие документы Гостехкомиссии и стандарты издаваемые Госстандартом.

Органы исполнительной власти (Правительство) исполняют законы. Для этого Правитель ство принимает соответствующие постановления в области защиты информации и издает распоря жения, являющиеся подзаконными нормативными правовыми актами.

Министерства и ведомства в соответствии со своим предназначением разрабатывают и при

нимают постановления и решения, являющиеся нормативными правовыми актами своего уров
ня. Кроме того, они разрабатывают и утверждают такие нормативные акты как: положения, руковод
ства, инструкции, правила, методические рекомендации.

К нормативным актам этого уровня относятся также приказы и письма руководителей ведомств и ми
нистерств.

К ведомствам, регулирующим отношения в области защиты информации, относятся:

* Межведомственная комиссия по защите государственной тайны;
* Федеральное Агентство правительственной связи и информации (ФАПСИ);
* Государственная техническая комиссия;
* Госстандарт;
* Федеральная Служба безопасности (ФСБ РФ);

Кроме этого в обеспечении информационной безопасности принимают участие Служба внешней разведки (СВР), Федеральная пограничная служба (ФПС) и МВД.

Основным органом управления государственной системы защиты информации является Гостехко миссия. В соответствии со своими функциями она осуществляет:

- координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами;
- организационно-методическое руководство деятельностью по защите информации в КС;
- разработку и финансирование научно-технических программ по защите информации;
- утверждение нормативно-технической документации;
- функции государственного органа по сертификации продукции по требованиям безопасности ин формации;
- лицензирование деятельности предприятий по оказанию услуг в области защиты информации.

Для организации и осуществления защиты информации в России Гостехкомисссией разработа ны Руководящие документы по защите информации в СВТ и АС. Перечень этих документов и их со держание будут изучены при рассмотрении конкретных тем дисциплины.

Госстандарт разрабатывает стандарты в области защиты информации.

Органы ФСБ РФ выполняет функции защиты государственной тайны.

Органы МВД ведут борьбу с правонарушителями в информационной сфере и компьютерными

преступлениями. Для этого в структуре МВД создано специальное управление "Р" для предотвращения и раскрытия компьютерных преступлений и защиты авторских прав.

Органы Государственного таможенного комитета (ГТК) обязаны предупреждать незаконный ввоз и вывоз из России "пиратской" продукции, обеспечивая тем самым защиту авторских и патентных прав.

Руководители предприятий, организаций, учреждений, в соответствии со своими должностными обязанностями, при деятельности связанной с информацией, составляющей государственную или иную тайну, создают службу (подразделение) по защите информации. Для организации соответствующей деятельности они издают нормативные правовые акты: приказы,распоряжения; а также утверждают: руководства, инструкции, положения, правила, методические рекомендации связанные с защитой информации и деятельностью служб защиты информации.

Для деятельности, связанной с государственной тайной, предприятие должно иметь лицензию на этот вид деятельности, в его структуру вводится специальный отдел, все средства защиты должны быть сертифицированы.

Судебная власть осуществляет надзор и привлечение к ответственности за нарушения законодательства в информационной сфере. В своей деятельности суды руководствуются соответствующими статьями УК РФ, ГК РФ, КоАП.

Информационная безопасность является важной составляющей национальной безопасности России. Политика государства в этой сфере деятельности направлена в первую очередь на организацию защиты государственной тайны и развитие правовых основ защиты информации.
Правовая защита информации выступает как один из наиболее важных способов и методов защиты информации.

Режим защиты информации устанавливается в отношении сведений, составляющих государственную тайну и конфиденциальной информации.

Нормативная правовая база в области защиты информации ориентируется по четырем направлениям: защита сведений составляющих ГТ; защита конфиденциальной информации; защита авторского права; защита права на доступ к информации.

Источники:

1. Конституция РФ. Сборник законодательных актов СЗА РФ. ИСС "Гарант".

2. УП РФ от 17.12.97г. ╬1300 "Концепция национальной безопасности".

3. Закон РФ от 5.03.92г. ╬2446-1 "О безопасности". СЗА РФ. ИСС "Гарант".

4. УП РФ от 20.01.94г. ╬170 "Об основах государственной политики в сфере информатизации". СЗА РФ. ИСС "Гарант".

5. Закон РФ от 20.02.95г. "Об информации, информатизации и защите инфор мации". СЗА РФ.ИСС "Гарант".

6. Закон РФ от 4.07.96г. "Об участии России в международном информацион ном обмене. СЗА РФ. ИСС "Гарант".

7. Закон РФ от 27.12.91г. О средствах массовой информации". СЗА РФ. ИСС "Гарант".

Вопросы для самоконтроля и собеседования по теме:

1) Какими нормативными актами определяется система национальной безопасности РФ?

2) Что понимается под "национальной безопасностью", какие структурные элементы она включает?

3) Что понимается под "информационной безопасностью", каково ее место в системе наци ональной безопасности РФ?

4) Основные направления политики информационной безопасности РФ?

5) Важнейшие задачи в области информационной безопасности?

6) Какие нормативные правовые акты составляют Законодательство в области защиты инфор мации?

7) Какие ведомства регулируют правовые отношения в области защиты информации?

8) Какие виды нормативных правовых актов издаются и кем для регулирования отношений в области защиты информации?

9) Какие функции в области защиты информации выполняет Государственная т ехническая ко миссия РФ?

Тема╬2 Законодательство РФ об информационных правоотношениях и защите информации.

Вопросы:

2.1 Понятие информационных правоотношений;

2.2 Структура законодательства регулирующего информационные правоотношения.

2.3 Основные понятия законодательства.

2.4 Основные положения законодательства в сфере информационных правоотношений и защиты информации.

2.1 Понятие информационных правоотношений.

Создание и расширенное производство персональных компьютеров стало естественным разви тием стремления человечества получить более совершенный доступ к информационным ресурсам. Постепенно на наших глазах возникла информационная индустрия, чья самостоятельность и перс пектива развития целиком и полностью зависели от точного регулирования правоотношений, возни кающих при формировании и использовании информационных ресурсов.

"Информационная революция" застигла нашу страну в сложный экономический и политический период и потребовала срочного регулирования возникающих на ее пути проблем. Принятый в 1994г. Граж данский кодекс Российской Федерации впервые (ст.128) отнес к объектам гражданских прав инфор мацию и результаты интеллектуальной деятельности. Этим, а в последующем и другими законами, был официально закреплен юридический статус информации как собственности имеющей своих вла дельцев, создателей и пользователей (покупателей, потребителей) и информационных правоотноше ний. Понятие информационных правоотношений сформулиро

вано в Законе "Об информации, информатизации и защите информации". Информационные правоотноше ния - это отношения возникающие при:

* формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потре бителю документирован ной информации;
* создании и использовании информационных технологий и средств их обеспечения;
* защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Как видим, из определения следует, что защита информации, является составной частью информационных правоотношений и, следовательно, не может рассматриваться отдельно от информа ционных процессов и информатизации в целом. Таким образом, и правовую защиту информации, предусматривающую защиту прав собственников информации, следует рассматривать как неотъемлемую составляющую информационной безопасности.

Среди научных и других работ в области права и информационной безопасности, в последние годы, все чаще стало появляться выражение " "Информационное право", однако как отрасль пра ва "Информационное право" рассматривается лишь в теоретических исследованиях.

2.2 Структура законодательства регулирующего информационные правоотношения.

Учитывая тот факт, что в современном Российском законодательстве лишь часть законов направлена непосредственно на регулирование информационных правоотношений, а часть этих от ношений регулируются отдельными статьями законов (кодексов), его можно разделить на две группы.

К первой группе, следует отнести законы устанавливающие, в основном, нормы права в ин формационной сфере и в области защиты информации и прав субъектов. По своей сути они опре деляют правовой режим информационных ресурсов и защиты информации. Эта группа включает:

* Закон РФ от 20.02.95г. ╬24-ФЗ "Об информации, информатизации и защите информации";
* Закон РФ от 21.09.93г. ╬182 "О государственной тайне".

* Закон РФ от 4.07.96г.╬85-ФЗ "Об участии России в международном информационном обмене";

* Закон РФ от19.07.95г. ╬110-ФЗ "Об авторском праве и смежных правах";

* Закон РФ от 23.09.92г. ╬3523-1"О правовой охране программ для электронных вычислительных ма шин и баз данных";

* Закон РФ от 27.12.91г. "О средствах массовой информации";

* Закон "О связи"

* Закон "О федеральных органах правительственной связи и информации";

* другие законы, регламентирующие отдельные виды профессиональной деятельности.

Кроме того, к этой группе законодательных актов следует отнести Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера", посколь ку пока в этой области отсутствует соответствующий закон.

Ко второй группе относятся законодательные акты, которые в своем содержании предусматри вают, в основном, в части их касающейся, конкретные меры ответственности за нарушение право вого режима информационных ресурсов и защиты информации, и, нанесение ущерба собственникам и другим субъектам информационных правоотношений. К ним относятся:

* Уголовный кодекс (УК РФ);

* Гражданский кодекс (ГК РФ ч1 и ч2);

* Кодекс об административных правонарушениях (КоАП РСФСР);

По своей сути, вторая группа представляет часть законодательства РФ, которая обеспечива ет правовую защиту информации и субъектов информационных правоотношений.

В целом развитие законодательной базы в области информационной безопасности осуществ ляется по четырем основным направлениям:

* защита сведений составляющих государственную тайну;

* защита конфиденциальной информации;

* защита авторского права в сфере информатизации;

* защита права на доступ к информации.

2.3 Основные понятия законодательства.

Основу законодательства составляет закон "Об информации, информатизации и защите ин формации". Основные понятия в области информационных правоотношений сформулированы в этом законе :

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах неза висимо от формы их представления;

Объекты правоотношений:

документированная информация (документ) - зафиксированная на материальном носителе инфор мация с реквизитами, позволяющими ее идентифицировать;

информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и рас пространения информации;

информационная система - организационно упорядоченная совокупность документов реализую щих информационные процессы;

информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятель ствах жизни гражданина, позволяющие идентифицировать его личность;

конфиденциальная информация - документированная информация, доступ к которой ограничива ется в соответствии с законодательством РФ;

Субъекты правоотношений:

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распо ряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обес печения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

пользователь (потребитель) информации - субъект, обращающийся к ин формационной системе или посреднику за получением необходимой ему ин формации и пользующийся ею.

Как видно из приведенных определений, законодательство не рассматривает любую информа цию как самостоятельный объект регулирования. Она выступает в качестве такового только в том случае, когда является документом. Именно в виде документированной информации, входящей в состав информационных ресурсов, систем, она может выступать объектом со бственности. Важно, что и защите подлежит только документированная информация.

Ряд важных правовых определений кроме того дает Федеральный закон "Об участии в между народном информационном обмене", принятый в 1995г. В частности к ним следует отнести:

Информационные продукты (продукция) - документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетво рения потребностей пользователей;

Информационные услуги - действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Информационная сфера (среда) - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

2.4 Основные положения законодательства в сфере информационных правоотношений и защиты информации.

Основные положения в области информационных правоотношений и защите информации сфор мулированы также в законе "Об информации,информатизации и защите информации".

В целом этот закон, наряду с понятиями используемыми в законе и законодатель

стве, устанавливает:

* основные направления государственной политики в сфере информатизации;

* основы правового режима информационных ресурсов;

* цели защиты информации;

* режим защиты информации;

* основы защиты прав субъектов в информационной сфере;

* виды ответственности за нарушения законодательства.

Вся защищаемая информация в Законодательстве РФ подразделяется на сведения, составля

ющие государственную тайну и конфиденциальную информацию.

Система защиты государственной тайны рассмотрена в законе "О государственной тайне".

Правовой режим информационных ресурсов.

Правовой режим информационных ресурсов (ИР)определяется нормами устанавливающими:

* порядок документирования информации;

* право собственности на отдельные документы и их массивы;

* категорию информации по уровню доступа к ней;

* порядок правовой защиты информации.

Обязательным условием включения информации в информационные ресурсы является ее докумен

тирование.

Государство имеет право выкупа документированной информации у физических и юридических

лиц в случае отнесения этой информации к государственной тайне.

Собственник ИР, содержащих сведения отнесенные к государственной тайне, вправе распоря

жаться этой собственностью только с разрешения соответствующих органов государственной влас

ти.

Государственные ИР РФ являются открытыми и общедоступными, исключение составляет доку

ментированная информация, отнесенная законом к категориям ограниченного доступа.

Документированная информация с ограниченным доступом по условиям ее правового режима по

дразделяется на информацию отнесенную к государственной тайне и конфиденциальную.

Отнесение информации к государственной тайне осуществляется в соответствии с законом "О государственной тайне".

Отнесение информации к конфиденциальной осуществляется в порядке установленном законо дательством РФ, в соответствии с Перечнем сведений конфиденциального характера утвержденным Указом Президента РФ от 6.03.97г.№188.

К категории конфиденциальной информации закон относит информацию о гражданах (Персональ ные данные), однако перечни этих данных должны быть закреплены на уровне федерального закона. В связи с этим деятельность негосударственных организаций и частных лиц, связанная с обра боткой и представлением пользователям персональных данных подлежит обязательному лицензирова нию.

Запрещено относить к информации с ограниченным доступом:

* законодательные и другие нормативные акты, устанавливающие правовой статус органов го сударственной власти, органов местного самоуправления, организаций, общественных объедине ний, а также права, свободы и обязанности граждан, порядок их реализации;

* документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологи ческую, демографическую, санитарно-эпидемиологическую и другую информацию, необ ходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

* документы, содержащие информацию о деятельности органов государственной власти и ор ганов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;

* документы, накапливаемые в открытых фондах библиотек и архивов, ИС органов государст венной власти, органов местного самоуправления, общественных объединений, организаций, пред ставляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Все ИС, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации.ИС органов государственной власти, которые обрабатывают до

кументированную информацию с ограниченным доступом, а также средства защиты этих систем под лежат обязательной сертификации.

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

Цели защиты информации.

Целями защиты информации являются:

* предотвращение угроз безопасности личности, общества, государства;

* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм несанкционированного вмешательства в ИР и ИС, обеспечение правового режима документированной информации как объекта собственности;

*защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИС;

* сохранение государственной тайны, конфиденциальности документированной информации;

* обеспечение прав субъектов в ИП и при разработке, производстве и применении ИС, технологий и средств их обеспечения.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

* в отношении сведений, отнесенных к государственной тайне - уполномоченными органами на основании закона РФ "О государственной тайне";

* в отношении конфиденциальной информации - собственником ИР или уполномоченным лицом на основании Закона РФ "Об информации, информатизации и защите информации;

* в отношении персональных данных - Федеральным законом.

Органы государственной власти и организации ответственные за формирование и использова

ние ИР, подлежащих защите, разрабатывающие и применяющие ИС и информационные технологии для формирования и использования ИР с ограниченным доступом руководствуются в своей деятельнос ти Законодательством РФ.

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных прог раммно-технических средств защиты, а также обеспечение организационных мер защиты ИС,обрабаты вающих информацию с ограниченным доступом в негосударственных структурах, осуществляется органами государственной власти.

Собственник ИР имеет право осуществлять контроль за выполнением требований по защите ин формации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Риск, связанный с использованием несертифицированых ИС и СО, лежит на собственнике (вла дельце)этих систем и средств.Риск, связанный с использованием информации, полученной из несер тифицированной системы, лежит на потребителе информации.

Защита прав субъектов.

Защита прав субъектов в информационной сфере осуществляется в целях:

* предупреждения правонарушений;
* пресечения неправомерных действий;
* восстановления нарушенных прав;
* возмещения причиненного ущерба.

Защита прав осуществляется судом,третейским судом с учетом специфики правонарушений и нанесенного ущерба.

За правонарушения при работе с документированной информацией органы государственной власти,организации и их должностные лица несут ответственность в соответствии с законодатель ством (уголовным, гражданским, об административных правонарушениях).

Защита прав на доступ к информации.

Отказ в доступе к открытой информации или предоставление пользователям заведомонедос товерной информации могут быть обжалованы в судебном порядке.

Во всех случаях лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут от ветственность в соответствии с уголовным,гражданским законодательством и законодательством об административных правонарушениях. Обеспечение п олитики информационной безопасности РФ возложено на государственные органы и органы по защите конфиденциальной информации на предприятиях с негосударственной формой собственности.

Основой законодательства в сфере информационных правоотношений является закон "Об инфор мации, :". Он содержит массу ссылок на другие законы и отрасли права, в которых конкретизи рованы его положения. К числу наиболее важных положений этого закона с точки зрения право вых отношений является то, что объектом права является только документированная информация. Именно документированная информация подразделяется на категории по уровню доступа и в отноше нии этих категорий устанавливается режим защиты информации. Режим защиты информации устанавли вается: в отношении сведений, отнесенных к государственной тайне - уполномоченными органами на основании закона РФ "О государственной тайне"; в отношении конфиденциальной информации - собственником ИР или уполномоченным лицом на
основании Закона РФ "Об информации, информатизации и защите информации; -в отношении персональ ных данных - Федеральным законом. "Защите подлежит любая документированная информация, неправо мерное обращение с которой может нанести ущерб ее собственнику, владельцу,пользователю и иному лицу." - это принципиальное положение является правовой основой для защиты любой инфор мации кроме той, которую запрещено относить к информации с ограниченным доступом.

Источники:

1 Закон РФ от 20.02.95г. ╬24-ФЗ "Об информации, информатизации и защите информации";

2. Закон РФ от 21.09.93г. ╬182 "О государственной тайне".

3. Закон РФ от 4.07.96г.╬85-ФЗ "Об участии России в международном информационном обмене";

4. Закон РФ от19.07.95г. ╬110-ФЗ "Об авторском праве и смежных правах";

5. Закон РФ от 23.09.92г. ╬3523-1"О правовой охране программ для электронных вычислительных ма
шин и баз данных";

6. Закон РФ от 27.12.91г. "О средствах массовой информации";

7. Закон "О связи"

8. Закон "О федеральных органах правительственной связи и информации";

9. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального
характера";

10. Уголовный кодекс (УК РФ);

11. Гражданский кодекс (ГК РФ ч1 и ч2);

12. Кодекс об административных правонарушениях (КоАП РСФСР);

Вопросы для самоконтроля и собеседования:

1. Понятие информационных правоотношений.

2. Перечислите основные законы, регулирующие информационные правоотношения.

3. Перечислите объекты информационных правоотношений.

4. Дайте определение понятиям: информация, документированная информация, конфиденциаль
ная информация.

5. В чем принципиальное различие правовых понятий "собственник" и "владелец" информаци
онных ресурсов, "владелец" ИР и пользователь информации?

6. Перечислите основные положения в области информационных правоотношений и защите инфор
мации, сформулированные в законе "Об информации,информатизации и защите информации".

7. На какие категории подразделяется документированная информация с ограниченным досту
пом по условиям ее правового режима?

8. Какие сведения запрещено относить к информации с ограниченным доступом?

9. Каковы цели защиты информации, сформулированные в законе "Об информации:"?

10. В отношении каких сведений устанавливается режим защиты информации и кто обязан его поддерживать?

11. В каких целях и кем осуществляется защита прав субъектов в информационной сфере?

Тема ╬3: Правовая основа защиты информации, составляющей государственную тайну.

Вопросы:

3.1 Законодательство РФ о государственной тайне и основные понятия, используемые в нем;

3.2 Сведения, относимые к государственной тайне и их засекречивание.

3.3 Защита государственной тайны.

3.4 Контроль и надзор за обеспечением защиты государственной тайны.

Правовая основа защиты информации, составляющей государственную тайну,содержит в себе основные положения законодательства и нормативных актов, определяющих правовой статус такой информации, правовой режим и органы ее защиты, порядок контроля за обеспе чением защиты.

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

Законодательство РФ о государственной тайне основывается на Конституции РФ, Законе РФ "О безопасности" и включает:

1. Закон РФ от 21.09.93г. ╬182 "О государственной тайне"; положения других актов законода тельства, регулирующих отношения, связанные с защитой государственной тайны. К их числу от носятся :

2. УК РФ (ст.ст.275,276,283,284).

3. ГК РФ (в части трудовых договоров),

4. Закон РФ "Об органах ФСБ в РФ",

5. Закон РФ от 22.08.96г "О порядке выезда из РФ и въезда в РФ" (ст15.1).

Кроме того, правоотношения в этой области регулируют нормативные акты, издаваемые прези дентом РФ и правительством, Государственной технической комиссией (ГТК) и Федеральным агентст вом правительственной связи и информации (ФАПСИ) при президенте. К наиболее важным из них от носятся :

* Указ Президента РФ от 30.11.95г. ╬1203 "Об утверждении Перечня сведений, отнесенных к госу дарственной тайне";

* Указ Президента РФ от 3.04.95г. ╬334 "О мерах по соблюдению законности в области разработ ки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации.",

* Инструкция "О порядке допуска должностных лиц и граждан РФ к ГТ", утверждена постановлением Правительства РФ ╬ 1050 от 28.10.95г.,

* постановление Правительства РФ от 14.10.94г. ╬1161 "О порядке и условиях выплаты процентных надбавок к должностному окладу (тарифной ставке)должностных лиц и граждан, допущенных к го сударственной тайне".

Основные понятия, используемые в законодательстве.

Основы защиты государственной тайны установлены в Законе РФ "О государственной тайне". В нем сформулированы основные понятия, используемые в законодательстве:

государственная тайна - защищаемые государством сведения в области его военной, внешне политической, экономической, разведывательной, контрразведывательной и оперативно-розыскной де ятельности, 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 тай ну и их носителей, а также мероприятий проводимых в этих целях;

допуск к государственной тайне - процедура оформления права граждан на доступ к сведе ниям, составляющим государственную тайну, а предприятий, учреждений и организаций - на прове дение 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, со держащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной доку ментации;

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

3.2 Сведения, относимые к государственной тайне и их засекречивание.

Отнесение сведений к государственной тайне - прерогатива высших органов государствен ной власти.

Перечень категорий сведений, которые могут быть отнесены к государственной тай не, определен в Законе "О государственной тайне", ст.5. Он описывает довольно широкие груп

пы 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 дея тельности.

Однако при засекречивании сведений учреждения, организации, предприятия, органы госу дарственной власти обязаны руководствоваться перечнем сведений, отнесенных к ГТ, утверж денным Указом Президента РФ ╬1203 от 30.10.95г. Данный перечень содержит достаточно боль шой объем сведений (87 наименований), структурированных по областям деятельности: военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно - ро зыскной. В Указе определены конкретные органы государственной власти, наделенные полномочи ями по распоряжению соответствующими сведениями.

Кроме того, Перечень определяет сведения в области организации защиты ГТ, распростране ние которых может нанести ущерб безопасности РФ. К ним относятся:

* сведения в области защиты информации, раскрывающие организацию или фактическое состоя ние защиты ГТ;

* сведения, раскрывающие методы и средства защиты информации, содержащей сведения, составля ющие ГТ, планируемые и проводимые мероприятия по защите информации от несанкци онированного доступа, иностранных технических разведок и утечки по техническим кана лам;

* сведения о системе президентской, правительственной, шифрованной связи, в том числе кодиро ванной и засекреченной, о шифрах, их разработке и средствах анализа шифровальных средств специальной защиты, об информационно-аналитических системах специального назначения;

* сведения, раскрывающие силы, средства, методы, планы, состояние и результаты деятельнос ти органов радиоэлектронной разведки средств связи, а так же данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения.

Запрещено законом относить к государственной тайне следующие сведения:

* о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствия, а также о стихийных бедствиях, их официальных прогнозах и про исшествиях;
* о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
* о привилегиях, компенсациях и льготах, 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.

Засекречивание сведений и их носителей.

Засекречивание сведений и их носителей - введение ограничений на их распространение и на доступ к их носителям. Оно осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Устанавливаются три степени секретности сведений, составляющих ГТ, и соответствующие им грифы секретности для носителей этих сведений: "особой важности", "совершенно секретно", "секретно".

Степень секретности должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ. Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов го сударственной власти, предприятий, учреждений и организаций, является их соответствие дейст вующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присва ивается соответствующий гриф секретности и наносятся реквизиты.

Реквизиты включают данные:
* о степени секретности содержащихся сведений со ссылкой на соответствующий пункт пере чня;

* об органе, предприятии, учреждении, организации осуществляющих засекречивание;

* о регистрационном номере;

* о дате или условии рассекречивания.

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 ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих ГТ, в соответствии с законодательством. Закон "О государственной тайне" не лишает собственника его собственности, а лишь временно ограничивает его право распоряжаться ею. Распоряжение сведениями, составляющими ГТ, как то: передача или взаимная передача, осуществляется в соответствии со ст. 16-18 Закона "О государственной тайне". Решение о передаче сведений, составляющих ГТ, другим государствам принимается Правительством РФ в каждом отдельном случае при наличии экспертного заключения межведомственной комиссии по защите ГТ о такой возможности.

3.3 Защита государственной тайны.

Защита государственной тайны осуществляется органами защиты путем организации правового режима, предусматривающего допуск должностных лиц и граждан к ГТ, доступ и различные виды ответственности (уголовную, административную, гражданско-правовую, дисциплинарную) за нарушение законодательства.

К органам защиты ГТ относятся:

* межведомственная комиссия по защите ГТ;

* органы федеральной, исполнительной власти (ФСБ, МО, ФАПСИ, СВР РФ, Гостехкомиссия и их органы на местах);

* органы государственной власти, предприятия учреждения и организации и их структурные под разделения по защите ГТ.

Межведомственная комиссия по защите ГТ координирует деятельность федеральных, исполни тельных органов.

Органы федеральной, исполнительной власти и их органы на местах организуют и обеспечи вают защиту ГТ в соответствии со своими функциями. Реально они издают нормативные правовые акты по защите ГТ (положения. руководства, инструкции и др.) и контролируют исполнение зако нодательства в целом. Органы государственной власти, предприятия,учреждения организации обеспе чивают защиту сведений, составляющих ГТ, в соответствии с возложенными на них задачами и в пре делах своей компетенции. Ответственность за организацию защиты возлагается на их руководите лей.

Организация защиты в целом включает:

* организацию работы секретного органа;
* организацию секретного делопроизводства;
* организацию работы подразделения по защите информации;
* организацию допуска должностных лиц и граждан к ГТ и доступа к секретным сведениям;
* организацию контроля, за соблюдением режима секретности.

Допуск должностных лиц и граждан к ГТ предусматривает:

* принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих ГТ;
* согласие на частичные временные ограничения их прав (ст. 24 Закона о ГТ);
* письменное согласие на проведение в отношении их полномочными органами (ФСБ) провероч ных мероприятий;
* определение видов, размеров и порядка предоставления льгот, предусмотренных законом;
* ознакомление с нормами законодательства РФ о ГТ, предусматривающими ответственность за его нарушение;
* принятие решения руководителем о допуске лица к сведениям составляющим ГТ.

Допуск осуществляется в соответствии с Инструкцией о порядке допуска должностных лиц и

граждан РФ к ГТ, утвержденной постановлением Правительства РФ ╬ 1050 от 28.10.95г. Инструкци ей предусмотрена форма типового договора (контракта), заключаемого с должностными лицами и гражданами при оформлении допуска к ГТ.

Установлены три формы допуска к ГТ, соответствующие трем степеням секретности све дений, составляющих ГТ: к сведениям особой важности, совершенно секретным,секретным.

Для лиц, допущенных к ГТ 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" - 25%, сов.секретным - 20%, секретно" -10%. Данная норма реализована постановлением Правительства РФ от 14.10.94г. ╬1161 "О порядке и условиях выплаты процентных надбавок к должностному окладу(тарифной ставке) должностных лиц и граждан, допущенных к государственной тайне";

2) преимущественное право при прочих равных условиях на оставление на работе при проведе нии органами государственной власти, предприятиями и организациями организационных и штат ных мероприятий.

Ограничения прав могут касаться:

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

* права на распространение сведений, составляющих ГТ, и на использование открытий и изоб ретений, содержащих такие сведения;

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

Вопросы ограничения права гражданина РФ на выезд за границу в связи с его осведомлен ностью о ГТ и сроки таких ограничений отражены в Законе "О порядке выезда из РФ и въезда в РФ (ст15.1) от 22.08.96г.

Организация доступа к сведениям , составляющим ГТ.

Организация доступа должностного лица или гражданина к сведениям, составляющим ГТ, возла гается на руководителя организации, учреждения, предприятия, а также на их структурные подразде

ления по защите ГТ. Порядок доступа устанавливается нормативными документами, утверждаемыми Правительством РФ (как правило это секретный Приказ министра).Руководители несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знако мятся только с теми сведениями и в таких объемах, которые необходимы ему для выполнения дол жностных обязанностей. Допуск предприятий, учреждений и организаций к проведению работ, связан ных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государст венной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени сек ретности.

Порядок лицензирования установлен в "Положении о лицензировании деятельности предприя тий, организаций и учреждений по проведению работ, связанных с использованием сведений, сос тавляющих ГТ, созданием средств защиты информации, а также с осуществлением мероприятий и ока занием услуг по защите ГТ" утвержденном Постановлением Правительства РФ ╬333 от 15.04.95г. с дополнениями, внесенными Постановлениями ╬509 от 23.04.96г. и ╬513 от 30.04.97г. Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы пред приятия, учреждения и организации и государственной аттестации их руководителей, ответствен ных 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 про цессе 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 ква лификации которых достаточны для обеспечения защиты государственной тайны;
* наличие у них сертифицированных средств защиты.

Порядок сертификации средств защиты информации

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральная службу безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Министерство обороны Российской Федерации 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.

3.4 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. Межведомственный контроль за обеспечением защиты ГТ в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют органы федеральной исполнительной власти (ФСБ РФ, МО РФ, ФАПСИ), Служба внешней разведки РФ, Гостехкомиссия и их органы на местах, на которые эта функция возложена законодательством Российской Федерации. Органы государственной власти, наделенные в соответствии с настоящим Законом 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.

Прокурорский надзор

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны

и законностью принимаемых при этом решений осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Источники:

1. Конституция РФ. Сборник законодательных актов (СЗА) РФ. ИСС "Гарант".

2. Закон РФ от 5.03.92г. ╬2446-1 "О безопасности". СЗА РФ, ИСС "Гарант".

3. Закон РФ от 21.09.93г. ╬182 "О государственной тайне". СЗА РФ, ИСС "Гарант".

4. Закон РФ от 22.08.96г "О порядке выезда из РФ и въезда в РФ" (ст15.1). СЗА РФ, ИСС "Гарант".

5. Указ Президента РФ от 30.11.95г. ╬1203 "Об утверждении Перечня сведений, отнесенных к го сударственной тайне". СЗА РФ, ИСС "Гарант".

6. Указ Президента от 3.04.95г. ╬334 "О мерах по соблюдению законности в области разработ ки, производства, реализации и эксплуатации шифровальных средств, а также предоставления ус луг в области шифрования информации." СЗА РФ, ИСС "Гарант".

7. Инструкция "О порядке допуска должностных лиц и граждан РФ к ГТ", утверждена постановле нием Правительства РФ ╬ 1050 от 28.10.95г. ИСС "Гарант".

8. Постановление Правительства РФ от 14.10.94г. ╬1161 "О порядке и условиях выплаты про центных надбавок к должностному окладу (тарифной ставке) должностных лиц и граждан, допу щенных к государственной тайне". СЗА РФ, ИСС "Гарант".

Вопросы для самоконтроля и собеседования:

1. Какие нормативные правовые акты включает законодательство о государственной тайне?

2. Что понимается под "государственной тайной" и "средствами защиты информации"?

3. Распространение каких сведений в области организации защиты ГТ может нанести ущерб безопасности РФ?

4. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

5. Понятие "засекречивание сведений" и степени секретности документов.

6. Какие данные содержат реквизиты наносимые на носители секретных сведений?

7. Перечислите органы защиты ГТ.

8. Что предусматривает допуск должностных лиц и граждан к ГТ и в соответствии с каким нормативным документом он осуществляется?

9. Какие льготы устанавливаются для лиц допущенных к ГТ и каким нормативным документом они реализуются?

10.Какие ограничения прав граждан и должностных лиц могут наступить в связи с допуском к ГТ.?

11.Каким путем осуществляется допуск предприятий, организаций и учреждений к проведению работ связанных с использованием сведений, составляющих ГТ.?

12.Какими органами осуществляется контроль и надзор за обеспечением защиты ГТ?

Тема ╬4: Распоряжение информацией, составляющей государственную тайну и ее правовая защита.

Вопросы:

4.1 Распоряжение информацией, составляющей государственную тайну.

4.2 Виды посягательств на государственную тайну.

4.3 Уголовно-правовая защита государственной тайны в РФ.

4.1 Распоряжение информацией, составляющей государственную тайну.

Порядок и правила распоряжения информацией, составляющей государственную тайну установлены Законом "О государственной тайне" (Раздел 5, ст.ст.16-19). Право распоряжения сведениями, составляющими государственную тайну предусматривает:

* взаимную передачу сведений органами государственной власти, предприятиями, учреждениями и ор

ганизациями;

* передачу сведений в связи с выполнением совместных и других работ;

* передачу сведений другим государствам;

* защиту сведений при изменении функций субъектов правоотношений.

Взаимная передача сведений, составляющих государственную тайну, органами государствен ной власти, предприятиями, учреждениями и организациями Взаимная передача сведений, составляю щих ГТ (ст16), осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжении которого в соответствии со статьей 9 Закона о ГТ находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие све дения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных огра ничений по ознакомлению со сведениями, составляющими государственную тайну.

Обязательным условием для передачи сведений, составляющих государственную тайну, органам государственной власти, предприятиям, учреждениям и организациям является выполнение ими тре бований, предусмотренных в ст.27 Закона о ГТ.

Статья устанавливает основной принцип передачи сведений, составляющих государственную тайну, между органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ, -принцип санкциониро вания такой передачи органом государственной власти, в распоряжении которого в соответствии со статьей 9 Закона находятся эти сведения. Иными словами, право санкционирования передачи указан ных сведений закрепляется за органами государственной власти, включенными в общегосударствен ный Перечень сведений, отнесенных к государственной тайне. Кроме того, статья содержит еще два принципиальных момента, призванных обеспечить сохранение установленных для передаваемых сведе ний требований режима секретности:

 обязательность сохранения установленных для сведений ограничений по ознакомлению с ни ми, с возложением персональной ответственности за это на руководителей органов государствен ной власти, предприятий, учреждений и организаций, запрашивающих указанные сведения;

 обязательность выполнения в запрашивающей сведения организации условий предусмотренных в статье 27 Закона, обеспечивающих сохранность этих сведений. Важнейшим из таких условий является наличие у этой организации (юридического лица) лицензии для работы со сведениями, составляющими государственную тайну.

Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих ГТ, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан - соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении, в связи с этим, необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.В договоре на проведение совместных и других работ, заключаемом в установленном законом порядке, предусматриваются взаимные обязательства сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну.

Организация контроля за эффективностью защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора.При нарушении исполнителем в ходе совместных и других работ взя

тых на себя обязательств по защите ГТ, заказчик вправе приостановить выполнение заказа до уст ранения нарушений, а при повторных нарушениях - поставить вопрос об аннулировании заказа и ли цензии на проведение работ с использованием сведений, составляющих государственную тайну, и о привлечении виновных лиц к ответственности. При этом материальный ущерб, нанесенный исполни телем государству в лице заказчика, подлежит взысканию в соответствии с действующим законода тельством. Данные положения определяет ст.17 Закона о ГТ.

Статья предусматривает передачу сведений, составляющих государственную тайну, при про ведении совместных и других работ как предприятиям, учреждениям и организациям, так и гражда нам, индивидуально выполняющим указанные работы. Основные права, как и прежде, закреплены за заказчиком работ, на которого возложена ответственность за создание кооперации и подбор испол нителей работ.

Учитывая равенство прав предприятий с различными организационно правовыми формами и фор мами собственности на получение от государства заказов, введена норма, согласно которой при невозможности или нецелесообразности создания подразделений по защите государственной тайны руководителю предприятия разрешено заключать с государственными предприятиями, учреждениями и организациями договоры об использовании услуг их структурных подразделений по защите госу дарственной тайны.

Статьей определен механизм материальной ответственности исполнителей за обеспечение ре жима секретности при выполнении совместных и других работ, установлены права заказчика по осуществлению контроля за выполнением исполнителем договорных обязательств. В качестве основ ной меры воздействия предусмотрена возможность приостановления или прекращения выполнения го сударственного заказа, отзыв лицензии на право проведения работ с использованием сведений, составляющих государственную тайну, а при нанесении государству материального ущерба - компен сация его из средств предприятия.

Передача сведений, составляющих государственную тайну, другим государствам.

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения межведом

ственной комиссии по защите государственной тайны о возможности передачи этих сведений.

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором (соглашением).

Данное положение предусмотрено ст.18 Закона о ГТ.

Статьей устанавливается основной принцип межгосударственных отношений в области переда чи сведений, составляющих государственную тайну, - санкционирование такой передачи Прави тельством Российской Федерации. Статья корреспондируется со статьей 4 Закона, предусматри вающей оформление при передаче сведений правового акта, отражающего обязательства принимающей стороны по сохранению в тайне полученных сведений.

Вступивший в силу в 1996 году Федеральный закон "Об участии в международном информацион ном обмене" предусматривает, что возможность вывоза с территории Российской Федерации докумен тированной информации, отнесенной к государственной тайне или иной конфиденциальной информа ции "определяется Правительством Российской Федерации в каждом отдельном случае". Следует от метить, что идеальным вариантом является наличие действующего между Российской Федерацией и страной-получателем сведений, составляющих государственную тайну, двустороннего межправитель ственного соглашения о взаимной защите указанных сведений. Однако такой идеальный вариант не всегда реализуем, поэтому в подавляющем большинстве случаев обязательства сторон прописываются в общих договорах или соглашениях, например, о военном или военно-техническом сотрудничестве.

Вместе с тем, такой подход не исключает других возможных вариантов решения, когда оно принимается Президентом России. Так, например, рядом Указов Президента Российской Федерации оп ределены образцы вооружения и военной техники,
разрешенные к экспортной поставке в иностранные государства. Указом Президента Российской Феде рации от 26.08.96 года ╬ 1268 утвержден список товаров и технологий двойного назначения, экс порт которых контролируется. Ответственность за незаконный экспорт, например, технологий, науч но-технической информации и услуг, в отношении которых установлен специальный экспортный кон троль, предусмотрена в статье 189 Уголовного кодекса Российской Федерации.

Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений.

Органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, обязаны принять меры по обеспечению защиты этих сведений и их носителей. При этом носители сведений, составляющих ГТ, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:

- правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;

- органу государственной власти, в распоряжении которого находятся соответствующие сведения;

- другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

анное положение установлено ст.16 Закона о ГТ. Настоящая статья является одной из основополагающих в регулировании правоотношений между субъектами в вопросах распоряжения сведениями, составляющими государственную тайну. В соответствии с положениями статьи при изменении функций субъектов правоотношений, изменении формы собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, в обязательном порядке должны быть приняты меры по защите этих сведений и их носителей. Установлены варианты передачи носителей сведений, составляющих государственную тайну.

Возможность передачи составляющих государственную тайну сведений должна быть санкционирована, должны быть обеспечены сохранение установленных для передаваемых сведений требований режима секретности и персональная ответственность за их обеспечение.

4.2 Виды посягательств на государственную тайну.

За посягательства на государственную тайну установлена уголовная ответственность.

Виды посягательств определены в ст.ст.275,276,283,284 главы 29 УК России "Преступления про тив основ конституционного строя и безопасности государства".

Соответствующие статьи определяют следующие виды посягательств на государственную тайну :

* шпионаж;
* выдача государственной тайны иностранному государству;
* оказание помощи иностранному государству;
* разглашение государственной тайны;
* утрата документов, содержащих государственную тайну.

Шпионаж. Это либо одна их форм государственной измены, т.е. преступления, предусмотрен ного ст. 275 УК России, если оно совершено гражданином России, либо специальный состав прес тупления - при совершении иностранцем или лицом без гражданства (ст. 276 УК России). При лю бой форме шпионаж может быть двух видов.

Шпионаж первого вида состоит в передаче, а равно собирании, похищении или хранении в це лях 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.

Передача сведений может осуществляться устно, письменно, с помощью шифров и кодов, лично, через посредников, с использованием почтовой, радио, телефонной, телеграфной, компьютерной свя зи, тайников и т.п.

Собирание осуществляется путем выведывания (опроса), наведения справок, сбора образцов, наблюдения, обследования помещений, зданий, сооружений, участков местности, транспортных сред ств, исследования предметов и документов (включая их фотографирование, снятие копий, изготов ление выписок, чертежей, схем и зарисовок), контроля почтовых отправлений, телеграфных и иных сообщений, прослушивания телефонных переговоров, съема информации с технических каналов свя зи, обработки сообщений средств массовой информации, извлечения сведений из ЭВМ и т.д.

Похищение сведений, состоит в неправомерном изъятии у собственников или владельцев, поль зователей материальных носителей информации: документов, перфокарт, перфолент, фото-, кино-, видео-, аудиоматериалов, дискет для ЭВМ и т.д., содержащих сведения, составляющие государст венную тайну, а также предметов (изделий, приборов, оружия, веществ), сведения о которых, сос тавляют государственную тайну.

Хранение сведений представляет собой сбережение лицом у себя, у других лиц либо в специ ально подготовленных местах, хранилищах, помещениях и т.д. материальных носителей с информаци ей, составляющей государственную тайну, которые могут быть до этого похищены, изготовлены самим лицом (например, в виде копий, отчетов, сообщении и т.п.) или добыты каким-либо иным путем (например, получены от третьих лиц).

Выдача государственной тайны иностранному государству, иностранной организации или их представителям, как и шпионаж, совершенный гражданином Российской Федерации, является одной из форм государственной измены (ст. 275 УК России).

Выдача государственной тайны состоит в сообщении лицом перечисленным "адресатам" любым способом сведений, составляющих государственную тайну. Принято считать, что выдача государст венной тайны отличается от шпионажа способом завладения лицом сообщаемыми сведениями. При вы даче он не собирает и не похищает их, а становится их обладателем при каких-либо других обсто ятельствах (узнает по службе или работе, из случайного разговора, находит и т.п.).

Оказание помощи иностранному государству (ст. 275 УК России). Эта форма государственной измены охватывает все действия в ущерб внешней безопасности Российской Федерации, совершенные российским гражданином в сговоре с указанными в законе "адресатами", которые не охватываются составами шпионажа и выдачи государственной тайны.

В рамках иного оказания помощи могут быть совершены такие действия,как разглашение госу дарственной тайны по заданию иностранного государства, иностранной организации или их пред ставителей, но без передачи или выдачи им (например, в средствах массовой информации в целях компрометации Российской Федерации), уничтожение носителей государственной тайны, поврежде ние и фальсификация компьютерной информации, содержащей такую тайну, и т.п.

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 обстоятельст вах, например, в ходе предварительного следствия, судебного процесса и т.п. (Так Постановлени ем Конституционного Суда Российской Федерации от 27 марта 1996 г. разъясняется, что за разгла шение государственной тайны должны нести ответственность также и те, кому указанные сведения были доверены и при обстоятельствах, не связанных с их службой или работой.)

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

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

4.3 Уголовно-правовая защита государственной тайны в РФ.

За посягательства на государственную тайну установлена уголовная ответственность. Меры ответственности определены в главе 29 УК РФ, ст.ст.275,276.283,284 - государственная изме на, шпионаж, разглашение государственной тайны, утрата документов, содержащих государственную тайну, соответственно. Виды и меры ответственности граждан по этим статьям приведены в табл. 4.1.

Так статья 275 "Государственная измена" определяет, что государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, ино странной организации или их представителям в проведении враждебной деятельности в ущерб внеш ней безопасности Российской Федерации, совершенная гражданином Российской Федерации,

- наказывается лишением свободы на срок от двенадцати до двадцати лет с конфискацией иму щества или без таковой.

Статья 276 "Шпионаж" устанавливает, что передача, а равно собирание, похищение или хране ние в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иност ранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства,

- наказывается лишением свободы на срок от десяти до двадцати лет.

Статья 275 УК России содержит примечание о том, что лицо, совершившее преступления, пре дусмотренные статьями 275 и 276 настоящего кодекса, освобождается от уголовной ответственности, "если оно добровольным и своевременным сообщением органам власти или иным образом способство вало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления".

Статья 283 Разглашение государственной тайны устанавливает, что 1.разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков го сударственной измены

- наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определен ной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее тяжкие последствия,

- наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284 "Утрата документов, содержащих государственную тайну" устанавливает, что нару шение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержа

щими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких пос ледствий,

- наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать опреде ленные должности или заниматься определенной деятельностью на срок до трех лет или без таково го.

Источники:

1. Закон РФ "О государственной тайне" ст.ст.16-19. СЗА РФ, ИСС "Гарант";

2. Уголовный кодекс РФ Глава 29(ст.ст.275,276,283,284). СЗА РФ, ИСС "Гарант";

Литература:

1. Крылов В.В. Информационные компьютерные преступления. М: ИНФРА М-НОРМА, 1997, 276с.

2. Нормативные правовые акты по защите государственной тайны. Часть1. М: МВК по защите ГТ, 1998, 111с.

Вопросы для самоконтроля и собеседования:

1. Какие виды передачи сведений, составляющих ГТ, предусмотрены законом "О государствен ной тайне"?
2. С чьей санкции осуществляется взаимная передача сведений, составляющих ГТ, предприяти ями, организациями, учреждениями?
3. Особенности передачи сведений, составляющих государственную тайну, в связи с выполне нием совместных и других работ?

4. Особенности передачи сведений, составляющих государственную тайну, другим государствам?

5. Перечислите виды посягательств на государственную тайну.

6. Дайте характеристику понятию "шпионаж".

7. Что понимается под выдачей государственной тайны иностранному государству?

8. Приведите примеры такого посягательства на государственную тайну, как оказание помощи иностранному государству? Чем оно отличается от шпионажа и выдачи иностранному государству?

9. Что означает разглашение государственной тайны?

10. Что понимается под утратой документов, содержащих ГТ?

11. Виды и меры наказания, предусмотренные УК РФ за государственную измену?

12. Виды и меры наказания граждан, предусмотренные УК РФ за шпионаж?

13. Виды и меры наказания граждан, предусмотренные УК РФ за разглашение государственной тайны?

14. Виды и меры наказания граждан, предусмотренные УК РФ за утрату документов, содержащих государственную тайну?

Тема 5: Конфиденциальная информация как объект информационных правоотношений и защиты.

Вопросы:

5.1. Нормативно-правовые акты в области защиты конфиденциальной информации и прав субъектов информационных правоотношений.

5.2.Отнесение сведений к конфиденциальной информации.

5.3.Характеристика видов тайн, составляющих конфиденциальную информацию.

5.4.Примерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации.

Информатизация общества в настоящее время развивается в направлении создания глобальных инфраструктур, затрагивающих все сферы деятельности человека. Ускоренными темпами развиваются системы информационной поддержки принятия решений, глобальные телекоммуникационные сети, сис темы автоматизированного документооборота, электронные банки данных.

Широкое внедрение современных информационных технологий создает благоприятную обстановку для злоумышленников в плане доступа к конфиденциальной информации или ее незаконного распрост ранения, 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 оп ределенных Законодательством РФ, за исключением государственной тайны. Однако отсутствие от дельного закона определяющего правовые основы защиты конфиденциальной информации усложняет задачу изучения этой проблемы и вызывает необходимость анализа и оценки достаточно большого пе речня актов законодательства.

К конфиденциальной информации относится и коммерческая тайна. В настоящее время информа ция, составляющая коммерческую тайну, является наиболее распространенной, поскольку охватывает все сферы деятельности коммерческих и государственных предприятий, накапливается и хранится в налоговых органах, органах Минюста, других органах государственной власти, в учреждениях науки и культуры. Согласно закона "Об информации, информатизации и защите информации", конфиденциаль ная информация - информация ограниченного доступа и она защищается законодательством. Поэтому является важным установить структуру законодательства, которое регулирует правоотношения свя занные с конфиденциальной информацией, а также правовой режим сохранения конфиденциальности и правовой ответственности за ее нарушение.

1. Нормативно-правовые акты в области защиты конфиденциальной информации и прав субъектов информационных правоотношений.

Правовой статус конфиденциальной информации определен в Законе РФ "Об информации информа

тизации и защите информации": конфиденциальная информация - документированная информация, дос туп к которой ограничивается в соответствии законодательством РФ.

Таким образом, 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 опреде ляющие ответственность за нарушения установленных норм права в этой области.

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

1. Конституция РФ (ст.23,24,29,42 и др.)

2. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите ин формации.";

3. Гражданский кодекс Российской Федерации (части первая и вторая) (с изм. и доп. от 20 февра ля, 12 августа 1996 г., 24 октября 1997 г.).Статья 139, 857.;

4. Федеральный закон от 3 февраля 1996 г. N 17-ФЗ "О внесении изменений и дополнений в Закон РСФСР "О банках и банковской деятельности в РСФСР" (с изм. и доп. от 31 июля 1998 г.) ст.26

5. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциаль ного характера";

6. Постановление Правления ПФР от 30 августа 1996 г. N 123 "Об утверждении перечня сведений, составляющих конфиденциальную информацию";

7. "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" утвержденного Постановлением Правительства РФ от 3.11.94г.

8. УК РФ от13.06.96г. ст.183,137, 138,147, 155;

9. Уголовно-процессуальный кодекс РСФСР;

10. КЗоТ РФ (ст.15);

Кроме этого к законодательству в области защиты конфиденциальной информации относятся законодательные и нормативные акты регулирующие правоотношения в таможенных органах, пенсион ных фондах, банковской сфере, коммерческой деятельности, в органах налоговой полиции и стра хования, в сфере отдельных видов профессиональной деятельности. Большинство этих документов

или извлечений из них приводится в приложении к лекции.

Данные нормативные правовые акты определяют:

* перечни сведений конфиденциального характера (виды тайн);

* ограничение доступа к конфиденциальной информации и ее защиту;

* гражданскую, уголовную и другие виды ответственности за правонарушения при обращении с кон фиденциальной информацией.

5.2. Отнесение сведений к конфиденциальной информации.

Отнесение сведений к конфиденциальной информации осуществляется в порядке, устано вленном законодательством РФ и в соответствии с "Перечнем сведений конфиденциального характе ра", утвержденным Указом Президента РФ от 6.03.97г. ╬188. К сведениям конфиденциального харак тера данный перечень относит:

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

2. Сведения, составляющие тайну следствия и судопроизводства.

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

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответ ствии 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 РФ и федеральными законами (коммерческая тайна).

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

Кроме этого к сведениям конфиденциального характера относится банковская тайна (тайна об

операциях, счетах и вкладах) на основании "Заключения Президента РФ на проект Федерального закона "О внесении дополнения в статью 26 ФЗ "О банках и банковской деятельности" от 15.05.97г.

В своей основе законодательство относит к конфиденциальной информации различные виды тайн (рис1.).

Отнесение сведений, составляющих служебную, коммерческую и банковскую тайну, к конфиденциальной информации устанавливает Гражданский кодекс РФ (ст.ст.139,857).

Отнесение сведений, составляющих остальные виды тайн, осуществляется Федеральными законами регулирующими правовые отношения связанные с профессиональной деятельностью, со следствием и судопроизводством. Этими же законами устанавливается ограничение доступа к конфиденциальной информации.

Необходимость установления ограничений доступа к различным видам тайн определенным в законодательстве РФ не является самоцелью. Это реализация прав и свобод граждан, организаций, учреждений, определенных Конституцией РФ (ст.ст. 23, 24.1). Вместе с тем Конституция гарантирует права на доступ к определенной информации (ст.24.2, 29.4,5; 42) и ответственность должностных лиц за ее сокрытие. Поэтому в законе "Об информации:" приводится перечень сведений, которые запрещено относить к информации с ограниченным доступом.

Запрещено относить к информации с ограниченным доступом, и в том числе к конфиденциальной следующие документы:

* законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
* документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
* документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;

* документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах ор ганов государственной власти, органов местного самоуправления, общественных объединений, орга низаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обя занностей граждан.

На практике процедура отнесения сведений к конфиденциальной информации представляет со бой процедуру отнесения информации к конкретному виду тайны, являющейся конфиденциальной инфор мацией по закону. Соответственно и ответственность в законодательстве предусмотрена за наруше ния той или иной тайны.

5.3.Характеристика видов тайн, составляющих конфиденциальную информацию.

Общий перечень видов тайн и нормативные документы их определяющие приведены в табли це 5.1. Он представляет собой "согласованный" перечень, так как в Указе президента данные ви ды тайн перечисляются в обобщенном виде.

Служебная и коммерческая тайна.

Понятие и правовой статус служебной и коммерческой тайны определяет Гражданский кодекс РФ (ст.139).

"Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации, принимает меры к охране ее конфиденциальности". Из этого следует выделить, по крайней мере, три условия выполне ние которых с точки зрения права позволяет рассматривать информацию как служебную или коммер ческую тайну и относить ее к конфиденциальной.

Во-первых, информация должна иметь действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Это означает, что знание и использование ее третьими лицами может нанести материальный или иной ущерб органу государственной власти, предприятию, организации, учреждению как с государственной, так и не государственной формой собственности.

Во-вторых, к ней нет свободного доступа на законном основании. Это означает, что данная информация не относится к информации, которую законом запрещено относить к конфиденциальной.

В-третьих, обладатель информации принимает меры к охране ее конфиденциальности. Это озна чает, что обладатель обязан применять меры по ограничению доступа всеми законными способами предусмотренными законодательством РФ. К таким мерам следует отнести: организационные и норма тивно-правовые, ограничивающие доступ к носителям информации; использование только сертифициро ванных средств защиты (программных и технических) и другие.

Конкретный перечень сведений, составляющих коммерческую тайну, в законодательстве отсут ствует. Такие перечни определяет собственник информации, составляющей коммерческую тайну Следу ет также отметить, что при разработке законодательства о государственной тайне, предполагалось, что вопросы служебной тайны - регламенты использования конфиденциальных сведений служебного ха рактера - будут отражены в законе о государственной службе. Однако, это не было осуществлено. Заложенное в статье 139 Гражданского кодекса РФ фактическое отождествление понятий служебной и коммерческой тайны внесло лишь путаницу. Постановлением Правительства РФ от3.11.94г. ╬1233 было утверждено "Положение о порядке обращения со служебной информацией ограниченного распростране ния в федеральных органах исполнительной власти", которое в настоящее время является единст венным нормативным документом, определяющим порядок обращения с документами "для служебного пользования".

Банковская тайна представляет собой сведения об операциях, счетах и вкладах, а также све дения определяемые законодательством в сфере банковской деятельности.

Все остальные виды тайн представляют собой конкретные перечни сведений устанавливаемых тем или иным нормативным правовым актом.

5.4.Примерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации.

Ранее отмечалось, что конкретный перечень сведений, составляющих коммерческую тайну, в законодательстве отсутствует. Такие перечни определяет собственник информации, составляющей

коммерческую тайну. На основе опыта государственных и коммерческих предприятий разработан при мерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации.

Примерный перечень сведений, составляющих коммерческую и (или) служебную тайну организации.

1.ПРОИЗВОДСТВО

Сведения о структуре и масштабах производства, производственных мощностях, типе и разме щении оборудования, запасах сырья, материалов и готовой продукции.

2.УПРАВЛЕНИЕ

Сведения о применяемых оригинальных методах управления организацией. Сведения о подгото вке, принятии и исполнении отдельных решений руководства организации по коммерческим, органи зационным, 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 орга нов 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 рыноч ной конъюнктуры. Сведения о рыночной стратегии организации, о применяемых организацией ориги нальных методах осуществления продаж, об эффективности служебной и коммерческой деятельности организации

7. ПАРТНЕРЫ

Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, пот ребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, сос тоящих в деловых отношениях с организацией.

8. КОНКУРЕНТЫ

Обобщенные сведения о внутренних и зарубежных предприятиях как о потенциальных конкурен тах в деятельности организации, оценка качества деловых отношений с конкурирующими предприяти ями в различных сферах деловой активности.

9. ПЕРЕГОВОРЫ

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами органи зации.

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 ски док.

12. ТОРГИ, АУКЦИОНЫ

Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или про дажи 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 опти мальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.). Аналитические и гра фические 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 обеспече

ния.

14. ТЕХНОЛОГИЯ

Сведения об особенностях используемых и разрабатываемых технологий и специфике их приме нения, 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-партне ров и передаваемые ими в пользование на доверительной основе.

Источники:

1. Конституция РФ (ст.23,24,29,42 и др.)

2. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите ин формации.";

3. Гражданский кодекс Российской Федерации (части первая и вторая) (с изм. и доп. от 20 февра ля, 12 августа 1996 г., 24 октября 1997 г.).Статья 139, 857.;

4. Федеральный закон от 3 февраля 1996 г. N 17-ФЗ "О внесении изменений и дополнений в Закон РСФСР "О банках и банковской деятельности в РСФСР" (с изм. и доп. от 31 июля 1998 г.) ст.26

5. Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциаль ного характера";

6. Постановление Правления ПФР от 30 августа 1996 г. N 123 "Об утверждении перечня сведений, составляющих конфиденциальную информацию";

7. "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" утвержденного Постановлением Правительства РФ от 3.11.94г.

8. УК РФ от13.06.96г. ст.183,137, 138,147, 155;

9. Уголовно-процессуальный кодекс РСФСР;

10. КЗоТ РФ (ст.15);

Вопросы для самоконтроля и собеседования:

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

2. Перечислите сведения указанные в Указе Президента РФ ╬188 "Перечень сведений конфиденциаль ного характера.

3. Какие сведения запрещено относить к сведениям с ограниченным доступом? В каком правовом акте этот перечень указан.

4. Поясните схему формирования и отнесения сведений к конфиденциальной информации.

5. Дайте характеристику служебной и коммерческой тайны. Какой правовой акт устанавливает ее правовой статус.

6. Какие виды тайн составляют служебные сведения и относятся к служебной тайне.

7. Какие сведения составляют банковскую тайну, в каких нормативно-правовых актах закреплен ее правовой статус.

8. Какие виды тайны относятся к профессиональной тайне? Дайте краткие пояснения в каких право вых актах устанавливается правовой статус этих тайн.

9. Какие сведения составляют основу "примерного перечня сведений, составляющих коммерческую и или) служебную тайну организации".

Тема ╬6 Защита конфиденциальной информации и прав ее собственников.

Вопросы:

6.1. Нормативные требования по защите конфиденциальной информации.

6.2 Правовая защита конфиденциальной информации.

6.3 Защита права на доступ к информации.

Защита конфиденциальной информации основывается на конституционных положениях устанавли вающих права и свободы граждан и организаций о сохранении в тайне определенных данных об их законной деятельности, личной и семейной жизни, в состав которых входят тайны о доходах и ком мерческой деятельности, защита прав собственности, к которой относятся информационные ресурсы конфиденциального характера.

Законодательство, реализующее положения Конституции РФ, устанавливает:

* Нормативные требования по защите конфиденциальной информации;

* Ответственность граждан и должностных лиц за разглашение или нарушение конфиденциальности различных видов тайн;

* Защиту прав граждан на доступ к открытой информации.

Указанные вопросы рассматриваются в следующих нормативно-правовых актах: Закон "Об инфор мации, информатизации и защите информации; Кодекс Законов о Труде КЗОТ; Уголовный кодекс РФ; Гражданский кодекс РФ; другие кодексы и законы связанные с профессиональной деятельностью.

6.1. Нормативные требования по защите конфиденциальной информации.

Нормативные правовые положения по защите конфиденциальной информации определены в Законе РФ "Об информации, информатизации и защите информации".

В отношении нее целями защиты являются:

* предотвращение утечки, хищения, утраты, искажения информации;

* предотвращение угроз безопасности личности, общества, государства;

* предотвращение несанкционированных действий по уничтожению и копированию;

* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персо
нальных данных, имеющихся в информационных системах;

* сохранение конфиденциальности документированной информации.

Режим защиты в отношении конфиденциальной документированной информации устанавливается собственником информации или уполномоченным лицом на основании этого закона (ст.21.1). Владе
лец документов, массива документов, информационной системы обеспечивает уровень защиты информа
ции в соответствии с законодательством.

В качестве собственников конфиденциальной информации могут выступать:

* государство (государственные органы и предприятия, учреждения, организации);

* юридические лица (организации, учреждения предприятия с негосударственной формой собственнос
ти);

* физические лица (граждане).

Организации, обрабатывающие конфиденциальную информацию, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Деятельность негосударственных организаций и частных лиц, связанная с обработкой и пре
доставлением пользователям персональных данных, подлежит обязательному лицензированию.

Органы государственной власти и организации, ответственные за формирование и использова
ние информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использова
ния информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности зако
нодательством Российской Федерации.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных прог
раммно-технических средств защиты, а также обеспечение организационных мер защиты информацион
ных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяе
мом Правительством Российской Федерации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осущест

влять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы (Гостехкомиссия РФ и ФАПСИ) соблюдают условия конфиденциальности самой информации и результатов проверки.

Права и обязанности собственников и владельцев конфиденциальной информации в области ее защиты.

Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с Федеральным законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Если негосударственная организация использует шифровальные средства, предназначенные для криптографической защиты конфиденциальной информации, то деятельность связанная с эксплуатацией этих средств подлежит лицензированию. А в целом для защиты могут использоваться только

сертифицированные средства защиты.

Таким образом закон устанавливает, что государственные органы, предприятия, учреждения, организации обязаны иметь службы по защите конфиденциальной информации.
Для негосударственных структур эта норма реализуется необходимостью защиты коммерческой тайны в соответствии со ст.139 ГК РФ.

Органы защиты.

Органами защиты конфиденциальной информации являются те организации, учреждения предприятия, которые обрабатывают и хранят эту информацию и их специальные службы или подразделения, органы судебной власти осуществляющие правовую защиту собственников.

Защиту тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений обеспечивает кроме того ФАПСИ и его органы.

Допуск должностных лиц и граждан к конфиденциальной информации осуществляет руководитель организации, учреждения, предприятия.

Правовой основой для допуска является:

* обязательство должностного лица (работника) о неразглашении сведений конфиденциального харак тера, закрепленное в трудовом договоре (контракте) согласно ст.15 КЗоТ РФ;
* нормативный правовой акт (документ) изданный или утвержденный руководителем организации опре деляющий порядок допуска и доступа к сведениям конфиденциального характера.

Для обеспечения правовой защищенности в полной мере служебной и коммерческой тайны "обя зательство" (контракт) может составляться помимо трудового договора и содержать следующие обя зательства работника:

* не разглашать сведения, составляющие служебную или коммерческую тайну организации, которые ему будут доверены или станут известны по работе;
* Не передавать третьим лицам и не раскрывать публично сведения, составляющие служебную или коммерческую тайну организации без согласия администрации;
* выполнять требования приказов, инструкций и положений по обеспечению сохранности служебной и коммерческой тайны организации;
* В случае попытки посторонних лиц получить от него сведения о служебной или коммерческой тай

не организации немедленно сообщить об этом руководителю структурного подразделения и начальни ку службы безопасности организации;

* сохранять служебную и коммерческую тайну тех предприятий, с которыми организация имеет дело вые отношения;

* не использовать знания служебной или коммерческой организации для занятий любой деятельнос тью, которая в качестве конкурентного действия может нанести ущерб организации;

* в случае его увольнения все носители служебной или коммерческой тайны организации, которые находились в его распоряжении, передать организации;

* об утрате или недостаче носителей служебной и коммерческой тайны, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, личных печатей и о других фактах, которые мо гут привести к разглашению служебной или коммерческой тайны организации, а также о причинах и условиях возможной утечки сведений, немедленно сообщить начальнику службы безопасности.

Кроме того, такое обязательство должно содержать последствия за нарушения указанных пун ктов и применяемые меры со стороны администрации и со стороны органов судебной власти в соот ветствии с уголовным гражданским и административным законодательством.

Порядок оформления документов содержащих конфиденциальную информацию. При организации служебного делопроизводства, связанного с использованием служебной и иной тайны, на исполняе мых документах и носителях информации проставляются реквизиты, которые включают:

- гриф (для служебного пользования (ДСП) и др.);
- регистрационный номер и дату регистрации;
- наименование организации, учреждения, предприятия;
- наименование (название документа);
- фамилия и инициалы исполнителя.

6.1 Правовая защита конфиденциальной информации.

Защитить конфиденциальную информацию организационными мерами, программными и технически ми средствами в полной мере в современных условиях невозможно. Поэтому важным способом защиты

выступает правовая защита конфиденциальной информации, а вернее правовая защита собственников информационных ресурсов, содержащих конфиденциальную информацию, а также прав тех юридических и физических лиц которые предоставили в распоряжение той или иной организации конфиденциальные сведения в силу существующего закона. Например, те данные, которые предоставляются в налоговые органы. Эти данные могут содержать коммерческую или банковскую тайну, персональные данные и другие виды тайн. Или, например, данные которые накапливаются в пенсионных фондах, военных комиссариатах.

Следует отметить, что существующее законодательство, предусматривающее ответственность за разглашение тех или иных сведений относящихся к конфиденциальным, защищает права и распространяется на нарушителей независимо от того получили они конфиденциальные сведения законным путем или незаконным, из компьютерной системы или с бумажных и других видов носителей. Рассматривается сам факт нарушения конфиденциальности и его последствия. Если сведения получены из компьютерной системы в результате несанкционированного доступа, то к нарушителю дополнительно применяются правовые меры за несанкционированный доступ к конфиденциальной информации (компьютерные преступления).

Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

Российским законодательством предусматривается следующие виды правовой защиты конфиденциальных данных и прав их собственников:

* Уголовно-правовая;
* Гражданско-правовая;
* Административная;
* Дисциплинарная.

Уголовно-правовая защита.

Уголовно-правовая защита реализуется привлечением нарушителя конфиденциальности данных к уголовной ответственности на основании УК РФ.

Уголовный кодекс РФ предусматривает ответственность за нарушения и разглашение следующих видов тайн:

* личной и семейной тайны (ст.137);

* нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст.138);

* незаконное получение и разглашение сведений составляющих коммерческую или банковскую тайну (ст.183);

* нарушение изобретательских и патентных прав (ст.147).

* разглашение тайны усыновления (ст.155) и ряд других.

Ответственность за нарушение и разглашение личной и семейной тайны определяет статья 137. Нарушение неприкосновенности частной жизни.

Она определяет, что:

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, -

наказываются:

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев,

- либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов,

- либо исправительными работами на срок до одного года,

- либо арестом на срок до четырех месяцев.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, -

наказываются:

- штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в раз

мере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев,

- либо лишением права занимать определенные должности или заниматься определенной дея тельностью на срок от двух до пяти лет,

-либо арестом на срок от четырех до шести месяцев.

Ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений устанавливает ст.183.

В частности она определяет, что

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

-штрафом в размере от пятидесяти до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца;

-либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов,

-либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, -наказы вается:

- штрафом в размере от ста до трехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до трех месяцев,

- либо лишением права занимать определенные должности или заниматься определенной дея тельностью на срок от двух до пяти лет,

- либо арестом на срок от двух до четырех месяцев.

3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации, -

наказываются:

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в

размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев;

- либо ограничением свободы на срок до трех лет,

- либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Ответственность за незаконные получение и разглашение сведений, составляющих коммер ческую или банковскую тайну устанавливает ст.183.

В частности она определяет что:

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо неза конного использования этих сведений -

наказывается:

- штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев;

- либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинте ресованности и причинившие крупный ущерб, -

наказываются:

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в разме ре заработной платы или иного дохода осужденного за период от двух до пяти месяцев;

- либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минималь ных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за пе риод до одного месяца либо без такового.

Ответственность за нарушение изобретательских и патентных прав устанавливает

ст.147.

В частности она определяет. что:

1. Незаконное использование изобретения, полезной модели или промышленного образца, раз глашение без согласия автора или заявителя сущности изобретения, полезной модели или промышлен ного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, -

наказываются:

- штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев;

- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов;

- либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, -

наказываются:

- штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев;

- либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

Ответственность за разглашение тайны усыновления (удочерения) устанавливает ст.155.

В частности она определяет, что:

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений, -

наказывается:

- штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере за работной платы или иного дохода осужденного за период от одного до двух месяцев;

- либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев с лишением права занимать определенные должности или заниматься определенной деятель ностью на срок до трех лет или без такового.

Гражданско - правовая защита.

Гражданско -правовая защита реализуется привлечением нарушителя конфиденциальности данных к гражданской ответственности на основании ГК РФ. В своей основе гражданско-правовая ответст веность предусмвтривает возмещение различного рода убытков потерпевшему (собственнику) в ре зультате разглашения принадлежащих конфиденциальных сведений (например коммерческая тайна) или конфиденциальных сведений о нем (персональные данные). Рассмотрим лишь наиболее важные виды тайн и гражданскую ответственность за их разглашение.

Служебная и коммерческая тайна.

Гражданскую ответственность за разглашение служебной или коммерческой тайны устанавлива ет Ст.139 ч.2 ГК РФ.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предус мотренными Гражданским Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммер ческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работ ников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Банковская тайна.

Гражданскую ответственность за разглашение банковской тайны устанавливает Ст.26 закона "О банках и банковской деятельности"(с изм.от31.06.98г.)

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесен

ного ущерба, в порядке, установленном федеральным законом.

6.3 Защита права на доступ к информации.

Конституционные положения по защите прав на доступ к открытой информации реализованы в законодательстве. Установленные нормы сформулированы в законе "Об информации...:." Ст.24.

В частности ст.24 предусматривает, что отказ в доступе к открытой информации или предос тавление пользователям заведомо недостоверной информации могут быть обжалованы в судебном по рядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-прода жи, по другим формам обмена информационными ресурсами между организациями рассматриваются ар битражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недос товерную информацию, имеют право на возмещение понесенного ими ущерба.

Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предостав лении информации пользователям или в результате других нарушений прав пользователей.

Руководители, другие служащие органов государственной власти, организаций, виновные в не законном ограничении доступа к информации и нарушении режима защиты информации, несут ответст венность в соответствии с уголовным, гражданским законодательством и законодательством об адми нистративных правонарушениях.

Источники:

1. Конституция РФ. ИСС Гарант.

2. Закон "Об информации, информатизации и защите информации ".

3. УК РФ.

4. ГК РФ.

Вопросы для самоконтроля и собеседования по теме:

1. Каковы цели защиты информации и для каких собственников они предназначены.

2. Кто организует и осуществляет защиту конфиденциальной информации.

3. Кто осуществляет допуск к конфиденциальной информации и в чем он заключается?

4. Содержание контракта о неразглашении конфиденциальных сведений служащим или работником?

5. Порядок оформления документов конфиденциального характера.

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

7. Какая уголовно-правовая ответственность предусмотрена за разглашение коммерческой или бан ковской тайны?

8. В чем суть гражданско-правовой ответственности за разглашение коммерческой или банковской тайны?

9. В чем основная суть защиты прав на доступ к информации?

Тема ╬7. Правовая защита интеллектуальной собственности в сфере информатизации.

Вопросы:

7.1 Нормативно - правовая база в области авторского права и защиты интеллектуальной собственности в сфере информатизации.

7.2 Объекты и субъекты правовой охраны.

7.3 Авторские права на программы для ЭВМ и базы данных.

7.4 Регистрация программ для ЭВМ и баз данных.

7.5 Использование программ для ЭВМ и баз данных.

7.6 Защита авторского права на программу для ЭВМ и базу данных.

В период перехода страны к рыночным отношениям система законодательства претерпела карди нальные изменения. Это относится и к правовым нормам, регулирующим создание, правовую охрану и использование продуктов интеллектуального творчества. Появились новые охраняемые объекты и программы (программное обеспечение) электронно-вычислительных машин. Введение в качестве объек та охраны программ для ЭВМ и баз данных явилось следствием изменения отношения к продуктам ин теллектуальной деятельности человека, оно стало более "рыночным", а сами продукты интеллекту альной деятельности все более отчетливо приобретают черты товара (продукта интеллектуального труда, созданного для функционирования его на рынке).

Как следствие, понятие "интеллектуальной собственности" стало правовым понятием и удосто илось конституционного внимания. Статья 144 Конституции Российской Федерации, имеющая прямое действие, гарантирует каждому свободу творчества и предусматривает охрану интеллектуальной собственности законом.

Интеллектуальная собственность - совокупность прав на продукт интеллектуального творчест ва. Владение, пользование, распоряжение плодами творчества носит такой же специфический харак тер, как и само понятие интеллектуальной собственности.

Таким образом, с точки зрения права, к интеллектуальной собственности относится авторс кое право, которое и необходимо защищать. Применительно к области информатизации таким правом является авторское право на программы для ЭВМ и базы данных.

7.1 Нормативно - правовая база в области авторского права и защиты интеллектуальной собственности в сфере информатизации.

Нормативно - правовая база в области авторского права и защиты интеллектуальной собст венности в сфере информатизации базируется на Конституции РФ. Она включает законы,норматив ные акты правительства и различных министерств и ведомств .

Законодательные акты по защите авторского права:

* "Об авторском праве и смежных правах" ╬5351-1 от 9.07.93г;

* "О правовой охране программ для электронных вычислительных машин и баз данных" ╬3523-1 от 23.09.92г.(Гражданское законодательство).

* УК РФ (ст.146);

* КоАП РСФСР (ст.150.4).

Нормативные акты по защите интеллектуальной собственности (нормативные правовые акты Государственного таможенного комитета):

* Письмо ГТК от 28.10.97г. ╬01-15/20508 "О мерах по защите прав на интеллектуальную собственность.";

* Письмо ГТК России от 13.06.96г. ╬01-54.10565 "О мерах по обеспечению сохранности объектов интеллектуальной собственности." (утверждено МВД, ГТК, ГКАП И ФСНП России),

Нормативные акты правительства РФ, РосАПО, Роспатента:

* Временное положение "О государственном учете и регистрации баз и банков данных." Утверждено Постановлением Правительства ╬226 от 28.02.96г.;

* Положение "О регистрационных сборах за официальную регистрацию программ для ЭВМ, баз данных и топологий интегральных схем". Утверждено Постановлением Правительства РФ ╬793 от 12.08.93г.;

* Приказ Роспатента от 31 декабря 1998 г. N 245 "Об утверждении Правил регистрации договоров на программы для электронных вычислительных машин, базы данных и топологии интегральных микро схем"

* Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для ЭВМ и баз данных. " Утверждено Приказом РосАПО от 5.03.93г. ╬7п.

Закон "Об авторском праве и смежных правах" является частью Гражданского законодатель ства РФ. Закон "О правовой охране программ для ЭВМ и БД" является составной частью законода тельства об авторском праве и смежных правах. В своей основе он устанавливает:

* правовые понятия используемые в законодательстве, объекты правовой охраны и субъекты защиты;

* правовые нормы использования программ для ЭВМ и БД;

* правовую основу защиты авторского права на программы для ЭВМ и БД.

К основным правовым понятиям, используемым в данном законодательстве относятся:

Объекты правовой охраны:

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 подразумевают ся 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;

Субъекты правовой охраны:

автор - физическое лицо, творческим трудом которого создано произведение;

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

Понятия, связанные с использованием программ для ЭВМ и БД:

адаптация - это внесение изменений, осуществляемых исключительно в целях обеспечения фун

кционирования программы для ЭВМ или базы данных на конкретных технических средствах пользовате ля или под управлением конкретных программ пользователя;

модификация (переработка) - это любые их изменения, не являющиеся адаптацией;

декомпилирование программы для ЭВМ - это технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ;

использование - это выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается ис пользованием программы для ЭВМ или базы данных передача средствами массовой информации сообще ний о выпущенной в свет программе для ЭВМ или базе данных.

воспроизведение - это изготовление одного или более экземпляров программы для ЭВМ или базы данных в любой материальной форме, а также их запись в память ЭВМ;

распространение - это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также пу тем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих це лей;

выпуск в свет (опубликование) - это предоставление экземпляров программы для ЭВМ или базы данных с согласия автора неопределенному кругу лиц (в том числе путем записи в память ЭВМ и выпуска печатного текста), при условии, что количество таких экземпляров должно удовлет ворять потребности этого круга лиц, принимая во внимание характер указанных произведений;

7.2 Объекты и субъекты правовой охраны

Авторское право распространяется на любые программы для ЭВМ и базы данных, как выпущен ные, так и не выпущенные в свет, представленные в объективной форме, независимо от их матери ального носителя, назначения и достоинства.

Предоставляемая Законом правовая охрана распространяется на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на

любом языке и в любой форме, включая исходный текст и объектный код.

Базы данных охраняются независимо от того, являются ли данные, на которых они основаны или которые они включают, объектами авторского права.Правовая охрана не распространяется на идеи и принципы, лежащие в основе программы для ЭВМ или базы данных или какого-либо их элемен та, в том числе на идеи и принципы организации интерфейса и алгоритма, а также языки программи рования.

Авторское право на программы для ЭВМ и базы данных не связано с правом собственности на их материальный носитель. Любая передача прав на материальный носитель не влечет за собой пере дачи каких-либо прав на программы для ЭВМ и базы данных.

Авторское право на программу для ЭВМ или базу данных возникает в силу их создания. Для признания и осуществления авторского права на программу для ЭВМ или базу данных не требуется депонирования, регистрации или соблюдения иных формальностей. Однако, для того чтобы считаться объектом интеллектуальной собственности и охраняться законом, выпускаемое в свет произведение должно иметь знак охраны. Поэтому закон предусматривает, что правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, ис пользовать знак охраны авторского права, состоящий из трех элементов:

- буквы С в окружности или в круглых скобках;

- наименования (имени) правообладателя;

- года первого выпуска программы для ЭВМ или базы данных в свет.

Авторское право на базу данных, состоящую из материалов, не являющихся объектами авторс кого права, принадлежит лицам, создавшим базу данных.

Авторское право на базу данных признается при условии соблюдения авторского права на ка ждое из произведений, включенных в эту базу данных.

Авторское право на каждое из произведений, включенных в базу данных, сохраняется. Эти произведения могут использоваться независимо от такой базы данных.

Авторское право на базу данных не препятствует другим лицам осуществлять самостоятельный подбор и организацию произведений и материалов, входящих в эту базу данных.

Авторское право имеет ограничения во времени.

Авторское право действует с момента создания программы для ЭВМ или базы данных в течение

всей жизни автора и 50 лет после его смерти, считая с 1 января года, следующего за годом смер
ти автора.

Срок окончания действия авторского права на программу для ЭВМ и базу данных, созданные в составе, исчисляется со времени смерти последнего автора, пережившего других соавторов.

Авторское право на программу для ЭВМ или базу данных, выпущенные анонимно или под псевдо
нимом, действует с момента их выпуска в свет в течение 50 лет. Если автор программы для ЭВМ
или базы данных, выпущенных в свет анонимно или под псевдонимом, раскроет свою личность в тече
ние указанного срока или принятый автором псевдоним не оставляет сомнений в его личности, то
применяется срок охраны, предусмотренный пунктом 1 данной статьи.

Личные права автора на программу для ЭВМ или базу данных охраняются бессрочно.

Субъектом авторского права на программы для ЭВМ и базы данных признается правообладатель, под которым понимаются автор и его правопреемники. В число последних, включаются наследники, а также любые физические или юридические лица, которые обладают исключительными имущественными правами, полученными в силу закона или договора.

7.3 Авторские права на программы для ЭВМ и базы данных.

Автором программы для ЭВМ или базы данных признается физическое лицо, в результате твор
ческой деятельности которого они созданы.

Если программа для ЭВМ или база данных, созданы совместной творческой деятельностью двух и более физических лиц, то, независимо от того, состоит программа для ЭВМ или база данных из
частей, каждая из которых имеет самостоятельное значение, или является неделимой, каждое из
этих лиц признается автором такой программы для ЭВМ или базы данных.

В случае, если части программы для ЭВМ или базы данных имеют самостоятельное значение, каждый из авторов имеет право авторства на созданную им часть.

Личные (неимущественные) права

Автору программы для ЭВМ или базы данных независимо от его имущественных прав принадле жат следующие личные права:

- право авторства - то есть право считаться автором программы для ЭВМ или базы данных;

- право на имя - то есть право определять форму указания имени автора в программе для ЭВМ или базе данных: под своим именем, под условным именем (псевдонимом) или анонимно;

- право на неприкосновенность (целостность) - то есть право на защиту как самой програм мы для ЭВМ или базы данных, так и их названий от всякого рода искажений или иных посягательств, способных нанести ущерб чести и достоинству автора.

Имущественные (исключительные) права.

Автору программы для ЭВМ или базы данных или иному правообладателю принадлежит исключи тельное право осуществлять и (или) разрешать осуществление следующих действий:

- выпуск в свет программы для ЭВМ или базы данных;

- воспроизведение программы для ЭВМ или базы данных (полное или частичное) в любой фор ме, любыми способами;

- распространение программы для ЭВМ или базы данных;

- модификацию программы для ЭВМ или базы данных, в том числе перевод программы для ЭВМ или базы данных с одного языка на другой;

- иное использование программы для ЭВМ или базы данных (в том числе импортировать экзем пляры в целях распространения).

Передача имущественных прав.

Имущественные права на программу для ЭВМ или базу данных могут быть переданы полностью или частично другим физическим или юридическим лицам по договору.

Договор заключается в письменной форме и должен устанавливать следующие, существенные ус ловия:

* объем и способы использования программы для ЭВМ или базы данных,

* порядок выплаты и размер вознаграждения,

* срок действия договора.

Имущественные права на программу для ЭВМ или базу данных переходят по наследству в установ ленном законом порядке.

Имущественные права на программу для ЭВМ или базу данных, созданные в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное. Порядок выплаты и размер вознаграждения устанавлива ются договором между автором и работодателем.

Право на регистрацию

Правообладатель всех имущественных прав на программу для ЭВМ или базу данных непосредственно или через своего представителя в течение срока действия авторского права может по своему жела нию зарегистрировать программу для ЭВМ или базу данных путем подачи заявки в Российское агент ство по правовой охране программ для ЭВМ, баз данных и топологии интегральных микросхем.

7.4 Регистрация программ для ЭВМ и баз данных.

Регистрация осуществляется путем подачи заявки непосредственно в Российской агентство по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем по адресу: 103621, Москва, Малый Черкасский пер., д.2/6.

Регистрация осуществляется в соответствии нормативными документами определяющими порядок и правила регистрации. Такими документами являются:

-Временное положение "О государственном учете и регистрации баз и банков данных." Утверж дено Постановлением Правительства ╬226 от 28.02.96г.;

-Положение "О регистрационных сборах за официальную регистрацию программ для эвм, баз данных и топологий интегральных схем". Утверждено Постановлением Правительства РФ ╬793 от

12.08.93г.;

- Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для ЭВМ и баз данных." Утверждено Приказом РосАПО от 5.03.93г. ╬7п.

- Приказ Роспатента от 31 декабря 1998 г. N 245 "Об утверждении Правил регистрации дого воров на программы для электронных вычислительных машин, базы данных и топологии интегральных микросхем"

Заявка на официальную регистрацию должна содержать:

* заявление с указанием правообладателя а также автора и их местонахождение (местожительства);
* депонируемые материалы, идентифицирующие программу или базу данных;
* документ, подтверждающий уплату регистрационного сбора.

Правила оформления депонируемых материалов заявки на регистрацию.

Агентством депонируются материалы, обеспечивающие однозначную идентификацию регистрируе мых программы для ЭВМ или базы данных, включая реферат. В целях депонирования материалы, иден тифицирующие программу для ЭВМ, должны быть представлены в форме исходного текста.

В целях идентификации депонируемой программы для ЭВМ следует представлять материалы в объеме 25 первых и 25 последних страниц листинга (печатной копии) исходного текста, включая страницу, содержащую уведомление об авторском праве (знак охраны), и страницу, содержащую наз вание программы для ЭВМ. Если объем регистрируемой программы для ЭВМ составляет менее 50 стра ниц листинга исходного текста, то депонируется листинг в полном объеме.

В целях идентификации депонируемой программы для ЭВМ, содержащей сведения конфиденциаль ного характера (например, относящиеся к "ноухау"), данный факт следует указать на странице, содержащей название программы для ЭВМ, а также представить депонируемые материалы в одном из следующих видов:

- первых и 25 последних страниц листинга исходного текста с исключенными частями, содержащими конфиденциальные материалы;
- 10 первых и 10 последних страниц листинга исходного текста без каких либо исключенных частей;

- 25 первых и 25 последних страниц объектного кода, а также идущих подряд 10 или более страниц листинга исходного текста без каких-либо исключенных частей;
- если регистрируемая программа для ЭВМ составляет менее 50 страниц листинга исходного текста, последний депонируется в полном объеме с исключенными частями, содержащими сведения конфиденци ального характера.

В целях идентификации депонируемой базы данных, содержащей один файл (совокупность свя занных записей, рассматриваемых как одно целое), следует представлять материалы в объеме 25 первых и 25 последних страниц листинга.

В целях идентификации депонируемой базы данных, содержащей более одного файла, следует представлять материалы, относящиеся к каждому файлу, в объеме 50 страниц листинга или в полном объеме, если он не превышает 50 страниц.

В целях идентификации депонируемых новых редакций зарегистрированных ранее баз данных содержащих как один файл, так и более одного файла) следует представлять материалы, относящи еся к их измененным частям в объеме 50 страниц листинга или в полном объеме, если он не превы шает 50 страниц.

Для депонирования представляется один экземпляр идентифицирующих материалов.

Для визуально воспринимаемой формы публикации программы для ЭВМ или базы данных (опубли кованная распечатка исходного текста) представляется два экземпляра депонируемых идентифицирую щих материалов.

Если регистрируемая программа для ЭВМ включает охраноспособные по нормам авторского пра ва изображения на экране дисплея, обладателем права на которые является лицо, обладающее пра вом на саму программу для ЭВМ, в комплект идентифицирующих такую программу для ЭВМ материалов следует включать материалы, позволяющие однозначно определить изображения на экране дисплея. Указанные материалы могут быть представлены в виде распечатки этого изображения, его фотогра фии или рисунка. Если изображения на экране дисплея являются аудиовизуальными (например, в компьютерных видеоиграх), соответствующие материалы могут быть представлены на стандартных ви деокассетах VSH.

Если регистрируемая программа для ЭВМ включает охраноспособные по нормам авторского пра ва музыкальные произведения, обладателем права на которые является лицо, обладающее правом на

саму программу для ЭВМ, в комплект идентифицирующих такую программу для ЭВМ материалов следует включать материалы, позволяющие однозначно определить соответствующие музыкальные произведения. Эти материалы могут быть представлены в виде звукозаписи на стандартных аудиокассетах С-60 или С-90 или на оптических дисках.

Реферат программы для ЭВМ или базы данных, включаемый в состав депонируемых идентифицирующих материалов, представляется в двух экземплярах и должен содержать следующие сведения:

а) название программы для ЭВМ или базы данных;

б) наименование (имя) заявителя;

в) дату создания;

г) область применения, назначения и функциональные возможности;

д) основные технические характеристики;

е) язык программирования;

ж) тип реализующей ЭВМ.

Средний объем текста реферата - до 700 печатных знаков.

Договор о полной уступке всех имущественных прав на зарегистрированную программу для ЭВМ или БД подлежит регистрации в Роспатенте.

Для осуществления регистрации договоров необходимо представить в Роспатент (121858, Москва, Бережковская наб., 30, корп.1) следующие документы:

* заявление о регистрации соответствующего договора;

* договор о полной уступке всех имущественных прав или договор о передаче имущественных прав на программу для электронных вычислительных машин, базу данных - в 3 экз.;

* документ, подтверждающий уплату регистрационного сбора в установленном размере или основания для освобождения от уплаты регистрационного сбора, а также для уменьшения его размера.

При регистрации договора о полной уступке всех имущественных прав на официально зарегистрированные программу для ЭВМ или базу данных необходимо представить также свидетельство об их официальной регистрации (подлинник или дубликат).

7.5 Использование программ для ЭВМ и баз данных.

Законом предусматриваются следующие виды правомерного использования программ для ЭВМ и БД:

* на основании договора с правообладателем;

* свободное воспроизведение и адаптация;

* свободная перепродажа экземпляра.

Договор на использование программ для ЭВМ и БД пользователями заключается в письменной форме. При продаже и предоставлении массовым пользователям условия договора могут быть изложены на передаваемых экземплярах.

Свободное воспроизведение и адаптация программы для ЭВМ или базы данных.

Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения дополнительного разрешения правообладателя осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ, а также исправление явных ошибок. Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем.

Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без согласия правообладателя и без выплаты ему дополнительного вознаграждения:

* осуществлять адаптацию программы для ЭВМ или базы данных;

* изготавливать или поручать изготовление копии программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей и при необходимости, для замены правомерно приобретенного экземпляра. При этом копия программы для ЭВМ или базы данных не может быть использована для иных целей;

* декомпилировать программы для ЭВМ с тем, чтобы изучать кодирование и структуру этой программы.

В то же время право декомпилировать программы ограничено, оно реализуется лишь при следую щих условиях:

- информация, необходимая для взаимодействия независимо разработанной данным лицом прог раммы для ЭВМ с другими программами, недоступна из других источников;

- информация, полученная в результате этого декомпилирования, может использоваться лишь для организации взаимодействия независимо разработанной данным лицом программы для ЭВМ с други ми программами, а не для составления новой программы для ЭВМ, по своему виду существенно схо жей с декомпилируемой программой для ЭВМ или для осуществления любого другого действия, наруша ющего авторское право;

- декомпилирование осуществляется в отношении только тех частей программы для ЭВМ, кото рые необходимы для организации такого взаимодействия.

Свободная перепродажа экземпляра.

Перепродажа или передача иным способом права собственности либо иных вещных прав на эк земпляр программы для ЭВМ или базы данных после первой продажи или другой передачи права собст венности на этот экземпляр допускается без согласия правообладателя и без выплаты ему дополни тельного вознаграждения.

7.6 Защита авторского права на программы для ЭВМ и БД.

Защита авторского права на программы для ЭВМ и БД предусматривает различные виды правовой ответственности за его нарушения: уголовную, гражданскую и административную.

Под нарушителем понимается физическое или юридическое лицо, которое не выполняет требо ваний закона в отношении прав правообладателей.

Программы для ЭВМ и БД, изготовление или использование которых влечет за собой нарушение авторского права признаются законом контрафактными.

Защита прав осуществляется судом, арбитражным или третейским судом.

Уголовная ответственность.

Уголовная ответственность предусматривается статьей 146 УК РФ "Нарушение авторских и смежных прав". Она в частности определяет, что:

1. Незаконное использование объектов авторского права или смежных прав, а равно присвое ние авторства, если эти деяния причинили крупный ущерб, -

наказываются:

- штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев;

- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,;

- либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, -

наказываются:

- штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев;

- либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

Гражданская ответственность.

Гражданская ответственность предусмотрена статьей 18 Закона "О правовой охране программ для ЭВМ и БД". При этом автор или иной правообладатель вправе требовать через суд:

- признания прав;

- восстановления положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушения;

- возмещения причиненных убытков, в размер которых включается сумма доходов, неправомер но полученных нарушителем;

- выплаты нарушителем компенсации в определяемой по усмотрению суда, арбитражного или третейского суда сумме от 5000-кратного до 50000-кратного установленного законом размера мини мальной месячной оплаты труда в случаях нарушения с целью извлечения прибыли вместо возмещения убытков;

- помимо возмещения убытков или выплаты компенсации по усмотрению суда или арбитражного суда может быть взыскан штраф в размере десяти процентов от суммы, присужденной судом или ар битражным судом в пользу истца, в доход республиканского бюджета Российской Федерации;

- принятия иных предусмотренных законодательными актами мер, связанных с защитой их прав.

Административная ответственность.

Административную ответственность предусматривает статья 150.4 Кодекса РСФСР об администра тивных правонарушениях от 20 июня 1984 г. (действующая редакция). Согласно этой статьи незакон ными считаются продажа, сдача в прокат и иное использование экземпляров произведений в случа ях, если:

- экземпляры произведений являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах, или - на экземплярах произведе ний или фонограмм указана ложная информация об их изготовителях и о местах производства, а так же иная информация, которая может ввести в заблуждение потребителей, или

- на экземплярах произведений или фонограмм уничтожен либо изменен знак охраны авторско го права или знак охраны смежных прав, проставленные обладателем авторских или смежных прав.

Все эти неправомерные действия влекут за собой наложение штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда, а на должностных лиц в размере от десяти до двадцати минимальных размеров оплаты труда с конфискацией контрафактных экземпляров произведе ний.

Те же действия, совершенные лицом, которое в течение года подвергалось административному взысканию за одно из нарушений, влекут наложение штрафа на граждан в размере от десяти до двад цати минимальных размеров оплаты труда, а на должностных лиц в размере от тридцати до пятидеся

ти минимальных размеров оплаты труда с конфискацией контрафактных экземпляров произведений или фонограмм.

Конфискованные экземпляры произведений подлежат уничтожению, за исключением случаев их передачи обладателю авторских или смежных прав по его просьбе.

Источники:

1. Закон "Об авторском праве и смежных правах" ╬5351-1 от 9.07.93г;

2. "О правовой охране программ для электронных вычислительных машин и баз данных" ╬3523-1 от 23.09.92г.(Гражданское законодательство).

3. УК РФ (ст.146);

4. КоАП РСФСР (ст.150.4).

5. Письмо ГТК от 28.10.97г. ╬01-15/20508 "О мерах по защите прав на интеллектуальную собствен ность.";

6. Письмо ГТК России от 13.06.96г. ╬01-54.10565 "О мерах по обеспечению сохранности объектов интеллектуальной собственности." (утверждено МВД, ГТК, ГКАП И ФСНП России),

7. Временное положение "О государственном учете и регистрации баз и банков данных." Утверждено Постановлением Правительства ╬226 от 28.02.96г.;

8. Положение "О регистрационных сборах за официальную регистрацию программ для ЭВМ, баз данных и топологий интегральных схем". Утверждено Постановлением Правительства РФ ╬793 от 12.08.93г.;

9. Приказ Роспатента от 31 декабря 1998 г. N 245 "Об утверждении Правил регистрации договоров на программы для электронных вычислительных машин, базы данных и топологии интегральных микро схем";

10. Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для ЭВМ и баз данных. " Утверждено Приказом РосАПО от 5.03.93г. ╬7п.

Вопросы для самоконтроля и собеседования .

1. Что понимается под интеллектуальной собственностью? Интеллектуальная собственность в

области информатизации.

2. Какие нормативные правовые акты включает Законодательство об авторском праве?

3. Какие правовые понятия из области информатизации используются в Законодательстве об автор ском праве?

4. Каковы условия признания авторства на программу для ЭВМ и базу данных?

5. Что включают личные права автора на программу для ЭВМ или БД?

6. Что включают имущественные права на программу для ЭВМ или БД?

7. Какими нормативными документами реализуется право автора на регистрацию программ для ЭВМ и БД?

8. Какие виды правомерного использования программ для ЭВМ и БД установлены законодательством?

9. Кем осуществляется защита права на программы для ЭВМ и БД и какие виды правовой ответствен ности предусмотрены Законодательством РФ за нарушения авторского права?

Темы индивидуальных заданий (практических занятий (ПЗ 4ч.)):

ИЗ (ПЗ)╬1 Оформление заявки на официальную регистрацию программы для ЭВМ и БД.

ИЗ (ПЗ)╬2 Оформление договора для передачи прав на программу для ЭВМ и БД.

ИЗ (ПЗ)╬3 Практические примеры нарушения авторского права на программы для ЭВМ и БД. Правовая оценка, квалификация нарушения, меры ответственности.

Тема ╬8 Компьютерные преступления и ответственность за их совершение.

Вопросы:

8.1 Неправомерный доступ к компьютерной информации;

8.2 Создание, использование и распространение вредоносных программ для ЭВМ;

8.3 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Достижения компьютерных технологий за последние годы не только способствовали развитию экономики, торговли и коммуникаций, обеспечили эффективный информационный обмен, но и предос тавили уникальный инструментарий лицам, совершающим компьютерные преступления. Чем более интен сивно идет процесс компьютеризации, тем все более реальным становится рост компьютерной прес тупности, причем современное общество не только ощущает экономические последствия компьютерных преступлений, но и становится все более зависимым от компьютеризации. Она затрагивает многие стороны общественной жизни от контроля за воздушным и наземным транспортом до решения проблем национальной безопасности.

К компьютерным преступлениям относят совершенные с помощью вычислительной техники, тради ционные по характеру преступные деяния такие, как кража, мошенничество, подделка и причинение вреда, за которые предусматриваются уголовные санкции в законодательных системах всех стран.

В практической деятельности Российских правоохранительных органов использование автомати зированных информационных систем для совершения любых преступлений оценивается как способ со вершения преступления, а используемые программные средства выступают как орудия совершения прес туплений. К орудиям и средствам совершения преступления относятся: компьютерная техника, прог раммные средства, магнитные носители.

С 1 января 1997г. России введен в действие новый Уголовный кодекс РФ, в главе 28 которого впервые даются определения преступлений в сфере компьютерной информации. Глава помещена в раз деле IX "Преступления против общественной безопасности и общественного порядка".

К подобным преступлениям отнесены:

* неправомерный доступ к компьютерной информации;
* создание, использование и распространение вредоносных программ для ЭВМ;
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

За все эти преступления УК РФ предусмотрена уголовная ответственность.

8.1 Неправомерный доступ к компьютерной информации.

Ответственность за это преступление устанавливает ст.272 УК РФ. В частности она определяет, что неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается:

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев;

- либо исправительными работами на срок от шести месяцев до одного года;

- либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

наказывается:

- штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев;

- либо исправительными работами на срок от одного года до двух лет;

- либо арестом на срок от трех до шести месяцев;

- либо лишением свободы на срок до пяти лет.

Способы неправомерного доступа к компьютерной информации могут быть самыми различными, например, представление фиктивных документов на право доступа к информации, изменение кода или адреса технического устройства, нарушение средств или системы защиты информации, кража носителя информации.

Ответственность по ст.272 УК наступает в том случае, если деяние повлекло указанные в ч. 1 этой статьи последствия.

Под уничтожением информации следует понимать ее утрату при невозможности ее восстановления.

Блокирование информации - это невозможность ее использования при сохранности такой инфор

мации.

Модификация информации означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Под копированием информации следует понимать ее переписывание, а также иное тиражирование при сохранении оригинала. Представляется, что копирование может означать и ее разглашение.

Нарушение работы ЭВМ, системы ЭВМ или их сети может выразиться в их произвольном отключении, в отказе выдать информацию, в выдаче искаженной информации при сохранении целости ЭВМ, системы ЭВМ или их сети.

8.2 Создание и распространение вредоносных программ для ЭВМ.

Относительно новую и существенную угрозу представляет появление вирусов и вредоносных программ. Сложные вирусы, "логические бомбы", "троянские кони" могут использоваться для совершения в определенных отраслях промышленности самых разных традиционных преступлений от простого причинения вреда до вымогательства. Эти преступления могут совершаться не только немедленно, но и планироваться на конкретный будущий период.

Ответственность за это преступление устанавливает ст.273 УК РФ. В частности она определяет, что создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются:

- лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

В части второй этой статьи предусмотрено, что те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам. Представляется, что под рас пространением вредоносных программ следует понимать и их копирование.

С субъективной стороны преступление может быть совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зави симости от цели, которую перед собой ставил виновный, а когда наступили последствия, к достиже нию которых он стремился, - и в зависимости от наступивших последствий. В этом случае действия, предусмотренные ст.273 УК, оказываются лишь способом достижения поставленной цели.

Совершенное деяние подлежит квалификации по совокупности совершенных преступлений.

К тяжким последствиям, наступившим по неосторожности, могут быть отнесены, например, ги бель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или в от расли промышленности, осложнение дипломатических отношений с другим государством, возникнове ние вооруженного конфликта. При этом необходимо иметь в виду, что наступившие последствия мо гут привести и к необходимости квалификации данного преступления по совокупности с другими преступлениями в зависимости от характера последствий и отнесения "заведомости" к легкомыслию или к косвенному умыслу в виде безразличного отношения к последствиям.

8.3 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Ответственность за это преступление устанавливает ст.274 УК РФ. В частности она определя ет, что Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой зако ном информации ЭВМ, если это деяние причинило существенный вред, -

наказывается:

- лишением права занимать определенные должности или заниматься определенной деятельнос тью на срок до пяти лет;

- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов;

- либо ограничением свободы на срок до двух лет.

Часть вторая этой статьи определяет, что то же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок до четырех лет.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из их технических характеристик, правил внутреннего распорядка, а также правил обращения с компьютерной информацией, установлен ных собственником или владельцем информации либо законом или иным нормативным актом.

Под охраняемой законом информацией следует понимать информацию, изъятую из публичного открытого) оборота на основании закона, других нормативных (включая ведомственные) актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По обще му правилу такая информация имеет гриф ограниченного пользования.

Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать огра ничительные грифы в целях сохранения коммерческой или банковской тайны.

Для наступления ответственности по ст.274 УК необходимо установить, что упомянутое нару шение правил эксплуатации повлекло уничтожение, блокирование или модификацию охраняемой законом информации при условии причинения существенного ущерба. Что касается существенности ущерба, причиненного нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, то это оценочное по нятие, которое зависит в каждом конкретном случае от многих показателей, относящихся к применя емым техническим средствам (ЭВМ и др.), к содержанию информации, степени повреждения и многим другим показателям, которые должны оцениваться следователем и судом. Во всяком случае сущест венный вред должен быть менее значительным, чем причинение тяжких последствий, о которых гово рится в ч.2 этой статьи.

С субъективной стороны преступление может быть совершено по неосторожности в виде как не брежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации ЭВМ, системы ЭВМ и их сети деяние, предусмотренное ст.274 УК, становится лишь способом совершения преступления. Преступление в этом случае подлежит квалификации по наступившим последствиям, ко торые предвидел виновный, по совокупности с преступлением, предусмотренным данной статьей УК.

Субъект преступления специальный - лицо, имеющее доступ к эксплуатации упомянутых техни ческих средств. Это могут быть программисты, операторы ЭВМ, техники-наладчики, другие лица, по работе имеющие к ним доступ.

Тяжкие последствия имеют такой же характер как и в ст.273.

Источники:

1.Уголовный кодекс РФ, ст.ст. 272,273,274.

Литература:

1.Крылов В.В. Информационные компьютерные преступления.-М.: Издательская группа ИНФРА М-НОРМА,1997.-285с.

Вопросы для самоконтроля и собеседования на семинаре.

1. Какие виды преступлений в сфере компьютерной информации определены Законодательством РФ?
2. Что понимается под "неправомерным доступом к компьютерной информации" и какая ответствен ность за это предусмотрена УК РФ?
3. Будет ли нести уголовную ответственность лицо осуществившее несанкционированный доступ к конфиденциальной информации, если указанные в ст.272 УК последствия не наступили?
4. Какая правовая ответственность предусмотрена УК РФ за создание и распространение вредонос ных программ для ЭВМ?
5. Какая правовая ответственность предусмотрена УК РФ за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети?

Тема 9: Правовая регламентация лицензирования деятельности связанной с защитой информации.

Вопросы:

9.1 Лицензирование деятельности, связанной с государственной тайной, ее защитой, созданием средств защиты информации.

9.2 Лицензирование деятельности в области защиты информации.

9.3 Перечень Лицензиатов Гостехкомиссии России

В Сибирской территориально-промышленной зоне.

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 ин формации. Лицензирование деятельности, в этом случае является допуском предприятия к проведению работ связанных с использованием сведений, составляющих государственную тайну, как того требует Закон "О государственной тайне" (ст.27). Оно осуществляется на основе Положения " О лицензиро вании деятельности предприятий, учреждений и организаций по проведению работ, связанных с ис пользованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите государственной тайны", утвер жденным постановлением Правительства РФ.

Второе направление связано с защитой всей информации с ограниченным доступом. Оно осущест вляется на основе Положения "О государственном лицензировании деятельности в области защиты ин формации", которое утверждено Решением Гостехкомиссии РФ и ФАПСИ.

В любом случае лицензирование осуществляется государственными органами или уполномоченны ми им организациями.

9.1 Лицензирование деятельности, связанной с государственной тайной, ее защитой,

созданием средств защиты информации.

Цель лицензирования - допуск предприятий, учреждений организаций к проведению работ, свя занных:

* с использованием сведений, составляющих государственную тайну;

* с созданием средств защиты информации;

* с осуществлением мероприятий и оказанием услуг по защите государственной тайны.

Таким образом, обязательному лицензированию подлежат перечисленные виды работ, допуск к которым осуществляется на основании лицензии.

Лицензирование осуществляется на основе требований Закона РФ "О государственной тайне" в порядке и по правилам установленным нормативными документами утвержденными Правительством РФ и другими органами по защите государственной тайны. К этим документам относятся:

* Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием сред ств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите госу дарственной тайны. Утверждено Постановлением Правительства РФ ╬333 от 15.04.95г.;

* Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений составляющих государствен ную тайну. Утверждена директором ФСБ РФ 23.08.95г.,╬28;

* Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и оказания услуг в области противодействия иностранной тех нической разведке. Утверждена председателем ГТК 17.11.95г.

* Методические рекомендации по организации и проведению государственной аттестации руководите лей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих го сударственную тайну. Положение устанавливает порядок лицензирования деятельности предприятий, учреждений и организаций независимо от их организационно-правовых форм.

Органами, уполномоченными на ведение лицензионной деятельности, являются:

* по допуску предприятий к проведению работ, связанных с использованием сведений, состав ляющих государственную тайну, - ФСБ РФ и ее территориальные органы (на территории Российской

Федерации), СВР РФ (за рубежом);

* на право проведения работ, связанных с созданием средств защиты информации, - Гостехко миссия, ФАПСИ, СВР РФ, МО РФ (в пределах их компетенции);

* на право осуществления мероприятий и (или) оказания услуг в области защиты государст венной тайны - ФСБ и ее территориальные органы, ФАПСИ, Гостехкомиссия, СВР РФ (в пределах их компетенции).

Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Меж ведомственной комиссией по защите государственной тайны.

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

а) заявление о выдаче лицензии с указанием:

-наименования и организационно-правовой формы, юридического адреса предприятия, номера его расчетного счета в банке;

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

-срока действия лицензии;

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

в) копию свидетельства о государственной регистрации предприятия;

г) копии документов, подтверждающих право собственности, право полного хозяйственного ведения и (или) договора аренды на имущество, необходимое для ведения заявленного вида деятельности;

д) справку о постановке на учет в налоговом органе;

е) документ, подтверждающий оплату рассмотрения заявления. Заявитель несет ответственность за достоверность представляемых им сведений. Все документы, представленные для получения лицензии, регистрируются органом, уполномоченным на ведение лицензионной деятельности.

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 необходи мыми документами.

В случае необходимости может назначаться дополнительная экспертиза.

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государст

венной аттестации их руководителей, ответственных за защиту сведений, составляющих государствен ную тайну и при выполнении следующих условий:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

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

- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Лицензии оформляются на бланках, имеющих степень защиты, соответствующую степени защиты ценной бумаги на предъявителя.

В лицензии указываются:

-наименование органа, ее выдавшего;

-наименование и юридический адрес предприятия, ее получившего;

-вид деятельности, на осуществление которого выдана лицензия;

-условия осуществления данного вида деятельности;

-срок действия лицензии;

-ее регистрационный номер и дата выдачи.

Специальная экспертиза предприятия проводится путем проверки выполнения требований норма тивно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других усло вий, необходимых для получения лицензии. Порядок проведения экспертизы определяет инструкция о порядке проведения экспертиз на соответствующий вид деятельности.

Государственная аттестация руководителей предприятий организуется органами, уполномочен ными на ведение лицензионной деятельности, а также министерствами и ведомствами РФ, руководите ли которых наделены полномочиями по отнесению к государственной тайне сведений в отношении под ведомственных 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.

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;
* отрицательное заключение по результатам государственной аттестации руководителя предприятия.

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

9.2 Лицензирование деятельности в области защиты информации.

В качестве целей лицензирования деятельности в области защиты информации необходимо рассматривать допуск юридических лиц - предприятий организаций и учреждений, независимо от их организационно-правовой формы, к деятельности по защите информации, циркулирующей в технических средствах и помещениях, и представляющей собой государственную и иную охраняемую законом тайны.

Лицензирование осуществляется на основании требований законов:

* "О государственной тайне",
* "Об информации, информатизации и защите информации",
* "О федеральных органах правительственной связи и информации",
* Указа Президента РФ от 3.04.95г. ╬334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации."

Основным нормативным документом, устанавливающим основные принципы, организационную структуру системы государственного лицензирования, порядок проведения лицензирования и контроля за деятельностью лицензиатов, является Положение "О государственном лицензировании деятельности в области защиты информации.". Положение утверждено Решением Гостехкомиссии и ФАПСИ от 27.04.94г. ╬10.

В своем приложении Положение содержит два перечня видов деятельности, подлежащих лицензированию Гостехкомиссией и ФАПСИ. С точки зрения специалиста (математика -программиста) в области защиты информации интерес могут представлять следующие виды деятельности подлежащие лицензированию Гостехкомиссией:

1. Сертификация и сертификационные испытания всех видов средств защиты информации;

2. Аттестация систем информатизации, АСУ, систем связи и всех других средств защиты информации, а также помещений, в которых защищенная информация обрабатывается, на соответствие требованиям руководящих и нормативных документов по безопасности информации.

3.Разработка, производство, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание...:

* защищенных ТСОИ,
* технических средств защиты информации,
* технических средств контроля, эффективности мер защиты информации,
* защищенных программных средств обработки информации,
* программных средств защиты информации,
* программных средств контроля защищенности информации.

4.Проведение специсследований на побочные электромагнитные излучения (ПЭМИН) ТСОИ.

5.проектирование объектов в защищенном исполнении;

6.подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленных в данном перечне;

Более детально перечень видов приведен в табл.9.1

Таблица 9.1

Перечень видов деятельности по защите информации, на которые выдается лицензия.

Вид деятельности. Системы и средства.

1

1.1 Сертификация

А) технических средств защиты информации;

Б) защищенных технических средств обработки информации(ТСОИ);

В)технических средств контроля эффективности мер защиты информации от НСД;

Г) программных средств защиты информации от НСД ;

Д)защищенных программных средств обработки информации от НСД;

Е) программных средств контроля защищенности информации от НСД;

Ж) программных средств по требованиям безопасности.

1.2 Сертификационные испытания.

2

2.1 Контроль защищенности информации ограниченного доступа

А) автоматизированных систем различного уровня и назначения;

Б) систем связи, приема, обработки и передачи данных;

В) систем отображения и размножения;

Г) технических средств(систем), не обрабатывающих информацию ограниченного доступа, но размещенных в помещениях, где она обрабатывается;

Д) помещений со средствами (системами), подлежащими защите;

Е) помещений, предназначенных для ведения конфиденциальных переговоров;

2.2 Аттестация средств и систем на соответствие требованиям по защите информации.

3

3.1 Разработка

А) технических средств защиты информации;

Б) защищенных ТСОИ;

В) технических средств контроля эффективности мер защиты информации;

Г) программных средств защиты информации от НСД;

Д) защищенных программных средств обработки информации от НСД;

Е) программных средств контроля защищенности информации от НСД;

Ж) программных средств по требованиям безопасности.

3.2 Производство 3.3 Реализация 3.4 Установка 3.5 Монтаж 3.6 Наладка 3.7 Испытания

3.8 Ремонт 3.9 Сервисное обслуживание.

4 Проведение специсследований на ПЭМИН ТСОИ.

5 Проектирование объектов в защищенном исполнении

А) автоматизированных систем различного уровня и назначения;

Б) систем связи, приема, обработки и передачи данных

В) систем отображения и размножения;

Д) помещений со средствами (системами), подлежащими защите;

Е) помещений, предназначенных для ведения конфиденциальных переговоров.

6.Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечис ленным в данном перечне.

В лицензии вид деятельности записывается так, например: 3.3А,В; 4; 5А,Е; и т.д.

Перечень видов деятельности, подлежащих лицензированию ФАПСИ, в своей основе включает все возможные виды деятельности по защите информации в высших органах государственной власти. Кроме того он содержит следующие виды:

* разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт шифровальных средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг по шифрованию информации;

* эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащей сведения, составляющие ГТ;

* подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.

Органы лицензирования.

Деятельность системы лицензирования организуют государственные органы по лицензированию, которыми являются Гостехкомиссия России и ФАПСИ.

Организационную структуру системы государственного лицензирования деятельности предприятий в области защиты информации образуют:

* государственные органы по лицензированию,
* лицензионные центры (в регионах и в ведомствах РФ),
* предприятия заявители.

Порядок проведения лицензирования.

Порядок проведения лицензирования предприятий заявителей в области защиты информации включает следующие действия:

-проведение экспертизы заявителя;

-подачу, рассмотрение заявления на лицензирование, оформление и выдачу лицензий;

-учет лицензиатов.

Для получения лицензии представляются:

* заявление;
* представление органа государственной власти РФ;
* материалы экспертизы, подтверждающие наличие необходимых условий для проведения работ по заявленным видам деятельности, а также профессиональную пригодность руководителя предприятия-заявителя, или лиц, уполномоченных им для руководства лицензируемой деятельностью;
* копии документов о государственной регистрации предпринимательской деятельности и устава предприятия.

Экспертиза предприятия-заявителя осуществляется экспертной комиссией соответствующего лицензионного центра на основании заявки предприятия.

Заявка должна содержать:

-лицензируемые виды деятельности и перечни необходимых для их обеспечения производственного и испытательного оборудования;

-нормативную и методическую документацию, имеющуюся на предприятии.

Экспертиза проводится на основе хозяйственного договора между лицензионным центром и предприятием-заявителем.

Нормативные требования по осуществлению деятельности лицензиатов определены в Положении "О государственном лицензировании деятельности в области защиты информации". В соответствии с ними лицензиаты обязаны:

* осуществлять свою деятельность в строгом соответствии с требованиями нормативных документов по защите информации;

* обеспечивать тайну переписки, телефонных переговоров, документальных и иных сообщений физи ческих и юридических лиц, пользующихся их услугами;

* ежегодно представлять непосредственно в государственный орган по лицензированию или в лицен зионный центр сведения о количестве выполненных работ по конкретным видам указанной в лицензии деятельности.

Лицензиаты несут юридическую и финансовую ответственность за полноту и качество выполне ния работ и обеспечение сохранности государственных и коммерческих секретов, доверенных им в ходе практической деятельности.

Контроль и надзор за полнотой и качеством проводимых лицензиатами работ в области защи ты информации осуществляется Гостехкомиссией России, ФАПСИ и отраслевыми органами контроля в пределах их компетенции в ходе проверок состояния защиты информации на предприятиях-потребите лях, воспользовавшихся услугами лицензиатов.

9.3 Перечень Лицензиатов Гостехкомиссии России В Сибирской территориально -промышленной зоне

Перечень лицензиатов в Сибирской территориально- промышленной зоне.

Новосибирская область.

ОАО <Новосибирский завод химконцентратов> (Минатом России)630110, г. Новосибирск, ул. Б. Хмельницкого, дом 94, т.(383-2) 74-83-46 2; 3.3-3.9а-е; 4; 5.

ЗАО Научно-технический центр <РАСТР> 630000, г. Новосибирск, ул.1905 года, 13,

т.(383-2) 21-84-84 2.1д-е; 3.1-3.2а; 3.5а; 3.3а,г;3.9а.

ООО Программно-технический центр <ДЕЛОНА> 630118, г. Новосибирск, ул. Б. Богаткова, 228/1, к.207, т.(383-2) 69-14-90 2; 3г,д,е; 4.

ЗАО <Специализированное монтажно-наладочное управление ╬ 70> 630075, г. Новосибирск, а/я 327,т.(383-2) 74-33-44, 76-49-88 3.3-3.6а,б,г; 3.9а,б,г; 5а,б,д.

Государственное образовательное учреждение <Новосибирский государственный технический университет> (Минобразования России)630092, г. Новосибирск, пр. К. Маркса, д.20, корп.7, т.(383-2) 46-50-01 3.1а,б;д; 4;

ООО <Техническая испытательная лаборатория>630092, г. Новосибирск, пр.К. Маркса, д.20, корп.7, т.(383-2) 462987, 495195 2.2б,д,е; 3.3б,г; 3.7ж; 3.9б.

ЗАО <Центр информационной безопасности> 630091, г. Новосибирск, Красный пр., д.54, т.(383-2) 21-42-71, 21-72-44 2.1б,г,д,е; 3.3-3.4а-в; 4; 5а-в.

ФГУП <Сибирский научно-исследовательский институт авиации им. Чаплыгина> (Росавиакосмос) 630051, г. Новосибирск, ул. Ползунова, д.21, т.(383-2) 77-01-561.2а,в.

Управление внутренних дел Новосибирской области МВД России)630099, г. Новосибирск, ул. Октябрьская, д.78,т.(383-2) 16-71-00, 16-70-33 2б-е; 3.3-3.6а-в; 3.8-3.9а-в; 4.

ЗАО <Компания <Кардинал>630004, г. Новосибирск, ул. Челюскинцев, дом 18 т.(383-2) 101-917, 101-275 2.1а,б,г-е; 3.3а-г; 3.4а,в,г; 3.5а,в; 4; 3.6а,в,г; 3.9а-в;5а,б

ООО <Контур-М>630091, г. Новосибирск, ул. Фрунзе, 5т.(383-2) 66-51-25 3.3а,в,г.

Алтайский край

ФГУП <Барнаульское специализированное конструкторское бюро <Восток> (Российское агентство систем управления)656002, г. Барнаул, пр. Калинина, 15/7, т.(385-2) 77-07-56 2; 3.1-3.3б; 4; 5а,б.

ТОО <Объединение частных детективов <Агентство ДИСБИ> г. Барнаул, пр. Социалистический, д. 63, т.(385-2) 24-47-18, 24-47-11 2.1е,д.

Управление внутренних дел Алтайского края (МВД России)656025, г. Барнаул-25, пр. Ленина, д. 74,т.(385-2) 24-37-47 2б-е; 3.3 -3.6а-в; 3.8 -3.9а-в;4.

ООО <СКАНЕР> 656099, г. Барнаул, пр. Комсомольский, 73,т.(385-2)23-84-46

2.1д-е; 3.5а; 3.9а.

Томская область

ФГУП <СИБИРСКИЙ ХИМИЧЕСКИЙ КОМБИНАТ> (Минатом России)636070, Томская область,

г. Северск., ул. Курчатова, 1,т.(382-2) 225028, 779612 2; 3.3-3.9а,б; 4; 5а-в.

Кемеровская область

ОАО <Электросвязь> -Кемеровская городская телефонная сеть>

650099, г. Кемерово, ул. Красноармейская, 99т.(384-2) 25-14-4 2.1б,е; 3.3-3.4а.

Омская область

ГП <Омский научно-исследовательский институт приборостроения>(Российское агентство систем

управления)644009, г. Омск, ул. Масленникова, 231, т.(381-2) 33-89-14 2; 3.1-3.6а,г,д,е;

3.9а,г,д,е; 4.

ОАО <ОКБ <КАРАТ>644065, г. Омск, пос. Первомайский, 2,т.(381-2) 64-54-55

2.2а; 3.3б,г,д,е;3.4г-е; 3.9г-е; 5а.

Красноярский край

ЗАО <МХМ-ЕНИСЕЙ>660028, г. Красноярск, ул. Мечникова, 49, т.(391-2) 44-66-04

3.3-3.9а-е.

ГП <Красноярский машиностроительный завод> (Росавиакосмос)660123, г. Красноярск,

пр. Им. газеты <Красноярский рабочий, 29,т.(391-2) 64-65-19, 64-66-01

2; 3.3-3.7;3.8-3.9а-в; 4.

Источники:

1. Положение о лицензировании деятельности предприятий, учреждений и организаций по прове дению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите го сударственной тайны. Утверждено Постановлением Правительства РФ ╬333 от 15.04.95г.;

2. Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учрежде ний и организаций к проведению работ, связанных с использованием сведений составляющих государ ственную тайну. Утверждена директором ФСБ РФ 23.08.95г.,╬28;

3. Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и органи заций на право осуществления мероприятий и оказания услуг в области противодействия иностранной технической разведке. Утверждена председателем ГТК 17.11.95г.

4. Методические рекомендации по организации и проведению государственной аттестации руко водителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну. Положение устанавливает порядок лицензирования деятельности предприятий, учреждений и организаций независимо от их организационно-правовых форм.

5.Положение "О государственном лицензировании деятельности в области защиты информации.". Утверждено Решением Гостехкомиссии и ФАПСИ от 27.04.94г.╬10.

Вопросы для самоконтроля и собеседования по теме:

1. Нормативные документы по лицензированию деятельности предприятий, связанной с использо ванием сведений, составляющих государственную тайну, её защитой созданием средств защиты государственной тайны?
2. Органы уполномоченные лицензировть деятельность по защите государственной тайны?
3. Какие документы должен представить заявитель для лицензирования деятельности связанной с

защитой государственной тайны?

4. Что включает в себя государственная экспертиза предприятия для получения лицензии на дея тельность по защите гостайны?

5. В чем суть государственной аттестации руководителя предприятия для получения лицензии?

6. На основе каких нормативных правовых документов осуществляется лицензирование в области защиты информации?

7. Перечень видов деятельности в области защиты информации лицензируемый Гостехкомиссией РФ?

8. Перечень видов деятельности в области защиты информации лицензируемый ФАПСИ?

9. Нормативные требования по осуществлению деятельности лицензиатов в области азщиты информа ции?

Литература:

1.Крылов В.В. Информационные компьютерные преступления.-М.: Издательская группа ИНФРА М-НОРМА,1997.-285с.

2.Кураков Л.П., Смирнов С.Н.Информация как объект павовой защиты.-М.:Гелиос, 1998.-240с.

3.Рассолов М.М. Информационное право: Учебное пособие.-М.: Юрист, 1999.-400с.

4.Право интеллектуальной собственности (конспект лекций в схемах).-М.: "Издательство ПРИОР", 1999.-144с.

ПРИЛОЖЕНИЕ 1 Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информати зации и защите информации"

Принят Государственной Думой 25 января 1995 года

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

формировании и использовании информационных ресурсов на основе создания, сбора, обработки, на копления, хранения, поиска, распространения и предоставления потребителю документированной ин формации;создании и использовании информационных технологий и средств их обеспечения;

защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

2. Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Феде рации "Об авторском праве и смежных правах".

Статья 2. Термины, используемые в настоящем Федеральном законе, их определения

В настоящем Федеральном законе используются следующие понятия:

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информатизация - организационный социально - экономический и научно-технический процесс созда ния оптимальных условий для удовлетворения информационных потребностей и реализации прав граж дан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распростра нения информации;

информационная система - организационно упорядоченная совокупность документов (массивов документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

средства обеспечения автоматизированных информационных систем и их технологий - программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы;

должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

пользователь (потребитель) информации - субъект, обращающийся к информационной системе или по среднику за получением необходимой ему информации и пользующийся ею.

Статья 3. Обязанности государства в сфере формирования информационных ресурсов и информатизации

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения реше

ния стратегических и оперативных задач социального и экономического развития Российской Федера
ции.

2. Основными направлениями государственной политики в сфере информатизации являются:

обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
формирование и защита государственных информационных ресурсов;
создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;
создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;
обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;
содействие формированию рынка информационных ресурсов, услуг, информационных систем, техноло
гий, средств их обеспечения;
формирование и осуществление единой научно-технической и промышленной политики в сфере информа
тизации с учетом современного мирового уровня развития информационных технологий;
поддержка проектов и программ информатизации;
создание и совершенствование системы привлечения инвестиций и механизма стимулирования разра
ботки и реализации проектов информатизации;
развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Глава 2. Информационные ресурсы

Статья 4. Основы правового режима информационных ресурсов

1. Информационные ресурсы являются объектами отношений физических, юридических лиц, государст
ва, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

2. Правовой режим информационных ресурсов определяется нормами, устанавливающими:
порядок документирования информации;

право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

категорию информации по уровню доступа к ней;

порядок правовой защиты информации.

Статья 5. Документирование информации

1. Документирование информации является обязательным условием включения информации в информаци онные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию докумен тов и их массивов, безопасность Российской Федерации.

2. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Россий кой Федерации.

3. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизи рованных информационных и телекоммуникационных систем, может подтверждаться электронной цифро вой подписью.Юридическая сила электронной цифровой подписи признается при наличии в автоматизи рованной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

4. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании ли цензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Статья 6. Информационные ресурсы как элемент состава имущества и объект права собственности

1. Информационные ресурсы могут быть и негосударственными и как элемент состава имущества нахо дятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информацион ные ресурсы регулируются гражданским законодательством Российской Федерации.

2. 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.

3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюд

жетов субъектов Российской Федерации, а также полученных путем иных установленных законом спо собов.Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.Собственник информационных ресур сов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собст венностью только с разрешения соответствующих органов государственной власти.

4. Субъекты, представляющие в обязательном порядке документированную информацию в органы госу дарственной власти и организации не утрачивают своих прав на эти документы и на использование информации, содержащейся в них.

Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо о их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона, форми рует информационные ресурсы, находящиеся в совместном владении государства и субъектов, предс тавляющих эту информацию.

5. Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их иму щества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов го сударственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

6. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законода тельством Российской Федерации.

7. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодатель ством Российской Федерации, в том числе он имеет право:

назначить лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;

устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

определять условия распоряжения документами при их копировании и распространении.

8. Право собственности на средства обработки информации не создает права собственности на ин формационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулиру ются договором.

Статья 7. Государственные информационные ресурсы

1. Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

федеральные информационные ресурсы;

информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Рос сийской Федерации (далее - информационные ресурсы совместного ведения);

информационные ресурсы субъектов Российской Федерации.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 на стоящего Федерального закона осуществляется гражданами, органами государственной власти, орга нами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспе чивают их использование в соответствии с установленной компетенцией.

3. Деятельность органов государственной власти и организаций по формированию федеральных инфор мационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъек тов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов "Информатика" ("Информационное обеспечение").

4. Организации, которые специализируются на формировании федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора, обязаны получить лицен зию на этот вид деятельности

в органах государственной власти. Порядок лицензирования определяется законодательством Российс кой Федерации.

Статья 8. Обязательное представление документированной информации для формирования государственных информационных ресурсов

1. Граждане, органы государственной власти, органы местного самоуправления, организации и об
щественные объединения обязаны представлять документированную информацию органам и организаци
ям, ответственным за формирование и использование государственных информационных ресурсов.
Перечни представляемой в обязательном порядке документированной информации и перечни органов и
организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает
Правительство Российской Федерации.
2. Порядок и условия обязательного представления документированной информации доводятся до све
дения граждан и организаций.
Порядок обязательного представления (получения) информации, отнесенной к государственной тайне,
и конфиденциальной информации устанавливается и осуществляется в соответствии с законодательст
вом об этих категориях информации.
3. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представля
емых в обязательном порядке документов и адресами их представления. Перечень представляемой в
обязательном порядке документированной информации прилагается к уставу каждого юридического ли
ца (положению о нем).Необеспечение регистрационными органами регистрируемых юридических лиц пе
речнем представляемых в обязательном порядке документов с адресами их представления не является
основанием для отказа в регистрации.
Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических
лиц перечнями представляемых в обязательном порядке документов с адресами их представления при
влекаются к дисциплинарной ответственности вплоть до снятия с должности.
4. Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собст
венника в состав государственных информационных ресурсов по правилам, установленным для включе
ния документов в соответствующие информационные системы.
Статья 9. Отнесение информационных ресурсов к общероссийскому национальному достоянию
1. Отдельные объекты федеральных информационных ресурсов могут быть объявлены общероссийским
национальным достоянием.
2. Отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому нацио
нальному достоянию и определение их правового режима устанавливаются федеральным законом.
Статья 10. Информационные ресурсы по категориям доступа

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

3. Запрещено относить к информации с ограниченным доступом:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

4. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации "О государственной тайне".

5. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 настоящего Федерального закона.

Статья 11. Информация о гражданах (персональные данные)

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, инфор мационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых него сударственными организациями, должны быть закреплены на уровне федерального закона. Персональ ные данные относятся к категории конфиденциальной информации.

Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных перего воров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

2. Персональные данные не могут быть использованы в целях причинения имущественного и морально го вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограни чение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запре щено и карается в соответствии с законодательством.

3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодатель ством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4. Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицен зирования определяется законодательством Российской Федерации.

5. Неправомерность деятельности органов государственной власти и организаций по сбору персональ ных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 настоящего Федерального закона и законодательства о персональных дан ных.

Глава 3. Пользование информационными ресурсами

Статья 12. Реализация права на доступ к информации из информационных ресурсов

1. Пользователи - граждане, органы государственной власти, органы местного самоуправления, ор ганизации и общественные объединения - обладают равными правами на доступ к государственным ин формационным ресурсам и не обязаны обосновывать перед владельцами этих ресурсов необходимость получения запрашиваемой ими информации.

Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению.

Информация, полученная на законных основаниях из государственных информационных ресурсов граж данами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании про изводной информации, но не исходная информация, полученная из государственных ресурсов.

3. Порядок получения пользователем информации (указание места, времени, ответственных должност ных лиц, необходимых процедур) определяет собственник или владелец информационных ресурсов с соблюдением требований, установленных настоящим Федеральным законом.

Перечни информации и услуг по информационному обеспечению, сведения о порядке и условиях дос тупа к информационным ресурсам владельцы информационных ресурсов и информационных систем предос тавляют пользователям бесплатно.

4. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользо вателю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций.

5. Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные вид и массивы информации, в соответствии с их компетенцией либо непосредствен но ее собственником в соответствии с законодательством.

Статья 13. Гарантии предоставления информации

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользова телей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, пред ставляющим общественный интерес.

2. Отказ в доступе к информационным ресурсам, предусмотренным в пункте 1 настоящей статьи, мо жет быть обжалован в суд.

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистра цию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспе чения права граждан на доступ к информации.

4. Перечень информационных услуг, предоставляемых пользователям из государственных информацион ных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги, устанав ливает Правительство Российской Федерации.

Расходы на указанные услуги компенсируются из средств федерального бюджета и бюджетов субъектов Российской Федерации.

Статья 14. Доступ граждан и организаций к информации о них

1. Граждане и организации имеют право на доступ к документированной информации о них, на уточ нение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и орга низаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.

2. Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотрен

ных законодательством Российской Федерации.

3. Субъекты, представляющие информацию о себе для комплектования информационных ресурсов на основании статей 7 и 8 настоящего Федерального закона, имеют право бесплатно пользоваться этой информацией.

4. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

Статья 15. Обязанности и ответственность владельца информационных ресурсов

1. Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством Российской Федерации или собственником этих информационных ресурсов, в соответствии с законодательством.

2. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

Глава 4. Информатизация, информационные системы,
технологии и средства их обеспечения

Статья 16. Разработка и производство информационных систем, технологий и средств их обеспечения

1. Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

2. Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

3. Государство создает условия для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения.

Правительство Российской Федерации определяет приоритетные направления развития информатизации и устанавливает порядок их финансирования.

4. Разработка и эксплуатация федеральных информационных систем финансируются из средств федерального бюджета по статье расходов "Информатика" ("Информационное обеспечение").

5. Органы государственной статистики совместно с Комитетом при Президенте Российской Федерации по политике информатизации устанавливают правила учета и анализа состояния отрасли экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

Статья 17. Право собственности на информационные системы, технологии и средства их обеспечения

1. Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства.

2. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

3. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков.

Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

Статья 18. Право авторства и право собственности на информационные системы, технологии и средства их обеспечения

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам.

Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством Российской Федерации.

Статья 19. Сертификация информационных систем, технологий, средств их обеспечения и лицензирование деятельности по формированию и использованию информационных ресурсов

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Глава 5. Защита информации и прав субъектов в области информационных процессов и информатизации

Статья 20. Цели защиты

Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

обеспечение прав субъектов в информационных процессах и при разработке, производстве и примене
нии информационных систем, технологий и средств их обеспечения.

Статья 21. Защита информации

1. Защите подлежит любая документированная информация, неправомерное обращение с которой может
нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основа
нии Закона Российской Федерации "О государственной тайне";

в отношении конфиденциальной документированной информации - собственником информационных ресур
сов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных - Федеральным законом.

2. Органы государственной власти и организации, ответственные за формирование и использование
информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и
применяющие информационные системы и информационные технологии для формирования и
использования
информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законода
тельством Российской Федерации.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных програм
мно-технических средств защиты, а также обеспечение организационных мер защиты информационных
систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осу
ществляются органами государственной власти. Контроль осуществляется в порядке, определяемом
Правительством Российской Федерации.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собствен
ностью государства, создают специальные службы, обеспечивающие защиту информации.

5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять ко
нтроль за выполнением требований по защите информации и запрещать или приостанавливать обработ
ку информации в случае невыполнения этих требований.

6. Собственник или владелец документированной информации вправе обращаться в органы государст

венной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают ус ловия конфиденциальности самой информации и результатов проверки.

Статья 22. Права и обязанности субъектов в области защиты информации

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным законом устанавливают порядок предоставления пользоват елю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных систем и средств их обес печения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

4. Собственник документов, массива документов, информационных систем может обращаться в органи зации, осуществляющие сертификацию средств защиты информационных систем и информационных ресур сов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консуль таций.

5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты ин формации.

Статья 23. Защита прав субъектов в сфере информационных процессов и информатизации

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информацион ными ресурсами, разработки, производства и применения информационных систем, технологий и сред ств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомер ных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

Статья 24. Защита права на доступ к информации

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным

судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответствен

ность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Статья 25. Вступление в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Предложить Президенту Российской Федерации привести в соответствие с настоящим Федеральным законом изданные им правовые акты.

3. Поручить Правительству Российской Федерации:

привести в соответствие с настоящим Федеральным законом изданные им правовые акты;

подготовить и внести в Государственную Думу в трехмесячный срок в установленном порядке предложения о внесении изменений и дополнений в законодательство Российской Федерации в связи с принятием настоящего Федерального закона;

принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

Президент Российской Федерации Б.Ельцин

Москва, Кремль

20 февраля 1995 года

N 24-ФЗ

ПРИЛОЖЕНИЕ 2 Практические задания из юридической практики (к теме ╬7.)

Решение задачи должно основываться на соответствующих статьях Законодательства об авторском праве и законах, регулирующих информационные правоотношения.

? Задача 7.1 (3)

Инженер-программист Неров был принят на работу в акционерное общество "Центр", где на него возлагались функции оператор ПЭВМ по вводу законодательства в информационные базы, которые "Центр" продавал на коммерческой основе предприятиям легкой промышленности. В свободное

от ввода информации время Нерову удалось разработать и внедрить более совершенный алгоритм обработки правовой информации в информационной базе, что заметно повысило ее ценность и при вело к получению значительной прибыли.На собрании учредителей акционерного общества "Центр" было предложено премировать Нерова, а его разработку использовать в ходе реализации модерни зированной программы на выгодных коммерческих условиях. Однако Неров заявил руководству об щества, что оно нарушает его авторские права, и потребовал отчисления ему всей приб ыли за использование его программного продукта.

Как разрешить этот спор с позиции норм информационного права?

? Задача ╬7.2 (4)

Программист Авдеев использовал в личных целях программу своего коллеги Базарова, умер шего три месяца назад. Надо заметить, что регистрация данного программного продукта была осу ществлена программистом Базаровым в установленном законом порядке. Несмотря на это, Авдеев предложил ее коммерческому банку "Огни Москвы" в качестве средства по управлению системой кредитования клиентов. Программный продукт позволил банку повысить эффективность обработки данных и принес ему дополнительную прибыль в конце года. Эти обстоятельства стали известны сыну умершего Базарова - Василию, который обратился с жалобой в прокуратуру и потребовал от Авдеева отказаться от права пользования программой отца.

Законны ли претензии сына программиста Базарова - Василия - к Авдееву?

? Задача ╬7.3 (5)

Системщик Шурыгин использовал при создании ИПС "Контроль" часть программы своего коллеги Мамаева, уехавшего полгода назад в США. При этом Шурыгин, являясь соавтором программы, заре гистрировал ее в установленном законом порядке, но договор с Мамаевым, определяющий дальней шее использование программного продукта, заключать не захотел.После отъезда Мамаева системщик Шурыгин объявил себя единственным правообладателем программы и стал выгодно продавать ее на

рынке информационных услуг. Это стало известно Мамаеву, который обратился в суд с иском к свое му коллеге и потребовал взыскать с него половину средств, полученных от продажи программного продукта.Квалифицируйте действия Шурыгина и Мамаева.

? Задача ╬7.4 (6)

Программист Голанов , поступая на работу в фирму "Сокол", формально отнесся к заполнению документов по типовым формам, предложенным руководством фирмы. В течение двух лет Голанов создал ряд программных продуктов, реализация которых принесла фирме "Сокол" значительную при быль и известность в республике. Видя это, Голанов обратился к руководству фирмы с просьбой выплатить ему денежное вознаграждение как автору программ, обеспечивших заметный успех коллек тиву. Однако генеральный директор фирмы Валентинов, ссылаясь на регулярную выплату заявителю высокого должностного оклада, отказался удовлетворить его просьбу. При этом он заявил, что свои программы Голанов создал в служебное время и, кроме того, программист не осуществил ре гистрацию программ в установленном законом порядке.

Кто прав, Голанов или Валентинов?

? Задача ╬7.5 (7)

Сотрудник акционерного общества "Урожай" Харитонов приобрел на основе норм существующего бух галтерского учета дистрибутив программы с прилагаемым к нему сертификатом на право личного пользования. В процессе установки программы на ПЭВМ им была допущена грубая ошибка и в результате дистрибутив полностью испорчен. Харитонов без промедления принял решение: устано вить другое программное обеспечение с дистрибутива, взятого в коммерческой фирме "Весна".

Правомерны ли действия Харитонова?

? Задача ╬7.6 (8)

Компьютерщику лаборатории новых технологий предприятия "Алмаз" Слепцову в соответствии с годо вым планом-графиком было поручено разработать базу данных для учета и движения измерительных приборов предприятия, и с этим заданием он успешно справился.При этом трудовой договор прог раммист Слепцов со своим предприятием не заключал. Копия разработанной им программы по управ лению базой данных хранилась у заведующего лабораторией Семкина, а программный продукт исполь зовался в информационно-аналитической работе программистом Барановым.По истечение года автор программного продукта Слепцов уволился с работы по собственному желанию и, став учредителем акционерного общества открытого типа "Бур", передал в качестве уставного взноса в это общест во свои права на разработанную программу. Директор предприятия "Алмаз" Карпов, ссылаясь на мнение Семкина и Баранова, обратился в акционерное общество "Бур" с претензиями к Слепцову и потребовал исключить его из состава учредителей общества.

Как разрешить этот спор?

? Задача ╬7.7 (18)

Фирма "Крокус" оказывала различного рода правовые услуги гражданам с использованием право вых информационно-поисковых систем "Право" и "Юрисконсульт", являвшихся ее собственностью. Через год эта фирма открыла свое дочернее предприятие "Миф" и передала ему часть технических средств со всем программным обеспечением, которое ранее было установлено на них. Прошел год и предприятие "Миф" объявило себя самостоятельным и независимым от фирмы "Крокус", выкупив у нее ПЭВМ, на которых оставались правовые системы, принадлежащие "Крокусу". Однако в своей дея тельности сотрудники дочернего предприятия продолжали использовать эти информационно-правовые системы.

Имеются ли нарушения законодательства при использовании формой "Крокус" и ее дочерними предприятиями технических средств и программ?

? Задача ╬7.8 (32)

Фирма "Локон" купила у правообладателя (в магазине) за наличный расчет (по чеку) програм

мный продукт, который потребовался этой фирме для разработки собственных электронных карт. Программное обеспечение было установлено на 25 ЭВМ, составляющих локальную вычислительную сеть, с целью ее использования в автоматизированной информационно-правовой системе.

Нарушила ли в этом случае фирма "Локон" информационное законодательство?

? Задача ╬7.9 (33)

Акционерное общество "Росинка" купило у холдинга "Сабина" (по чеку) программный продукт без заключения соответствующего договора. Впоследствии данный программный продукт был установлен на нескольких ЭВМ (на станциях), образующих локальную вычислительную сеть, и успешно функционировал.

Нарушен ли здесь закон?

? Задача ╬7.10 (42)

Доцент Любичев, будучи очень занятым на кафедре, поручил аспиранту Горбункову зарегистрировать свою базу данных в Российском агентстве по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем. Горбунков в установленном порядке подал заявку на регистрацию базы в указанное агентство и стал ждать. Однако из агентства неожиданно позвонил Любичеву эксперт Полухин и сказал, что его база данных не может быть зарегистрирована через Горбункова, так как последний очень рассеян и специалисты отказываются признать его полноценным представителем. Доцент Любичев рассердился и пожаловался на Полухина руководителю агентства.

Каким образом должен зарегистрировать свою базу данных доцент Любичев?