

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Организационно-правовые механизмы обеспечения
информационной безопасности»
для студентов направления подготовки
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Практическое занятие №1

Информационные отношения как объект правового регулирования

Формируемые компетенции или их части: ПК-1

Теоретическая часть

Право – это с овокупность общеобязательных правил и норм поведения,

установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Законодательство Российской Федерации представляет собой совокупность Конституции и принимаемых в соответствии с ней законов и подзаконных актов.

Внутреннее строение системы права РФ можно представить в вертикальном и горизонтальном срезе.

Вертикальное строение права – совокупность элементов, включающих: отрасль, подотрасль, институт, субинститут и правовое предписание.

Горизонтальное строение права позволяет увидеть все отрасли, его составляющие. Если их классифицировать, то можно выделить две группы отраслей.

В первую группу объединяются **регулятивные отрасли права**, т. е. отрасли, в которых основной упор делается на установление прав и обязанностей участников правоотношений.

Вторую группу отраслей составляют **охранительные отрасли права**, основной задачей которых является защита правоотношений.

Структура правоотношений и виды юридической ответственности

Правоотношение – это такое общественное отношение, в котором стороны связаны между собой взаимными юридическими правами и обязанностями, охраняемыми государством. Правоотношение есть та мера внешней свободы, которая предоставляется его участникам нормами позитивного (писаного) права.

Структура правового отношения имеет четыре необходимых элемента: субъекты, объект, право и обязанность:

Субъекты правоотношений – это отдельные индивиды и организации, которые в соответствии с нормами права являются носителями юридических прав и обязанностей. В реальной жизни не все индивиды и организации могут быть субъектами правоотношений, например, малолетние дети, душевнобольные, организации, прекратившие свое существование, фактически не могут участвовать в правоотношениях по понятным причинам.

Мера участия субъектов в правовых отношениях определяется их правоспособностью и дееспособностью.

Правоспособность – это способность субъекта иметь юридические права и нести юридические обязанности. Она начинается с момента рождения индивида и прекращается смертью. Однако чтобы стать реальным участником правоотношения, правоспособный субъект должен быть дееспособным.

Дееспособность – это способность субъекта самостоятельно, своими действиями осуществлять юридические права и нести обязанности.

1. Объект правоотношений – это то, на что воздействует правоотношение. Объектом правоотношения является фактическое поведение его участников. В соответствии с содержанием субъективного права и юридической обязанности участники правоотношения строят свое поведение. Вступая в правоотношения, субъекты удовлетворяют определенные материальные, духовные и иные потребности (например, приобретают вещи, пользуются авторскими правами, правами изобретателя). Объектом правоотношений выступает поведение людей, которое может быть различным по

содержанию.

2. Субъективное право – это предоставляемая и охраняемая государством возможность (свобода) субъекта по своему усмотрению удовлетворять те интересы, которые предусмотрены позитивным правом. Право, принадлежащее субъекту, называется субъективным потому, что только от воли субъекта зависит, как им распорядиться. Это возможность не произвольная, а правовая, устанавливающая меру дозволенного поведения.

3. Юридическая обязанность – это предусмотренная законодательством и охраняемая государством необходимость должного поведения участника правового отношения в интересах управомоченного субъекта (индивида, организации, государства в целом). Если содержание субъективного права образует мера дозволенного поведения, то содержание обязанности – мера должного, необходимого поведения в правоотношении.

Юридическая ответственность – это применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера. Фактическим основанием для юридической ответственности является правонарушение. Лицо может быть привлечено к ответственности только при наличии в его действии всех элементов состава правонарушения.

Состав правонарушения состоит из четырех составляющих:

объект правонарушения – область общественных отношений, регулируемых и охраняемых правом, в котором произошло деяние и (или) которой данным деянием причинен вред;

объективная сторона – характеристика деяния, способа его совершения (группой, с применением оружия, систематически, повторно), обстоятельств (во время военных действий, стихийных бедствий и т. п.);

– **субъект** – лицо, которое совершило правонарушение, характеристика правонарушителя;

– **субъективная сторона** – форма вины (умысел или неосторожность).

Само по себе правонарушение не порождает автоматически возникновения ответственности, а является лишь основанием для такого применения. Для реального же осуществления юридической ответственности необходим **правоприменительный акт** – решение компетентного органа, который возлагает юридическую ответственность, устанавливает объем и форму принудительных мер к конкретному лицу. Это может быть приговор суда, приказ администрации и т. п. Наибольшее распространение получило деление юридической ответственности по отраслевому признаку. По данному основанию различают ответственность *уголовную, административно-правовую, гражданско-правовую, дисциплинарную и материальную.*

Уголовная ответственность наступает за совершение преступлений и в отличие от других видов ответственности устанавливается только уголовным законом. Никакие иные нормативные акты не могут определять общественно опасные деяния как преступные и устанавливать за них меры ответственности. В Российской Федерации исчерпывающий перечень преступлений зафиксирован в Уголовном кодексе. Порядок привлечения к уголовной ответственности регламентируется Уголовно-процессуальным кодексом. Полномочиями привлечения к уголовной ответственности обладает только суд.

Административно-правовая ответственность наступает за совершение административных проступков, предусмотренных Кодексом об административных правонарушениях. Кроме того, этот вид ответственности может устанавливаться указами Президента Российской Федерации, постановлениями Правительства Российской Федерации и нормативными актами субъектов Федерации. Дела об административных правонарушениях рассматриваются компетентными органами государственной власти, круг которых закреплен в кодексе. Меры административного принуждения – предупреждение, штраф, лишение специального права, административный арест.

Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. Ее сущность состоит в принуждении лица нести отрицательные имущественные последствия. Полное возмещение вреда – основной принцип гражданско-правовой ответственности (статья 1064 ГК). Возмещение убытков в некоторых случаях дополняется штрафными санкциями, например, выплатой неустойки.

Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Привлекать к дисциплинарной ответственности может руководитель, осуществляющий распорядительно-дисциплинарную власть над конкретным работником. Меры дисциплинарной ответственности – выговор, строгий выговор, отстранение от занимаемой должности и т. п.

Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению, заключается в необходимости возместить ущерб в порядке, установленном законом. Основанием этого вида ответственности является нанесение ущерба во время работы предприятию, с которым работник находится в трудовых отношениях. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

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

Предметом правового регулирования в информационной сфере являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация права на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают гарантии, обязанности, механизмы защиты и ответственность.

Информационное законодательство имеет вертикальную (по видам правовых актов) и горизонтальную (по отраслям законодательства) структуру. Вертикальная структура строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов.

Структура информационного законодательства как комплексной отрасли включает в себя:

- Международные акты информационного законодательства.
- Информационно-правовые нормы Конституции РФ.
- Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.
- Отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

Совокупность вышеперечисленных документов составляет правовую базу, обеспечивающую нормативное регулирование процессов информационного обмена, в том числе и защиту информации.

Информация имеет ряд особенностей, отличающих ее от других видов товаров:

- нематериальность (идеальность) информации;
- информационный продукт подвергается только моральному износу;
- информация находится на материальном носителе;
- информация не исчезает при потреблении и может быть использована многократно;
- производство информации требует значительных затрат по сравнению с затратами на тиражирование;

- при копировании количество информации не изменяется, а цена снижается.

Основные определения в области информационного права:

Информация – это сведения о лицах, предметах, фактах, явлениях, процессах независимо от формы их представления.

Документированная информация – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Объект правоотношений – это то, на что воздействуют правоотношения.

Субъект правоотношений – предоставленная и охраняемая государством возможность субъекта по своему усмотрению удовлетворять потребности, предусмотренные позитивным правом.

Юридическая ответственность – применение предусмотренных санкций, юридических норм, мер государственного принуждения.

Юридические обязанности – предусмотренная законодательством и охраняемая государством необходимость должностного поведения участника правоотношений.

Правовые принципы защиты информации:

- полнота правового регулирования;
- принципы единства нормативно-правовой базы;
- непротиворечивость законодательной базе;
- принцип соблюдения рациональных пропорций между правовыми и технико-юридическими нормами;
- нормативно-правовые акты должны предусматривать развернутую защиту прав граждан.

Вопросы и задания:

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по установке «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности:

Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.

7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.

8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №2

Информационные отношения как объект правового регулирования

Цель работы: ознакомиться с нормативно-правовыми актами РФ в области информационной безопасности

Формируемые компетенции или их части: ПК-1

Теоретическая часть

В настоящее время с учетом сложившейся практики обеспечения информационной безопасности принято выделять следующие направления защиты информации:

- правовая защита – это специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

Правовое обеспечение информационной безопасности любой страны содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения информационной безопасности составляют Конституция РФ, Законы РФ, Кодексы, Указы и другие нормативные акты, регулирующие отношения в области информации.

Правовая защита информации как ресурса признана на международном уровне и определяется межгосударственными договорами, конвенциями, декларациями, реализуется правовыми механизмами защиты патентных и авторских прав.

В реализации государственной политики в сфере информатизации участвуют следующие структуры власти:

- Президент Российской Федерации;
- Совет Федерации;
- Государственная дума Федерального собрания Российской Федерации;
- Правительство Российской Федерации;
- Совет безопасности Российской Федерации;
- федеральные органы исполнительной власти;
- органы государственной власти Российской Федерации;
- органы местного самоуправления.

Совет безопасности Российской Федерации рассматривает наиболее важные вопросы, связанные с безопасностью Российской Федерации в современном мире, в том числе и вопросы информационной безопасности.

Структуру аппарата системы безопасности Российской Федерации составляют:

- Управление информационной безопасности и стратегического

прогнозирования;

- Межведомственная комиссия Совета безопасности Российской Федерации по информационной безопасности.

В Государственной думе Российской Федерации функционируют:

- Комитет по информационной политике и связи;
- Комитет по безопасности, составной частью которого является комитет по информационной безопасности.

На внутригосударственном уровне правовая защита регулируется государственными и ведомственными актами. Государственными актами являются Конституция РФ, законы РФ, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями.

Информационное законодательство – совокупность норм права, регулирующих общественные отношения в информационной среде. Предметом правового регулирования в информационной среде являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация прав граждан на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

Таким образом, законодательство по информационной безопасности является неотъемлемой частью всей системы законов Российской Федерации.

Федеральный закон «Об информации, информационных технологиях и о защите информации»

Со дня вступления в силу Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» утратили силу Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» и Федеральный закон от 04 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене».

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Термины, используемые в законе, их определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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

Доступ к информации – возможность получения информации и ее использования.

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

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель.

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

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Важнейшие задачи обеспечения информационной безопасности Российской Федерации:

1. Противодействие угрозе развязывания противоборства в информационной

сфере.

2. Реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности.

3. Совершенствование и защита отечественной информационной структуры, интеграция России в мировое информационное пространство.

Доктрина информационной безопасности РФ развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для:

1) формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

2) подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

3) разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под *информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы *личности* в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы *общества* в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы *государства* в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в

информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Федеральный закон «О техническом регулировании»

Федеральный закон «О техническом регулировании» от 27 декабря 2002 года № 184-ФЗ регулирует отношения, возникающие при:

1) разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;

2) разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;

3) оценке соответствия продукции установленным законодательством требованиям.

Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

Действие закона не распространяется на государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

Термины, используемые в законе, их определения

Аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

Безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов.

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

Заявитель – физическое или юридическое лицо, осуществляющее обязательное подтверждение соответствия.

Знак обращения на рынке – обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов.

Знак соответствия – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

Идентификация продукции – установление тождественности характеристик продукции ее существенным признакам.

Контроль (надзор) за соблюдением требований технических регламентов – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки.

Международный стандарт – стандарт, принятый международной организацией.

Национальный стандарт – стандарт, утвержденный национальным органом Российской Федерации по стандартизации.

Орган по сертификации – юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации.

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

Подтверждение соответствия – документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Продукция – результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях.

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда.

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

Сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

Система сертификации – совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом.

Стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Техническое регулирование – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции,

процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.

Технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

Форма подтверждения соответствия – определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Закон Российской Федерации «О безопасности»

Закон РФ «О безопасности» от 5 марта 1992 года № 2446-1 закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Термины, используемые в законе, их определения

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся:

- 1) личность – ее права и свободы;
- 2) общество – его материальные и духовные ценности;
- 3) государство – его конституционный строй, суверенитет и территориальная целостность.

Субъект обеспечения безопасности – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

Принципы обеспечения безопасности

Безопасность достигается проведением единой государственной политики в

области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

Вопросы и задания:

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.
12. Назовите и охарактеризуйте направления защиты информации.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.-

М.: Академия, 2008. – 192 с.

7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.

8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №3

Правовое обеспечение защиты государственной тайны

Цель работы: ознакомиться с предметом информационного права в информационной безопасности.

Формируемые компетенции или их части: ПК-1.

Теоретическая часть

Информация ограниченного доступа, включающая государственную тайну и конфиденциальную информацию, имеет особую важность для государства и общества. В той или иной мере правовые институты тайн есть во всех развитых демократиях мира.

Опыт показывает, что с ростом значимости информации в общей системе государственного и муниципального управления (ГМУ) наиболее важным элементом с годами становится достижение превосходства в информационной сфере. Этим обстоятельством и определяется существование институтов тайн, создающих возможность для ГМУ проводить независимую информационную политику, защищать свои интересы, осуществлять управление обществом, регионом, муниципальным образованием.

Система секретной и конфиденциальной информации – наиболее сильное звено регулирования общественных отношений в информационной сфере. Вследствие возможного существенного ущерба от ее разглашения информация ограниченного доступа занимает особое место в системе управления. Институт тайн – важнейший элемент системы государственного и муниципального управления.

Основу нормативно-правового обеспечения защиты информации ограниченного доступа в России составляют Конституция РФ, законы «О безопасности» от 5 марта 1992 года № 2446-1, «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ и другие.

В условиях сегодняшней России (расширяющееся международное сотрудничество, либерализация экономики, увеличение количества объектов иностранных инспекций, свободное перемещение иностранцев по большей части территории страны, внедрение компьютерной техники иностранного производства) значительной возросла опасность утечки сведений, составляющих информацию ограниченного доступа. Вследствие этого важнейшими задачами органов ГМУ являются обеспечение необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями на ее распространение, а также развитие и защита государственного и муниципального ресурса.

В действующем законодательстве РФ встречается упоминание более чем о 30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная, тайна следствия, связи, почтовых отправок и другие).

Приведем наиболее важные определения в этой области и дадим необходимую классификацию.

Защищаемой информацией называется информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации относится информация с ограниченным доступом, а также открытая информация, представляющая ценность.

Информацией с ограниченным доступом называется информация, доступ к которой ограничен в соответствии с Законом с целью защиты прав и законных интересов субъектов права на тайну. Она состоит из государственной тайны и конфиденциальной информации.

Конфиденциальная информация в свою очередь включает множество видов тайны, которые сводятся к шести основным видам:

- 1) персональные данные;
- 2) тайна следствия и судопроизводства;
- 3) служебная тайна;
- 4) профессиональная тайна;
- 5) коммерческая тайна;
- 6) тайна изобретения, полезной модели и промышленного образца.

Особую важность с точки зрения безопасности государства имеет защита информации, составляющей государственную и служебную тайну.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Конфиденциальная информация – информация, не составляющая государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Тайна следствия и судопроизводства – защищаемая по закону конфиденциальная информация, ставшая известной в органах следствия и судопроизводства только на законных основаниях в ходе следствия и судопроизводства, а также служебная информация о деятельности органов следствия и судопроизводства, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, банковская тайна и т. д.).

Коммерческая тайна – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности меры охраны.

Тайна изобретения, полезной модели или промышленного образца – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Согласно законодательству обязательными признаками информации с ограниченным доступом должны быть:

1. Информация имеет действительную или потенциальную ценность для ее обладателя в силу неизвестности ее третьим лицам. Таковыми лицами могут быть государство, юридические или физические лица.

2. К информации нет свободного доступа на законном основании. Возможность сохранения ее неизвестной для третьих лиц установлена законом.

3. Обладатель информации принимает меры по ее защите.

К государственной тайне относятся сведения, удовлетворяющие следующим признакам:

1. Сведения в строго установленных сферах деятельности государства (военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно розыскной деятельности) и ни в каких других.

2. Сведения, не известные широкому, точнее – неопределенному неконтролируемому кругу лиц, и представляющие ценность именно в силу такой неизвестности.

3. Сведения, распространение которых может нанести ущерб безопасности РФ. При этом величина ущерба такова, что влияет на безопасность государства.

4. Сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

Система документов по защите государственной тайны

Документы по защите государственной тайны по функционально-целевому назначению подразделяются на следующие основные классы:

- нормативные правовые;
- организационно-распорядительные;
- нормативные;
- плановые;
- информационные.

Нормативные правовые акты в области защиты государственной тайны включают:

- федеральные законы;
- указы и распоряжения Президента РФ;
- постановления и распоряжения высших органов исполнительной и судебной властей РФ.

Базовыми законами в области защиты государственной тайны являются специальные законы «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, а также нормативные правовые акты более общего характера: Конституция РФ, Гражданский и Уголовный кодексы РФ и др.

На их основе **организационно-распорядительные документы** определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны. Эти документы по характеру регламентируемых вопросов (решаемых задач) и продолжительности действия подразделяют на два вида:

- основополагающие (руководящие) документы;
- распорядительные документы (документы оперативного управления).

Основополагающие (руководящие) документы помимо самостоятельного использования служат основой при разработке нормативных, плановых и информационных документов. Они являются подзаконными актами, детализирующими и раскрывающими положения нормативных правовых актов, и устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их задач, функций, прав,

обязанностей и мер ответственности.

Положения по защите государственной тайны издаются на основе нормативных правовых актов и принятых концепций и детализируют указные документы, в основном по вопросам организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

- основные направления работ по защите государственной тайны;
- структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;
- порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;
- финансово-экономические вопросы обеспечения работ по защите государственной тайны;
- вопросы государственного лицензирования в области защиты государственной тайны.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие руководства, наставления, инструкции и правила.

Распорядительные документы – документы текущего (оперативного) управления издают во исполнение или в дополнение к основополагающим документам. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

Нормативные документы устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну, обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых регламентируются вопросы защиты государственной тайны, являются:

- специальные нормативные документы федеральных органов исполнительной власти, ответственных за обеспечение защиты государственной тайны;
- нормативные документы государственной системы стандартизации.

К специальным нормативным документам относятся:

- требования и нормы по защите государственной тайны;
- методики проведения работ в области защиты государственной тайны;
- лицензии предприятиям на право осуществления работ в области защиты государственной тайны;
- сертификаты соответствия средств защиты информации;
- аттестаты на объекты защиты.

Плановые документы включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

Информационные документы служат для информационного обеспечения решения задач организации и осуществления защиты государственной тайны.

По форме представления информационные документы могут быть следующих видов:

- справочные документы;
- отчетная научно-техническая документация;
- учебная и научная литература;
- формы документов служебного делопроизводства.

Федеральный закон «О государственной тайне»

Положения федерального закона «О государственной тайне» от 21 июля 1993 года № 5485-1 обязательны для исполнения на территории Российской Федерации и за ее

пределами органами *законодательной*, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Термины, используемые в законе, их определения

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

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

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

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

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

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

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

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

Правовой режим защиты государственной тайны

Перечневый подход к организации защиты государственной тайны

В настоящее время в России существуют как открытые, так и закрытые перечни сведений. Открытыми перечнями являются приведенный в Законе «О государственной тайне» перечень сведений, составляющих государственную тайну, а также утверждаемый Указом Президента РФ перечень сведений, отнесенных к государственной тайне. Кроме того, существуют ведомственные перечни сведений, подлежащих засекречиванию, которые могут быть как открытыми, так и закрытыми.

С их помощью реализуется подход к организации защиты государственной тайны в виде системы перечней, включающей:

- перечень сведений, составляющих государственную тайну (определен в Законе «О государственной тайне»);
- перечень сведений, отнесенных к государственной тайне (утверждается Указом Президента РФ);
- развернутый перечень сведений, подлежащих засекречиванию в органе государственной власти (утверждается руководителями органов власти, руководители

которых наделены полномочиями по отнесению сведений к государственной тайне);

– перечни сведений, подлежащих засекречиванию, на предприятии, в учреждении и организации (представляют собой выписки из развернутых перечней сведений, подлежащих засекречиванию).

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

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделяемых полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Перечень не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Такой подход должен позволить системе засекречивания адаптироваться к динамичному развитию нашего общества, ослабить искусственную секретность, наносящую ущерб экономическим интересам РФ.

Установлена персональная ответственность конкретных должностных лиц за принятие решения по отнесению сведений к государственной тайне. Именно за ними сохраняется ответственность за обоснованность, в том числе экономическую, установленной степени секретности конкретных сведений. Именно на них возложена функция гибкого и своевременного реагирования на внешние условия изменения режима секретности, чтобы последний не превращался в фактор, тормозящий развитие экономики, науки и межгосударственных отношений.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- 1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- 2) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- 3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- 4) о фактах нарушения прав и свобод человека и гражданина;
- 5) о размерах золотого запаса и государственных валютных резервах РФ;
- 6) о состоянии здоровья высших должностных лиц РФ;
- 7) о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Вопросы и задания:

1. Перечислите основные виды тайн. Охарактеризуйте каждый вид.
2. Назовите обязательные признаки информации с ограниченным доступом.
3. На какие классы по функциональному назначению подразделяются документы

по защите государственной тайны?

4. Дайте определение понятию «гриф секретности».
5. Какие сведения не относятся к государственной тайне и не подлежат засекречиванию?
6. Перечислите органы защиты государственной тайны.
7. Какие существуют методы защиты сведений, составляющих государственную тайну?
8. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по установке «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №4
Система защиты государственной тайны

Цель работы: ознакомиться с системами защиты государственной тайны

Формируемые компетенции или их части: ПК-1

Теоретическая часть

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

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны), Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне.

Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом РФ.

Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны, Служба внешней разведки РФ, Государственная техническая комиссия при президенте РФ и их органы на местах организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Защита государственной тайны является основным видом деятельности органов государственной власти, предприятий, учреждений или организаций.

Цель защиты государственной тайны заключается в предотвращении или снижении величины ущерба безопасности государства путем исключения (существенного затруднения) утечки информации по всем возможным каналам.

Методы защиты сведений, составляющих государственную тайну, подразделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения защиты сведений, составляющих государственную тайну, относится разработка нормативных правовых актов, регламентирующих отношения в области защиты государственной тайны, и нормативных методических документов по вопросам обеспечения защиты государственной тайны.

Организационно-техническими методами обеспечения защиты сведений, составляющих государственную тайну, являются:

- создание и совершенствование системы защиты государственной тайны в РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, включая предупреждение и пресечение правонарушений в области защиты государственной тайны, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;

- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах жизни и деятельности общества и государства, в том числе и по вопросам обеспечения защиты государственной тайны.

Экономические методы обеспечения защиты государственной тайны включают в себя:

- разработку федеральных программ в области защиты государственной тайны и определение порядка их финансирования;

- установление и наложение штрафов на должностных и юридических лиц за нарушения требований по защите государственной тайны.

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:

- бумажные документы;

- магнитные носители информации в электронно-вычислительных машинах;

- электромагнитные поля, создаваемые радиоэлектронными средствами при передаче информации;

- физические проявления объектов (органов управления, промышленных предприятий и др.), сведения о которых составляют государственную тайну, в виде разнообразных полей и следов деятельности.

Как носители сведений в современных условиях особую роль имеют технические средства сбора, передачи, хранения и обработки информации. С их использованием обрабатывается основной объем информации, составляющей государственную тайну. Их недостатком является уязвимость для широкого спектра угроз несанкционированного распространения защищаемой информации. защите информации на таких носителях уделяется особое внимание.

Человек в действующем Законе РФ «О государственной тайне» не рассматривается как специфический носитель сведений, хотя он в своей памяти может хранить эти сведения. Тем самым человек не ставится на один уровень с техническими носителями. Он в проблеме защиты государственной тайны рассматривается как субъект общественных отношений, возникающих в процессе защиты государственной тайны.

Полномочия органов государственной власти и должностных лиц в области защиты государственной тайны

Палаты Федерального собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны;

- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

- определяют полномочия должностных лиц в аппаратах палат Федерального собрания по обеспечению защиты государственной тайны.

Президент РФ:

- утверждает государственные программы в области защиты государственной тайны;
- утверждает по представлению Правительства РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства РФ перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры РФ о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

Правительство РФ:

- организует исполнение Закона РФ «О государственной тайне» ;
- представляет на утверждение Президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает порядок разработки Перечня сведений, отнесенных к государственной тайне;
- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства РФ;
- устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;
- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства РФ;
- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства РФ о государственной тайне;

- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;

- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;

- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

Допуск должностных лиц и граждан к государственной тайне

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

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

Допуск должностных лиц и граждан к государственной тайне предусматривает:

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

- согласие на частные, временные ограничения их прав в соответствии со статьей 24 Закона «О государственной тайне»;

- письменное согласие на проведение в отношении их полномочий органами проверочных мероприятий;

- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом «О государственной тайне»;

- ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;

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

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

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

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

Основанием для отказа гражданину в допуске к государственной тайне в соответствии со статьей 22 Закона «О государственной тайне» могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

– наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ;

– постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное место жительства в другое государство;

– выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;

– уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

– **первая форма** – для граждан, допускаемых к сведениям особой важности;

– **вторая форма** – для граждан, допускаемых к совершенно секретным сведениям;

– **третья форма** – для граждан, допускаемых к секретным сведениям.

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Основными **целями** контроля и надзора являются:

– обеспечение выполнения единых правил и норм в организации работ по защите государственной тайны;

– своевременное выявление предпосылок к утечке информации, составляющей государственную тайну.

Основными **задачами** контроля и надзора являются:

– оценка полноты и качества выполнения органами, организациями и должностными лицами, осуществляющими деятельность в области защиты государственной тайны, возложенных на них обязанностей и функций;

– оценка целесообразности и обоснованности принимаемых управленческих решений и мер по защите государственной тайны с целью предупреждения возможных неблагоприятных последствий их выполнения;

– выявление нарушений установленных требований или норм по защите государственной тайны, установление их причин, подготовка в необходимых случаях материалов для привлечения виновных к ответственности;

– профилактика различных видов нарушений;

– выявление нерешенных проблем и противоречий в правовом, организационном, научно-техническом, информационном и других видах обеспечения эффективной защиты государственной тайны.

Рассмотрим основные термины в области контроля и надзора за обеспечением защиты государственной тайны.

Контроль состояния защиты государственной службы – проверка соответствия организации и эффективности защиты информации, составляющей государственную тайну, установленным требованиям и/или нормам по защите государственной тайны.

Контроль организации защиты информации – проверка соответствия организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации.

Надзор – наблюдение, разновидность контроля, одна из форм деятельности различных государственных органов по обеспечению законности. Надзор – это контроль в форме правового регулирования. Эта форма применяется, прежде всего, для осуществления контроля за соблюдением законов, установленных норм, требований, стандартов. Органы надзора вправе при соответствующих обстоятельствах применять к объектам надзора меры административного принуждения. Необходимым условием надзора является отсутствие между субъектами и объектами надзора организационной соподчиненности.

Вопросы и задания:

1. Какие существуют методы защиты сведений, составляющих государственную тайну?
2. Перечислите органы защиты государственной тайны.
3. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
4. Назовите цели и задачи контроля и надзора за обеспечением защиты государственной тайны.
5. Поясните сущность ведомственного контроля над обеспечением защиты государственной тайны.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №5

Правовое обеспечение защиты банковской, профессиональной и служебной тайны

Цель работы: ознакомиться с правовым обеспечением защиты банковской, профессиональной и служебной тайны.

Формируемые компетенции или их части: ПК-1

Теоретическая часть

Банковская тайна – защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов. К основным объектам банковской тайны относятся: тайна банковского счета, тайна операций по банковскому счету, тайна банковского вклада, тайна частной жизни клиента.

Банковская тайна является видом конфиденциальной информации или видом сведений, перечень которых достаточно четко определен законом. Статья 857 «Гражданского кодекса РФ (Часть вторая)» от 26 января 1996 года № 14-ФЗ «Банковская тайна» содержит следующие нормы:

- 1) банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;
- 2) сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренном законом;
- 3) в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 года № 395-1 содержит более расширенную группу норм (статья 26):

– Кредитная организация. Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

– Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям). Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.

– Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия прокурора – органами предварительного следствия по делам, находящимся в их производстве.

– Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.

– Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

– Аудиторские организации не вправе раскрывать третьим лицам сведения об

операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

– За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

Таким образом, сведения, составляющие банковскую тайну, не устанавливаются по волеизъявлению субъекта предпринимательской деятельности – банка или иной кредитной организации, а это определенные законом сведения, которые принадлежат клиентам банка (банковский счет, банковский вклад, операции по счету, сведения о клиенте). При этом обязанность сохранять эти сведения является односторонней обязанностью банка – клиент не связан этими обязательствами. Вторым отличием банковской тайны, выводящим ее за пределы частного случая коммерческой тайны, является тот факт, что банковская тайна может выступать как охранительный институт для личной и семейной тайны, если граждане желают сохранять в тайне свое финансовое положение.

Пользование информацией, составляющей профессиональную тайну

В сфере ГМУ широко распространена **профессиональная тайна**, которая представляет собой одну из самых специфических систем ограничений на доступ к информации. Профессиональная тайна чаще всего имеет дело с информационными блоками, защита от несанкционированного распространения которых является обязанностью субъекта в силу выполняемых им профессиональных функций. При этом в качестве субъекта, на который возлагается обязанность сохранения профессиональной тайны, может выступать как физическое, так и юридическое лицо. Соблюдение тайн представителями определенных профессий является их обязанностью, возникающей вне зависимости от того, урегулирована она какими-либо юридическими нормами либо нет. В этом случае обязательства по нераспространению сведений являются неотъемлемой частью самой профессии. Гражданин не обратился бы к адвокату, нотариусу или частнопрактикующему врачу, если бы не был уверен, что доверенные этому лицу сведения не будут сохранены в тайне от посторонних, которыми в данном случае являются любые третьи лица.

Система исходящих от государства норм поведения также не может оставаться в стороне от регулирования этой группы общественных отношений.

Нормы законодательства, регулирующие данные отношения, характеризуются в целом двумя моментами:

- данные нормы содержатся в соответствующих профильных законах;
- как правило, эти нормы содержат только запреты на распространение определенных категорий сведений, не описывая механизма их защиты.

Объектом профессиональной тайны является, прежде всего, информация, принадлежащая гражданам, обращающимся за профессиональными услугами (нотариальными, страховыми, медицинскими и др.). С развитием рыночных отношений и появлением большого числа субъектов предпринимательской деятельности в России юридические лица также стали полноправными участниками этих отношений. Нотариальная тайна, тайна связи, адвокатская тайна – действие этих правовых институтов в равной степени распространяется и на сведения, обладателями которых являются юридические лица.

Профессиональная тайна является неотъемлемой частью определенных видов профессиональной деятельности вне зависимости от того, ведется она от имени государства или от частного лица. И даже если она ведется от имени государства, это не значит, что государство в лице других органов ГМУ может без ограничений получать доступ к таким сведениям.

К примеру, по действующему законодательству РФ информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при обследовании и лечении, составляют **врачебную (медицинскую) тайну**.

Включаемый в данный институт перечень сведений достаточно подробно представлен в действующем законодательстве РФ. Прежде всего следует отметить нормы статьи 61 «Основ законодательства РФ об охране здоровья граждан», утвержденные ВС РФ 22 июля 1993 года № 5487-1, которая именуется «Врачебная тайна». На основе этих норм к медицинской тайне относятся:

- факт обращения гражданина за медицинской помощью;
- состояние здоровья гражданина;
- диагноз заболевания;
- иные сведения, полученные при обследовании и лечении.

Допускается предоставление сведений, составляющих медицинскую тайну, без согласия гражданина или его законного представителя:

- в целях обследования гражданина, не способного выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему в возрасте до 15 лет для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий.

Нотариальная тайна вытекает из законодательной базы деятельности нотариата в РФ, которую определяет Конституция РФ и Основы законодательства РФ о нотариате.

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

Процессуальные тайны – тайна совещания судей, тайна совещания присяжных заседателей, данные предварительного следствия (дознания) – содержат в себе признаки как служебной тайны, так и профессиональной.

Первые два вида направлены на обеспечение невмешательства в отправление правосудия и представляют из себя административно-правовой запрет на контакт с судьями в период их совещания по поводу вынесения приговора (вердикта, решения).

Тайна страхования – это разновидность служебной, а также коммерческой тайны. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о застрахованном лице, о состоянии его здоровья, а также о его имущественном положении.

Тайна связи – регулируется конституционными нормами (часть 2 статьи 23 Конституции РФ), а также соответствующими нормами федеральных законов «О связи» от 07 июля 2003 года № 126-ФЗ, «О почтовой связи» от 17 июля 1999 года № 176-ФЗ.

Пользование информацией, составляющей служебную тайну

В сфере ГМУ нередко фигурирует служебная тайна, которая наиболее сложна с точки зрения определения ее понятия и правового режима, поскольку в этот вид тайны в разное время включалось и теперь включается различное содержание. Служебная тайна является разновидностью конфиденциальной информации. Согласно Закону РФ «О государственной тайне» от 21 июля 1993 года № 5485-1, прежний режим служебной тайны упразднен, и секретные сведения относятся к государственной тайне. Однако в различных правовых актах термин «служебная тайна» продолжает упоминаться и в него вкладывается различное значение, причем в большинстве случаев оно даже не раскрывается.

Объектами служебной тайны являются преднамеренно скрываемые интересы и

сведения о различных сторонах и сферах государственной, военной, управленческой, научно-технической, финансовой, экономической и др. деятельности хозяйствующего субъекта, охрана которых обусловлена возможной угрозой безопасности хозяйствующего субъекта.

Субъектами служебной тайны являются собственник служебной информации ограниченного распространения (юридическое лицо, обладающее на законном основании служебной конфиденциальной информацией), конфиденент служебной информации ограниченного распространения (физическое или юридическое лицо, использующее служебную информацию ограниченного распространения в пределах, установленных собственником или владельцем служебной информации ограниченного распространения на основании договора или распорядительных документов).

Содержащие служебную тайну документы:

- печатаются в специально выделенной комнате;
- учитываются, как правило, отдельно от несекретной документации;
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются только с письменного разрешения соответствующего руководителя;
- хранятся в надежно запираемых и опечатываемых шкафах.

Вопросы и задания:

1. Какие сведения относятся к банковской тайне?
2. Перечислите известные вам виды профессиональной тайны.
3. Раскройте порядок обращения с документами, содержащими служебную тайну.
4. Какая информация относится к сведениям конфиденциального характера?
5. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?
6. Опишите структуру законодательства РФ о коммерческой тайне.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №6

Правовое обеспечение защиты коммерческой тайны

Цель работы: ознакомиться с предметом информационного права в информационной безопасности.

Формируемые компетенции или их части: ПК-1.

Теоретическая часть

Конфиденциальная информация – достаточно широкое понятие, поскольку к этой категории (за исключением сведений, относящихся к государственной тайне) относятся все виды информации ограниченного доступа, защищаемой законами.

В соответствии с Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188 к этим сведениям относятся:

- 1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- 2) сведения, составляющие тайну следствия и судопроизводства;
- 3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
- 4) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);
- 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.

Расширительному толкованию этот перечень не подлежит. Поэтому произвольное отнесение кем-либо к разряду конфиденциальной другой, не предусмотренной перечнем информации не влечет за собой правовых последствий. Более того, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ запрещено относить к конфиденциальной информации:

- 1) 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;
- 2) 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;
- 3) 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 сведений, отнесенных к государственной тайне;
- 4) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений и организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей

граждан.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК.

Под **технической защитой конфиденциальной информации** понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

В соответствии с Положением «О лицензировании деятельности по технической защите конфиденциальной информации» лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

1) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности «компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

2) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами РФ, руководящими и нормативно-методическими документами, утвержденными приказами ФСТЭК, которые зарегистрированы в Министерстве юстиции РФ;

3) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

4) использование третьими лицами программ для ЭВМ или баз данных на основании договора с их правообладателем.

Законодательство Российской Федерации о коммерческой тайне

В условиях рыночного хозяйствования коммерческая тайна защищает производителя от недобросовестной конкуренции, к которой относятся противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т. п.

Законодательство Российской Федерации о коммерческой тайне есть совокупность федеральных законодательных актов, которые содержат правовые нормы, регулирующие группу однородных общественных отношений, возникающих в связи и по поводу коммерческой тайны между ее обладателем и иными субъектами.

Закон «О предприятиях и предпринимательской деятельности» от 25 декабря 1990 года № 445-1 впервые закрепил понятие «коммерческая тайна»: информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Федеральный закон «О коммерческой тайне»

Федеральный закон «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Положения закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована и не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Основные понятия и определения

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

Информация, составляющая коммерческую тайну (секрет производства) – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

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

Обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информация, относящаяся к коммерческой тайне

Состав сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых предприятием по защите своей интеллектуальной собственности. Ошибочное или несвоевременное выделение предмета защиты существенно снижает эффективность системы информационной безопасности предприятия, что чревато существенным экономическим ущербом для него.

Перечень сведений, составляющих коммерческую тайну предприятия, следует формировать по следующим признакам:

- эта информация должна быть экономически выгодной для предприятия или выгодной для его конкурента в случае ее утечки. В качестве критерия важности конкретной информации принимается количественный показатель величины наносимого ущерба;

- эта информация не должна быть общеизвестной или общедоступной на законных основаниях;
- эти сведения не должны содержать государственной тайны или защищаться согласно нормам авторского или патентного права;
- информация, которая зафиксирована в письменной или иной материальной форме или находится в исключительном ведении предприятия;
- такая информация должна быть понятным образом специально обозначена («грифована») и в отношении нее должны быть обеспечены необходимые меры по сохранению конфиденциальности;
- эти сведения не должны напрямую касаться деятельности предприятия, способной нанести ущерб обществу, жизни и здоровью людей.

При этом информация, подтверждающая сведения, компрометирующие компанию, не может быть только на этом основании отнесена к коммерческой тайне.

Обеспечение конфиденциальности требует определенных затрат, в число которых входят, с одной стороны, затраты на обеспечение режимных мероприятий, а с другой – потери от ограничений в использовании конфиденциальной информации. Экономический же эффект от утаивания информации может выразиться как в получении реальной прибыли, так и в предотвращении возможного ущерба предприятию. Сравнение положительных и отрицательных последствий ограничения доступа к рассматриваемым сведениям и их открытого использования, анализ возможностей предприятия по обеспечению необходимых защитных мер позволит определить экономическую или иную целесообразность отнесения тех или иных сведений к коммерческой тайне.

С течением времени ценность информации уменьшается, а суммарные затраты растут. Чем выше уровень защиты, тем дороже обходится ее обеспечение, поэтому необходимо оценивать оптимальный уровень защиты.

Самое сложное из приведенных понятий – отсутствие доступа на законном основании. За этой формулировкой стоят перечни сведений, которые запрещено относить к тому или иному виду тайны.

В законе «О коммерческой тайне» приведены сведения, которые не могут составлять коммерческую тайну.

Таким образом, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения

к ответственности за совершение этих нарушений;

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

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

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

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

В статье 10 закона «О коммерческой тайне» приведены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

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

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

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

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

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, приведенных выше.

Наряду с приведенными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Кроме того, меры по охране конфиденциальности информации признаются разумно достаточными, если:

- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

- 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Контрольные вопросы:

1. Что представляет собой информация, составляющая коммерческую тайну?
2. Что понимается под разглашением информации, составляющей коммерческую тайну?
3. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?

4. В отношении каких сведений не может быть установлен режим коммерческой тайны?
5. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №7

Правовое обеспечение защиты персональных данных

Цель работы: ознакомиться с правовым обеспечением защиты персональных данных.

Формируемые компетенции или их части: ПК-1

Теоретическая часть

По смыслу Конституции РФ **личность** – это человек как член общества и как носитель индивидуального начала. Главное в конституционном понятии личности – это социальная ценность человека, в соответствии с чем он является субъектом различных прав, свобод и обязанностей.

Сущность информационной свободы состоит, по крайней мере, из четырех правомочий: право на индивидуализацию; право на защиту чести и достоинства; право на дачу согласия на сбор, хранение и использование материалов о частной жизни; право на неприкосновенность частной жизни, личную и семейную тайну.

Право на неприкосновенность частной жизни, личную и семейную тайну означает, что человек вправе строить свою жизнь в семье, в неформальном общении с друзьями и другими лицами таким образом, как он сам того желает.

В Российском законодательстве существуют следующие источники права на личную или семейную тайну:

1. Конституция РФ признает права и свободы человека высшей ценностью, а их защиту – обязанностью государства.
2. Федеральный Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ регулирует отношения, возникающие при:

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

3. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ регулирует отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

4. Уголовный кодекс РФ. Статья 137. Нарушение неприкосновенности частной жизни.

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.

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

4. Трудовой кодекс РФ. Осуществляет защиту персональных данных работника – информации, необходимой работодателю в связи с трудовыми отношениями.

5. Гражданский кодекс РФ. Статьи 150-152, призванные защитить право человека на неприкосновенность частной жизни.

Наиболее емким потоком конфиденциальной информации являются сведения о гражданах. Действующее законодательство определяет их как персональные данные. Это понятие было введено Федеральным Законом «Об информации, информатизации и о защите информации» и получило дальнейшее развитие в Указе Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188.

Предметом личной и семейной тайны являются следующие сведения:

1. О фактах биографии.
2. О состоянии здоровья человека.
3. Об имущественном положении.
4. О роде занятий и совершенных поступках.
5. О взглядах, оценках, убеждениях человека.
6. Об отношениях в семье, а также отношениях человека с другими людьми.

В соответствии с Федеральным законом «О персональных данных» под **персональными данными** понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место

рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

К персональным данным относятся: биграфические и опознавательные данные, личные характеристики, сведения о семейном положении, социальном положении, образовании, навыках, профессии, служебном положении, финансовом положении, состоянии здоровья и прочее.

Обработка персональных данных должна осуществляться на основе принципов:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных за исключением следующих случаев:

1) если обработка персональных данных осуществляется на основании Федерального закона «О персональных данных», устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

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

Независимо от вида деятельности на любом предприятии имеется информация, требующая защиты. На коммерческом предприятии это коммерческая тайна и персональные данные сотрудников (ПДР).

Персональные данные работника – информация о конкретном лице, необходимая работодателю в связи с возникновением трудовых отношений. Данная информация в соответствии с законодательством (Закон РФ «Об информации, информационных технологиях и о защите информации») является конфиденциальной. На каждого работника ведется личное дело, в состав которого входят данные, представленные на рисунке 2.3.

Согласно «Перечню типовых управленческих документов, образующихся в деятельности организаций с указанием сроков хранения», личные дела рядовых работников предприятия должны храниться 75 лет, а руководителей – постоянно.

Личные дела работников хранятся как документы, доступ к которым ограничен.

Отбор документов предприятия на хранение или уничтожение осуществляется по решению экспертной комиссии, руководствующейся федеральными, отраслевыми и внутренними нормативными актами, например:

- «Положение об Архивном фонде РФ»;
- «Основные правила работы ведомственных архивов»;
- «Положение об экспертной комиссии»;
- «Номенклатура дел»;
- «Инструкция по делопроизводству» и др.

Экспертиза ценности документов производится ежегодно. Документы по личному составу или содержащие КТ, отобранные на хранение, требуют дополнительного оформления:

- производится нумерация листов в правом верхнем углу;
- составляется внутренняя опись;
- дело переплетается и прошивается в четыре прокола.

Опись дел по личному составу обозначают: опись №1 л/с.

Очень важной и дорогостоящей информацией фирмы являются сведения о клиентах и конкурентах. Западные специалисты рекомендуют использовать два документа: «профиль клиента» и «профиль конкурента», которые должны постоянно пополняться и обновляться информацией. Эти базы данных позволяют найти индивидуальный подход к деловому партнеру и предвидеть шаги конкурентов.

Доказательством высокого качества делового партнерства и обеспечения интересов клиента служит наличие на фирме сертификата по Международной системе стандартов качества ISO 9000. В настоящее время система ISO оценивает не только качество конечного продукта бизнеса, но и сам бизнес-процесс предприятия: проектирование, разработку, закупку сырья и комплектующих, создание, обработку, документирование, заключение контрактов, обучение персонала, обслуживание и поддержку клиентов и информационную безопасность.

По имеющимся данным к 2002 году 76 стран мира проводят сертификацию на соответствие стандартам ISO 9000. Сертификат получили более 100000 компаний. Наличие сертификата позволяет заключать сделки с ведущими мировыми компаниями, получать госзаказы, принимать участие в международных проектах.

Исследования поведения компаний при проведении такой сертификации позволяет заглянуть под маску рекламного имиджа, что значительно увеличивает безопасность деловых отношений.

Неоправданный риск сомнительных сделок может серьезно отразиться на жизнеспособности предприятия. Результатом недобросовестной конкуренции может стать уничтожение или потеря значительной части информационных ресурсов предприятия. В ряде случаев такие потери могут привести к банкротству и ликвидации предприятия.

В Российской Федерации принят закон «О несостоятельности (банкротстве)» от 26

октября 2002 года № 127-ФЗ, определяющий условия банкротства и регламент действий и процедур в отношении должника.

Ответственность за нарушение норм защиты персональных данных

В соответствии с Трудовым кодексом РФ работодатель обязан соблюдать следующие требования при работе с персональными данными.

В соответствии со статьей 13.11 КоАП нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

В УК РФ уголовная ответственность в отношении ПДР дана в ст. 137 «Нарушение неприкосновенности частной жизни»: штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати 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.

То же преступление, совершенное лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Вопросы и задания:

1. Назовите основные источники права в области защиты персональных данных.
2. Какие сведения являются предметом личной и семейной тайны?
3. Что понимается под обработкой персональных данных?
4. Поясните понятие «трансграничная передача персональных данных».
5. Перечислите принципы обработки персональных данных.
6. Какие требования необходимо выполнить при работе с персональными данными работника?

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по установке «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы

организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №8

Правовое обеспечение защиты интеллектуальной собственности

Цель работы: ознакомиться с правовым обеспечением защиты интеллектуальной собственности

Формируемые компетенции или их части: ПК-1

Теоретическая часть

Понятие интеллектуальной собственности (ИС) используется с момента создания 14 июля 1967 года Всемирной организации интеллектуальной собственности (ВОИС), но в советском законодательстве этот термин появился впервые в Законе СССР «О собственности

в

СССР»

(6 марта 1990 года), а в российском был утвержден в декабре 1993 года – с принятием Конституции РФ и с принятием первой части Гражданского кодекса РФ.

Наряду с упоминанием в ГК РФ был принят ряд законов:

- «Патентный закон Российской Федерации» от 23 сентября 1992 года № 3517-1;
- «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23 сентября 1992 года № 3520-1;
- «О правовой охране топологий интегральных микросхем» от 23 сентября 1992 № 3526-1;
- «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 № 3523-1;
- «Об авторском праве и смежных правах» от 9 июля 1993 года № 5351-1.

К настоящему времени в Российской Федерации в отношении ИС действует четвертая часть Гражданского кодекса РФ от 18 декабря 2006 г., вступившего в силу с 1 января 2008 г. В Федеральном законе «О введении в действие части четвертой Гражданского кодекса Российской Федерации» от 18 декабря 2006 г. в ст. 2 приведен перечень нормативно-правовых актов, утративших силу с 1 января 2008 г., среди которых были и перечисленные выше законы. Нормы Гражданского кодекса РФ (в дальнейшем – ГК) образуют в своей совокупности особую подотрасль российского гражданского права – право интеллектуальной собственности. С учетом общности ряда объектов интеллектуальной собственности указанная подотрасль российского гражданского права обычно подразделяется на четыре относительно самостоятельных института. Несмотря на тесную взаимосвязь и наличие целого ряда общих моментов, каждый из этих институтов имеет присущие лишь ему черты, которые находят отражение в нормах российского законодательства.

Прежде всего выделяется *институт авторского права и прав, смежных с авторским*. Им регулируются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного и кабельного вещания (смежные права). Объединение в едином институте, который в дальнейшем для краткости будет именоваться авторским правом, двух указанных групп норм объясняется теснейшей зависимостью возникновения и осуществления смежных прав от прав авторов творческих произведений, а также регулирование соответствующих отношений единым законом.

Другим правовым институтом, входящим в систему подотрасли «право интеллектуальной собственности», является *патентное право*. Оно регулирует имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием и использованием изобретений, полезных моделей и промышленных образцов.

С развитием товарно-денежных отношений в России все более важным элементом рыночной экономики становятся такие объекты промышленной собственности, как фирменные наименования, товарные знаки, знаки обслуживания и наименования мест происхождения товаров. Создание равных условий хозяйствования для всех товаровладельцев, внедрение конкурентных начал в их деятельность и повышение ответственности за ее результаты, необходимость насыщения рынка товарами и услугами для удовлетворения потребностей населения обуславливают объективную потребность в правовом механизме, обеспечивающем должную индивидуализацию предприятий и организаций, а также производимых ими товаров и услуг. Такой правовой механизм представлен особым институтом рассматриваемой подотрасли гражданского права, а именно *институтом средств индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг)*. Данный правовой институт, как и патентное право, имеет дело с так называемой промышленной собственностью, то есть с исключительными правами, реализуемыми в сфере производства, торгового обращения, оказания услуг и т. п. Основной функцией рассматриваемого института интеллектуальной собственности является обеспечение должной индивидуализации производителей и их товаров, работ и услуг.

Творения, признаваемые произведениями науки, литературы или искусства, а также изобретениями, полезными моделями и промышленными образцами, не исчерпывают всего многообразия результатов творческой деятельности. Наряду с ними имеется немало объектов, которые создаются творческими усилиями людей, представляют ценность для общества и также нуждаются в общественном признании и правовой охране. Помимо традиционных объектов, охраняемых авторским и патентным правом, а также институтом средств индивидуализации участников гражданского оборота, российское гражданское право предоставляет охрану селекционным достижениям, топологиям интегральных микросхем, информации, составляющей служебную и коммерческую тайну, и некоторым другим результатам интеллектуальной деятельности. Опираясь на отличия указанных результатов интеллектуальной деятельности от традиционных объектов интеллектуальной собственности, все их можно условно отнести к сфере единого правового института, а именно *института охраны нетрадиционных объектов интеллектуальной собственности*.

Современное российское законодательство об ИС подразделяется на пять основных частей:

- авторское право;
- охрана смежных прав;
- патентное право;
- законодательство о средствах индивидуализации участников гражданского оборота, товаров и услуг;
- законодательство о нетрадиционных объектах ИС (научные открытия, рацпредложения, ноу-хау);
- законодательство о защите против недобросовестной конкуренции.

Каждый из этих институтов имеет свои особенности. Рассмотрим основные из них при краткой характеристике каждого по структуре: источники права; объекты и субъекты права; основные права субъектов; способы их охраны и защиты.

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

Свойство информационного продукта, такое как трудность производства и

относительная простота тиражирования создает немало проблем в связи с определением прав собственности в области информационной деятельности.

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

Под **интеллектуальной собственностью** понимаются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

Конкретизация понятия интеллектуальная собственность дана в Конвенции, учреждающей Всемирную организацию интеллектуальной собственности (ВОИС). Конвенция была принята на Стокгольмской конференции в 1967 году и ратифицирована в 1968 году СССР.

Правовая охрана интеллектуальной собственности

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

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

Смежные права – это права, примыкающие к авторскому праву, они защищают исполнителей (актеров, певцов, танцоров и т. д.); производителей фонограмм; организации эфирного и кабельного вещания.

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

Коммерческая тайна – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. К информации, составляющей КТ, относят сведения, которые называют «ноу-хау».

Ноу-хау – не являющиеся общеизвестными и практически применяемые в производственной и хозяйственной деятельности: различного рода технические знания и опыт, включая методы, способы и навыки; разработки и использования технологических процессов; методы и способы лечения и т. п.

Объекты патентного права

Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным настоящим кодексом требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере художественного конструирования, отвечающие установленным ГК РФ требованиям к промышленным образцам. На изобретения, содержащие сведения, составляющие государственную тайну (секретные изобретения), положения ГК РФ распространяются, если иное не предусмотрено специальными правилами статей 1401–1405 ГК РФ и изданными в соответствии с ними иными правовыми актами. Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана в соответствии с настоящим кодексом не предоставляется.

Не могут быть объектами патентных прав:

- 1) способы клонирования человека;
- 2) способы модификации генетической целостности клеток зародышевой линии человека;
- 3) использование человеческих эмбрионов в промышленных и коммерческих целях;

4) иные решения, противоречащие общественным интересам, принципам гуманности и морали.

В качестве **изобретения** охраняется техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств). Изобретению предоставляется правовая охрана, если оно является:

- новым – оно не известно из уровня техники
- имеет изобретательский уровень – если для специалиста оно не следует из уровня техники явным образом.
- промышленно применимо – если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

При установлении новизны изобретения в уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патентов на изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо и запатентованные в Российской Федерации изобретения и полезные модели.

Раскрытие информации, относящейся к изобретению, автором изобретения, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности изобретения стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности изобретения, при условии, что заявка на выдачу патента на изобретение подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности изобретения, имели место, лежит на заявителе.

Не являются изобретениями:

- 1) открытия;
- 2) научные теории и математические методы;
- 3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;
- 4) правила и методы игр, интеллектуальной или хозяйственной деятельности;
- 5) программы для ЭВМ;
- 6) решения, заключающиеся только в представлении информации.

В соответствии с ГК РФ исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

Не предоставляется правовая охрана в качестве изобретения:

- 1) сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами;
- 2) топологиям интегральных микросхем.

В качестве **полезной модели** охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой (если совокупность ее существенных признаков не известна из уровня техники) и промышленно применимой (если она может быть использована в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере).

Уровень техники включает опубликованные в мире сведения о средствах того же

назначения, что и заявленная полезная модель, и сведения об их применении в Российской Федерации, если такие сведения стали общедоступными до даты приоритета полезной модели. В уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патента на изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения и полезные модели.

Раскрытие информации, относящейся к полезной модели, автором полезной модели, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности полезной модели стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности полезной модели, при условии, что заявка на выдачу патента на полезную модель подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности полезной модели, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве полезной модели:

- 1) решениям, касающимся только внешнего вида изделий и направленным на удовлетворение эстетических потребностей;
- 2) топологиям интегральных микросхем.

В качестве **промышленного образца** охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным. К существенным признакам промышленного образца относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида изделия, в частности, форма, конфигурация, орнамент и сочетание цветов.

Промышленный образец является новым, если совокупность его существенных признаков, нашедших отражение на изображениях изделия и приведенных в перечне существенных признаков промышленного образца (пункт 2 статьи 1377), не известна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца. При установлении новизны промышленного образца также учитываются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на промышленные образцы, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации промышленные образцы.

Промышленный образец является оригинальным, если его существенные признаки обусловлены творческим характером особенностей изделия.

Раскрытие информации, относящейся к промышленному образцу, автором промышленного образца, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности промышленного образца стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности промышленного образца, при условии, что заявка на выдачу патента на промышленный образец подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности промышленного образца, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве промышленного образца:

- 1) решениям, обусловленным исключительно технической функцией изделия;

2) объектам архитектуры (кроме малых архитектурных форм), промышленным, гидротехническим и другим стационарным сооружениям;

3) объектам неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ.

Субъекты патентного права

К основным субъектам патентного права относятся авторы (изобретения, полезной модели, промышленного образца), патентообладатели, их правопреемники, патентное ведомство, патентные поверенные.

Автор – любое физическое лицо, творческим трудом которого созданы изобретение, полезная модель, промышленный образец, селекционное достижение.

За лиц до 14 лет права осуществляют их законные представители (родители, опекуны).

Не признаются авторами физические лица, не внесшие личного творческого вклада в создание объекта промышленной собственности, оказавшие автору только техническую, организационную или материальную помощь, либо только способствовавшие оформлению прав на его использование.

Патентообладатель – лицо, владеющее патентом на изобретение, промышленный образец, свидетельством на полезную модель, селекционное достижение и вытекающими из патента (свидетельства) исключительными правами на использование указанных объектов.

Патентообладателями могут быть:

- авторы изобретения, полезной модели, промышленного образца, селекционного достижения; их наследники или иные правопреемники;

- физические и юридические лица (при условии их согласия), указанные автором или его правопреемником в заявлении, поданном в Патентное ведомство до момента регистрации изобретения, полезной модели, промышленного образца;

- работодатели – в отношении объектов промышленной собственности, созданных работником в связи с выполнением служебного задания, с выплатой последнему вознаграждения в размере и на условиях специального соглашения между ними.

Наследники – могут быть по закону и по завещанию. Если умерший патентообладатель не оставил завещания и не имел законных наследников, то в качестве наследника, в отличие от авторского права, выступает государство в лице Федерального фонда изобретений России.

Патентное ведомство – федеральный орган исполнительной власти, обеспечивающий формирование и осуществление единой государственной политики в области правовой охраны промышленной собственности.

На Патентное ведомство возложены также задачи приема и рассмотрения заявок на изобретения, полезные модели и промышленные образцы; проведения экспертизы по заявкам; государственной регистрации; выдачи патентов; публикации официальных сведений; издания патентных правил и разъяснений по применению Патентного закона и др.

Патентные поверенные – граждане РФ, имеющие в соответствии с законом право на представительство физических и юридических лиц перед Роспатентом и организациями, входящими в единую патентную службу.

В качестве патентного поверенного может быть аттестован (проверка документов и квалификационный экзамен) и зарегистрирован в Роспатенте (на основании личного заявления) гражданин РФ, имеющий постоянное место жительства в РФ, высшее образование и не менее четырех лет практической работы в этой сфере. Полномочия поверенных на ведение дел подтверждаются доверенностью.

Порядок получения патента

Заявка на выдачу патента на изобретение, полезную модель или промышленный

образец подается в федеральный орган исполнительной власти по интеллектуальной собственности лицом, обладающим правом на получение патента в соответствии с настоящим кодексом (заявителем).

Заявление о выдаче патента на изобретение, полезную модель или промышленный образец представляется на русском языке. Прочие документы заявки представляются на русском или другом языке. Если документы заявки представлены на другом языке, к заявке прилагается их перевод на русский язык.

Заявление о выдаче патента на изобретение, полезную модель или промышленный образец подписывается заявителем, а в случае подачи заявки через патентного поверенного или иного представителя – заявителем или его представителем, подающим заявку.

Требования к документам заявки на выдачу патента на изобретение, полезную модель или промышленный образец устанавливаются на основании 4 части ГК РФ федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности.

К заявке на выдачу патента на изобретение, полезную модель или промышленный образец прилагается документ, подтверждающий уплату патентной пошлины в установленном размере, или документ, подтверждающий основания освобождения от уплаты патентной пошлины, либо уменьшения ее размера, либо отсрочки ее уплаты.

Заявка на выдачу патента на изобретение (заявка на изобретение) должна относиться к одному изобретению или к группе изобретений, связанных между собой настолько, что они образуют единый изобретательский замысел (требование единства изобретения).

Заявка на изобретение должна содержать:

- 1) заявление о выдаче патента с указанием автора изобретения и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;
- 2) описание изобретения, раскрывающее его с полнотой, достаточной для осуществления;
- 3) формулу изобретения, выражающую его сущность и полностью основанную на его описании;
- 4) чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
- 5) реферат.

Датой подачи заявки на изобретение считается дата поступления в федеральный орган исполнительной власти по интеллектуальной собственности заявки, содержащей заявление о выдаче патента, описание изобретения и чертежи, если в описании на них имеется ссылка, а если указанные документы представлены не одновременно, – дата поступления последнего из документов.

Правовая охрана патентных прав

Правовая охрана на объекты промышленной собственности начинается с даты поступления заявки в Патентное ведомство и подтверждается патентом на изобретение, промышленный образец или свидетельством на полезную модель.

Заявка на выдачу патента подается автором, работодателем или их правопреемником в Патентное ведомство и должна содержать в себе:

- заявление о выдаче патента;
- описание разработки;
- формулу изобретения, полезной модели;
- чертежи, необходимые для понимания сущности разработки;
- реферат;
- комплект фотографий, макет или рисунок об общем виде изделия.

Заявитель имеет право внести исправления и уточнения в материалы заявки без

изменения сущности разработки до принятия решения о выдаче патента. Если изменения были внесены по инициативе заявителя в течение двух месяцев со дня подачи заявки, патентная пошлина за внесение изменений не взимается.

После проведения экспертизы заявки Патентное ведомство при положительном результате устанавливает приоритет разработки и принимает решение о выдаче патента, по истечении 18 месяцев с даты поступления заявки публикует сведения о заявке, публикует в официальном бюллетене сведения о выдаче патента, одновременно внося разработку в соответствующий Государственный реестр, выдает патент лицу, на имя которого он испрашивался.

В патентном праве различают:

- 1) личные неимущественные права автора изобретения (право на авторство, право на имя, право на вознаграждение);
- 2) право на получение патента
- 3) исключительные (имущественные) права патентообладателя на использование разработок по своему усмотрению;
- 4) права патентообладателя по распоряжению патентом (уступка прав, выдача разрешения на использование запатентованных разработок).

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Имущественные (исключительные) права патентообладателя действуют с даты поступления заявки в Патентное ведомство в течение срока действия патента (на изобретение – 20 лет, на полезную модель – 10 лет, на промышленный образец – 15 лет) и могут быть продлены. За поддержание патента и его продление патентообладатель обязан платить пошлины.

При признании патента полностью недействительным, при неуплате в установленный срок пошлины либо на основании заявления патентообладателя, действие патента прекращается досрочно.

Правовая охрана в соответствии с Патентным законом не предоставляется секретным изобретениям, полезным моделям, промышленным образцам. Порядок обращения с такими разработками регулируется специальным законодательством.

Защита патентных прав

Так же, как и в авторском праве, различают две основные формы защиты:

1. Неюрисдикционная – самозащита гражданами и организациями своих прав. Применяется редко.

2. Юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов авторов и патентообладателей в общем судебном порядке (через суды) и административном порядке (через Апелляционную палату Патентного ведомства и Высшую патентную палату).

В судебном порядке рассматриваются следующие споры:

- об авторстве на изобретение, полезную модель, промышленный образец;
- об установлении патентообладателя;
- о нарушении исключительного права на использование охраняемого объекта промышленной собственности и других имущественных прав патентообладателя;
- о заключении и исполнении лицензионных договоров на использование охраняемого объекта промышленной собственности;
- о выплате вознаграждения автору работодателем;
- о выплате компенсаций, предусмотренных Патентным законом.

Обязанность доказывания факта нарушения патента возлагается на патентообладателя.

В судебном порядке различают гражданско-правовые и уголовно-правовые способы защиты прав и законных интересов патентообладателей.

К основным способам гражданско-правовой защиты прав авторов и патентных прав относятся права требовать возмещение убытков виновными нарушителями.

Основным средством уголовно-правовой защиты является жалоба потерпевшего. Уголовная ответственность может наступить лишь в случае причинения крупного ущерба при незаконном использовании изобретения, полезной модели или промышленного образца, разглашения до официальной публикации без согласия автора или заявителя их сущности, присвоения авторства или принуждения к соавторству, и наказывается штрафом либо лишением свободы на срок до двух лет.

Общие положения об авторских и смежных правах

Источники авторского права

Основным источником авторского права РФ является четвертая часть Гражданского кодекса РФ, а также подзаконные нормативные акты – постановления Правительства РФ, ведомственные нормативно-правовые акты, судебная практика, международные договоры и соглашения: Бернская конференция (1971 г.) об охране литературных и художественных произведений, Всемирная конвенция (1952 г.) об авторском праве, Римская конвенция (1961 г.) об охране прав артистов-исполнителей, изготовителей фонограмм и вещательных организаций и др.

Объекты авторского права

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:

- литературные произведения;
- драматические и музыкально-драматические произведения, сценарные произведения;
- хореографические произведения и пантомимы;
- музыкальные произведения с текстом или без текста;
- аудиовизуальные произведения;
- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
- произведения декоративно-прикладного и сценографического искусства;
- произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;
- фотографические произведения и произведения, полученные способами, аналогичными фотографии;
- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;
- другие произведения.

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

Кроме того, к объектам авторских прав относятся производные произведения, то есть произведения, представляющие собой переработку другого произведения, и составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 ГК РФ.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования. Не являются объектами авторских прав:

1) официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;

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

3) произведения народного творчества (фольклор), не имеющие конкретных авторов;

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

Авторские права распространяются на часть произведения, на его название, на персонаж произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора.

Объектами смежных прав являются:

1) исполнения артистов-исполнителей и дирижеров, постановки режиссеров-постановщиков спектаклей (исполнения), если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств;

2) фонограммы, то есть любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;

3) сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;

4) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

5) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений.

Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей. Предоставление на территории Российской Федерации охраны объектам смежных прав в соответствии с международными договорами Российской Федерации осуществляется в отношении исполнений, фонограмм, сообщений передач организаций эфирного или кабельного вещания, не перешедших в общественное достояние в стране их происхождения вследствие истечения установленного в такой стране срока действия исключительного права на эти объекты и не перешедших в общественное достояние в Российской Федерации вследствие истечения предусмотренного настоящим кодексом срока действия исключительного права.

Субъекты авторского права

К субъектам авторского права относятся:

- авторы (в том числе соавторы);
- наследники и иные правопреемники;
- организации, управляющие имущественными правами авторов на коллективной основе.

Субъектами смежных прав являются исполнители, производители фонограмм, организации эфирного или кабельного вещания.

Автор – это любое физическое лицо, независимо от возраста, гражданства и состояния дееспособности, творческим трудом которого создано произведение. Если произведение (в том числе программа для ЭВМ, база данных, топология) создано совместным творческим трудом двух и более физических лиц, каждое из этих лиц

признается автором (соавтором).

Наследниками по закону являются только граждане (согласно очередности), а наследниками по завещанию – физические и юридические лица. Если умерший автор не оставил завещания и не имел законных наследников, то его авторские права прекращаются.

Организации, управляющие имущественными правами авторов и обладателей смежных прав на коллективной основе, создаются непосредственно обладателями авторских и смежных прав, действуют на основании устава и выполняют три основных функции: предоставление лицензий пользователям на соответствующие способы использования авторских произведений и объектов смежных прав, сбор вознаграждения за их использование и распределение этого вознаграждения обладателям авторских и смежных прав.

Правовая охрана прав автора и смежных прав

Авторское право на произведение возникает в силу факта его создания, для своего осуществления не требует регистрации произведения, иного специального оформления или соблюдения каких-либо формальностей и носит исключительный характер.

Автору в отношении его произведения принадлежат личные неимущественные права и имущественные (исключительные) права.

Личные неимущественные права принадлежат автору независимо от его имущественных прав, сохраняются за ним в случае уступки (передачи) исключительных прав на использование произведения и включают в себя следующие основные права:

- 1) право авторства – право признаваться автором произведения;
- 2) право автора на имя – право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом или анонимно;
- 3) право на неприкосновенность произведения – не допускается без согласия автора внесение в его произведение изменений, сокращений и дополнений, снабжение произведения при его использовании иллюстрациями, предисловием, послесловием, комментариями или какими бы то ни было пояснениями;
- 4) право на обнародование – право обнародовать или разрешать обнародовать произведение в любой форме, включая право на отзыв. Право на отзыв реализуется с возмещением возможных убытков за счет автора.

Права на авторство, на имя, на защиту являются неотчуждаемыми и охраняются бессрочно.

Имущественные права – это исключительные права на использование произведений в любой форме и любым способом, которые включают в себя следующие права:

- 1) воспроизведение произведения, то есть изготовление одного и более экземпляра произведения или его части в любой материальной форме, в том числе в форме звуко- или видеозаписи, изготовление в трех измерениях одного и более экземпляра двухмерного произведения и в двух измерениях одного и более экземпляра трехмерного произведения. При этом запись произведения на электронном носителе, в том числе запись в память ЭВМ, также считается воспроизведением, кроме случая, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование записи или правомерное доведение произведения до всеобщего сведения;
- 2) распространение произведения путем продажи или иного отчуждения его оригинала или экземпляров;
- 3) публичный показ произведения, то есть любая демонстрация оригинала или экземпляра произведения непосредственно либо на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация отдельных кадров аудиовизуального произведения без соблюдения их последовательности непосредственно либо с помощью технических средств в месте,

открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его демонстрации или в другом месте одновременно с демонстрацией произведения;

4) импорт оригинала или экземпляров произведения в целях распространения;

5) прокат оригинала или экземпляра произведения;

6) публичное исполнение произведения, то есть представление произведения в живом исполнении или с помощью технических средств (радио, телевидения и иных технических средств), а также показ аудиовизуального произведения (с сопровождением или без сопровождения звуком) в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его представления или показа либо в другом месте одновременно с представлением или показом произведения;

7) сообщение в эфир, то есть сообщение произведения для всеобщего сведения (включая показ или исполнение) по радио или телевидению (в том числе путем ретрансляции), за исключением сообщения по кабелю. При этом под сообщением понимается любое действие, посредством которого произведение становится доступным для слухового и (или) зрительного восприятия независимо от его фактического восприятия публикой. При сообщении произведений в эфир через спутник под сообщением в эфир понимается прием сигналов с наземной станции на спутник и передача сигналов со спутника, посредством которых произведение может быть доведено до всеобщего сведения независимо от его фактического приема публикой. Сообщение кодированных сигналов признается сообщением в эфир, если средства декодирования предоставляются неограниченному кругу лиц организацией эфирного вещания или с ее согласия;

8) сообщение по кабелю, то есть сообщение произведения для всеобщего сведения по радио или телевидению с помощью кабеля, провода, оптического волокна или аналогичных средств (в том числе путем ретрансляции). Сообщение кодированных сигналов признается сообщением по кабелю, если средства декодирования предоставляются неограниченному кругу лиц организацией кабельного вещания или с ее согласия;

9) перевод или другая переработка произведения. При этом под переработкой произведения понимается создание производного произведения (обработки, экранизации, аранжировки, инсценировки и тому подобного). Под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя;

10) практическая реализация архитектурного, дизайнерского, градостроительного или садово-паркового проекта;

11) доведение произведения до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору (доведение до всеобщего сведения).

Имущественные права автора могут быть ограничены случаями свободного использования:

1. Свободное воспроизведение произведения в личных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, за исключением:

– воспроизведения произведений архитектуры в форме зданий и аналогичных

сооружений;

- воспроизведения баз данных или их существенных частей;
- воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса;
- репродуцирования (пункт 2 статьи 1275) книг (полностью) и нотных текстов;
- видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;
- воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.

2. Свободное использование произведения в информационных, научных, учебных или культурных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования:

- цитирование в оригинале и в переводе в научных, полемических, критических или информационных целях правомерно обнародованных произведений в объеме, оправданном целью цитирования, включая воспроизведение отрывков из газетных и журнальных статей в форме обзоров печати;
- использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, радио- и телепередачах, звуко- и видеозаписях учебного характера в объеме, оправданном поставленной целью;
- воспроизведение в прессе, сообщение в эфир или по кабелю правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам или переданных в эфир произведений такого же характера в случаях, когда такое воспроизведение или сообщение не было специально запрещено автором или иным правообладателем;
- воспроизведение в прессе, сообщение в эфир или по кабелю публично произнесенных политических речей, обращений, докладов и других аналогичных произведений в объеме, оправданном информационной целью. При этом за авторами таких произведений сохраняется право на их опубликование в сборниках;
- воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, кинематографии, путем сообщения в эфир или по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий, в объеме, оправданном информационной целью;
- воспроизведение без извлечения прибыли рельефно-точечным шрифтом или другими специальными способами для слепых правомерно опубликованных произведений, кроме произведений, специально созданных для воспроизведения такими способами.

В случае, когда библиотека предоставляет экземпляры произведений, правомерно введенные в гражданский оборот, во временное безвозмездное пользование, такое пользование допускается без согласия автора или иного правообладателя и без выплаты вознаграждения. При этом выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, в том числе в порядке взаимного использования библиотечных ресурсов, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Создание произведения в жанре литературной, музыкальной или иной пародии либо в жанре карикатуры на основе другого (оригинального) правомерно обнародованного произведения и использование этой пародии либо карикатуры допускаются без согласия автора или иного обладателя исключительного права на оригинальное произведение и без выплаты ему вознаграждения.

3. Свободное использование произведения путем репродуцирования. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования репродуцирования в единственном экземпляре без извлечения прибыли:

- правомерно опубликованного произведения библиотеками и архивами для восстановления, замены утраченных или испорченных экземпляров произведения и для предоставления экземпляров произведения другим библиотекам, утратившим их по каким-либо причинам из своих фондов;

- отдельных статей и малообъемных произведений, правомерно опубликованных в сборниках, газетах и других периодических изданиях, коротких отрывков из правомерно опубликованных письменных произведений (с иллюстрациями или без иллюстраций) библиотеками и архивами по запросам граждан для использования в учебных или научных целях, а также образовательными учреждениями для аудиторных занятий.

Под репродуцированием (репрографическим воспроизведением) понимается факсимильное воспроизведение произведения с помощью любых технических средств, осуществляемое не в целях издания. Репродуцирование не включает воспроизведение произведения или хранение его копий в электронной (в том числе в цифровой), оптической или иной машиночитаемой форме, кроме случаев создания с помощью технических средств временных копий, предназначенных для осуществления репродуцирования.

4. Свободное использование произведения, постоянно находящегося в месте, открытом для свободного посещения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение, сообщение в эфир или по кабелю фотографического произведения, произведения архитектуры или произведения изобразительного искусства, которые постоянно находятся в месте, открытом для свободного посещения, за исключением случаев, когда изображение произведения таким способом является основным объектом этого воспроизведения, сообщения в эфир или по кабелю либо когда изображение произведения используется в коммерческих целях.

5. Свободное публичное исполнение музыкального произведения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения публичное исполнение музыкального произведения во время официальной или религиозной церемонии либо похорон в объеме, оправданном характером такой церемонии.

6. Свободное воспроизведение произведения для целей правоприменения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью.

7. Свободная запись произведения организацией эфирного вещания в целях краткосрочного пользования. Организация эфирного вещания вправе без согласия автора или иного правообладателя и без выплаты дополнительного вознаграждения делать запись в целях краткосрочного пользования того произведения, в отношении которого эта организация получила право на сообщение в эфир, при условии, что такая запись делается организацией эфирного вещания с помощью ее собственного оборудования и для собственных передач. При этом организация обязана уничтожить такую запись в течение шести месяцев со дня ее изготовления, если более продолжительный срок не согласован с правообладателем или не установлен законом. Такая запись может быть сохранена без согласия правообладателя в государственных или муниципальных архивах, если она носит исключительно документальный характер.

8. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного

вознаграждения:

- внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программ или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;

- изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные выше, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных предыдущим подпунктом.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

По общему правилу авторское право действует в течение всей жизни автора и 70 лет после его смерти, начиная с 1 января года, следующего после смерти.

Имущественные права передаются по договору. Имущественные права на использование служебного произведения принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное.

Правообладатель для оповещения о своих авторских правах на каждом экземпляре произведения вправе использовать знак охраны авторского права, состоящий из трех элементов: буквы «С» в окружности или в круглых скобках (С); имени правообладателя, года первого опубликования (выпуска в свет) произведения; для оповещения о смежных правах на фонограмму – указывать знак охраны в виде прописной буквы «Р», информации о самом правообладателе, года первого наименования фонограммы.

Исполнители (артисты, режиссеры, дирижеры) имеют как личные

преимущественные, так и имущественные права при условии соблюдения ими прав автора исполняемого произведения, остальные объекты – только имущественные права.

Имущественные права обладателей смежных прав обеспечиваются их исключительным правом на использование исполнения, постановки, фонограммы, передачи в любой форме, в том числе право на вознаграждение за каждый вид использования исполнения, постановки, фонограммы, представления разрешения на использование передачи.

Защита авторских и смежных прав

Под защитой понимается совокупность мер, предусмотренных законом, по признанию, восстановлению прав и законных интересов их обладателей при нарушении или оспаривании этих прав и интересов.

Различают две основные формы защиты:

1) неюрисдикционная – самозащита гражданами и организациями своих прав и законных интересов в порядке необходимой обороны и крайней необходимости (отказ совершить определенные действия; отказ от исполнения договора в целом и т. п.). Применяется редко;

2) юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов их обладателей в судебном порядке или административном порядке.

Основным средством защиты в судебном порядке является иск, а в административном порядке – жалоба.

В судебном порядке различают по способам защиты прав и ответственности гражданско-правовые, административные и уголовно-правовые.

К основным способам гражданско-правовой защиты исключительных прав и законных интересов относится право требовать от нарушителя:

- признания прав;
- восстановления положения, существовавшего до нарушения права;
- прекращения действий, нарушающих право или создающих угрозу его нарушению (запрет на воспроизведение, на выпуск в свет, на распространение и т. п.);
- возмещение убытков;
- взыскания дохода, полученного нарушителем вследствие нарушения прав;
- выплаты компенсации в определенных законом пределах;
- возмещения морального ущерба;
- прекращения или изменения договора в связи с действиями нарушителя;
- запрет совершать определенные действия ответчику (изготовление, воспроизведение, продажу, прокат и др.).

В случае наступления административной ответственности применяются:

- взыскание штрафа;
- обязательная конфискация по решению суда контрафактных (изготовленных или используемых с нарушением авторских прав) экземпляров произведений или фонограмм либо материалов и оборудования, используемых для их изготовления.

Вопросы и задания:

1. Перечислите основные законодательные акты, регламентирующие защиту интеллектуальной собственности.
2. Какие существуют институты защиты интеллектуальной собственности?
3. Перечислите и охарактеризуйте основные объекты интеллектуальной собственности.
4. Дайте определение понятиям «Изобретение», «полезная модель», «промышленный образец».
5. Назовите объекты патентного права.
6. Какие объекты патентного права не являются изобретениями?

7. Охарактеризуйте правовую основу защиты промышленного образца.
8. Перечислите и охарактеризуйте субъекты патентного права.
9. Перечислите объекты и субъекты авторского права.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №9
Документы Гостехкомиссии России.
Единые критерии, стандарты

Цель работы: ознакомиться со стандартами и критериями гостехкомиссии России.

Формируемые компетенции или их части: ПК-1

Теоретическая часть

В Российской Федерации традиционно деятельность в области обеспечения информационной безопасности делилась на техническую и криптографическую защиту информации. Контроль в области технической защиты информации осуществляла Государственная техническая комиссия (Гостехкомиссия), которая в 2004 году была преобразована в Федеральную службу по техническому и экспортному контролю при Министерстве обороны Российской Федерации (ФСТЭК). Большинство руководящих документов Гостехкомиссии было унаследовано без изменений. Несмотря на то, что данные документы разрабатывались в начале 90-х годов прошлого века, они до сих пор применяются в формальных процедурах стандартизации и сертификации систем и средств защиты информации.

Показатели защищенности СВТ от НСД

Данный руководящий документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Эти показатели содержат требования защищенности СВТ от НСД к информации и

применяются к общесистемным программным средствам и операционным системам. Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований. Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ).

Установлено семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, однако при оценке защищенность СВТ оказалась ниже уровня требований шестого класса

Требования к защищенности автоматизированных систем

Требования сгруппированы вокруг реализующих их подсистем защиты. В отличие от остальных стандартов в этом документе отсутствует раздел, содержащий требования по обеспечению работоспособности системы, зато присутствует раздел, посвященный криптографическим средствам. Другие же стандарты информационной безопасности не содержат даже упоминания о криптографии, т. к. рассматривают ее исключительно в качестве механизма защиты реализующего требования аутентификации, контроля целостности и т. д. Исключением являются только «Единые критерии», однако и в них требования раздела криптографии касаются распределения ключей, все остальное регламентируется отдельными стандартами.

Классы защищенности автоматизированных систем

Документы ГТК устанавливают девять классов защищенности АС от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации в АС. Группа определяется на основании следующих признаков:

- 1) наличие в АС информации различного уровня конфиденциальности;
- 2) уровень полномочий пользователей АС на доступ к конфиденциальной информации;
- 3) режим обработки данных в АС (коллективный или индивидуальный).

В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA , где N – номер группы (от 1 до 3). Следующий класс обозначается NB и т. д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и/или хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Таким образом, разработка руководящих документов ГТК явилась следствием бурно развивающегося в России процесса внедрения информационных технологий. До начала 90-х годов необходимости в подобных документах не было, т. к. в большинстве случаев обработка и хранение конфиденциальной информации осуществлялись без применения вычислительной техники. Поэтому разработка стандартов подобного рода представляет собой абсолютно новую и незнакомую область деятельности для соответствующих институтов и учреждений, что позволяет трактовать данные документы как первую стадию формирования отечественных стандартов в области информационной безопасности.

К недостаткам стандарта относятся уже упоминавшиеся отсутствие требований к защите от угроз работоспособности, ориентация на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Понятие «политика безопасности» трактуется исключительно как поддержание режима секретности и отсутствие НСД, что принципиально неверно. Из-за этого средства защиты ориентируются исключительно на противодействие внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется никаких требований. Ранжирование требований по классам защищенности по сравнению с остальными стандартами информационной безопасности максимально упрощено и сведено до определения наличия/отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения.

Общие сведения об «Единых критериях безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 15408

«Единые критерии безопасности информационных технологий» (CommonCriteriaforInformationTechnologySecurityEvaluation, далее просто «Единые критерии») являются результатом совместных усилий авторов «Европейских критериев безопасности информационных технологий», «Федеральных критериев безопасности информационных технологий» и «Канадских критериев безопасности компьютерных систем», направленных на объединение основных положений этих документов и создание единого международного стандарта безопасности информационных технологий. Версия 2.1 этого стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 году в качестве международного стандарта информационной безопасности ISO/IEC 15408.

Этот стандарт явился основой для принятия и введения в действие Постановлением Госстандарта России Государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Настоящий стандарт, состоящий из трех частей, также определяет критерии, за которыми в России закрепилось название «Общие критерии» (ОК).

Часть 1 стандарта включает методологию оценки безопасности ИТ, определяет виды требований безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах трех категорий пользователей: потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть 2 стандарта включает универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 стандарта включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют

предъявленным к ним функциональным требованиям. В этой же части содержатся оценочные уровни доверия, определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования комплекса средств безопасности, оценку уязвимостей продукта или системы ИТ, стойкости механизмов защиты и сделать заключение об уровне безопасности объекта оценки.

Поскольку ГОСТ Р ИСО/МЭК 15408 полностью соответствует международному стандарту ИСО/МЭК 15408, рассмотрим и охарактеризуем международные «Единые критерии».

Международный стандарт сохраняет совместимость с существующими стандартами и развивает их путем введения новых концепций, соответствующих современному уровню развития информационных технологий и интеграции национальных информационных систем в единое мировое информационное пространство. Этот документ разработан на результатах анализа опыта применения положенных в его основу стандартов и поэтому оперирует уже знакомым по Федеральным критериям понятием «продукт информационных технологий», или ИТ-продукт, и использует предложенную в них концепцию Профиля защиты.

Для противодействия угрозам ИТ-продукты должны включать в свой состав средства защиты, противодействующие этим угрозам и направленные на устранение уязвимостей, однако ошибки в средствах защиты, в свою очередь, могут приводить к появлению новых уязвимостей. Сертификация средств защиты позволяет подтвердить их адекватность угрозам и рискам.

Характеристика основных положений «Единых критериев»

«Единые критерии» регламентируют все стадии разработки квалификационного анализа и эксплуатации ИТ-продуктов.

Задачи защиты – базовое понятие «Единых критериев», выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты – специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты – специальный нормативный документ, предоставляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. В ходе квалификационного анализа служит в качестве описания ИТ-продукта.

Для проведения квалификационного анализа разработчик продукта должен представить следующие материалы:

- 1) Профиль защиты, описывающий назначение ИТ-продукта и характеризующий среду его эксплуатации, а также устанавливающий Задачи защиты и требования, которым должен отвечать продукт;
- 2) Проект защиты, включающий спецификации средств защиты, а также обоснование соответствия ИТ-продукта задачам защиты из Профиля защиты и указанным в нем требованиям «Единых критериев»;
- 3) обоснования и подтверждения свойств и возможностей ИТ-продукта, полученные разработчиком;
- 4) сам ИТ-продукт;
- 5) дополнительные сведения, полученные путем проведения различных независимых экспертиз.

Процесс квалификационного анализа включает три стадии:

1. Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для

анализируемого продукта.

2. Анализ Проекта защиты на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе ИТ-продукта.

3. Анализ ИТ-продукта на предмет соответствия Проекту защиты.

Результатом квалификационного анализа является заключение о том, что проанализированный ИТ-продукт соответствует представленному Проекту защиты. Заключение состоит из нескольких отчетов, отличающихся уровнем детализации и содержащих мнение экспертов по квалификации об ИТ-продукте на основании критериев квалификации – «Единых критериев». Эти отчеты могут использоваться как производителями, так и потребителями ИТ-продукта.

Существо профиля защиты. Профиль защиты определяет требования безопасности к определенной категории ИТ-продуктов, не уточняя методы и средства их реализации. С помощью Профилей защиты потребители формулируют свои требования к производителям.

Рассмотрим назначение и содержание разделов Профиля защиты.

Введение содержит информацию, необходимую для поиска Профиля защиты в библиотеке профилей. Идентификатор Профиля защиты представляет собой уникальное имя, пригодное для его поиска среди подобных ему профилей и обозначения ссылок на него. Обзор содержания содержит краткую аннотацию Профиля защиты, на основании которой потребитель может сделать вывод о соответствии данного профиля его запросам.

Описание ИТ-продукта содержит его краткую характеристику, функциональное назначение, принципы работы, методы использования, и эта информация не подлежит анализу и сертификации, но предоставляется экспертам для пояснения требований безопасности и определения их соответствия задачам, решаемым с помощью ИТ-продукта, а также для понимания его структуры и принципов работы.

Среда эксплуатации – раздел, содержащий описание среды функционирования ИТ-продукта с точки зрения безопасности.

Условия эксплуатации. Описание условий эксплуатации ИТ-продукта должно содержать исчерпывающую характеристику среды его эксплуатации с точки зрения безопасности, в том числе ограничения на условия его применения.

Угрозы безопасности. Описание угроз безопасности, действующих в среде эксплуатации, которым должна противостоять защита ИТ-продукта. Для каждой угрозы должен быть указан ее источник, метод и объект воздействия.

Политика безопасности. Описание политики безопасности должно определять и при необходимости объяснять правила политики безопасности, которая должна быть реализована в ИТ-продукте.

Задачи защиты отражают потребности пользователей в противодействии указанным угрозам безопасности и/или реализации политики безопасности.

Задачи защиты ИТ-продукта отражают потребности пользователей в противодействии угрозам безопасности и/или реализации политики безопасности.

Другие задачи защиты отражают необходимость участия средств защиты ИТ-продукта в противодействии угрозам безопасности и/или реализации политики безопасности совместно с другими компонентами информационных технологий.

Требования безопасности. В этом разделе Профиля защиты содержатся требования безопасности, которым должен удовлетворять ИТ-продукт для решения задач защиты.

Раздел функциональных требований должен содержать только типовые требования, предусмотренные соответствующими разделами «Единых критериев». Необходимо обеспечить такой уровень детализации требований, который позволяет продемонстрировать их соответствие задачам защиты. Функциональные требования могут предписывать или запрещать использование конкретных методов и средств защиты.

Дополнительные сведения – необязательный раздел, содержащий любую

дополнительную информацию, которая может быть полезна для проектирования, разработки, квалификационного анализа и сертификации ИТ-продукта.

Обоснование должно демонстрировать, что Профиль защиты содержит полное и связанное множество требований, и что удовлетворяющий им ИТ-продукт будет эффективно противостоять угрозам безопасности среды эксплуатации.

Обоснование задач защиты должно демонстрировать, что задачи защиты, предложенные в профиле, соответствуют параметрам среды эксплуатации, и их решение позволит эффективно противостоять угрозам безопасности и реализовать политику безопасности. Обоснование требований безопасности показывает, что эти требования позволяют эффективно решить задачи защиты, поскольку:

- 1) совокупность целей, преследуемых отдельными функциональными требованиями, соответствует установленным задачам защиты;
- 2) требования безопасности являются согласованными, т. е. не противоречат друг другу, а наоборот, взаимно усиливают;
- 3) выбор требований является оправданным (особенно это относится к дополнительным требованиям, не содержащимся в «Единых критериях»);
- 4) выбранный набор функциональных требований и уровень требований адекватности соответствуют Задачам защиты.

Существо Проекта защиты. Проект защиты содержит требования и задачи защиты ИТ-продукта, а также описывает уровень функциональных возможностей реализованных в нем средств защиты, их обоснование и подтверждение степени их адекватности.

Обоснование Проекта защиты включает следующие разделы:

1. Обоснование задач защиты должно демонстрировать, что задачи защиты, предложенные в Проекте защиты, соответствуют свойствам среды эксплуатации, и что их решение позволит эффективно противодействовать угрозам безопасности и реализовать требуемую политику безопасности.

2. Обоснование требований безопасности показывает, что выполнение этих требований позволяет решить задачи защиты, т. к.:

- совокупность функциональных требований и требований адекватности, а также условий эксплуатации ИТ-продукта соответствуют задачам защиты;
- все требования безопасности являются непротиворечивыми и взаимно усиливают друг друга;
- выбор требований является оправданным;
- уровень функциональных возможностей средств защиты соответствует задачам защиты.

3. Обоснование общих спецификаций ИТ-продукта должно демонстрировать, что средства защиты и методы обеспечения их адекватности соответствуют предъявляемым требованиям, поскольку:

- совокупность средств защиты удовлетворяет функциональным требованиям;
- требуемый уровень безопасности и надежности защиты обеспечивается предложенными средствами;
- меры, направленные на обеспечение адекватности реализации функциональных требований, соответствуют предъявленным требованиям адекватности.

4. Обоснование соответствия Профилю защиты показывает, что требования Проекта защиты поддерживают все требования Профиля защиты. Для этого должно быть показано, что:

- все усовершенствования задач защиты, по сравнению с Профилем защиты, осуществлены корректно и в направлении их развития и конкретизации;
- все усовершенствования требований безопасности, по сравнению с Профилем защиты, осуществлены корректно и в направлении их развития и конкретизации;
- все задачи защиты Профиля защиты успешно решены и все требования

Профиля защиты удовлетворены;

– никакие дополнительно введенные в Проект защиты специальные задачи защиты и требования безопасности не противоречат Профилю защиты.

Анализ требований безопасности компонентов автоматизированных систем в рамках «Единых критериев»

«Единые критерии» разделяют требования безопасности на две категории: функциональные требования и требования адекватности.

Функциональные требования регламентируют функционирование обеспечивающих безопасность компонентов ИТ-продукта и определяют возможности средств защиты.

Адекватность представляет собой характеристику ИТ-продукта, которая показывает, насколько эффективно обеспечивается заявленный уровень безопасности, а также степень корректности реализации средств защиты. Адекватность определяется технологиями, используемыми в процессе проектирования, создания и эксплуатации ИТ-продукта. Поэтому требования адекватности регламентируют технологию и процесс создания ИТ-продукта, а также необходимость проведения анализа слабых мест защиты.

Вопросы и задания:

1. Перечислить и раскрыть сущность классов защищенности СВТ от НСД к информации.
2. Раскрыть понятие «проект защиты».
3. Перечислите стандартные уровни адекватности.
4. Что понимается под лицензированием в области защиты информации?
5. Какие сведения относятся к охраняемым?
6. Дайте определение безопасности информации.

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

Практическое занятие №10

Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию

Цель работы: ознакомиться с видами деятельности предприятий в области защиты информации, подлежащих лицензированию.

Формируемые компетенции или их части: ПК-1

Теоретическая часть

Одним из основных видов государственного контроля над предпринимательской деятельностью является лицензирование. Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока. Лицензия действительна на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей. Именно поэтому многим организациям для начала своей деятельности необходимо получить разрешение на ведение работ (лицензию). В настоящее время документом, который регулирует процесс лицензирования в России является Федеральный Закон «О лицензировании отдельных видов деятельности» от 08 августа 2001 года № 128-ФЗ.

Правила и принципы, положенные в основу деятельности государственных органов по лицензированию в области защиты информации, базируются на приведенном выше законе, а также Законе «О государственной тайне» от 21 июля 1993 года № 5485-1 и Положениях о лицензировании соответствующих видов деятельности.

Лицензирование в области защиты информации является обязательным. Это требование распространяется на все без исключения направления и отдельные виды деятельности, которые перечисляются в соответствующих нормативных актах. Деятельность в области защиты информации физических или юридических лиц, не прошедших лицензирование, запрещена.

Субъекты, не получившие права на деятельность в области защиты информации и продолжающие ее осуществлять, нарушая установленный порядок, занимаются тем самым противоправной деятельностью. В отношении таких субъектов могут быть применены санкции, предусмотренные действующим Гражданским кодексом и законодательством об административной и уголовной ответственности.

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

Обратим внимание на несколько положений данной статьи:

- лицензия выдается только на основании результатов специальной экспертизы – иными словами, проверки готовности организации к работе со сведениями, составляющими государственную тайну;
- требуется наличие в структуре организации подразделения по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации;
- требуется наличие в организации сертифицированных средств защиты информации;
- необходима государственная аттестация руководителей организации, ответственных за защиту сведений, составляющих государственную тайну.

Основные термины и их определения, используемые в Положениях о лицензировании деятельности в области защиты информации

Лицензирование в области защиты информации – деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации, оформленная лицензионным соглашением (договором).

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации, оформленное лицензионным соглашением (договором).

Лицензиат в области защиты информации – сторона, получившая право на проведение работ в области защиты информации.

Защита информации – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п.

Эффективность защиты информации – степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Безопасность информации – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п.

Охраняемые сведения – сведения, составляющие государственную и иную охраняемую законом тайны.

Аттестация объекта в защищенном исполнении – официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации.

Техническое средство обработки информации (ТСОИ) – техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

Система государственного лицензирования предприятий в области защиты информации

Система государственного лицензирования деятельности предприятий в области защиты информации является составной частью государственной системы защиты информации. Деятельность системы лицензирования организуют государственные органы по лицензированию, которыми являются Федеральная служба безопасности Российской Федерации (ФСБ России) и Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Требования к получению лицензии

Лицензия выдается подавшему заявку на ее получение предприятию-заявителю, располагающему производственной и испытательной базой, нормативной и методической документацией, научным и инженерно-техническим персоналом, при условии их соответствия требованиям государственного органа по лицензированию на основании результатов экспертизы деятельности предприятия по заявленному направлению работ. С этими требованиями заявитель имеет право ознакомиться в государственном органе по лицензированию.

Для получения лицензии представляются: заявление, а также иные документы, перечень которых определяется положением о лицензировании соответствующего вида деятельности.

Отказ в выдаче лицензии производится в случаях, если: отсутствуют необходимые условия для проведения работ по заявленному виду деятельности; профессиональная подготовка руководителя предприятия-заявителя, или лиц, уполномоченных им для руководства лицензируемой деятельностью, не соответствует установленным требованиям; в представленных для получения лицензии документах указаны недостоверные сведения; заявитель в установленном законом порядке признан виновным

в недобросовестной конкуренции в лицензируемой деятельности.

Лицензия выдается за плату, размер которой устанавливается государственными органами по лицензированию по согласованию с Министерством финансов Российской Федерации.

Положение «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»

Положение «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» устанавливает порядок лицензирования деятельности предприятий, учреждений и организаций независимо от их организационно-правовых форм по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Для получения лицензии заявитель представляет в Центр «ЛСЗ» ФСБ России (либо в территориальные органы Федеральной службы безопасности по месту расположения соискателя лицензии):

- 1) 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;
- 2) копии учредительных документов (с предъявлением оригиналов, в случае, если копии не заверены нотариусом);
- 3) копию документа, подтверждающего факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц;
- 4) копии документов, подтверждающих право собственности, право полного хозяйственного ведения и (или) договора аренды на имущество, необходимое для ведения заявленного вида деятельности;
- 5) справку о постановке на учет в налоговом органе;
- 6) документ, подтверждающий уплату государственной пошлины за рассмотрение лицензирующим органом заявления о предоставлении лицензии.

Центр «ЛСЗ» ФСБ России принимает решение о выдаче или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.

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

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

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, и при выполнении следующих условий:

- 1) 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;

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

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

Основанием для отказа в выдаче лицензии является:

- невыполнение вышеперечисленных условий;
- наличие в документах, представленных заявителем, недостоверной или искаженной информации;
- отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Лицензии выдаются на срок от 3 до 5 лет, в зависимости от специфики вида деятельности. По просьбе заявителя лицензии могут выдаваться на срок менее трех лет.

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

Положение «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»

Положение «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» определяет порядок лицензирования деятельности по разработке и (или) производству средств защиты конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

В этом Положении устанавливаются лицензионные требования и условия при осуществлении деятельности по разработке и (или) производству средств защиты конфиденциальной информации, лицензирование которой отнесено к компетенции Федеральной службы безопасности Российской Федерации.

В случае выполнения лицензионных условий и отсутствии нарушений в предоставленных документах выдается лицензия сроком на 5 лет. По окончании срок лицензии может быть продлен по заявлению лицензиата в порядке, предусмотренном для переоформления документа с приложением документов, необходимых для получения лицензии.

Положение «О лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность»

Положение «О лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность» определяет порядок лицензирования деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации (специальные средства), индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Центр «ЛСЗ» ФСБ России принимает решение о предоставлении или об отказе в предоставлении лицензии в течение 45 дней с даты получения заявления и необходимых документов.

Лицензия предоставляется на срок 5 лет, с возможностью продления по заявлению лицензиата в порядке переоформления документа, подтверждающего наличие лицензии.

Положение «О лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Положение «О лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» определяет порядок лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), осуществляемой юридическими лицами или индивидуальными предпринимателями. Это положение не распространяется на деятельность, связанную с защитой государственной тайны.

Осуществление лицензируемой деятельности с нарушением, в том числе с грубым нарушением, лицензионных требований и условий влечет за собой ответственность, установленную законодательством Российской Федерации. При этом под грубым нарушением понимается невыполнение лицензиатом требований и условий, предусмотренных подпунктами 1, 2 и 5 либо одновременное нарушение 2 и более требований.

Центр «ЛСЗ» ФСБ России проводит проверку полноты, а также достоверности сведений, содержащихся в представленных документах. В случае выявления неполноты сведений в срок, не превышающий 10 дней, соискателю лицензии направляется (вручается) уведомление о необходимости представления недостающих сведений.

Лицензия предоставляется на срок 5 лет с возможностью продления по заявлению лицензиата в порядке переоформления документа, подтверждающего наличие лицензии.

Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСТЭК России

Организационную структуру системы лицензирования ФСТЭК России образуют:

- ФСТЭК России (государственный орган по лицензированию);
- управления ФСТЭК России по федеральным округам;
- аттестационные (лицензионные) центры;
- предприятия-лицензиаты.

ФСТЭК России осуществляет следующие функции в области лицензирования:

- организует обязательное государственное лицензирование деятельности предприятий;
- выдает государственные лицензии организациям-заявителям;
- осуществляет научно-методическое руководство лицензионной деятельностью;
- аккредитует аттестационные (лицензионные) центры;
- согласовывает составы экспертных комиссий, представляемые аттестационными (лицензионными) центрами;
- осуществляет контроль за соблюдением лицензионных требований и условий;
- обеспечивает публикацию необходимых сведений о лицензионной деятельности;
- рассматривает спорные вопросы, возникающие в ходе экспертизы организаций-заявителей.

Управления ФСТЭК России по федеральным округам осуществляют следующие функции в области лицензирования:

– участвуют в работе по проведению специальных экспертиз организаций-заявителей;

– рассматривают лицензионные дела организаций-заявителей, подготовленные аттестационными (лицензионными) центрами, и выдают заключения о полноте представленного лицензионного дела;

– ведут учет и осуществляют хранение лицензионных дел;

– принимают участие в работе государственного органа по лицензированию при рассмотрении спорных вопросов, возникающих в процессе экспертизы предприятий-заявителей, и фактов некачественной работы лицензиатов.

Аттестационные (лицензионные) центры осуществляют следующие функции:

– формируют экспертные комиссии и представляют их состав на согласование в ФСТЭК России;

– планируют и проводят работы по специальной экспертизе заявителей;

– систематизируют отчеты лицензиатов и ежегодно представляют сводный отчет в государственный орган по лицензированию;

– принимают участие в работе государственного органа по лицензированию при рассмотрении спорных вопросов, возникающих в процессе экспертизы организаций-заявителей, и фактов некачественной работы лицензиатов.

На рисунке 4.16 представлены виды деятельности, подлежащие лицензированию ФСТЭК.

В обязанности предприятий-лицензиатов входит:

– осуществление своей деятельности в строгом соответствии с требованиями нормативных документов ФСТЭК России по защите информации;

– обеспечение тайны переписки, телефонных переговоров, документальных и иных сообщений физических и юридических лиц, пользующихся их услугами;

– ежегодное представление непосредственно в государственный орган по лицензированию или в лицензионный центр сведения о количестве выполненных работ по лицензионным направлениям деятельности, указанным в лицензии.

Вопросы и задания:

1. Какие средства относятся к шифровальным?
2. Перечислите функции лицензионных центров.
3. Что указывается в заявлении о выдачи лицензии?
4. На основании каких документов выдаются лицензии?
5. Какие документы требуются для получения лицензии?
6. Разработка каких шифровальных средств подлежит лицензированию?
7. Что образует организационную структуру системы лицензирования ФСТЭК России?
8. Какие функции осуществляет ФСТЭК России в области лицензирования?
9. Какие функции осуществляет аттестационные центры?

Список литературы, рекомендуемый к использованию по данной теме:

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»)
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты:

учебное пособие.- СПб.: Питер, 2008.- 272 с.

6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.

7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.

8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.