Н.В. Филиппова

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВОРОНЕЖ 2012

Воронежский институт МВД России

Н.В. Филиппова

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Учебное пособие

Воронеж
2012

ББК 67.99(2)
Ф53

Рецензенты: ведущий научный сотрудник группы по Черноземью отдела по ЦФО ФГКУ «ВНИИ МВД России» к.ю.н. А.В.Маслов; начальник центра информационных технологий, связи и защиты информации ГУ МВД России по Воронежской области А.В.Сячин.

Филиппова Н.В.

Ф53 Правовое обеспечение информационной безопасности Российской Федерации: учебное пособие. — Воронеж: Воронежский институт МВД России, 2012. — 91 с.

В учебном пособии изложены основные положения правового обеспечения информационной безопасности РФ: определены содержание организационного и правового обеспечения информационной безопасности, место информационной безопасности в системе национальной безопасности РФ, приведены основные положения законодательства в области обеспечения информационной безопасности РФ. Рассмотрены вопросы правового регулирования защиты государственной тайны, конфиденциальной информации, информационной безопасности в сфере интеллектуальной собственности, а также юридической ответственности за нарушение правовых норм в области информационной безопасности.

Учебное пособие предназначено для курсантов и студентов, а также специалистов по защите информации.

ф 2404010000-39 **16(1)-11** **ББК 67.99(2)**
221-12

ОГЛАВЛЕНИЕ

Раздел 1. Организационное и правовое обеспечение информационной безопасности Российской Федерации

Глава 1. ОСНОВЫ ОРГАНИЗАЦИОННОГО И ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятие и сущность защиты информации

В настоящее время большинство авторов в определение комплексной системы защиты информации включают три основных компонента: объект, угроза, защита[1]. *Объектом* защиты в данном случае являются информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации[2]. В связи с возможностью перехода информации из одной формы в другую, а также с многообразием видов носителей информации определить полный перечень объектов защиты практически невозможно. Обычно объекты защиты определяют по основному признаку — содержат ли они или циркулирует ли в них информация ограниченного доступа. В соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006) к объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Носитель информации — это материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин[3].

Различают следующие виды носителей информации:

[1] См.: Комплексная защита информации на предприятии: учебник для вузов / под ред. проф. Б.И. Пугинского. — М.: Издательский Дом «Городец», 2008. — 368 с.

[2] См.: Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).

[3] См. там же

- люди (обслуживающий персонал, пользователи информации и информационных ресурсов и др.; способность мозга человека познавать внешний мир, накапливать в памяти информацию, а также анализировать и перерабатывать ее с целью создания новой информации ставит человека на первое место как носителя конфиденциальной информации);

- документ (согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» 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[1]; данный термин указывает на три основных признака документа: наличие материального носителя информации; идентифицируемость зафиксированных на носителе сведений; возможность изменения форм ее закрепления, т.е. возможность копирования информации; могут быть классифицированы по ряду признаков: по видам деятельности, по происхождению, по месту возникновения, по содержанию, по гласности, по форме, по срокам хранения, в зависимости от способа воспроизведения, по стадиям создания и др.; являются наиболее информативными носителями, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде; особую ценность имеют подписанные и утвержденные документы);

- публикации (информационные носители в виде разнообразных изданий: книги, статьи, обзоры, сообщения, доклады, рекламные проспекты и т.д.; ограничивают содержание различных конференций, симпозиумов, научных семинаров и других подобных публичных форумов, где опытные специалисты собирают новую и самую ценную информацию);

- технические носители (носители любой формы, кино-, фотоматериалы, магнитные носители, видеодиски, распечатки данных и программ на принтерах и др.);

- технические средства обеспечения производственной и трудовой деятельности (телефоны, телевизоры, радиоприемники, системы

[1] См.: Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

громкоговорящей связи, усилительные системы, охранные и пожарные системы, автоматизированные системы обработки данных и др.);

- промышленные и производственные отходы (несут сведения об используемых материалах, их составе, особенностях производства, технологии).

Угроза — одно из ключевых понятий в сфере обеспечения информационной безопасности. В соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006) под *угрозой* (безопасности информации) понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Фактором, воздействующим на защищаемую информацию, считается явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней. Источником угрозы безопасности информации является субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

К наиболее важным свойствам угрозы относятся *избирательность, предсказуемость и вредоносность.* Избирательность характеризует нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности. Предсказуемость характеризует наличие признаков возникновения угрозы, позволяющих заранее прогнозировать возможность появления угрозы и определять конкретные объекты безопасности, на которые она будет направлена. Вредоносность характеризует возможность нанесения вреда различной тяжести объекту безопасности. Вред, как правило, может быть оценен стоимостью затрат на ликвидацию последствий проявления угрозы либо на предотвращение ее появления.

Необходимо выделить два наиболее важных типа угроз:

намерение нанести вред, которое появляется в виде объявленного мотива деятельности субъекта;

возможность нанесения вреда — существование достаточных для этого условий и факторов.

Особенность первого типа угроз заключается в неопределенности возможных последствий, неясности вопроса о наличии у угрожающего субъекта сил и средств; достаточных для осуществления намерения.

Возможность нанесения вреда заключается в существовании достаточных для этого условий и факторов. Особенность угроз данного типа состоит в том, что оценка потенциала совокупности факторов, которые могут послужить превращению этих возможностей и условий во вред, может быть осуществлена только собственно субъектами угроз.

Между угрозой и опасностью нанесения вреда всегда существует устойчивая причинно-следственная связь.

Угроза всегда порождает опасность. Опасность также можно представить как состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту. Главное отличие между ними заключается в том, что опасность является свойством объекта информационной безопасности и характеризует его способность противостоять проявлению угроз, а угроза — свойством объекта взаимодействия или находящихся во взаимодействии элементов объекта безопасности, выступающих в качестве источника угроз. Понятие угрозы имеет причинно-следственную связь не только с понятием опасности, но и с возможным вредом как последствием негативного изменения условий существования объекта. Возможный вред определяет величину опасности.

Под *защитой информации* понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию[1].

Более широким понятием защиты информации является комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Выделяют следующие виды защиты информации:

[1] **См.:** Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).

правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

криптографическая защита информации — защита информации с помощью ее криптографического преобразования;

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

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

Понятие «защита информации» тесно связано с понятием «информационная безопасность». Сущность защиты информации заключается в предупреждении, выявлении, обнаружении угроз, ликвидации их последствий, т.е. в обеспечении безопасности информации. Под *безопасностью информации*[1] принято считать состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность, целостность. *Информационная безопасность* — это состояние защищенности информационной среды, информационная безопасность государства — состояние защищенности его национальных интересов в инфор-

[1] См.: Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).

мационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[1].

1.2. Понятие и содержание правового обеспечения информационной безопасности

В большинстве первых отечественных работ правовые меры защиты информации принято рассматривать в рамках организационно-правового обеспечения защиты информации. Объединение организационных и правовых мер вызвано отчасти объективно сложившимися обстоятельствами:

- недостаточное количество нормативных правовых актов, регулирующих вопросы обеспечения информационной безопасности на федеральном уровне;

- преобладающее количество ведомственных нормативных документов, содержащих организационные требования по обеспечению защиты информации;

- внедрение автоматизированных информационных систем требовало соответствующего правового обеспечения их защиты, однако на практике в развитии правовой базы долгое время не происходило существенных изменений и приоритет оставался за организационными мерами.

Как следствие указанного положения дел, сложилась такая категория, как *организационно-правовое обеспечение защиты информации*, представляющее собой совокупность законов и других нормативных правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем.

В настоящее время в связи с пересмотром законодательной базы в сфере информационной безопасности и изданием новых нормативных правовых актов следует говорить именно о правовом обеспечении защиты информации как самостоятельном направлении в структуре комплексной защиты информации.

[1] См.: Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 №Пр-1895).

Правовая защита в указанной области направлена на достижение следующих *целей:*

1) формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;

2) определение мер ответственности за нарушение правил защиты информации;

3) придание юридической силы технико-математическим решениям обеспечения защиты информации;

4) придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Под *правовым обеспечением информационной безопасности* следует понимать совокупность законов и других нормативных правовых актов, регламентирующих как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем.

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.

В системе правовой защиты информации можно выделить 4 уровня.

Первый уровень правовой охраны информации и защиты состоит из международных договоров о защите информации и законов РФ.

Второй уровень правовой защиты информации — это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ.

Третий уровень — ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем, а также руководящие документы, нормы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

Четвертый уровень образуют локальные нормативные акты, инструкции, положения по информационной безопасности и документация по комплексной защите информации.

1.3. Понятие и содержание организационного обеспечения информационной безопасности

Исполнение законов и других нормативных правовых актов, регламентирующих вопросы обеспечения защиты информации, прежде всего, основано на организаторской деятельности соответствующих структур, создаваемых а государстве, ведомствах, учреждениях и организациях. Именно эта деятельность составляет содержание организационного обеспечения информационной безопасности.

Под *организационным обеспечением информационной безопасности* следует понимать совокупность специализированных органов, а также методов, сил и средств, реализующую задачи по защите информации.

Основной целью организационного обеспечения информационной безопасности является реализация на практике мер по защите информации с помощью выбранных сил и средств.

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации тесно связана с правовым и инженерно-техническим направлением защиты информации: на основе законов и иных нормативных правовых актов и с помощью инженерно-технических решений организуется защита информации. На организационном уровне решаются следующие задачи обеспечения безопасности информации:

организация работ по разработке системы защиты информации;

ограничение доступа к информации;

разграничение доступа к информации;

планирование мероприятий;

разработка документации;

воспитание и обучение обслуживающих пользователей;

сертификация средств защиты информации;

лицензирование деятельности по защите информации;

аттестация объектов защиты;

совершенствование системы защиты информации;

оценка эффективности функционирования системы защиты информации;

контроль выполнения установленных правил работы.

Применительно к защите конкретного объекта организационная защита представлена следующими *направлениями:*

- организация режима и охраны;

- организация работы с сотрудниками (подбор и расстановка персонала, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.);

- организация работы с документами и документированной информацией;

- организация использования технических средств сбора, обработки, накопления и хранения информации;

- организация работы по анализу внутренних и внешних угроз информации и выработке мер по обеспечению ее защиты;

- организация работы по проведению систематического контроля за обеспечением защиты информации.

Контрольные вопросы:

1. Что понимается под объектом защиты?
2. Перечислите основные виды носителей информации.
3. Что такое угроза?
4. Перечислите наиболее важные свойства угроз.
5. Что такое защита информации?
6. Перечислите виды защиты информации.
7. Что такое безопасность информации?
8. Что такое информационная безопасность?
9. Что такое правовое обеспечение информационной безопасности?

10. Каково содержание правового обеспечения информационной безопасности?

11. Перечислите уровни системы правовой защиты информации.

12. Что такое организационное обеспечение информационной безопасности?

13. Перечислите задачи обеспечения безопасности информации, решаемые на организационном уровне.

14. Перечислите основные направления организационной защиты конкретного объекта.

Глава 2. МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

2.1.Безопасность государства: содержание и принципы обеспечения

Основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством, определяет *Федеральный закон от 28 декабря 2010 г. М390-ФЗ «О безопасности».*

В соответствии со ст. 2 Федерального закона №390-ФЗ «О безопасности» основными *принципами* обеспечения безопасности являются:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность;

3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

4) приоритет предупредительных мер в целях обеспечения безопасности;

5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Деятельность по обеспечению безопасности включает в себя:

1) прогнозирование, выявление, анализ и оценку угроз безопасности;

2) определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;

3) правовое регулирование в области обеспечений безопасности;

4) разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;

5) применение специальных экономических мер в целях обеспечения безопасности;

6) разработку, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;

7) организацию научной деятельности в области обеспечения безопасности;

8) координацию деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;

9) финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;

10) международное сотрудничество в целях обеспечения безопасности;

11) осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федерации.

Государственная политика в области обеспечения безопасности является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер. Государственная политика в области обеспечения безопасности реализуется на основе стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, разрабатываемых Советом Безопасности и утверждаемых Президентом Российской Федерации.

2.2.Стратегия национальной безопасности Российской Федерации

Стратегия национальной безопасности Российской Федерации утверждена *Указом Президента Российской Федерации от 12 мая 2009 г. № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года".*

Стратегия национальной безопасности Российской Федерации до 2020 года — официально признанная система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу. Стратегия является базовым документом по планированию развития системы обеспечения национальной безопасности Российской Федерации, в котором излагаются порядок действий и меры по обеспечению национальной безопасности.

Стратегия включает в себя следующие *основные разделы:*

I. Общие положения.

II. Современный мир и Россия: состояние и тенденции развития.

III. Национальные интересы Российской Федерации и стратегические национальные приоритеты.

IV. Обеспечение национальной безопасности.

V. Организационные, нормативные правовые и информационные основы реализации Стратегии.

VI. Основные характеристики состояния национальной безопасности.

Основные понятия, вводимые в Стратегии:

«национальная безопасность» — состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

«угроза национальной безопасности» —прямая или косвенная возможность нанесения ущерба конституционным правам, сво-

бодам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства;

«национальные интересы Российской Федерации» — совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства.

Национальные интересы Российской Федерации заключаются:

в развитии демократии и гражданского общества, повышении конкурентоспособности национальной экономики;

в обеспечении незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации;

в превращении Российской Федерации в мировую державу, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях многополярного мира.

2.3. Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации утверждена Президентом РФ от 9 сентября 2000 г. №Пр-1895.

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

На основе Доктрины формируется государственная политика в области обеспечения информационной безопасности Российской Федерации, подготавливаются предложения по совершенствованию основных направлений обеспечения информационной безопасности, а также разрабатываются целевые программы в указанной сфере.

Доктрина включает в себя следующие *основные разделы:*

1. Информационная безопасность Российской Федерации.

II. Методы обеспечения информационной безопасности Российской Федерации.

III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации.

IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации.

В условиях технического прогресса зависимость национальной безопасности Российской Федерации от обеспечения информационной безопасности все больше возрастает.

Доктрина информационной безопасности приводит следующее определение 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, это, прежде всего реализация конституционных прав человека и гражданина:

- на доступ к информации и ее использование в интересах осуществления не запрещенной законом деятельности;

- на защиту информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере:

- обеспечение интересов личности в этой сфере;

- упрочение демократии;

- создание правового социального государства и пр.

Интересы государства в информационной сфере:

- реализация конституционных прав и свобод человека и гражданина в информационной сфере;

- незыблемость конституционного строя, суверенитета и территориальной целостности России;

- поддержание государственной стабильности;

- обеспечение законности и правопорядка и пр.

Указанные национальные интересы Российской Федерации в информационной сфере положены в основу формирования за-

дач государственной политики по обеспечению информационной безопасности.

Доктрина информационной безопасности выделяет следующие *виды угроз:*

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

- угрозы информационному обеспечению государственной политики Российской Федерации;

- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Доктрина также выделяет два вида *источников угроз* информационной безопасности Российской Федерации: внутренние и внешние.

Контрольные вопросы:

1. Перечислите основные принципы обеспечения безопасности в Российской Федерации.

2. Каково содержание деятельности по обеспечению безопасности?

3. Что представляет собой Стратегия национальной безопасности Российской Федерации?

4. Что такое национальная безопасность?

5. Что такое угроза национальной безопасности?

6. Что такое национальные интересы Российской Федерации и каково их содержание?

7. Что представляет собой Доктрина информационной безопасности?

8. Что понимается под информационной безопасностью в соответствии с Доктриной информационной безопасности Российской Федерации?

9. Каково содержание интересов личности в информационной сфере?

10. Каково содержание интересов общества в информационной сфере?

11. Каково содержание интересов государства в информационной сфере?

12. Приведите виды угроз личности, обществу и государству в соответствии с Доктриной информационной безопасности.

Раздел 2. Основы правового обеспечения информационной безопасности Российской Федерации

Глава 3. ОСНОВЫ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. Классификация и структура нормативных правовых актов в сфере обеспечения информационной безопасности

Информационные правоотношения в настоящее время выделяют в самостоятельный вид правоотношений. *Информационные правоотношения* — это отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, а также обеспечении защиты информации

Отрасль законодательства, регулирующая информационные правоотношения, получила название «информационное законодательство» и является самостоятельной в современном российском законодательстве. Информационное законодательство включает:

- законодательства об интеллектуальной собственности;
- законодательства о средствах массовой информации;
- законодательства о формировании информационных ресурсов и предоставлении информации из них;
- законодательства о реализации права на поиск, получение и использование информации;
- законодательства о создании и применении информационных технологий и средств их обеспечения;
- законодательства по защите национальных интересов государства в информационной сфере.

Рассмотрим более подробно классификацию нормативных правовых актов, в совокупности образующих законодательство. Критерием данной классификации является юридическая сила нормативного правового акта.

Нормативный правовой акт — это правовой акт, содержащий нормы права и направленный на урегулирование определенных общественных отношений.

Центральным документом в соответствии с рассматриваемой классификацией является закон. *Закон* — это нормативный правовой акт, обладающий высшей юридической силой, выражающий государственную волю по наиболее важным вопросам общественной жизни. Законы принимаются в особом порядке высшими органами власти или непосредственно народом в ходе референдума.

Различают законы: федеральные конституционные, о поправке к Конституции РФ, обычные федеральные, законы субъектов РФ.

Подзаконные акты по общему правилу не должны противоречить законам и должны приниматься во исполнение законов.

Виды подзаконных актов:

1. Акты федеральных органов представительной власти (постановления Совета Федерации по политическим вопросам).

2. Акты Президента РФ: указы, распоряжения.

3. Акты Правительства РФ (постановления, распоряжения).

4. Акты министерств и ведомств, государственных комитетов, федеральных служб, агентств и т.д. — приказы, инструкции, указания.

5. Акты органов власти и управления субъектов РФ — постановления главы администрации края, области, города. Эти акты имеют локальный характер.

6. Акты государственных и негосударственных организаций — приказ руководителя, устав общественного объединения.

На основании приведенной классификации нормативных правовых актов можно предложить следующую структуру нормативных правовых актов в области информационной безопасности:

1 -й уровень — международные правовые акты;

2-й уровень — нормативные правовые акты федерального уровня;

3-й уровень — нормативные акты субъектов Российской Федерации;

4-й уровень — нормативные акты органов местного самоуправления;

5-й уровень — нормативные документы уровня организаций, предприятий, учреждений.

Перечень основных нормативных правовых актов в области информационной безопасности

Международные правовые акты:

- «Конвенция, учреждающая Всемирную организацию интеллектуальной собственности (Стокгольм, 14 июля 1967 года, в редакции от 2 октября 1979 года. Вступила в силу для СССР 26 апреля 1970 года);

- «Всемирная конвенция об авторском праве» (Женева, 6 сентября 1952 года. Пересмотрена в Париже 24 июля 1971 года. Вступила в силу для СССР 27 мая 1973 года);

- «Брюссельская конвенция о распространении несущих программы сигналов, передаваемых через спутники. (Конвенция по спутникам)», 1974 год. Российская Федерация присоединилась 20 января 1989 года;

- «Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года». Российская Федерация присоединилась 13 марта 1995 года;

- «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». Ратифицирована Законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ;

- «Окинавская хартия глобального информационного общества». Окинава, 22 июля 2000 года;

- Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии». Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 10 декабря 2003 года;

- «Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций» (Рим, 26 октября 1961 года. Вступила в силу в Российской Федерации 26 мая 2003 года);

- «Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм» (Женева, 29 октября 1971 года; вступила в силу для Российской Федерации 13 марта 1995 года);

- «Всеобщая декларация прав человека» от 10.12. 1948;

- Соглашения в области информации, заключенные в рамках Содружества Независимых Государств:

«Соглашение о сотрудничестве в области информации» от 09.10.1992;

«Соглашение об обмене правовой информацией» от 21.10.1994;

«Соглашение о межгосударственном обмене научно-технической информацией» от 26.06.1992;

«Соглашение о взаимоотношениях министерств внутренних дел в сфере обмена информацией» от 24.04.1992.

Нормативные правовые акты федерального уровня:

- Конституция Российской Федерации от 12 декабря 1993 г.;
- Закон РФ от 27 декабря 1991 г. №2124-1 «О средствах массовой информации» (с изменениями 14 июня, 11,21 июля 2011 г.);
- Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» (в ред. от 18, 19 июля 2011 г.);
- Федеральный закон от 03.04.1995 № 40-ФЗ (ред. от 18.07.2011) «О Федеральной службе безопасности»;
- Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 28.12.2010) «Об оперативно-розыскной деятельности»;
- Федеральный закон от 10.01.1996 № 5-ФЗ (ред. от 14.02.2007) «О внешней разведке»;
- Федеральный закон Российской Федерации от 31.05.2002 № 62-ФЗ «О гражданстве Российской Федерации» (в ред. от 28.06.2009);
- Федеральный закон от 27.12.2002 № 184-ФЗ (ред. от 21.07.2011) «О техническом регулировании»;
- Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 18.07.2011) «О связи» (с изм. и доп., вступающими в силу с 29.09.2011);
- Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне»;
- Федеральный закон от 22.10.2004 № 125-ФЗ (ред. от 27.07.2010) «Об архивном деле в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных».

3.2. Конституция о правах и обязанностях граждан России в сфере обеспечения информационной безопасности

Право граждан на информацию закреплено в Конституции РФ. Это закрепление вводит законодательство России в систему международных норм.

В соответствии с п. 4 ст.29 каждому предоставлено право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Из общей системы информации выделяется государственная тайна, перечень сведений, относимых к ней, определяется федеральным законом. Также, отдельно речь идет об информации, касаемой граждан. В ст. 23 Конституции РФ среди информации о гражданах различаются личная, семейная тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. На основании судебного решения возможно ограничение права на этот вид информации.

В соответствии с*п.1 ст. 24 Конституции РФ* сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается.

Далее Конституция РФ обязывает органы государственной власти и органы местного самоуправления, их должностные лица предоставить возможность ознакомления граждан с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом *(п. 2 ст. 24 Конституции РФ).*

Ст. 41 Конституции РФ закрепляет наступление ответственности должностных лиц за сокрытие фактов и обстоятельств, создающих угрозу для жизни и здоровья людей.

Ст. 42 Конституции РФ закрепляет право на достоверную информацию об окружающей среде.

Ст. 46 Конституции РФ гарантирует свободу литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

Каждый вправе обращаться в межгосударственные органы по защите прав и свобод человека, если исчерпаны все имею-

щиеся внутригосударственные средства правовой защиты *(ст. 46),* включая случаи нарушения права на информацию.

В то же время Конституция определяет, что осуществление гражданином права на информацию не должно нарушать права и свободы других лиц РФ *(ч. 3 ст. 17).*

Контрольные вопросы:

1. Дайте определение информационным правоотношениям.
2. Раскройте содержание информационного законодательства как самостоятельной отрасли права.
3. Что понимается под законодательством в области обеспечения информационной безопасности?
4. Что такое нормативный правовой акт?
5. Приведите классификацию нормативных правовых актов по юридической силе.
6. Что такое закон и каковы его основные признаки?
7. Перечислите и опишите виды подзаконных нормативных актов.
8. Приведите структуру нормативных правовых актов в области информационной безопасности.
9. Перечислите основные международные правовые акты в области информационной безопасности.
10. Перечислите основные нормативные правовые акты федерального уровня в области информационной безопасности.
11. Перечислите основные концептуальные документы в области информационной безопасности.
12. Перечислите основные подзаконные нормативные документы в области информационной безопасности.
13. Каково содержание Конституции Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?

Глава 4. ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВООТНОШЕНИЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Объект правоотношений в сфере обеспечения информационной безопасности

Информационная сфера, или среда, — сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации.

Информационная сфера как сфера правового регулирования — совокупность субъектов права, осуществляющих такую деятельность, объектов права, по отношению к которым или в связи с которыми эта деятельность осуществляется, и социальных отношений, регулируемых правом или подлежащих правовому регулированию[1].

Основным объектом правоотношений в информационной сфере является информация.

Информация (от лат. informatio, разъяснение, изложение, осведомленность) — сведения о чем-либо независимо от формы их представления.

С.И. Ожегов дает следующее определение информации: 1) сведения об окружающем мире и протекающих в нем процессах; 2) сообщения, осведомляющие о положении дел, о состоянии чего-либо[2].

В современной науке рассматриваются два подхода к понятию информации:

Объективная (первичная) информация — свойство материальных объектов и явлений (процессов) порождать многообразие состояний, которые посредством взаимодействий (фундаментальные взаимодействия) передаются другим объектам и запечатлеваются в их структуре[3].

[1] См.: Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев [и др.]; под ред. С.Я. Казанцева. — М.: Издательский центр «Академия», 2005. — 240 с.

[2] См.: Ожегов С. И. Словарь русского языка. — М., 1990.

[3] См.: Энциклопедия кибернетики/ГлушковВ.М. [и др.]. — Киев, 1975.

Субъективная (семантическая, смысловая, вторичная) информация — смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов (слов, образов и ощущений) и зафиксированное на каком-либо материальном носителе.

При рассмотрении информации в качестве предмета правоотношений в правовой системе, предмета отношений государства, юридических и физических лиц приходится возвращаться к определению информации в его исходном смысле: под информацией понимается содержание сообщений, сведений и сигналов.

Это верно постольку, поскольку при движении информации в процессе ее создания, распространения, преобразования и потребления подавляющее большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений. Такой подход к определению понятия «информация» получил название антропоцентрический[1].

Ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее Закон «Об информации») дает следующее определение информации:

информация — сведения (сообщения, данные) независимо от формы их представления.

В соответствии со ст. 5 Закона «Об информации» информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

При рассмотрении информации как объекта правового регулирования сферы информационной безопасности необходимо уточнить понятие и сущность *правовой информации.* Правовая

[1] См.: Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев [и др.]; под ред. С.Я. Казанцева. — М.: Издательский центр «Академия», 2005. — 240 с.

информация является разновидностью информации. Ее источники: правовые нормы, институты, отрасли права, законодательство.

Существует большое количество *критериев классификации правовой информации:*

- по видам источников информации (люди, документы, публикации, технические носители, продукция, технические средства обеспечения производственной деятельности);
- роли информации в правовой системе (нормативная правовая, ненормативная правовая);
- степени доступа к информации (открытая, ограниченного доступа);
- степени официальности (официальная, неофициальная);
- организационным формам представления (документальная, архивный документ, информационные ресурсы, информационные продукты) и др.

Обеспечение безопасности информации требует сохранения следующих ее свойств:

1) целостности;
2) доступности;
3) конфиденциальности.

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

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

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

4.2. Понятие и виды защищаемой информации

В соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006) *защищаемая информация* — это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защищаемая информация имеет следующие *отличительные признаки:*

- засекречивать информацию, то есть ограничивать к ней доступ, может только ее обладатель;

- чем важнее для обладателя информация, тем тщательнее он ее защищает в соответствии с присвоенной ей степенью секретности;

- защищаемая информация должна иметь определенную ценность и приносить пользу ее обладателю, оправдывая затрачиваемые на ее защиту силы и средства.

Появление новой защищаемой информации есть результат деятельности субъекта — обладателя информацию. После создания она как бы отчуждается от субъекта-автора, самостоятельно диктуя всем, кто с нею сталкивается, правила ее использования. Уровень защиты информации определяется установленным ее автором или обладателем грифом секретности или конфиденциальности.

Созданная один раз защищаемая информация (как и несекретная) может быть использована многократно в течение неограниченного времени сколь угодно большим количеством потребителей. Она обладает способностью не уничтожаться, не убывать со временем и даже возрастать по мере использования, то есть порождать новую информацию. Свойство возрастания информации создает объективные предпосылки для ее уязвимости.

Существует и такая особенность, как распространение информации. Для открытой информации оно имеет случайный характер, тогда как распространение защищаемой информации происходит детерминированно: заранее определяется возможное количество потребителей засекреченной информации, в соответ-

ствии с которым размножается определенное количество экземпляров соответствующего документа, которые и рассылаются заранее определенным адресатам.

Классификация защищаемой информации может осуществляться по различным основаниям. Рассмотрим наиболее распространенные: по принадлежности, степени секретности и по содержанию.

По принадлежности защищаемая информация может быть классифицирована в соответствии с тем, кто является ее обладателем:

- *государство и его структуры (органы)* — они могут использовать сведения, составляющие государственную, служебную или коммерческую тайну, а также иные виды защищаемой информации, принадлежащей государству или ведомству;

- *предприятия, товарищества, акционерные общества и др.* — принадлежащая им защищаемая информация обычно составляет коммерческую тайну, но в некоторых случаях они могут использовать и сведения, составляющие государственную или служебную тайну;

- *общественные организации* — используемая ими защищаемая информация является партийной тайной, однако в некоторых случаях они могут также располагать сведениями, составляющими государственную или коммерческую тайну;

- *граждане* — их права на тайну переписки, телефонных и иных переговоров, врачебную тайну и другие конституционные права гарантируются государством.

Классификация информации *по степени секретности* (для негосударственных структур — конфиденциальности) выглядит несколько абстрактной, однако она дает возможность ранжировать защищаемую информацию по степени ее важности. Всю информацию по степени ее секретности (конфиденциальности) можно разделить на пять уровней: особой важности (особо важная), совершенно секретная (строго конфиденциальная), секретная (конфиденциальная), для служебного пользования (не для печати, рассылается по списку), несекретная (открытая).

По *содержанию* защищаемая информация может быть разделена на политическую, экономическую, военную, разведыва-

тельную и контрразведывательную, оперативно-розыскную, научно-техническую, технологическую, деловую и коммерческую.

По категории доступа информация делится на *общедоступную информацию и информацию с ограниченным доступом* (информация ограниченного доступа) (п.3 ст.5 Закона «Об информации»),

В п. 4 ст. 8. Закона «Об информации» имеется перечень сведений, к которым *не может быть ограничен доступ. К такой информации относятся:*

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

- сведения о состоянии окружающей среды;

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

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

- иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация с ограниченным доступом, в свою очередь, подразделяется на *сведения, составляющие государственную тайну,* и *конфиденциальную информацию.*

В ст. 2 Закона «Об информации» установлено, что такое свойство информации, как «конфиденциальность», обусловлено обязательным выполнением лицом, получившим к такой информации доступ, требования не передавать эту информацию третьим лицам без согласия ее обладателя.

Виды конфиденциальной информации установлены Указом Президента РФ №188 от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера», в соответствии с которым к конфиденциальной информации относятся:

- персональные данные;

- сведения, составляющие тайну следствия и судопроизводства;

- служебная тайна;

- профессиональные тайны (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- коммерческая тайна;

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие.

В настоящее время единой и четкой классификации конфиденциальной информации в литературе не существует, тем не менее, в соответствии с действующими нормативными актами названо свыше 20 разновидностей конфиденциальной информации.

Контрольные вопросы:

1. Что понимается под информационной сферой как сферой правового регулирования?

2. Приведите известные Вам понятия «информация».

3. Каковы особенности правовой информации?

4. Приведите известные Вам критерии классификации правовой информации.

5. Что означает термин «целостность информации»?

6. Что означает термин «доступность информации»?

7. Что означает термин «конфиденциальность информации»?

8. Что такое защищаемая информация и каковы ее отличительные признаки?

9. Перечислите известные Вам критерии классификации защищаемой информации.

10. К какой информации не может быть ограничен доступ?

11. Какие сведения относятся к информации с ограниченным доступом?

Глава 5. ГОСУДАРСТВЕННАЯ ТАЙНА КАК ОСОБЫЙ ВИД ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

5.1. Понятие и сущность государственной тайны

Понятие *«государственная тайна»* занимает одно из ключевых положений в системе обеспечения безопасности любого государства. Определение этого понятия дано в ст. 2 Закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» (далее Закон «О государственной тайне»): «Г*осударственная тайна* — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

В ст. 5 указанного закона приведен *перечень сведений, составляющих государственную тайну* (указаны лишь разделы): в военной области; о внешнеполитической и внешнеэкономической деятельности; в области экономики, науки и техники; в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Какие сведения могут быть отнесены к государственной тайне, определено в Указе Президента РФ от 30 ноября 1995 г. № 1203 (с изменениями от 24 января 1998 г., 6 июня, 10 сентября 2001 г., 29 мая 2002 г., 3 марта 2005 г., 11 февраля 2006 г., 24 декабря 2007 г., 8, 30 апреля, 28 июля, 6 сентября 2008 г., 18 мая, 10 июня, 30 сентября 2009 г., 10 декабря 2010 г., 8 апреля 2011 г.). Данным Указом существенно конкретизирован перечень групп сведений, составляющих государственную тайну, и увеличен до 113.

Закон и Перечень содержат только категории сведений, составляющих государственную тайну, а не сами сведения, которые являются государственной тайной. Соответственно, ни закон, ни Перечень не устанавливают степени секретности сведений, т.е. не засекречивают их.

В соответствии со статьей 7 Закона «О государственной тайне» *не подлежат засекречиванию и подлежат обязательному*

рассекречиванию без ограничения хронологических рамок документы, содержащие сведения:

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

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

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- о фактах нарушения прав и свобод человека и гражданина;

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

- о состоянии здоровья высших должностных лиц Российской Федерации;

- о фактах нарушения законности органами государственной власти и их должностными лицами,

В соответствии с той же ст. 7 Закона «О государственной тайне» в случае засекречивания перечисленных выше сведений должностные лица, принявшие такое решение, могут быть привлечены к юридической ответственности (уголовной, административной или дисциплинарной ответственности). Таким образом, если гражданину было отказано в ознакомлении с информацией, которая не подлежит засекречиванию, то он имеет право обжаловать подобные действия должностных лиц в вышестоящей инстанции или требовать ее предоставления через судебные органы.

5.2. Правовое обеспечение защиты государственной тайны

Одним из наиболее эффективных способов защиты информации является ее засекречивание. Под *засекречиванием сведении и их носителей* следует понимать ограничения на их распространение и на доступ к их носителям.

Основными *принципами* отнесения сведений к государственной тайне и их засекречивания являются принципы законности, обоснованности и своевременности.

Согласно Перечню должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, утвержденному Указом Президента РФ от 16 апреля 2005 г. № 151-рп, в него входят:

Руководитель Администрации Президента Российской Федерации;

Министр внутренних дел Российской Федерации;

Министр Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;

Министр иностранных дел Российской Федерации;

Министр обороны Российской Федерации;

Министр юстиции Российской Федерации;

Руководитель Аппарата Правительства Российской Федерации — Министр Российской Федерации;

Министр здравоохранения и социального развития Российской Федерации;

Министр образования и науки Российской Федерации;

Министр природных ресурсов Российской Федерации;

Министр промышленности и энергетики Российской Федерации;

Министр сельского хозяйства Российской Федерации;

Министр транспорта Российской Федерации;

Министр информационных технологий и связи Российской Федерации;

Министр финансов Российской Федерации;

Министр экономического развития и торговли Российской Федерации;

Председатель Банка России;

Директор ГФС России;

Директор СВР России;

Директор ФСБ России;

Директор ФСКН России;

Директор ФСО России;

Начальник ГУСПа;

Руководитель Росгидромета;

Руководитель Росатома;

Руководитель Роскосмоса;

Директор ФСТЭК России.

В ст. 8 Закона «О государственной тайне» установлены степени секретности сведений и грифы секретности носителей этих сведений. *Степень секретности* сведений, составляющих государственную тайну, соответствует степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации в случае распространения этих сведений. Законом «О государственной тайне» установлены *три степени секретности:*

«особой важности»;

«совершенно секретно»;

«секретно».

В соответствии с Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности (утв. Постановлением Правительства РФ от 4 сентября 1995 г. № 870) к сведениям *особой важности* следует относить сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей; к *совершенно секретным* сведениям — сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации; к *секретным* сведениям — все иные сведения из числа сведений, составляющих государственную тайну.

Проект перечня разрабатывает специально созданная *экспертная комиссия.* В ее состав включаются компетентные специалисты, работающие со сведениями, составляющими государственную тайну. Для определения этих сведений специалисты анализируют деятельность органов государственной власти, предприятий, учреждений и организаций. Собственники информации готовят обоснование необходимости отнесения сведений к государственной тайне с указанием соответствующей степени секретности. В случае, если сведения находятся в распоряжении нескольких органов государственной власти, степень секретности устанавливается по взаимному согласованию между ними.

Проект перечня утверждается руководителем органа государственной власти. Для координации работ утвержденные пе-

речни направляются в Межведомственную комиссию по защите государственной тайны.

Каждые 5 лет перечни подлежат пересмотру. Возможен пересмотр в случае необходимости (например, в случае изменения международной обстановки). Пересмотр перечней осуществляется в том же порядке, что и их разработка.

Порядок засекречивания сведений и их носителей установлен ст.11 Закона «О государственной тайне». Перечень сведений, подлежащих засекречиванию, является основанием для засекречивания сведений. На носителях, содержащих сведения, составляющие государственную тайну, проставляется соответствующий гриф секретности.

В случае, если на носителе невозможно нанести указанные реквизиты, они отмечаются в сопроводительной документации на этот носитель.

Порядок рассекречивания сведений предусмотрен ст. 13 Закона «О государственной тайне». *Рассекречивание сведений и их носителей* — снятие ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям. Закон «О государственной тайне» выделяет два *основания* рассекречивания сведений:

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

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

Общий срок засекречивания сведений, составляющих государственную тайну, не может быть более 30 лет. По решению межведомственной комиссии по защите государственной тайны срок может быть продлен.

Ограничение допуска к государственной тайне

Под допуском к государственной тайне в соответствии с Законом «О государственной тайне» следует понимать процедуру оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений. Допуск осуществляется в добровольном порядке (ст. 21).

Вопросы, связанные с допуском к государственной тайне, регламентированы Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденной Постановлением Правительства РФ от 6 февраля 2010 г. № 63.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне регламентирован Постановлением Правительства РФ от 22 августа 1998 г. № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне".

Наличие *допуска* должностных лиц и граждан к государственной тайне выражено в следующем:

лицо принимает на себя обязательства перед государством по нераспространению доверенных ему сведений;

лицо дает согласие на частичные, временные ограничения их прав;

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

определяются виды, размеры и порядок предоставления социальных гарантий;

лицо должно ознакомиться с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение.

Решение о допуске оформляемого лица к сведениям, составляющим государственную тайну, принимает руководитель

органа государственной власти, предприятия, учреждения или организации.

Законом «О государственной тайне» предусмотрены две социальные гарантии для лиц, допущенных к государственной тайне на постоянной основе, а именно:

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.

Постановлением Правительства РФ от 18 сентября 2006 г. № 573 утверждены Правила выплаты ежемесячных процентных надбавок к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе, и сотрудников структурных подразделений по защите государственной тайны.

Законом «О государственной тайне» установлены *три формы допуска:*

- 1-я форма допуска предполагает *доступ к* сведениям особой важности, совершенно секретным и секретным сведениям;

- 2-я форма допуска — *доступ к* совершенно секретным и секретным сведениям;

- 3-я форма допуска — *доступ к* секретным сведениям.

При оформлении той или иной формы допуска в трудовом договоре отражаются обязательства гражданина по соблюдению требований законодательства о государственной тайне.

Основаниями для отказа гражданину в допуске к государственной тайне могут являться:

а) признание гражданина судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у гражданина неснятой судимости за эти преступления;

б) наличие у гражданина медицинских противопоказаний для работы с использованием сведений, составляющих государ-

ственную тайну, согласно перечню, утверждаемому Приказом Министерства здравоохранения и социального развития Российской Федерации (Минздравсоцразвития России) от 26 августа 2011 г. № 989н г. Москва "Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну";

в) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными гражданами документов для выезда на постоянное место жительства в другие государства;

г) выявление в результате проведения проверочных мероприятий действий гражданина, создающих угрозу безопасности Российской Федерации;

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

Прекращение допуска осуществляется по решению должностного лица, принявшего решение о его допуске к государственной тайне. Закон «О государственной тайне» выделяет 3 случая:

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

- однократного нарушения обязательств, связанных с защитой государственной тайны;

- при возникновении обстоятельств, являющихся основанием для отказа гражданину в допуске к государственной тайне.

Гражданин имеет право обжаловать решение о прекращении допуска к государственной тайне в вышестоящей организации или в суде.

Прекращение допуска к государственной тайне не дает право гражданину разглашать доверенные ему государством сведения.

Руководители организаций несут персональную ответственность за подбор граждан, допускаемых к государственной тайне.

Контрольные вопросы:

1. Что понимается под термином «государственная тайна»?
2. В каких нормативных правовых документах содержатся категории сведений, составляющих государственную тайну?
3. Какие сведения не подлежат засекречиванию?
4. Что такое засекречивание сведений и их носителей?
5. Каковы принципы засекречивания информации?
6. Перечислите должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.
7. Какие степени секретности установлены Законом «О государственной тайне»?
8. Что такое защищаемая информация и каковы ее отличительные признаки?
9. Каковы правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?
10. Что такое рассекречивание информации и их носителей?
11. Что такое допуск к государственной тайне?
12. Что для гражданина предусматривает допуск к государственной тайне?
13. Перечислите социальные гарантии, установленные для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе.
14. Перечислите основания для отказа гражданину в допуске к государственной тайне.
15. Перечислите основания прекращения допуска к государственной тайне.

Глава 6. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

6.1. Персональные данные как вид защищаемой информации

Законодательство Российской Федерации в области персональных данных (далее — ПДн) основывается на Конституции РФ и международных договорах Российской федерации и состоит из Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», других федеральных законов, определяющих случаи и особенности обработки персональных данных, отраслевых нормативных актов, инструкций и требований регуляторов.

В 1981 году Совет Европы принял Конвенцию «О защите личности в связи с автоматической обработкой персональных данных». 25 ноября 2005 г. Государственная Дума ратифицировала данную Конвенцию (ФЗ от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»), возложив на Российскую Федерацию обязательства по приведению в соответствие с нормами европейского законодательства деятельность в области защиты прав субъектов ПДн. Первым шагом в реализации взятых обязательств стало принятие Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных». Закон вступил в силу в январе 2007 года.

В соответствии с Законом №152-ФЗ *персональными данными* является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПДн). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн. Состав и содержание персональных данных определяют операторы ПДн в зависимости от целей их обработки.

Законодательство определяет следующие *категории персональных данных:* общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных сис-

темах персональных данных (далее ИСПДн), биометрические ПДн и другие.

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

К *специальным категориям* относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Категории персональных данных, обрабатываемых в ИСПДн

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет следующие категории персональных данных, которые обрабатываются в ИСПДн:

Категория 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Категория 2 — персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 — персональные данные, позволяющие идентифицировать субъекта ПДн.

Категория 4 — обезличенные и (или) общедоступные персональные данные.

Категорирование персональных данных при обработке в ИСПДн может также проводиться по параметру «объем обрабатываемых персональных данных». Под этим подразумевается количество субъектов, данные которых обрабатываются в информационной системе. Этот параметр может принимать следующие значения:

1. В информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта РФ или Российской Федерации в целом.

2. В информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.

3. В информационной системе одновременно обрабатываются данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации.

Такое категорирование персональных данных необходимо для определения класса ИСПДн, от которого зависят меры по обеспечению безопасности ПДн при обработке в информационных системах.

Биометрические персональные данные — это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Россййскую Федерацию, уголовно-исполнительным законодательством. Исходя из определения биометрических ПДн, к ним относятся фотографии

и видеоизображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения — в системах видеонаблюдения и т.п.

Закон № 152-ФЗ определил высокоуровневые требования, которые затем были конкретизированы в подзаконных актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России) и Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор). К ним относятся:

- Постановление Правительства РФ №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 г.;

- Постановление Правительства РФ от 2 июня 2008 г. №419 «О федеральной службе по надзору в сфере связи и массовых коммуникаций» (Россвязькомнадзор);

- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Совместный приказ № 55/86/20 ФСТЭК, ФСБ, Мининформсвязь от 13.02.2008 г., утверждающий порядок проведения классификации информационных систем персональных данных;

- Методические документы ФСТЭК России:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных;

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- Методические документы ФСБ РФ:

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации;

- Документы Россвязькомнадзора:

Приказ от 28 марта 2008 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных»;

Приказ от 17 июля 2008 г. №8 «Об утверждении образца формы уведомления об обработке персональных данных».

Функциями контроля и надзора государство наделило Роскомнадзор, ФСТЭК и ФСБ.

В соответствии с Федеральным законом Российской Федерации от 23 декабря 2010 г. № 359-ФЭ "О внесении изменения в статью 25 Федерального закона "О персональных данных" срок для приведения информационных систем персональных данных в соответствие с Законом о защите персональных данных перенесен с 1 января 2010 года на 1 июля 2011 года. Перенос сроков связан с существенным увеличением затрат на приведение информационных систем в соответствие с требованиями по безопасности и защите персональных данных и особенно — затрат на поддержание таких систем, которые сложно осуществимы в условиях финансового кризиса. Следствием этого могло бы

стать массовое несоответствие хозяйствующих субъектов требованиям Федерального закона, при том, что с начала 2010 года государственные регуляторы были бы вправе осуществлять проверки исполнения требований закона в отношении информационных систем персональных данных и привлекать к ответственности нарушителей,

6.2. Служебная тайна как вид защищаемой информации

В настоящее время законодательство о служебной тайне состоит всего из двух правовых актов: Постановления Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" и Указа Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера".

В соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» к *служебной информации ограниченного распространения* относится несекретная информация, касающаяся деятельности организаций, ограничение на распространение которой диктуется служебной необходимостью. Руководители федеральных органов исполнительной власти в пределах своей компетенции определяют категорию должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения и обеспечивать ее защиту.

К разновидностям служебной тайны можно отнести: налоговую тайну; аудиторскую тайну; тайну следствия; тайну судопроизводства; тайну совещания судей; военную тайну и др.

Служебная тайна распространяется на информацию, которая находится в распоряжении органов власти (государственных и муниципальных), является охраноспособной и обладает свойством конфиденциальности.

Выделяют *два вида сведений, на которые распространяется служебная тайна органов власти:*

сведения, созданные непосредственно самим органом власти, в отношении которых действует требование конфиденциальности, обеспечивающее их сохранность от незаконного доступа;

сведения, касающиеся других лиц, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности (конфиденциальные сведения о гражданах и организациях).

Признаки информации, относящейся к служебной тайне:

получена представителем государственного органа (или органа местного самоуправления) в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом;

не относится к информации, составляющей государственную тайну;

не подпадает под перечень сведений, доступ к которым не может быть ограничен;

отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);

является охраноспособной информацией, отвечающей требованию конфиденциальности другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна).

Исходя из сказанного выше, можно предложить следующее определение информации, составляющей служебную тайну. *Информация, составляющая служебную тайну,* — это сведения, ставшие известными государственным органам и органам местного самоуправления на законных основаниях и в силу исполнения ими служебных обязанностей, а также сведения о деятельности государственных органов и органов местного самоуправления, доступ к которым ограничен федеральным законом, не являющиеся государственной тайной, к которым у третьих лиц нет свободного доступа на законном основании.

А непосредственно *служебная тайна* — это режим обеспечения конфиденциальности информации, включающий в себя совокупность правовых и организационных мер.

В настоящее время в законодательстве имеется правовой пробел по ограничению доступа к информации, составляющей служебную тайну. Необходимо в срочном порядке принять Федеральный закон "О служебной тайне", в котором следует закрепить понятие служебной тайны, определить перечень сведений, составляющих служебную тайну, определить права и обязанности субъектов по предоставлению указанных сведений и охране их конфиденциальности, а также установить виды и случаи наступления юридической ответственности за нарушение соответствующего законодательства.

6.3. Коммерческая тайна как вид защищаемой информации

Законодательство о коммерческой тайне включает: Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне», а также главу 75 IV части Гражданского кодекса РФ «Право на секрет производства (ноу-хау)».

Под *коммерческой тайной* понимается 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) — это 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.

Федеральный закон от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне» в ст. 5 содержит *перечень сведений, которые не могут составлять коммерческую тайну.* Это сведения:

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

содержащиеся 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, составе работников, системе оплаты труда, условиях труда (в том числе об охране труда), показателях производственного травматизма и профессиональной заболеваемости и наличии свободных рабочих мест;

о задолженности работодателя по выплате заработной платы и 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, размерах и составе их имущества, расходах, численности и оплате труда их работников, 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 федеральными законами.

На практике к информации, составляющей коммерческую тайну (секрет производства), принято относить:

а) содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности организации, которое должно быть отнесено к коммерческой тайне в любом случае — в силу п. 4 статьи 10 Федерального закона от 21 ноября 1996 года № 129-ФЗ «О бухгалтерском учете»;

б) информацию о полезных моделях, промышленных образцах, изобретениях и иных объектах интеллектуальной собственности, находящихся на стадии разработки (регистрации);

в) информацию о партнерах и клиентах (покупателях, поставщиках, посредниках, контрагентах и др.), об условиях заключаемых сделок, ценообразовании, предполагаемых скидках, акциях, расчетах цен и формируемых на основе этих сведений клиентских базах;

г) информацию личного характера — все сведения об источниках доходов, личной жизни руководства и главного бухгалтера, членов их семей, адреса, расписание деловых встреч, данные об их контактных телефонах, пагубных привычках, маршрутах передвижений и т. д.;

д) информацию о технических средствах охраны имущества организации, системах охранной и иной сигнализации, методах и приемах обеспечения безопасности деятельности организации, местах хранения материальных ценностей.

6.4. Правовое регулирование защиты сведений, связанных с профессиональной деятельностью

Информацию, защита которой является обязанностью субъекта в силу выполняемых им профессиональных полномочий, принято относить к категории *профессиональная тайна. Субъектом* профессиональной тайны может выступать и физическое, и юридическое лица.

К профессиональной тайне относятся следующие виды тайн:

- банковская тайна;
- нотариальная тайна;
- адвокатская тайна;

- врачебная тайна;
- тайна страхования;
- тайна исповеди;
- иные виды тайн.

Банковская тайна.

В ГК РФ, а именно в ст. 857 установлена обязанность банка гарантировать тайну следующих сведении:

- банковского счета и банковского вклада;
- операций по счету и сведений о клиенте.

Указанные сведения предоставляются:

- самим клиентам или их представителям;
- в бюро кредитных историй;
- государственным органам и их должностным лицам (в определенных случаях).

Федеральный закон от 02.12.1990 № 395-1 (ред. от 11.07.2011) "О банках и банковской деятельности" (с изм. и доп., вступающими в силу с 29.09.2011) в ст. 26 устанавливает обязанность служащих кредитной организации хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией.

К банковской тайне относятся сведения, касающиеся:

- клиентов банка — их паспортные данные, сведения о местонахождении (местожительстве), банковских реквизитах юридического лица, сведения о его руководстве;
- банковского счета клиента — вид счета, дата его открытия, номер счета, данные о суммах на счете, количество счетов клиента, сведения о владельце счета;
- банковского вклада — вид вклада, сумма вклада, порядок начисления и размер процентов, срок вклада;
- операция по счетам и вкладам клиентов — валюта счета, суммы, зачисляемые и списываемые со счета, документы, на основании которых проводятся операции по счету, выписки со счетов;
- корреспондентов банка — валюта и сумма операций, условия и даты сделок;

- иной деятельности банка, связанной с управлением финансами, внутренними технологическими процессами, имеющие ценность для банка в силу неизвестности их третьим лицам.

Банковская тайна должна строго соблюдаться банком и не подлежит разглашению, а также опубликованию в средствах массовой информации и передаче третьим лицам.

Рассматриваемые сведения могут быть предоставлены без нарушения законодательства следующим органам и организациям:

- судам и арбитражным судам;
- Счетной палате Российской Федерации;
- налоговым органам;
- таможенным органам;
- федеральному органу исполнительной власти в области финансовых рынков;
- Пенсионному фонду;
- Фонду социального страхования;
- органам принудительного исполнения судебных актов, актов других органов и должностных лиц;
- органам предварительного следствия по делам, находящимся в их производстве;
- органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений;
- уполномоченному органу, осуществляющему меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, в случаях, порядке и объеме, которые предусмотрены Федеральным законом "О противодействии легализации (отмыванию) доходов, полученных преступным путем";
- органу валютного контроля.

С согласия юридического лица, индивидуального предпринимателя или физического лица информация по их операциям представляется банками в целях формирования кредитных историй в бюро кредитных историй в соответствии с Федеральным законом «О кредитных историях».

Банки и организации, в силу федеральных законов имеющие отношение к банковской тайне, а также их служащие, имеющие отношение к банковской тайне в силу исполнения

своих должностных обязанностей, несут ответственность за разглашение банковской тайны.

Врачебная тайна.

В соответствии со ст. 61 "Основ законодательства Российской Федерации об охране здоровья граждан" (утв. ВС РФ 22.07.1993 № 5487-1) (ред. от 18.07.2011) к *врачебной тайне следует относить следующие сведения:*

- о факте обращения за медицинской помощью;
- о состоянии здоровья гражданина;
- о диагнозе заболевания гражданина;
- иные сведения, полученные при его обследовании и лечении.

При наличии согласия гражданина или его законного представителя возможна передача рассматриваемых сведений, например, для проведения научных исследований, использования в учебном процессе.

Законодательством установлены случаи, когда предоставление сведений, составляющих врачебную тайну, возможно *без согласия гражданина.* Таковыми являются:

1) для обследования и лечения лица, которое не в состоянии выразить свою волю;

2) в случае наличия угрозы распространения инфекционных заболеваний, массовых отравлений и поражений;

3) в случае проведения расследования или судебного разбирательства (при наличии запроса органов дознания и следствия и суда);

4) в случае оказания помощи несовершеннолетнему в целях информирования его родителей или законных представителей;

5) в случае, если имеются основания полагать, что вред здоровью является последствием противоправных действий;

6) в целях проведения военно-врачебной экспертизы в порядке, установленном положением о военно-врачебной экспертизе, утверждаемым уполномоченным федеральным органом исполнительной власти.

Обязанность сохранения врачебной тайны не прекращается и со смертью пациента. *Нарушение врачебной тайны* — это разглашение ее хотя бы одному лицу, умышленное или неосторож-

ное (небрежное хранение документации или беседа медиков в людном месте). Необходимый обмен информацией в ходе оказания специалистами медицинской помощи не рассматривается как нарушение врачебной тайны. Вся информация в медицинских документах гражданина также является врачебной тайной.

Адвокатская тайна.

Статья 8 Федерального закона от 31.05.2002 № 63-ФЗ (ред. от 11.07.2011) "Об адвокатской деятельности и адвокатуре в Российской Федерации" определяет, что *адвокатской тайной* являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Режим адвокатской тайны распространяется на следующие сведения:

- факт обращения к адвокату;
- о доказательствах, подготовленных адвокатом по делу;
- сведения, переданные доверителем адвокату;
- сведения о самом доверителе, которые стали известны адвокату в ходе рассмотрения дела;
- содержание юридических рекомендаций доверителю;
- делопроизводство адвоката по делу;
- условия соглашения об оказании юридической помощи;
- иные сведения, связанные с оказанием юридических услуг.

Гарантии обеспечения адвокатской тайны реализуются в следующем:

- адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах дела, имеющегося у него в производстве;
- оперативно-розыскные мероприятия и следственные действия в отношении адвоката проводятся только на основании судебного решения, причем полученные сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей (за исключением орудия преступления, а также предметов, запрещенных к обращению или с ограниченным оборотом).

Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации» установлено: «помощник адвоката и стажер адвоката обязаны хранить адвокатскую тайну».

Нотариальная тайна (тайна нотариальных действий).

Согласно ст. 5 Основ законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1), *нотариусу* при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, *запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения,* за исключением случаев, предусмотренных Основами. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия.

Справки о совершенных нотариальных действиях выдаются по требованию суда, прокуратуры, органов следствия в связи с находящимися в их производстве уголовными, гражданскими или административными делами, а также по требованию судебных приставов-исполнителей в связи с находящимися в их производстве материалами по исполнению исполнительных документов.

Тайна страхования.

В соответствии со ст. 946 ГК Российской Федерации *тайну страхования* составляют сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

В соответствии с Законом РФ от 27.11.1992 № 4015-1 (ред. от 18.07.2011) "Об организации страхового дела в Российской Федерации" в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица — *страховые агенты и страховые брокеры.*

Доступ к сведениям, составляющим тайну страхования, на законных основаниях *имеют*: 1) представитель страхователя (выгодоприобретателя) — на основании нотариально удостоверенной доверенности; 2) орган дознания и предварительного

следствия — по находящимся в его производстве уголовным делам; 3) суд — на основании определения суда по находящимся в его производстве делам; 4) прокурор — на основании постановления о производстве проверки в пределах его компетенции по находящимся у него на рассмотрении материалам.

Тайна усыновления.

В соответствии со ст. 139 Семейного кодекса РФ *тайна усыновления ребенка охраняется законом.* Тайна усыновления распространяется на:

- судей, вынесших решение об усыновлении, и всех работников суда, причастных к судебному делопроизводству, и всех участвующих в рассмотрении дела лицам;

- должностные лица, осуществляющие государственную регистрацию усыновления (работники органов записи актов гражданского состояния, представители органов опеки и попечительства, медицинские работники).

Тайна исповеди.

Тайна исповеди — самостоятельный вид охраняемых законом тайн, одна из гарантий свободы вероисповедания.

Обеспечение тайны исповеди является внутренним делом священника, юридической ответственности за ее разглашение он не несет. Согласно ч. 2 ст. 51 Конституции РФ и ч. 7 ст. 3 Федерального закона «О свободе совести и религиозных объединениях», священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Согласно церковному каноническому праву, священник не может нарушить тайну исповеди ни при каких условиях. Это строго запрещено 120-м правилом Номоканона при Большом Требнике: за открытие греха исповедовавшегося духовный отец отстраняется на три года от служения и каждый день должен класть сто поклонов.

Контрольные вопросы:

1. Что понимается под термином «персональные данные»?
2. Какие сведения могут относиться к категории персональных данных?
3. Какими нормативными документами регулируются вопросы защиты персональных данных?
4. Раскройте содержание основных категорий персональных данных?
5. Что понимается под термином «информация, составляющая служебную тайну»?
6. Какими нормативными документами регулируются вопросы защиты служебной тайны?
7. Какая информация относится к служебной информации ограниченного распространения?
8. Что такое коммерческая тайна?
9. Что понимается под термином «информация, составляющая коммерческую тайну»?
10. Какими нормативными правовыми документами регулируются вопросы защиты коммерческой тайны?
11. Какие сведения не могут составлять коммерческую тайну?
12. Что относится к мерам по обеспечению конфиденциальности информации, составляющей коммерческую тайну?
13. Какая информация относится к категории профессиональная тайна?
14. Приведите характеристику банковской тайны как вида защищаемой информации.
15. Приведите характеристику врачебной тайны как вида защищаемой информации.
16. Приведите характеристику адвокатской тайны как вида защищаемой информации.
17. Приведите характеристику нотариальной тайны как вида защищаемой информации.
18. Приведите характеристику тайны страхования как вида защищаемой информации.
19. Приведите характеристику тайны усыновления и тайны исповеди как видов защищаемой информации.

Глава 7. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

7.1. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности

Впервые понятие интеллектуальной собственности используется с момента учреждения в 1967 году в Стокгольме Всемирной организации интеллектуальной собственности (ВОИС). В советском законодательстве термин «интеллектуальная собственность» появился впервые в Законе СССР «О собственности в СССР» (6 марта 1990 года). В российском законодательстве данный термин был утвержден Конституцией РФ, принятой в декабре 1993 года, и первой частью Гражданского кодекса РФ от 30.11.1994 № 51-ФЗ. Вместе с этими нормативными правовыми актами был принят ряд других, а именно:

- «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 года№ 3526-1;
- «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 года№ 3523-1.

В настоящее время законодательство в области защиты прав на результаты интеллектуальной деятельности включает в себя положения части четвертой ГК (от 18 декабря 2006 г., вступившего в силу с 1 января 2008 г.), международные договоры РФ, другие нормативные правовые акты, регулирующие отношения в области интеллектуальной собственности.

Интеллектуальные права или право интеллектуальной собственности — юридический термин, обозначающий совокупность прав, которыми обладают лицо или лица (авторы или иные правообладатели) на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации.

Термин «интеллектуальная собственность» определён в ст. 1225 части четвертой Гражданского кодекса РФ как список результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, которым предоставляется правовая защита. Термин «интеллектуальные права» определён в ст. 1226 как права на «результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации)».

Результатами интеллектуальной собственности, в соответствии с п.1 ст. 1225 ГК РФ, являются произведения науки, литературы и искусства, программы для электронных вычислительных машин (программы для ЭВМ), базы данных, исполнения, фонограммы, сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания), изобретения, полезные модели, промышленные образцы, селекционные достижения, топологии интегральных микросхем, секреты производства (ноу-хау), фирменные наименования, товарные знаки и знаки обслуживания, наименования мест происхождения товаров, коммерческие обозначения.

В настоящее время интеллектуальная собственность как подотрасль гражданского права состоит из следующих институтов:

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

7.2. Основы авторского права

Авторское право (англ. copyright) — часть гражданского права, регулирующая отношения, возникающие в связи с использованием произведений науки, литературы, искусства.

Авторское право представляет собой совокупность правовых норм, регулирующих отношения, возникающие между объектами и субъектами права в отношении созданного произведения.

Авторское право распространяется на произведения:

- обнародованные на территории РФ или необнародованные, но находящиеся в какой-либо объективной форме на территории РФ, — признается за авторами (их правопреемниками) независимо от их гражданства;

- обнародованные за пределами территории РФ или необнародованные, но находящиеся в какой-либо объективной форме за пределами территории РФ, — признается за авторами, являющимися гражданами РФ (их правопреемниками);

- обнародованные за пределами территории РФ или необнародованные, но находящиеся в какой-либо объективной форме за пределами территории РФ, — признается на территории РФ за авторами (их правопреемниками) — гражданами других государств в соответствии с международными договорами РФ. Произведение также считается впервые опубликованным в РФ, если в течение 30 дней после даты первого опубликования за ее пределами оно было опубликовано на территории РФ.

Распространение авторского права возникает в силу факта создания произведения. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления или соблюдения каких-либо формальностей.

Объектами авторского права являются:

- первичные произведения, в том числе литературные (включая программы для ЭВМ);

- вторичные, то есть производные произведения (переводы, обработки, аннотации, рефераты т.п.), а также сборники и другие составные произведения, представляющие собой по подбору и расположению материала результаты творческого труда (энциклопедии, антологии, базы данных).

К числу произведений, не являющихся объектами авторского права, относятся:

- официальные документы, их официальные переводы;

- сообщения о событиях и фактах, имеющих информационный характер;

- идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Субъектами авторского права являются правообладатели, среди которых выделяются:

- автор;

- наследник автора;

- любое физическое или юридическое лицо, которое обладает исключительными имущественными правами, полученными в силу закона или договора.

Автором признается физическое лицо или группа физических лиц, в результате творческой деятельности которых создан результат интеллектуальной деятельности.

В случае, если база данных состоит из материалов, не являющихся объектами авторского права, авторское право принадлежит лицам, ее создавшим. В противном случае необходимо согласие авторов на включение этих данных в общую базу.

Не признаются авторами физические лица:

- не внесшие личного творческого вклада;

- оказавшие только техническую, организационную или материальную помощь, в том числе в оформлении документов.

Знак охраны авторского права состоит из трех элементов:

- латинской буквы С в окружности ©;

- имени (наименования) обладателя исключительных авторских прав;

- года первого опубликования произведения.

Автору принадлежат следующие права:

- личные неимущественные права, а именно право авторства, право на имя, псевдоним или анонимность, право на неприкосновенность, целостность как самого объекта, так и их названий, право на обнародование произведения, право на защиту своей репутации;

- имущественные права: исключительные права на использование произведения в любой форме и любым способом, в частности право на воспроизведение, распространение, публичный показ, передачу в эфир, перевод, переработку.

Личные неимущественные права принадлежат автору независимо от его имущественных прав и сохраняются за ним в случае уступки исключительных прав на использование произведения.

Имущественные права могут быть переданы полностью или частично любому лицу по договору, который заключается в письменной форме и должен устанавливать объемы и способы использования объекта, порядок и размеры выплаты вознаграждения, срок действия. Имущественные права переходят по наследству.

В случае, если результат интеллектуального творчества создан при выполнении служебных обязанностей, заданий работодателя или работ по договору с заказчиком, права принадлежат работодателю или заказчику, если договором не предусмотрено иное. Получение вознаграждения, порядок его выплаты и размер указываются в договоре между автором и работодателем.

Срок действия авторского права определяется в течение всей жизни автора и 70 лет после его смерти.

Для произведения, выпускаемого периодически анонимно или под псевдонимом, авторское право действует 70 лет с момента выпуска в свет.

За нарушение авторских и смежных прав предусмотрены следующие виды ответственности:

- гражданско-правовая;
- административная;
- уголовная.

При нарушении требований закона, признаваемых как нарушение исключительных прав, их правообладатель имеет право:

- требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации;
- требовать возмещения морального вреда;
- обратиться для защиты своих прав в суд, арбитражный суд, третейский суд, органы прокуратуры, органы дознания, органы предварительного следствия в соответствии с их компетенцией.

Нарушителем авторского права является лицо, не выполняющее требования законодательства в отношении исключительных прав правообладателей, в том числе ввозящее в Россию

экземпляры программ или баз данных, изготовленных без разрешения их правообладателей.

Контрафактными являются экземпляры произведения, изготовление или использование которых влечет за собой нарушение авторского права, в том числе ввозимые в Россию из государства, в котором эти произведения никогда не охранялись или перестали охраняться.

Программы для ЭВМ и базы данных являются объектами авторского права. Программы для ЭВМ охраняются как произведения литературы, а базы данных — как сборники.

Не являются объектами авторского права:

- идеи и принципы, лежащие в основе программы для ЭВМ;
- базы данных или какой-либо их элемент, в том числе идеи и принципы организации интерфейса и алгоритма;
- языки программирования.

Особенностью авторского права на программы для ЭВМ и базы данных является то, что право не связано с правом собственности на их материальный носитель и любая передача прав на материальный носитель не влечет за собой передачи каких-либо прав на программы для ЭВМ и базы данных. Автору программы для ЭВМ и базы данных принадлежат личные неимущественные и имущественные права.

Основными нарушениями авторских прав иных правообладателей в отношении программы для ЭВМ или базы данных, материалов и оборудования, используемых для их воспроизведения, являются:

- изготовление;
- воспроизведение;
- распространение;
- продажа, ввоз или иное использование;
- выпуск под своим именем чужой программы или базы данных.

В отношении контрафактных экземпляров программ, базы данных, материалов и оборудования, используемых для их воспроизведения, суд или арбитражный суд может вынести решение:

- о конфискации, их уничтожении;

- о передаче в доход бюджета РФ, передаче истцу по его просьбе в счет возмещения убытков;

- об аресте в порядке, установленном законом;

- об уголовной ответственности.

7.3. Основы патентного права

Патентное право —- подотрасль гражданского права, регулирующая правоотношения, связанные с созданием и использованием (изготовление, применение, продажа, иное введение в гражданский оборот) объектов интеллектуальной собственности, охраняемых патентом.

На основании ст. 1349 ГК РФ *объектами патентных прав* являются:

- изобретения;

- полезные модели;

- промышленные образцы.

Изобретение — новое, обладающее существенными отличиями техническое решение задачи в любой области экономики, социального развития, культуры, науки, техники, обороны, дающее положительный эффект и удовлетворяющее некоторым критериям патентоспособности.

К *объектам изобретения* относятся:

- устройство;

- способ;

- вещество;

- штамм микроорганизма;

- культуры клеток растений и животных;

- применение известного ранее устройства, способа, вещества, штамма по новому назначению.

Не признаются патентоспособными изобретениями:

- научные теории и математические методы;

- методы организации и управления хозяйством;

- условные обозначения, расписания, правила;

- методы выполнения умственных операций;

- алгоритмы и программы для вычислительных машин;

- проекты и схемы планировки сооружений, зданий, территорий;

- решения, касающиеся только внешнего вида изделий, направленные на удовлетворение эстетических потребностей;

- топологии интегральных микросхем;

- сорта растений и породы животных;

- решения, противоречащие общественным интересам, принципам гуманности и морали.

Полезные модели — технические решения, представляющие собой конструктивное выполнение средств производства и предметов потребления, а также их составных частей и отвечающие требованиям патентоспособности.

Не подлежат правовой защите как полезные модели:

- способы;

- вещества;

- штаммы микроорганизмов;

- культуры клеток растений и животных, а также их применение по новому назначению.

Промышленные образцы — художественно-конструкторские решения, определяющие внешний вид изделия. Предоставление правовой защиты промышленному образцу осуществляется при соответствии его требованиям патентоспособности.

Не признаются патентоспособными промышленными образцами:

- решения, обусловленные исключительно технической функцией изделия;

- объекты архитектуры (кроме малых архитектурных форм), промышленных, гидротехнических и других стационарных сооружений;

- печатная продукция как таковая;

- объекты неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ;

- изделия, противоречащие общественным интересам, принципам гуманности и морали.

Правовая охрана не предоставляется изобретениям, полезным моделям, промышленным образцам, признанным государ-

ством секретными, и обращение с ними регулируется специальным законодательством РФ.

Правовая защита рассмотренных объектов промышленной собственности предоставляется в случае их удовлетворения показателям патентоспособности. К таким показателям относится *новизна, наличие изобретательского уровня, промышленная применимость, оригинальность.*

Для *изобретения* установлены такие показатели, как *новизна, наличие изобретательского уровня, промышленная применимость.*

Новизна изобретения: в случае если существенные признаки формулы изобретения включают сведения, ставшие общедоступными в мире до даты приоритета. Изобретательский уровень означает, что изобретение должно быть результатом творческой, а не основанной на распространенных представлениях или общедоступных знаниях работы. Показатель промышленной применимости предполагает установление того, что техническое решение может быть использовано в промышленности, сельском хозяйстве, здравоохранении и других областях деятельности.

Для полезной модели приняты показатели новизны и промышленной применимости.

Новая полезная модель — модель, в которой совокупность ее существенных признаков неизвестна из уровня техники. Промышленно применимая полезная модель — модель, которая может быть использована в промышленности, сельском хозяйстве, здравоохранении и других отраслях.

Для промышленного образца приняты показатели возможности многократного воспроизведения образца путем производства соответствующего изделия, новизны, оригинальности и промышленной применимости.

Новый промышленный образец — образец, у которого совокупность его существенных признаков, определяющих эстетические и (или) эргономические особенности изделия, неизвестна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца. Оригинальный промышленный образец — образец, у которого его существенные признаки обусловливают творческий характер эстетических особен-

ностей изделия. Промышленно применимый промышленный образец — образец, который может быть многократно воспроизведен путем изготовления соответствующего изделия.

Основными *субъектами* патентного права являются авторы (изобретения, полезной модели, промышленного образца), патентообладатели, их правопреемники.

Автор — любое физическое лицо, творческим трудом которого созданы изобретение, полезная модель, промышленный образец, селекционное достижение. При создании объекта промышленной собственности несколькими физическими лицами все они считаются его авторами. Порядок пользования правами, принадлежащими авторам, определяется соглашением между ними. При отсутствии такого соглашения каждый автор может использовать изобретение по своему усмотрению, но не вправе передать свои права третьему лицу без согласия остальных авторов.

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.

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Правообладателем выступает лицо, которому выдан патент. Это может быть:

автор (авторы) изобретения, полезной модели, промышленного образца;

физические и юридические лица, которые указаны автором (авторами) или его (их) правопреемником в заявке на выдачу патента либо в заявлении, поданном в патентное ведомство до момента регистрации изобретения, полезной модели, промышленного образца

Патентные права подтверждаются особыми документами:

- патентами на изобретение или промышленный образец;
- свидетельством на полезную модель.

Начало срока действия патента (свидетельства) определяется с момента поступления авторской заявки на изобретение (полезную модель, промышленный образец) в патентное ведомство, где фиксируются год, месяц, день, час и минута.

Сроки действия документов:

патент на изобретение действует в течение 20 лет;

патент на промышленный образец— 10 лет;

свидетельство на полезную модель — 5 лет.

Сроки действия патента на промышленный образец и свидетельство на полезную модель могут быть продлены, но не более чем соответственно на 5 лет и 3 года.

На государственном уровне правом патентообладания пользуется Федеральный фонд изобретений РФ, который приобретает их на договорной основе и реализует в интересах государства.

Процесс патентования начинается с подачи заявки на изобретение. Заявка включает следующие документы:

заявление на бланке установленной формы, выдачу которого производит Федеральный институт промышленной собственности (ФИПС);

описание изобретения, раскрывающее его с полнотой, достаточной для промышленного применения;

формула изобретения;

чертежи и иные материалы;

реферат.

Заявка на выдачу патента подается автором, работодателем или их правопреемником в патентное ведомство. Затем проводится экспертиза (в течение 2 месяцев). После принятия решения о выдаче патента патентное ведомство публикует в своем официальном бюллетене сведения о выдаче патента. Одновременно с публикацией оно вносит в Государственный реестр изобретений РФ, Государственный реестр полезных моделей РФ или Государственный реестр промышленных образцов РФ соответственно изобретение, полезную модель или промышленный образец и выдает патент лицу, на имя которого он направляется.

В течение 2 месяцев со дня поступления заявки в патентное ведомство заявитель имеет право вносить в ее материалы исправления и уточнения без изменения сущности изобретения.

При положительном результате экспертизы принимается решение о выдаче патента. В случае отказа решение может быть обжаловано в апелляционной палате в течение 3 месяцев со дня его получения или копий материалов, на которые приводятся ссылки в решении. Возражение должно быть рассмотрено в 4-месячный срок. Решение апелляционной палаты может быть обжаловано в Высшей патентной палате в течение 6 месяцев с момента ею получения. Решение последней является окончательным.

При положительном решении о выдаче патента сведения о нем публикуются в официальном издании патентного ведомства, а само изобретение вносится в Государственный реестр изобретений РФ.

Нарушением исключительного права патентообладателя считается:

любое хозяйственное использование охраняемых сведений, вплоть до хранения продукта, содержащего объект промышленной собственности;

несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью продукта, содержащего запатентованное изобретение, полезную модель, промышленный образец;

применение способа, охраняемого патентом на изобретение, или введение в хозяйственный оборот либо хранение с этой целью продукта, изготовленного непосредственно способом, охраняемым патентом на изобретение. При этом новый продукт считается полученным запатентованным способом при отсутствии доказательств противного.

Контрольные вопросы:

1. Что понимается под термином «интеллектуальная собственость»?
2. Что понимается под термином «интеллектуальные права»?
3. Какими нормативными документами регулируются вопросы интеллектуальной собственности?
4. Что относится к результатам интеллектуальной собственности?
5. Что такое авторское право?
6. Перечислите объекты авторского права.
7. Перечислите субъекты авторского права.
8. Кто признается автором и соавтором?
9. Какие права принадлежат автору произведения?
10. Что такое исключительное право?
11. Каков срок действия исключительного права?
12. Каковы особенности защиты программ дня ЭВМ и баз данных институтом авторского права?
13. Что такое патентное право?
14. Перечислите объекты патентного права.
15. Перечислите субъекты патентного права.
16. Кто признается автором объектов патентного права?
17. Кто может являться патентообладателем?
18. Какими документами подтверждаются патентные права, каков срок их действия?
19. Что является нарушением исключительного права патентообладателя?

Глава 8. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВОВЫХ НОРМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Понятие юридической ответственности

Вопросы определения юридической ответственности в сфере информационной безопасности является одной из важнейших задач деятельности государства и его компетентных органов.

Юридическая ответственность является разновидностью социальной ответственности лица. Наступление юридической ответственности связано с нарушением юридических норм.

Юридическая ответственность выражается в необходимости виновному лицу подвергнуться мерам государственного воздействия, претерпеть определенные отрицательные последствия. Другими словами, юридическая ответственность — это способ реагирования государства на правонарушение.

Применительно к лицу юридическая ответственность выражается в виде наступления отрицательных последствий материального, морального, личного, организационного, физического характера (лишение или ограничение свободы, исправительные работы, конфискация имущества, штраф, арест, лишение права занимать определенные должности, смертная казнь).

Признаки юридической ответственности:

- предусмотрена действующим законодательством (уголовным, гражданским, административным и др.);
- наступает в случае наличия полного состава правонарушения;
- опирается на государственное принуждение;
- выражается в определенных отрицательных последствиях;
- возлагается и реализуется в установленной законом процессуальной форме, осуществляется уполномоченными на то компетентными органами и должностными лицами.

Основаниями юридической ответственности являются необходимые условия привлечения к юридической ответственности:

• нормативное основание — это наличие действующей нормы права, устанавливающей определенное деяние как правонарушение.

• фактическое основание — это фактически совершенное правонарушение;

• процессуальное основание — это вступивший в силу акт уполномоченного государственного органа или должностного лица о привлечении нарушителя к ответственности.

Функциями юридической ответственности являются: 1) карательная; 2) штрафная; 3) предупредительная, или превентивная; 4) воспитательная; 5) компенсационная, или правовосстановительная.

Принципами юридической ответственности являются:

- принцип законности;
- принцип обоснованности;
- принцип неотвратимости;
- принцип справедливости;
- принцип гуманизма;
- презумпция невиновности.

8.2. Виды юридической ответственности

Отдельные исследователи отмечают, что виды юридической ответственности соответствуют видам правонарушений. Рассмотрим более подробно понятие правонарушения, его состав и виды.

Правонарушение — это общественно вредное, противоправное, виновное деяние, за которое законом предусмотрена юридическая ответственность.

Признаки правонарушения:

- вред для общества;
- противоправность;
- виновность;
- реальность правонарушения;
- наказуемость.

Состав правонарушения — это совокупность установленных законом элементов, наличие которых позволяет, квалифицировать деяние как определенное правонарушение.

Состав правонарушения включает четыре взаимосвязанных компонента, при отсутствии хотя бы одного из которых отсутствует состав правонарушения.

Объект правонарушения — это общественные отношения, которым правонарушением причинен вред. Это различного рода публичные и частные ценности: правопорядок, окружающая природная среда, собственность, права и свободы человека и т.п.

Субъект правонарушения — это деликтоспособный индивид или организация, совершившие правонарушение. Для физического лица деликтоспособность включает достижение определенного возраста и вменяемость, для организации — наличие статуса юридического лица.

Объективная сторона правонарушения — это характеристика противоправного деяния: время, место, орудие, способ, обстановка совершения правонарушения, размер и характер вредных последствий, причинная связь между деянием и вредными последствиями. Таким образом, объективная сторона представляет собой единство трех элементов — противоправного деяния, вреда и причинной связи между ними.

Субъективная сторона правонарушения — это сознательно-волевые признаки правонарушения, основным из которых является вина (умысел или неосторожность), а факультативными — мотивы и цели правонарушителя. Мотивы представляют собой побудительные причины, которыми руководствовался нарушитель, цели — конечный результат, к которому стремился правонарушитель.

Все правонарушения принято делить на две группы — преступления и проступки. Главными критериями их деления являются:

значимость регулируемого правом общественного отношения, ставшего объектом противоправного посягательства (жизнь человека, материальные ценности и т.д.);

размер причиненного ущерба;

способ, время и место совершения противоправного деяния;

личность правонарушителя.

По Уголовному кодексу *преступлением* признается виновное, общественно опасное деяние (действие или бездействие), запрещенное уголовным законом под угрозой наказания (ст. 14 УК РФ). За совершение уголовных преступлений предусмотрены следующие виды наказаний: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, лишение специального, воинского или почетного звания, классного чина и государственных наград, обязательные работы, исправительные работы, ограничение по военной службе, ограничение свободы, принудительные работы, арест, содержание в дисциплинарной воинской части, лишение свободы на определенный срок, пожизненное лишение свободы, смертная казнь (ст.44 УК РФ).

Все непреступные правонарушения или проступки классифицируются применительно к отраслям права:

административное — таковым признается посягающее на государственный или общественный порядок, собственность, права и свободы граждан, на установленный порядок управления противоправное виновное действие или бездействие, за которое законодательством предусмотрена административная ответственность.

За совершения административных правонарушений предусмотрены административные взыскания: предупреждение, административный штраф, конфискация орудия совершения или предмета административного правонарушения, лишение специального права, предоставленного физическому лицу, административный арест, административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства, дисквалификация, административное приостановление деятельности. Их полный перечень закреплен в законе (ст.3.2 КоАП РФ).

Гражданские проступки — это нарушение гражданами или организациями имущественных или неимущественных прав, принадлежащих субъектам права. Различают договорные и внедоговорные правонарушения. Первые связаны с нарушением обязательств стороной гражданско-правового договора (взыска-

ние: возмещение убытка), вторые — с несоблюдением или неисполнением требований гражданско-правовых норм (взыскание: опровержение).

Дисциплинарные проступки представляют собой противоправные деяния субъекта трудового права, состоящие в неисполнении, нарушении трудовых обязанностей и запрещенные санкциями, содержащимися в нормах, законодательства о труде. Совершая дисциплинарный проступок, правонарушитель нарушает трудовую, учебную, служебную, производственную, воинскую дисциплину (прогулы, опоздания на работу, пропуски учебных занятий, невыполнение распоряжений администрации). Санкции норм права выражаются в следующих взысканиях: замечание, выговор, строгий выговор, перевод на низшую должность, увольнение и пр.

На основании рассмотренных видов правонарушений выделим следующие виды юридической ответственности:

- гражданско-правовая ответственность (гражданское правонарушение);

- дисциплинарная ответственность (дисциплинарный, служебный проступок);

- административная ответственность (административный проступок);

- уголовная ответственность (преступление)[1],

На практике большое значение приобретает правильная классификация ответственности, так как для гражданской ответственности характерна презумпция ответственности, а для уголовной и административной — презумпция невиновности.

Уголовная ответственность применяется за совершение преступлений как наиболее общественно опасных деяний. В Российской Федерации их исчерпывающий перечень определен Уголовным кодексом. Наказания назначаются только по приговору суда. К уголовной ответственности в России привлекаются лишь физические лица.

[1] См.: Черданцев А.Ф., Кожевников С. Н. О понятии и содержании юридической ответственности // Правоведение. —2001. — №5. — С. 29.

Административная ответственность — применяется за совершение административных проступков. К административной ответственности привлекаются как физические лица, так и организации за нарушения норм отраслей публичного права. Субъектами, имеющими полномочия на привлечение к административной ответственности, являются многочисленные государственные органы исполнительной власти и их должностные лица. Административная ответственность применяется не в порядке подчиненности, не влечет судимости и увольнения с работы.

Дисциплинарная ответственность применяется за нарушения трудовой, служебной, учебной, воинской дисциплины в рамках линейных отношений «работник — работодатель» или «начальник — подчиненный». В Российской Федерации нормативную базу дисциплинарной ответственности составляет Трудовой кодекс РФ, Федеральный закон «О полиции» и другие нормативные акты. Таким образом, привлечение к дисциплинарной ответственности осуществляется в порядке служебной подчиненности. Дисциплинарные взыскания могут дополняться восстановительными мерами материального (имущественного) характера.

Гражданско-правовая ответственность применяется за нарушения гражданско-правовых обязательств. Данный вид ответственности в Российской Федерации регламентируется Гражданским кодексом РФ. Сфера применения гражданско-правовой ответственности находится в отраслях частного права. Она всегда носит имущественный характер. Главной целью здесь является полное возмещение вреда, причиненного правонарушением. Субъекты, привлекающие к гражданско-правовой ответственности, — это суды РФ и третейские суды.

8.3. Содержание УК РФ и КоАП РФ по вопросам ответственности в сфере информационной безопасности

№ статьи	Название статьи	Санкция (максимальная)
1	2	3
Уголовный кодекс РФ		
ст. 272	Неправомерный доступ к компьютерной информации	Лишение свободы на срок до пяти лет.
ст. 273	Создание, использование и распространение вредоносных компьютерных программ	Лишение свободы на срок до семи лет.
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	Лишение свободы на срок до пяти лет.
ст. 159	Мошенничество	Лишение свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.
ст. 165	Причинение имущественного ущерба путем обмана или злоупотребления доверием	Лишение свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до двух лет либо без такового.

1	2	3
ст. 275	Государственная измена	Лишение свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет.
ст. 276	Шпионаж	Лишение свободы на срок от десяти до двадцати лет.
ст. 283	Разглашение государственной тайны	Лишение свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.
ст. 284	Утрата документов, содержащих государственную тайну	Лишение свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
ст. 129	Клевета	Лишение свободы на срок до трех лет.
ст. 130	Оскорбление	Ограничение свободы на срок до двух лет.
ст. 137	Нарушение неприкосновенности частной жизни	Лишение свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.
ст. 138	Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений	Лишение свободы на срок до четырех лет.

1	2	3
Ст. 138.1	Незаконный оборот специальных технических средств, предназначенных для негласного получения информации	Лишение свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
ст. 140	Отказ в предоставлении гражданину информации	Лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет
ст. 146	Нарушение авторских и смежных прав	Лишение свободы на срок до шести лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.
ст. 147	Нарушение изобретательских и патентных прав	Лишение свободы на срок до пяти лет.
ст. 155	Разглашение тайны усыновления (удочерения)	Арест на срок до четырех месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
ст. 183	Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	Лишение свободы на срок до семи лет.

1	2	3
ст. 185.6	Неправомерное использование инсайдерской информации	Лишение свободы на срок от двух до шести лет со штрафом в размере до ста тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет либо без такового с лишением права занимать определенные должности либо заниматься определенной деятельностью на срок до четырех лет или без такового.
ст. 187	Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов	Лишение свободы на срок до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового.
Ст. 242	Незаконное распространение порнографических материалов или предметов	Лишение свободы на срок до двух лет.
Ст. 242.1	Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних	Лишение свободы на срок до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет или без такового и с ограничением свободы на срок до двух лет либо без такового
ст. 310	Разглашение данных предварительного расследования	Арест на срок до трех месяцев.
ст. 311	Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса	Лишение свободы на срок до пяти лет.

1	2	3
ст. 320	Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа	Лишение свободы на срок до пяти лет.
Кодекс об административных правонарушениях РФ		
ст. 5.39.	Отказ в предоставлении информации	Штраф в размере от одной тысячи до трех тысяч рублей.
ст. 7.12.	Нарушение авторских и смежных прав, изобретательских и патентных прав	Штраф на граждан в размере от одной тысячи пятисот рублей с конфискацией контрафактных экземпляров; штраф на юридических лиц — от тридцати тысяч до сорока тысяч рублей.
ст. 13.11.	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	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.

1	2	3
ст. 13.12.	Нарушение правил защиты информации	Штраф 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 — штраф на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от одной тысячи до одной тысячи пятисот рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц — от одной тысячи до одной тысячи пятисот рублей; на юридических лиц — от десяти тысяч до пятнадцати тысяч рублей или административное приостановление деятельности на срок до девяноста суток.

1	2	3
ст. 13.13.	Незаконная деятельность в области защиты информации	Штраф на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц — от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц — от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой — штраф на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц — от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.
ст. 13.14.	Разглашение информации с ограниченным доступом	Штраф на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц — от четырех тысяч до пяти тысяч рублей.

1	2	3
ст. 20.23.	Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	Штраф на должностных лиц в размере от четырех тысяч до пяти тысяч рублей — штраф на граждан в размере от двух тысяч до двух тысяч пятисот рублей с конфискацией специальных технических средств, предназначенных для негласного получения информации; на должностных лиц — от трех тысяч до пяти тысяч рублей с конфискацией специальных технических средств, предназначенных для негласного получения информации.

Контрольные вопросы:

1. Что понимается под термином «юридическая ответственность»?
2. Перечислите признаки юридической ответственности.
3. Перечислите основания юридической ответственности.
4. Перечислите принципы юридической ответственности.
5. Что такое правонарушение и каковы его признаки?
6. Что такое состав правонарушения?
7. Перечислите виды правонарушений.
8. Перечислите и раскройте сущность видов юридической ответственности.
9. Приведите составы преступлений в рбласти информационной безопасности, предусмотренные УК РФ.
10. Приведите составы правонарушений, предусмотренные КоАП РФ.

ЛИТЕРАТУРА

I. Официальные документы и нормативные акты.

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.). — М.: ИНФРА-М, 2005.48 с.

2. Всемирная конвенция об авторском праве» (Женева, 6 сентября 1952 года. Пересмотрена в Париже 24 июля 1971 года).

3. Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года.

4. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

5. Окинавская хартия глобального информационного общества. Окинава, 22 июля 2000 года.

6. Всеобщая декларация прав человека от 10.12.1948 г.

7. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.

8. Конвенция, учреждающая Всемирную организацию интеллектуальной собственности (Стокгольм, 14 июля 1967 года, в редакции от 2 октября 1979 года).

9. Закон РФ от 27 декабря 1991 г. №2124-1 «О средствах массовой информации» (с изменениями 14 июня, 11, 21 июля 2011г.).

10. Закон РФ от 21 июля 1993 г. №5485-1 «О государственной тайне» (в ред. от 18, 19 июля 2011 г.).

11. Федеральный закон от 27.12.2002 №184-ФЗ (ред. от 21.07.2011) «О техническом регулировании».

12. Федеральный закон от 07.07.2003 №126-ФЗ (ред. от 18.07.2011) «О связи» (с изм. и доп., вступающими в силу с 29.09.2011).

13. Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне».

14. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) «Об информации, информационных технологиях и о защите информации».

15. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 25.07.2011) «О персональных данных».

16. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности».

17. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 21.07.2011) (с изм. и доп., вступающими в силу с 07.08.2011).

18. Гражданский кодекс Российской Федерации (часть первая от 30.11.1994 N 51-ФЗ в ред. от 06.04.2011; часть вторая от 26.01.1996 №14-ФЗ в ред. от 19.10.2011; часть третья от 26.11.2001 №146-ФЗ в ред. от 30.06.2008; часть четвертая от 18.12.2006 №230-ФЗ в ред. от 04.10.2010).

19. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 19.07.2011).

20. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 21.07.2011) (с изм. и доп., вступающими в силу с 21.10.2011).

21. Доктрина информационной безопасности Российской Федерации.— Утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр-1895.

22. Стратегия Национальной безопасности Российской Федерации до 2020 года.— Утверждена Указом Президента Российской Федерации 12 мая 2009 года № 537.

23. Военная Доктрина Российской Федерации,— Утверждена Указом Президента Российской Федерации 5 февраля 2010 года №146.

24. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

25. Указ Президента Российской Федерации от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера».

26. Распоряжение Президента Российской Федерации от 16 апреля 2005 года № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».

27. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информа-

ционно-телекоммуникационных сетей международного информационного обмена».

28. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

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

30. Постановление Правительства Российской Федерации от 2 августа 1997 г. № 973 «Об утверждении положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам или международным организациям».

31. Постановление Правительства Российской Федерации от 22 августа 1998 г. № 1003 «Об утверждении положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне».

32. Постановление Правительства Российской Федерации от 1 8 сентября 2006 г. №573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны».

33. Постановление Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

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

II. Монографии, учебники, учебные пособия.

35. Корнеев И.К. Защита информации в офисе / И.К. Корнеев. — М.: ТК Велби, Проспект, 2007. — 336 с.

36. Степанов А.Г. Защита коммерческой тайны / Степанов А.Г., О.О. Шерстнева. — М.: Альфа-Пресс, 2006. — 180 с.

37. Ищейнов В.Я. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — М.: ФОРУМ, 2009. —256 с.

38. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. — СПб.: Питер, 2008. — 272 с.

39. Комплексная система защиты информации на предприятии: учебник для вузов / под ред. проф. Б.И. Пугинского. — М.: Издательский дом «Городец», 2008. — 368 с.

40. Гришина Н.В. Комплексная система защиты информации на предприятии: учебное пособие / Н.В. Гришина. — М.: ФОРУМ, 2009. — 240 с.

41. Компьютерные преступления: квалификация, расследование, экспертиза. Часть 2 / под ред. В.Н. Черкасова. — Саратов: СЮИ МВД России, 2004. — 372 с.

42. Мельников В. П. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб. заведений / В. П. Мельников, С.А. Клейменов, А.М. Петраков; под. ред. С.А. Клейменова. — 3-е изд., стер. — М.: Издательский центр «Академия», 2008. — 336 с.

43. Романов О.А. Организационное обеспечение информационной безопасности : учебник для студ. высш. учеб. заведений / О. А. Романов, С. А. Бабин, С. Г. Жданов. — М.: Издательский центр «Академия», 2008. —- 192 с.

44. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов.— Минск, 2005. — 304 с.

45. Правовое обеспечение информационной безопасности / под общей научной редакцией В.А. Минаева [и др.]. — М.: Маросейка, 2008. — 368 с.

46. Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С. Я. Казанцев [и др.]; под ред. С.Я. Казанцева. — М.: Издательский центр «Академия», 2005. — 240 с.

47. Клебанов Л.Р. Уголовно-правовая охрана коммерческой, налоговой и банковской тайны / Л.Р. Клебанов. — М.: Юрлитинформ, 2006. — 192 с.

Учебное издание

Филиппова Неля Викторовна

Правовое обеспечение информационной безопасности
Российской Федерации

Учебное пособие

Редактор Н.В. Соболева
Компьютерная верстка В.В. Павлов

Подписано в печать 10.02.2012 г. Формат 60x84'/16
Усл. печ. л. 5,25. Усл. кр.-отт.5,78. Уч.-изд. л. 5,0
Печать офсетная
Тираж 200 экз. Заказ №19

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53