

ФЕДЕРАЛЬНОЕ АГЕНТСТВО РФ ПО НАУКЕ И ОБРАЗОВАНИЮ

ГОУ ВПО «ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра социологии, психологии и права

Э.Н. Камышев

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Томск 2009

Камышев Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2009. - 95 с.

Учебное пособие по курсу «Информационная безопасность и защита информации» составлено профессором, доктором философских наук, действительным членом (академиком) международной академии наук высшей школы Эдуардом Николаевичем Камышевым по программе подготовки студентов в Томском политехническом университете. Оно предназначено для студентов специальности «Документоведение и документационное обеспечение управления» при подготовке к экзаменам и зачетам, а также для студентов других факультетов и специальностей при овладении правовыми основами бизнес-управления в условиях РФ и Томской области.

Пособие составлено исходя из требований государственного стандарта специальности «Документоведения» и разработанным в соответствии с ним учебным планом и рабочей программой по одноименному курсу.

Печатается по постановлению кафедры социологии, психологии и права Томского политехнического университета.

© Камышев Эдуард Николаевич, 2009.

Содержание

ПРЕДИСЛОВИЕ

ТЕМА 1. СТАНОВЛЕНИЕ КОНЦЕПТУАЛЬНЫХ ПРАВОВЫХ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ.....	6
1.1. Зарождение информационного права в РФ.....	6
1.2. Становление информационной безопасности в 90-е годы.....	8
ТЕМА 2. НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОЙ СФЕРЕ.....	9
2.1. Понятие информационной безопасности.....	9
2.2. Интересы Российской Федерации в информационной сфере.....	11
2.3. Виды угроз информационной безопасности РФ.....	13
2.3. Источники угроз информационной безопасности Российской Федерации.....	16
ТЕМА 3. СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ.....	17
3.1. Направления обеспечения информационной безопасности.....	17
.....	20
3.2. Понятие методов обеспечения информационной безопасности Российской Федерации.....	20
3.3. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.....	21
ТЕМА 4. ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ.....	24
4.1. Объект и предмет правового обеспечения информационной безопасности РФ.....	24
4.2. Задачи и основные принципы государственной политики обеспечения информационной безопасности РФ.....	29
ТЕМА 5. НОРМАТИВНАЯ ПРАВОВАЯ БАЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ.....	32
5.1. Состояние нормативного правового обеспечения информационной безопасности.....	32
5.2. Нормативное правовое регулирование отдельных направлений информационной безопасности.....	35
5.3. Основные направления совершенствования нормативного правового обеспечения информационной безопасности РФ.....	38
ТЕМА 6. ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ.....	41
6.1. Виды информации и право на нее.....	41
6.2. Организация доступа к информации и ограничение в праве на нее.....	43
6.3. Информационные ресурсы.....	45
6.4. Защита информации и прав субъектов в области информационных процессов и информатизации.....	47
6.5. Права и обязанности субъектов в области защиты информации.....	48
ТЕМА 7. ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ.....	50
7.1. Интересы личности в информационной сфере.....	50
7.2. Профессиональные тайны как подсистема информационной безопасности личности.....	54
ТЕМА 8. ЗАЩИТА ЛИЧНЫХ ИМУЩЕСТВЕННЫХ И НЕИМУЩЕСТВЕННЫХ ПРАВ ЛИЧНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ.....	57
8.1. Честь и достоинство.....	58
8.2. Авторское право.....	60
8.3. Доменные имена: проблемы правового регулирования.....	64
ТЕМА 9. СМИ КАК ОБЪЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО ОБЩЕСТВА.....	66
9.1. Правовые основы СМИ.....	66
9.2. Организация деятельности средств массовой информации.....	68
9.3. Отношения средств массовой информации с гражданами и организациями.....	71
9.4. Права и обязанности журналиста.....	72
9.5. Ответственность за нарушение законодательства о средствах массовой информации.....	74

ИНФОРМАЦИИ.....	74
ТЕМА 10. РЕКЛАМА КАК СОСТАВЛЯЮЩАЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА	75
10.1. Понятие рекламы.....	75
10.2. Особенности рекламы в радио- и телепрограммах	78
10.3. Особенности рекламы отдельных видов товара.....	78
10.4. Защита несовершеннолетних при производстве, размещении и распространении рекламы	80
10.5. Права и обязанности рекламодателей, рекламопроизводителей и рекламораспространителей	81
ТЕМА 11. ГОСУДАРСТВЕННАЯ ТАЙНА – ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУ- ДАРСТВА.....	82
11.1. Понятие государственной тайны, полномочия власти в области отнесения сведений к государственной тайне.....	82
11.2. Перечень сведений, составляющих государственную тайну	83
11.3. Отнесение сведений к государственной тайне и их засекречивание	85
11.4. Рассекречивание сведений и их носителей	88
11.5. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений	89
11.6. Шпионаж и разглашение государственной тайны.....	91
ТЕМА 12. ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ – НОВЫЙ МЕТОД ОБЕСПЕЧЕНИЯ ИНФОРМА- ЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА.....	92
12.1. Понятие электронной цифровой подписи.....	92
12.2. Принципы и условия использования электронной цифровой подписи.....	93
12.3. Обязательства владельца по принятии сертификата ключа подписи и защита персональных данных.....	95
12.4. Использование электронной цифровой подписи в сфере государственного управления и корпоративных информационных системах.....	96

ПРЕДИСЛОВИЕ

Настоящее учебное пособие создано с целью оказания помощи студентам специальности «документоведение и документационное обеспечение управления» в аудиторном и самостоятельном изучении сравнительно нового и сложного курса «Информационная безопасность и защита информации». Оно способно заменить собой лекции и практические занятия по курсу и стать основой для самостоятельной подготовки студентов к экзаменам и зачетам.

Необходимость написания учебного пособия вызвана, прежде всего, дефицитом учебной литературы в данной области, а также сложностью изучения многообразного нормативного материала, его постоянного изменения и корректирования.

Данное учебное пособие предполагает в процессе изучения курса дополнительное использование справочного материала по рассматриваемым вопросам, в частности, различного рода комментариев к различным статьям кодексов и федеральных законов, принятых в этой области, анализ уже имеющейся судебной практики.

В основу настоящего пособия положены официальные тексты действующих Гражданского Кодекса Российской Федерации (далее – ГК или ГК РФ), Всеобщей Декларации прав человека, Конституции Российской Федерации, Уголовного кодекса (УК), Доктрины информационной безопасности РФ, и Федеральных законов: «О средствах массовой информации», «Об информации, информатизации и защите информации», «О государственной тайне», «Об авторском праве и смежных правах», «О праве на информацию», «Об электронной цифровой подписи», а также материалы конференций, посвященных информационной безопасности.

Все замечания и предложения по улучшению настоящего пособия просим направлять по адресу: 634050, Томск, пр. Ленина, 30. Томский политехнический университет. Кафедра социологии, психологии и права.

Тел.: 8-3822-563466, 563545 (факс)

ТЕМА 1. СТАНОВЛЕНИЕ КОНЦЕПТУАЛЬНЫХ ПРАВОВЫХ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

1.1. Зарождение информационного права в РФ

В настоящее время информационно-коммуникативная глобализация является наиболее динамичным и ярким интеграционным процессом, включая в себя развитие телекоммуникационных систем с использованием космического пространства и быстрого роста информационных кабельных сетей и информационных комплексов, развития персональных систем связи и компьютеризации жизнедеятельности человечества. Человечество стало жить в “электронном поле”, оперативно получая богатую информацию путем слухового и зрительного восприятия.

В современном мире на государственном уровне формируется единый планетарный комплекс информационных ресурсов планеты. Открывается поле для восприятия информации всем населением земли. Растет сервисное обслуживающее устройство для мыслительной деятельности человека. С другой стороны, информатизация заостряет проблему развития самого человека, который должен соответствовать высокому уровню интеллектуальной техники.

На практике радио, телевидение, пресса, новые информационные технологии уже перекрывают и трансформируют воздействие таких традиционных факторов формирования духовного мира личности, как семья, школа, учитель, священник, библиотеки и т.д. Они непрерывно усиливают свое “мягкое давление” и влияние (soft power) на психику человека, его образовательный и культурный потенциал, личное поведение и жизненные интересы.

Информационные системы (и технологии, лежащие в их основе) существовали с момента появления общества, ибо на любой стадии развития общество требует для своего управления систематизированной (обработанной) информации. По мере развития менялись технологии, но, до самого последнего момента, не изменялись правовые основы существования информационных систем. Во времена бывшего СССР проблемы безопасности традиционно рассматривались, прежде всего, в их военном и военно-техническом аспекте, в рамках концепции защиты рубежей. Наконец, наступил момент (начало восьмидесятых годов), когда информационные технологии стали оказывать столь существенное влияние на общественные отношения, что появилась новая отрасль права – информационное законодательство. Ее формирование происходит в настоящий момент и будет продолжаться, следуя за потребностями человека, общества, государства.

Сам термин «информационная безопасность» начал употребляться в 90-х годах. Первоначально вопросы информационной безопасности ассоциировались с безопасностью самой информации, защитой информации, в большей степени – с защитой государственной тайны.

Тезис о том, что информационная безопасность – это показатель состояния информационной культуры общества, вопрос о необходимости законодательного регулирования института секретности в нашей стране впервые поднялся в прессе в 1988 году. Уже в 1990 году на проходившей в Обнинске конференции “Безопасность информации” рассматривался первый проект закона “О защите информации”. Вопросы информационных отношений в сфере научного творчества, доступа к информации, роли и места государственной секретности обсуждались научной общественностью на конференции “Свобода научной информации и охрана гостайн”, проходившей в Библиотеке Академии наук в Ленинграде осенью 1991 года. Созданный по рекомендации этой конференции общественный Совет по свободе научной информации сыграл определенную роль в пропаганде становления правового режима защиты государственной тайны в нашей стране.

В 1991 году Верховным Советом РСФСР была принята Декларация прав и свобод человека и гражданина, объявившая право каждого на поиск, получение и свободное распро-

странение информации и возможное законодательное ограничение этого права исключительно в целях охраны личной, семейной, профессиональной, коммерческой, государственной тайны, а также нравственности. В феврале 1992 года, после распада СССР в Ленинграде Гостехкомиссией при Президенте была проведена научно-практическая конференция "Правовая информатизация России", намечены конкретные шаги по разработке и совершенствованию нормативно-правовой базы информационных отношений. К обсуждению этих вопросов подключилась деловая и вузовская общественность, ряд конференций и семинаров был проведен в Москве и в Санкт-Петербурге.

Первые шаги по гармонизации информационного законодательства в рамках ставших независимыми государств, ранее входивших в состав СССР, были предприняты в 1993 году. 23 мая 1993 года на одном из первых заседаний Межпарламентской Ассамблеи государств – участников Содружества Независимых государств был принят рекомендательный законодательный акт "О принципах регулирования информационных отношений в государствах – участниках Межпарламентской Ассамблеи". Этим актом преследовалась цель создания единых правовых условий для:

- реализации прав граждан, организаций на информацию;
- использования современных информационных технологий;
- осуществления предпринимательской деятельности в этой сфере;
- информационного обмена внутри государств и между государствами – участниками Межпарламентской Ассамблеи;
- обеспечения защиты и конфиденциальности информации.

Принятие рекомендательного акта имело большое значение, поскольку национальное законодательство в этой сфере у государств Содружества в тот период практически отсутствовало. Данный рекомендательный законодательный акт закладывал основные принципы, на которых целесообразно создавать законы в области информационных отношений, был призван служить ориентиром при разработке национальных законодательств.

В целях обеспечения единства юридической терминологии, однозначного понимания используемых терминов в статье 2 рекомендательного акта приводились определения понятий, которые будут составлять исследовательскую базу данного пособия.

Информация – сведения о фактах, событиях, явлениях и процессах (независимо от формы их представления).

Информация с ограниченным доступом – информация, для которой установлен специальный режим хранения и использования.

Документ – зафиксированная на материальном носителе информация с указанием источника ее происхождения и других реквизитов в соответствии с установленными стандартами.

Информационная технология – организованная совокупность процессов, элементов, устройств или методов, используемых для обработки информации.

Правовой режим информации – нормативно установленные правила, определяющие степень открытости, порядок документирования, доступа, хранения, распространения и защиты информации, а также исключительные права на информацию.

Информационные отношения – отношения по поводу сбора, накопления, хранения и использования информации.

Учитывая степень проникновения современных информационных технологий в общественные отношения, можно говорить о существовании предметных информационных технологий. Попытки оставить за информационными технологиями только роль обеспечивающих (инструментарий по обработке информации) сегодня оказываются несостоятельными и приводят к многократным случаям преступных деяний с их использованием.

Повышение роли информации и информационных технологий в совершенствовании государства и общества, развитие информационных ресурсов в единое информационное пространство привело как к трансформации сложившихся, традиционных для права социальных

норм и отношений, так и к появлению новых отношений, отражающих особые условия и правила поведения субъектов в информационной среде – информационных отношений. И как следствие – информационного права.

Основные принципы правового регулирования информационных отношений, определенные вышеуказанным рекомендательным актом, включают в себя законодательное закрепление прав всех субъектов на свободный поиск, получение, использование и распространение информации; установление правового режима и правовых форм ее защиты, обеспечение доступности открытой информации.

Рекомендательный законодательный акт подразделил информацию на имеющую режим открытого либо ограниченного доступа, определив при этом, что правовой режим конкретных видов информации устанавливается национальным законодательством либо на его основе законным владельцем информации.

В рекомендательном акте также был приведен перечень видов информации, доступ к которой не может быть ограничен. Это информация о чрезвычайных ситуациях, угрожающих безопасности и здоровью граждан, стихийных бедствиях, катастрофах и их последствиях; о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства и обеспечения правопорядка; о законодательных актах; о фактах нарушения законности государственными органами и их должностными лицами; о привилегиях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям; об имевших место политических преследованиях и репрессиях.

Наряду с другими формами распространения информации рекомендательным законодательным актом предусмотрена возможность распространения информации в качестве товара в порядке и на условиях, установленных национальным законодательством.

Законодательный рекомендательный акт содержит общие положения о защите информации. Защита информации осуществляется в целях:

- предотвращения утечки, хищения, утраты, искажения, подделки, несанкционированных действий по ее уничтожению, модификации, копированию, блокированию информации и других форм незаконного вмешательства в информационные системы;
- обеспечения конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в информационных системах;
- обеспечения прав субъектов информационных отношений;
- сохранения секретности (конфиденциальности) информации.

Развитие этих положений должно осуществляться на уровне национального законодательства.

В акт включена международно-правовая норма, в соответствии с которой в случае, если государство не имеет законодательства по защите информации или это законодательство не соответствует международным стандартам, другие государства могут наложить ограничения на передачу информации в это государство.

1.2. Становление информационной безопасности в 90-е годы.

В последующие годы в России принят ряд законов по вопросам информационных отношений и информатизации (например, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «Об электронной цифровой подписи»).

В 1993 году в России был принят и введен в действие первый Закон «О государственной тайне».

В Российской Федерации вопросы информационной безопасности и основ защиты государственной тайны включены в новые образовательные стандарты и вузовские учебные планы.

Решением Высшего Совета Союза Беларуси и России 28 апреля 1999 года утверждена Концепция безопасности Союза, в которой указаны жизненно важные интересы Союза в информационной сфере.

Ориентиром в постановке работы по обеспечению информационной безопасности может служить утвержденная в сентябре 2000 года Президентом России Доктрина информационной безопасности Российской Федерации.

Она разработана в целях согласования усилий всех субъектов законодательной инициативы, федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации по совершенствованию и развитию нормативного правового обеспечения информационной безопасности Российской Федерации, а также федеральных органов исполнительной власти, осуществляющих подготовку проектов международных договоров Российской Федерации.

Правовой основой Концепции являются Конституция Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации, Концепция безопасности Союза Беларуси и России, Концепция национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации и федеральное законодательство, регулирующие вопросы формирования и развития системы обеспечения национальной безопасности Российской Федерации.

Концепция отражает совокупность официальных взглядов на состояние, цели, задачи, основные направления и первоочередные мероприятия по дальнейшему развитию системы правовых норм, регулирующих общественные отношения в области обеспечения информационной безопасности Российской Федерации.

Концепция нормативного правового обеспечения информационной безопасности дополняет положения других нормативных правовых актов Президента Российской Федерации, направленных на развитие информационной сферы Российской Федерации, обеспечение безопасности национальных интересов в этой сфере.

Концепция служит основой при разработке планов законодательной работы в области нормативного правового обеспечения информационной безопасности; планов законотворческой деятельности субъектов Российской Федерации в области формирования региональных систем обеспечения информационной безопасности; правовых доктрин регулирования отношений по отдельным вопросам нормативного правового обеспечения информационной безопасности Российской Федерации, а также концепций нормативных правовых актов, регулирующих отношения в области обеспечения информационной безопасности; планов подготовки проектов международных договоров Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти в области обеспечения

ТЕМА 2. НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОЙ СФЕРЕ

2.1. Понятие информационной безопасности

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

ства, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Появляется новый термин “информационно-психологическое оружие” – специальное оружие, основанное на применении разрушающего информационно-психологического и информационно-управляющего воздействия на психику человека для его принуждения или уничтожения.

Информационная война, которая уже идет, - новое понятие в области мировой науки, включающая различные аспекты политической, экономической и социально-культурной деятельности. В современной России это особенно заметно на примере средств массовой информации.

Объектом информационного воздействия современного вооружения является общественное сознание человека, его дух, воля, идейные установки и представления, при этом используются методы, ведущие к подавлению норм нравственности.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Это обусловлено, прежде всего, следующими основными обстоятельствами:

- в условиях реализации конституционных прав граждан на свободу экономической, информационной и интеллектуальной деятельности существенно расширяются потребности социально активной части общества в расширении информационного взаимодействия как внутри страны, так и с внешним миром;

- интенсивное развитие информационной инфраструктуры и, прежде всего, информационно- телекоммуникационных систем, средств и систем связи, интеграция в мировое информационное пространство, а также информатизация практически всех сторон общественной жизни, деятельности органов государственной власти и управления существенно усилили зависимость эффективности функционирования общества и государства от состояния информационной сферы;

- индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития человечества является одной из наиболее динамично развивающихся сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением и определяющей наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке;

- информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство, достижение противоборствующими странами определенных стратегических и тактических политических целей и с учетом возрастающей зависимости российского общества от устойчивого функционирования информационной инфраструктуры обеспечение безопасности интересов в этой сфере становится важным фактором национальной безопасности любого государства;

- индивидуальное, групповое и массовое сознание людей все в большей степени зависят от деятельности средств массовой информации и массовой коммуникации;

Информационная сфера представляет собой совокупность субъектов информационной сферы, информации, информационной инфраструктуры, системы сбора, формирования, обработки, распространения и использования информации, а также системы регулирования возникающих при этом общественных отношений.

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

Информационная безопасность предполагает и означает состояние, когда в обществе созданы условия, обеспечивающие свободное развитие личности, семьи, государства, которые дают возможность объективно оценивать исторический процесс, истинную обстановку в

мире, стране, регионе, вырабатывать и принимать самостоятельные решения на основе современной, достоверной информации, практического осознания и научного мировоззрения всего спектра гуманитарного знания, составляющего и создающего истинную духовность каждого народа.

Согласно Доктрине информационной безопасности, интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина:

- на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития
- на защиту информации, обеспечивающей личную безопасность.

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

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

В начале XXI века выдвигается одна из главных стратегических, геополитических задач России очень высокого политического уровня, которая заключается в создании предпосылок для развития единого информационного пространства, способного обеспечить вхождение Российской Федерации в мировую информационную систему, поднятие эффективности его использования в деле прогрессивного общественного развития, возрождения нашей страны. Гражданское общество и государство России уже имеют свои мощные информационные ресурсы, средства, источники, обеспечивающие информационную безопасность страны. Создается правовая база защиты человека и общества от информационных угроз. Информация играет важнейшую роль в развитии науки и техники, всех областей народного хозяйства и человеческой деятельности.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

2.2. Интересы Российской Федерации в информационной сфере

Доктрина информационной безопасности выделяет четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

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

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

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

Для достижения этого, в частности, требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

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

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

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

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2.3. Виды угроз информационной безопасности РФ.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
2. угрозы информационному обеспечению государственной политики Российской Федерации;
3. 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;
4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами; блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории и другое.

Угрозами 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 могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться: противоправные сбор и использование информации; нарушения технологии обработки информации; разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации и многое другое.

Нетрудно заметить, что приведенные выше четыре вида угроз информационной безопасности РФ составляют, по сути, две группы:

Первая группа (к ней относятся угрозы первого и второго вида) – угрозы, обусловленные негативными явлениями, процессами и действиями в сфере власти и гражданского общества, в сфере деятельности государственных структур разных уровней, средств массовой информации, правоохранительных органов. Появление этих угроз связано прежде всего с неадекватными формами взаимодействия государства и общества, власти и гражданина, личности и права.

В конкретизированной формулировке к угрозам данной группы относятся, например, следующие:

- Принятие властными органами разных уровней нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности.

- Противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений.

- Монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами.

- Низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики и т.д.

К основным характеристикам рассматриваемой группы угроз информационной безопасности РФ следует отнести прежде всего отсутствие или нечеткость критерия определения какого-то негативного явления в информационной сфере как “угрозы информационной безопасности РФ”. По ряду ключевых вопросов, касающихся информационной безопасности, нормативная база далеко неполна, несовершенна или даже противоречива.

Не менее важна и такая характеристика как мимикризация угроз информационной безопасности первой группы ставшей закономерным явлением в информационном пространстве России, которое имеет на современном этапе дискретный характер, является ареной постоянно меняющегося баланса различных социальных сил и потоков и внешних влияний.

Следует отметить также тотальность угроз информационной безопасности в рассматриваемой группе, выражающейся в их способности проникновения через самые традиционные и примитивные формы и каналы информации в самые широкие слои общества.

Долгосрочный и устойчивый характер действия указанных угроз, обусловленный тем, что их актуализация в реальной общественной жизни поражает такие сферы, как социально-психологическое состояние групп, коллективов, индивидуумов, сферу традиций и ценностей, т.е. такие пласты общественной жизни, которые отличаются консерватизмом и временной стабильностью.

Вторая группа угроз информационной безопасности (к ней в Доктрине отнесены угрозы третьего и четвертого видов) – это угрозы, которые обусловлены негативными явлениями и противозаконными действиями в рамках существующих информационных и телекоммуникационных систем, систем связи, а также на рынке информационных технологий.

Эти угрозы существенным образом отличаются от угроз, относящихся к первой группе, прежде всего тем, что в их формировании и реализации доминируют не правовые, духовно-идеологические и социально-психологические аспекты, а технические и организационно-технологические.

В этой группе угроз как для отдельных стран, так и для мирового сообщества в целом особую опасность представляет информационный терроризм. Определены различные приемы достижения террористических целей в информационном киберпространстве, как например модификации в информационных системах и системах управления; нанесение ущерба отдельным физическим элементам киберпространства (разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств, биологические и химические средства разрушения элементной базы и др.); кража или уничтожение информационного, программного или технического ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.; захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявление своих требований, уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и др.

Организованные преступные группировки, коммерческие структуры быстро оценили широкие возможности и преимущества специальных технических средств по добыванию конфиденциальной информации о деятельности как государственных структур, так и субъектов негосударственного сектора (бирж, банков, частных фирм и т.п.).

2.3. Источники угроз информационной безопасности Российской Федерации

Согласно Доктрине, источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

1. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
2. стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
3. обострение международной конкуренции за обладание информационными технологиями и ресурсами;
4. деятельность международных террористических организаций;
5. увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
6. деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
7. разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира.

Внутренними источниками угрозы информационной безопасности являются:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождаемая тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

ТЕМА 3. СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. Направления обеспечения информационной безопасности

Сегодня правомерно утверждать: чем большими информационными возможностями обладает государство, тем вероятнее (при прочих равных условиях) оно может добиться стратегических преимуществ. Если Россия, ее государственность, гражданское общество действительно стремятся стать благополучной, уважаемой всеми страной, то приоритетом государственной стратегии должна стать всемерная поддержка естественных и социально-общественных наук, высоких научных информационных технологий, образования и системы воспитания, так как сейчас в начале XXI века обнаруживается четкая корреляция между уровнем развития науки, образования, информационных ресурсов с материальным и духовно-нравственным благополучием и благосостоянием народов, их всесторонним развитием.

Другой характерной чертой развития исследуемой нами сферы является интенсивное правовое обеспечение отношений собственности в процессе поиска, производства, накопления, хранения и передачи (продажи) информации.

Проявление этой черты наблюдается в целом ряде тенденций. К ним относятся: во-первых, ужесточение мер организационного и экономического характера за нарушение прав собственности на информационные ресурсы и, в частности, за разглашение сведений, относящихся к государственной и коммерческой тайнам; во-вторых, усиление внимания к проблемам обеспечения авторских и патентных прав, прав на интеллектуальную собственность; в-третьих, наметившийся процесс осознания гражданами необходимости защиты интеллектуальной собственности в суде.

И, наконец, самая важная черта информационной сферы заключается в том, что определяющей тенденцией развития здесь является превращение ее в основной инструмент власти, о чем свидетельствует воздействие “информационного разума” на всю жизнь и деятельность человеческого социума.

При этом информационная борьба может носить информационно-технический и информационно-психологический характер. Если главным объектом первого вида борьбы выступают информационно-технические системы, то второго – биосоциальные, т.е. человек, его психика, нравственный и духовный мир, социально-политические, психологические ориентации, установки, отношения, рациональные и иррациональные аспекты поведения, системы общественного мнения и принятия решений.

Информационная сфера может быть заряжена не только положительным, но и отрицательным знаком. Последнее рождает проблему обеспечения информационной безопасности личности, которая может и должна функционировать на разных уровнях: общесоциальном, профессиональном, групповом и индивидуальном.

Надежная информационная безопасность возможна только тогда, когда она будет построена на совокупности научных принципов. К ним можно отнести:

Принцип первый – законность и правовая обеспеченность. Реализуя этот принцип, важно добиться неотвратимой административной и судебной ответственности за ложную информацию.

Принцип второй – баланс интересов личности, общества и государства. Данный принцип должен быть направлен на обеспечение оптимального соотношения конфиденциальной информации и информации, разоблачающей антисоциальные элементы общества.

Принцип третий – объективность, научность. Главное правило любых информационных систем – объективное отражение существующих реалий.

Принцип четвертый – интеграция с международными системами безопасности. Этого настоятельно требует усиливающаяся закономерность глобальной интеграции, развитие международных коммуникаций.

Принцип пятый – экономическая эффективность – другими словами, результаты от мер информационной безопасности должны превышать совокупные затраты на них.

И, наконец, принцип шестой – комплексность, системность. Данный принцип предполагает тесное увязывание всех видов безопасности, средств, методов и способов ее обеспечения во времени и пространстве.

Современная широкая общественность России все более осознает информацию, как один из важнейших ресурсов, без которого невозможна успешная целенаправленная деятельность в любой сфере природной и социальной среды. Обращаясь к Доктрине, видим, что сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;

- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения "информационного оружия";
- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

3.2. Понятие методов обеспечения информационной безопасности Российской Федерации.

Доктрина подразделяет общие методы обеспечения информационной безопасности Российской Федерации на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в

информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

К одному из важных направлений развития в этой сфере относится внесение изменений и дополнений в законодательство Российской Федерации, регулирующие отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации.

Следующим важным направлением является законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан.

Не менее важным направлением является разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну.

Кроме того, необходимо уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России; законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи; определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций; создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются: создание и совершенствование системы обеспечения информационной безопасности Российской Федерации; усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере и другие.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя, в частности:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

3.3. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

Но в каждой из них имеются и свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации.

Так, обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур-производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну.

Необходима организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются конституционные права и свободы человека и гражданина; конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации; открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере; недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей и распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом. Угрозой этой сфере может также являться

деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации; активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России и ряд других.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются: разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации; разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях; создание российским представительством и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации.

К числу основных внешних угроз информационной безопасности в области науки и техники следует отнести в первую очередь стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах; а также активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

Источником внутренних угроз информационной безопасности Российской Федерации в области науки и техники является сохраняющаяся сложная экономическая ситуация в России, ведущая к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники – это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности жизни относится достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания; свобода массовой информации; неприкосновенность частной жизни, личная и семейная тайна; русский язык как фактор духовного единения народов многонациональной России.

Наибольшую опасность в этой сфере представляет деформация системы массового информирования; а также неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются развитие в России основ гражданского общества; создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры; совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека.

Основными объектами обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию; средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля и другое.

Угрожает информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах является предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств; исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации.

К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относится информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации; информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные .

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются все виды разведывательной деятельности зарубежных государств; информационно-технические воздействия, направленная против интересов Российской Федерации в сфере обороны.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны является системати-

ческое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются: нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и используемой для расследования преступлений; недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах; отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера и другое.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главным из них является создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем; повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

ТЕМА 4. ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

4.1. Объект и предмет правового обеспечения информационной безопасности РФ

Правовое обеспечение информационной безопасности Российской Федерации представляет собой достаточно сложную правовую категорию, развитие которой во многом определяет способность государства использовать потенциал права для достижения национальных интересов России в информационной сфере и их защиты от угроз внешнего и внутреннего характера.

Одной из важных тенденций развития современного общества является интенсивное распространение современных информационных технологий, существенное усиление их влияния на все сферы общественной жизни и, как следствие, появление признаков перехода некоторых стран мира к новому этапу своего развития, получившему название «глобальное информационное общество».

Представляется, что основным признаком этого этапа развития является такое развитие экономики, при котором основная или значительная часть валового продукта производится за счет создания и внедрения наукоемких технологий, производства информационных продуктов и услуг, интеллектуального труда граждан.

Неравномерное экономическое развитие стран мира, различия в уровне развития их информационных сфер, в возможностях производить интеллектуальную продукцию, составляющую экономическую основу информационного общества, а также значимость экономических, политических, социальных, оборонных и экологических последствий отставания от передовых стран в области создания и использования современных информационных технологий, превращают формирование предпосылок информационного общества для многих стран в исторический вызов.

Необходимость адекватного ответа на этот вызов обусловила как содержание национальных интересов Российской Федерации в информационной сфере, так и то внимание, которое уделяется разработке государственной политики по обеспечению их безопасности.

Обеспечение безопасности национальных интересов в информационной сфере от угроз внутреннего и внешнего характера является одной из важных задач государства, называемой обеспечением информационной безопасности Российской Федерации. Ее решение составляет важное направление государственной политики в области национальной безопасности страны и содержание одной из основных функций государства, выполняемой с привлечением определенного материального, организационного и кадрового ресурса.

Основанием этой функции выступают такие свойства российского государства, как:

- социальный характер государства, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека;
- демократический и правовой характер государственной власти в Российской Федерации, для которой человек, его права и свободы являются высшей ценностью;
- выделение безопасности как одного из предметов ведения Российской Федерации.

Функция обеспечения информационной безопасности Российской Федерации государства, как и любая другая функция государства, обладает сложной структурой, включающей, по крайней мере, четыре элемента: объект функции; цель, на достижение которой направлена функция; социальное назначение государства; фактическую деятельность государства (в единстве с ее принципами, способами, методами и формами).

Как известно, функции государства осуществляются в определенных формах и при помощи специальных методов. Форма выступает как непосредственное выражение сущности и содержания функции.

В юридической литературе выделяются два вида форм реализации функций государства: **правовые и организационные**.

Правовая форма осуществления функции государства заключается в однородной по своим внешним признакам (характеру и юридическим последствиям) деятельности государственных органов, связанной с изданием юридических актов, организационная форма - в аналогичной деятельности, не влекущей за собой юридических последствий.

Совокупность правовых средств, методов их использования для регулирования общественных отношений, связанных с обеспечением безопасности национальных интересов России в информационной сфере, совместно с системой органов государства, осуществляющих это правовое регулирование, образуют правовое обеспечение информационной безопасности Российской Федерации.

С учетом этого и изложенного выше можно полагать, что правовая форма реализации функции государства по обеспечению информационной безопасности проявляется в виде **правового обеспечения информационной безопасности**.

Данное правовое обеспечение характеризуется его строением, основными элементами, внутренней структурой, а также методами его формирования и совершенствования.

Исходя из приведенного выше определения, правовое обеспечение информационной безопасности может рассматриваться как сложное явление, включающее:

- правовое регулирование общественных отношений в информационной сфере в целях обеспечения безопасности соответствующих национальных интересов или, иначе, правовое обеспечение безопасности в информационной сфере;
- правовое обеспечение деятельности системы органов государства в области обеспечения информационной безопасности.

Социальное назначение государства в структуре правового обеспечения определяется признанием человека, его прав и свобод высшей ценностью, а соблюдение и защиту прав и свобод - обязанностью государства, направленностью политики государства на создание условий, обеспечивающих достойную жизнь и свободное развитие человека, признанием и

защитой частной, государственной, муниципальной и иных форм собственности, закреплении идеологического многообразия и светского характера государства.

Основными объектами правового обеспечения безопасности в информационной сфере являются:

- общественные отношения, которые, с одной стороны, имеют предметами составляющие этой сферы – субъектов информационной сферы, информацию и информационную инфраструктуру, а с другой – представляются важными для достижения национальных интересов в информационной сфере;

- внешние и внутренние угрозы общественным отношениям в информационной сфере, могущие нанести ущерб предметам и интересам субъектов этих отношений и, как следствие, – нанести ущерб национальным интересам России в информационной сфере.

Фактическая деятельность государства в этой области направлена на разработку, принятие и применение юридических норм, регулирующих общественные отношения в информационной сфере в целях достижения соответствующих национальных интересов и их защиты от угроз.

Объектами правового обеспечения деятельности системы органов власти в области обеспечения информационной безопасности являются общественные отношения, возникающие при образовании, функционировании и прекращении деятельности этих органов государства, реализацией ими властных полномочий, организацией взаимодействия между ними, а также с гражданами и общественными организациями. Предметом этого вида правового обеспечения выступают методы и средства правового регулирования выделенных отношений в целях обеспечения эффективного функционирования механизма государства.

Правовое обеспечение безопасности в информационной сфере представляет собой деятельность государства и общества, осуществляемую в процессе подготовки и принятия норм права, их реализации в конкретных правоотношениях и применения государственного принуждения к правонарушителям.

Особое место в правовом регулировании занимают правовые нормы, совокупность которых образует нормативное правовое обеспечение информационной безопасности.

Данное нормативное правовое обеспечение может быть классифицировано по нескольким основаниям, наиболее важными из которых являются следующие:

- цели правового обеспечения безопасности в информационной сфере;
- вид подсистем нормативных правовых актов, закрепляющих нормы права в рассматриваемой области;
- тип регулируемых общественных отношений в информационной сфере, оказывающих значительное влияние на достижение национальных интересов в этой сфере;
- вид угроз общественным отношениям в информационной сфере, на противодействие которым направлено правовое регулирование.

По цели нормативное правовое обеспечение безопасности в информационной сфере подразделяется на составляющие, каждая из которых ориентирована на достижение одной из соответствующих национальных интересов Российской Федерации в информационной сфере. С учетом этого выделяются следующие составляющие нормативного правового обеспечения:

- правовые нормы, регулирующие отношения в целях соблюдения конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечения духовного обновления России, сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

- правовые нормы, регулирующие отношения в целях информационного обеспечения государственной политики Российской Федерации, связанного с доведением до россий-

ской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

- правовые нормы, регулирующие отношения в целях развития современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечения потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечения накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- правовые нормы, регулирующие отношения в целях защиты информационных ресурсов от несанкционированного доступа, обеспечения безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

По виду подсистем нормативных правовых актов, закрепляющих нормы права в рассматриваемой области, выделяются: общепризнанные принципы и нормы международного права и международные договоры Российской Федерации; федеральная система нормативных правовых актов; подсистема законодательства субъектов Российской Федерации; нормативные правовые акты местного самоуправления.

Анализ нормативного правового обеспечения безопасности в информационной сфере показывает, что основная часть правовых норм, регулирующих отношения в рассматриваемой области, закрепляется нормативными правовыми актами федеральной системы, что, видимо, обусловлено отнесением вопросов безопасности, а также федеральной информации и связи к ведению Российской Федерации.

По типам регулируемых общественных отношений в информационной сфере, оказывающим значительное влияние на достижение национальных интересов в этой сфере, нормативное правовое обеспечение может быть разделено на несколько составляющих в соответствии с предметами этих отношений: информация как формализованный объект информационного обмена; информация как содержательный объект информационного обмена; информационная инфраструктура.

Отношения, предметом которых является информация как формализованный объект информационного обмена, определяют многообразные связи, возникающие между людьми в процессе формирования и распространения информации. Среди них выделяются отношения, связанные со следующим:

- созданием информации и формированием информационных ресурсов в различных сферах деятельности человека, жизни общества и государства;
- владением, использованием и распоряжением информационными ресурсами;
- передачей, сбором и хранением информации;
- обеспечением безопасности информации и информационных ресурсов.

Общественные отношения, связанные с созданием информации и формированием информационных ресурсов, возникают в процессе экономической, социальной, политической и культурной жизни и деятельности общества и обусловлены превращением информации в значительный экономический, социальный и культурный ресурс общества. Примером таких отношений являются регистрация актов гражданского состояния, формирование архивных и библиотечных фондов, создание различных баз данных, литературное, художественное и научное творчество.

Общественные отношения, связанные с владением, использованием и распоряжением информационными ресурсами, включают доступ к сформированным информационным ресурсам физических и юридических лиц, использование результатов интеллектуального труда, ограничение доступа к конфиденциальной информации, производственные отношения в

информационной промышленности и т.д. Общественные отношения в области сбора, обработки, передачи, хранения и распространения информации отображают устойчивые связи между гражданами, общественными организациями, органами государственной власти и средствами массовой информации, складывающиеся в процессе удовлетворения потребностей граждан и представителей соответствующих структур в информации о тех или иных событиях общественной жизни.

Общественные отношения в области обеспечения безопасности информации и информационных ресурсов связаны с установлением ответственности за сохранность информации и информационных ресурсов, а также предоставлением соответствующих услуг и средств решения этой задачи.

Общественные отношения, предметом которых является информация как содержательный объект информационного обмена, отражают устойчивые связи между субъектами информационной сферы, возникающие в связи с осознанием и использованием получаемой информации, а также ответственности в связи с передачей или распространением информации. Эти отношения охватывают духовную жизнь общества.

Общественные отношения в области функционирования информационной инфраструктуры связаны с отношениями собственности на ее компоненты, их использования субъектами информационной сферы и обеспечение безопасности функционирования как отдельных компонентов, так и инфраструктуры в целом.

Отношения собственности связаны с реализацией функций владения, пользования и распоряжения компонентами информационной инфраструктуры и в демократическом обществе охватывают как органы государственной власти, так и гражданские организации, частных лиц. Эти субъекты могут вступать в отношения собственности на системы и средства электронной связи, телекоммуникации, подготовки кадров и т.д.

Отношения, связанные с использованием компонентов информационной инфраструктуры, отражают устойчивые связи субъектов информационной сферы с собственниками компонентов информационной инфраструктуры, а также собственников с персоналом, обслуживающим эти компоненты. Кроме того, в рамках этих отношений затрагиваются вопросы взаимной ответственности сторон за соблюдение установленных собственником правил использования этих компонентов и качество предоставляемых услуг обеспечения информационного взаимодействия.

Общественные отношения в области обеспечения безопасности информационной инфраструктуры связаны с ответственностью субъектов информационной сферы за устойчивое функционирование информационной инфраструктуры, предоставлением услуг по защите ее компонентов от угроз внутреннего и внешнего характера. По видам угроз общественным отношениям в информационной сфере, на противодействие которым направлено правовое регулирование, нормативное правовое обеспечение безопасности в информационной сфере может быть разделено на следующие группы: противодействия внешним угрозам и противодействия внутренним угрозам; противодействия угрозам общественным отношениям, предметом которых являются информация как формализованный объект, информация как содержательный объект и информационная инфраструктура.

Для регулирования отношений, связанных с достижением национальных интересов в информационной сфере и обеспечением их безопасности, используются методы и средства различных отраслей права и правовых институтов, включая методы и средства интенсивно развивающейся новой отрасли права - информационного права.

Итак, основными объектами данного правового обеспечения являются общественные отношения, оказывающие существенное влияние на достижение национальных интересов России в информационной сфере, угрозы этим отношениям, а также общественные отношения в области создания, функционирования и упразднения органов государства, осуществляющих правоприменение и правоохрану в области достижения и обеспечения безопасности этих национальных интересов.

Основным предметом данного правового обеспечения являются средства и методы правового регулирования выделенных общественных отношений в целях достижения и обеспечения безопасности национальных интересов Российской Федерации в информационной сфере.

4.2. Задачи и основные принципы государственной политики обеспечения информационной безопасности РФ

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере. Основные направления государственной политики приведены в формируемой "Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации".

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению. Оно организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации; оно также поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации. Важной функцией государства является осуществление контроля за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации.

Государство проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской

Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов. Оно способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям, формулирует и реализует государственную информационную политику России.

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

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;
- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации является разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере; разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Со-

вет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

В сфере государственного регулирования в сфере информационной безопасности выделяют некоторые основные принципы.

Принцип баланса интересов личности, общества и государства предусматривает установление и соблюдение приоритетов этих интересов при регулировании общественных отношений в информационной сфере. При определении баланса интересов личности, общества и государства необходимо исходить из того, что Российская Федерация – социальное государство, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека, реализует гарантии соблюдения прав и свобод человека и гражданина, организует противодействие угрозам национальной безопасности Российской Федерации с привлечением общественных организаций и отдельных граждан.

Принцип комплексности правового регулирования общественных отношений в области обеспечения достижения национальных интересов Российской Федерации в информационной сфере и противодействия угрозам этим интересам предполагает необходимость выявления всей совокупности общественных отношений, требующих такого регулирования, и согласование используемых для регулирования этих отношений правовых механизмов.

Принцип согласованности деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по нормативному правовому обеспечению информационной безопасности предполагает организацию этой деятельности на основе приоритетности компетенции Российской Федерации в области безопасности и полноты государственной власти субъектов Российской Федерации в области развития и использования региональных информационных и телекоммуникационных систем, сетей связи, региональных информационных ресурсов.

Принцип консолидированной ответственности государства и общества за обеспечение информационной безопасности Российской Федерации предполагает участие общественных организаций и граждан в контроле за деятельностью органов государственной власти в обла-

сти обеспечения информационной безопасности Российской Федерации, прежде всего, в области реализации государством гарантий прав и свобод человека и гражданина.

Принцип реализации единой государственной политики развития и применения норм международного права в системе нормативного правового обеспечения информационной безопасности Российской Федерации предполагает активное и согласованное участие федеральных органов исполнительной власти Российской Федерации в разработке международных документов, затрагивающих вопросы достижения национальных интересов Российской Федерации в информационной сфере и обеспечения их безопасности.

Принцип формирования и применения норм международного права как составной части правовой системы Российской Федерации предполагает прямое действие общепризнанных принципов и норм международного права, международных договоров на всей территории страны, а также активное и согласованное участие федеральных органов исполнительной власти Российской Федерации в разработке международных документов, затрагивающих вопросы достижения национальных интересов Российской Федерации в информационной сфере и обеспечения их безопасности.

Эффективность нормативного правового обеспечения информационной безопасности Российской Федерации определяется степенью защищенности национальных интересов Российской Федерации в информационной сфере, наличием необходимых правовых механизмов противодействия наиболее опасным угрозам этим интересам.

ТЕМА 5. НОРМАТИВНАЯ ПРАВОВАЯ БАЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

5.1. Состояние нормативного правового обеспечения информационной безопасности

Регулирование правовых вопросов в информационной сфере России является в настоящее время достаточно новой и сложной проблемой. Это связано прежде всего с тем, что правовая нормативная база создается для общественных отношений, находящихся на стадии формирования, противоречивого процесса становления. А противоречия в самом реальном процессе подчас предопределяют противоречия в сфере права. Поэтому мы зачастую сталкиваемся с такой ситуацией, когда уже принятые законодательные и нормативные акты, направленные, например, на урегулирование порядка, допуска и доступа граждан и юридических лиц к сведениям, составляющим государственную, коммерческую и иную тайну, компетенция средств массовой информации не всегда соответствуют сложности и многообразию реальных процессов.

Практически вне зоны правового регулирования находится сейчас огромный массив новых информационных средств, функционирование компьютерных информационных систем.

Все эти вопросы нуждаются в комплексном изучении и выработке целенаправленной стратегии их реализации в реально складывающихся условиях.

За последние годы в Российской Федерации уже был реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созда-

нию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Основными источниками права в области обеспечения гарантий прав и свобод человека и гражданина являются Конституция Российской Федерации, Европейская конвенция о защите прав и основных свобод, "Всеобщая декларация прав человека", другие международные нормативные правовые акты, признанные Российской Федерацией и регулирующие отношения в рассматриваемой области, решения Конституционного Суда Российской Федерации, Уголовный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Кодекс РСФСР об административных правонарушениях, Закон Российской Федерации "О средствах массовой информации", Федеральный закон "Об информации, информатизации и защите информации", Закон Российской Федерации "О государственной тайне", Федеральный конституционный закон "Об уполномоченном по правам человека в Российской Федерации", некоторые другие федеральные законы и подзаконные нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Зафиксированные в данных нормативных правовых актах правовые нормы обеспечения гарантий прав и свобод человека и гражданина в целом оказывают положительное влияние на состояние защищенности национальных интересов Российской Федерации в этой области.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти,

органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Итак, современное состояние нормативного правового обеспечения информационной безопасности Российской Федерации характеризуется фрагментарностью выбора объектов правового регулирования, недостаточными согласованностью используемых для этого правовых норм и скоординированностью деятельности субъектов законодательной инициативы по развитию и совершенствованию правовых норм, в ряде случаев противоречивостью этих норм.

В целом нормативное правовое обеспечение информационной безопасности Российской Федерации как единая система правового регулирования общественных отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере развито недостаточно, что заметно снижает потенциал Российской Федерации по противодействию угрозам ее информационной безопасности, укреплению национальной безопасности России.

5.2. Нормативное правовое регулирование отдельных направлений информационной безопасности.

В последние годы в стране принят ряд законодательных актов, которые частично решили проблему правового регулирования в информационной сфере. Вместе с тем целый ряд аспектов нуждаются в серьезной правовой проработке и закреплении в законах РФ. К числу таких вопросов относятся следующие:

- Интеллектуальная собственность и информационная безопасность.

- Информационная безопасность России и международное право.
- Предвыборная агитация через СМИ и информационная безопасность: правовые аспекты.
- Правовое регулирование отношений и субъекты права в сфере обращения охраняемой информации.
- Правонарушения и ответственность в сфере обращения охраняемой информации.
- Правовое регулирование в сфере криптографической защиты информации (лицензирование, сертификация и т.п.).
- Правовой режим электронного документа.

В разрабатываемой межведомственной рабочей группой "Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации" названы основные недостатки нормативного правового обеспечения различных сфер жизнедеятельности личности, общества и государства.

К числу основных недостатков нормативного правового обеспечения защиты **прав и свобод человека и гражданина** в информационной сфере следует отнести:

- неопределенность правовых механизмов обеспечения доступа к открытой информации органов государственной власти и органов местного самоуправления, что создает условия для ущемления прав и свобод человека и гражданина, включая право на информацию о состоянии окружающей среды, фактах и обстоятельствах, представляющих угрозу для жизни и здоровья людей;
- отсутствие правовых норм, устанавливающих ответственность за ограничение или нарушение права на доступ к открытой информации;
- отсутствие правового регулирования общественных отношений в области сбора и использования персональных данных, механизмов их внесудебной защиты, реализации права на личную и семейную тайны, неприкосновенность частной жизни, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, телеграфных и иных сообщений;
- недостаточную согласованность и полноту правовых норм, регулирующих установление режимов ограничения доступа к информации, обязанностей субъектов правоотношений по защите информации с ограниченным доступом, ответственности за нарушения установленных режимов ограничения доступа к информации;
- неурегулированность прав государства на объекты интеллектуальной собственности, полученные в результате выполнения работ, полностью или частично финансируемых за счет средств государственного бюджета, а также недостаточное правовое регулирование общественных отношений в области охраны таких объектов интеллектуальной собственности, как ноу-хау, изобретения, составляющие государственную или служебную тайны, фирменные наименования;
- недостаточное развитие правового регулирования отношений, связанных с ограничением распространения массовой информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- отсутствие правового регулирования распространения информации, предназначенной для неограниченного круга потребителей, в открытых информационно-телекоммуникационных сетях.

Целью нормативного правового регулирования отношений **в области развития российской информационной инфраструктуры** и эффективного использования отечественных информационных ресурсов являются развитие отечественной электронной промышленности и информационной индустрии, повышение конкурентоспособности их продукции, со-

здание условий для равноправного участия российских компаний в международной торговле на мировом информационном рынке, развитие информационной инфраструктуры российского общества, включение государственных информационных ресурсов в хозяйственный оборот, эффективное использование квалифицированных кадров.

В данной составляющей нормативного правового обеспечения информационной безопасности Российской Федерации выделяются:

- нормы, регулирующие отношения в области противодействия угрозам развитию технологической основы информационной инфраструктуры общества и государства;
- нормы, регулирующие отношения в области противодействия угрозам формированию и эффективному использованию российских информационных ресурсов.

Состояние нормативного правового обеспечения противодействия угрозам развитию технологической основы информационной инфраструктуры общества и государства характеризуется недостаточным участием России в системе международных договоров, регулирующих отношения на мировом информационном рынке в области развития международных информационно-телекоммуникационных систем и сетей связи, международного информационного обмена, международного сотрудничества в области создания современных информационных технологий, а также недостаточным развитием национального законодательства, регулирующего отношения в данной области.

В рамках международного сотрудничества Российской Федерацией заключены двусторонние договоры в области развития информатизации и вычислительной техники с Беларусью и некоторыми другими государствами-участниками Содружества Независимых Государств, Болгарией, Индией, Испанией, Францией, Кубой. Эти договоры создают определенную базу для обеспечения безопасности национальных интересов Российской Федерации в рассматриваемой области, но не обеспечивают необходимый уровень этой безопасности.

До настоящего времени Российская Федерация не присоединилась ни к одному основополагающему международному договору, регулирующему отношения в области международной торговли средствами информатизации, телекоммуникации и связи, развития международного информационного рынка, глобальных телекоммуникаций.

Правовые нормы национального законодательства в значительной степени ориентированы на регулирование отношений в области информатизации, развития региональных информационных и телекоммуникационных систем и сетей связи, что в определенной мере способствует развитию технической основы информационной инфраструктуры России. В то же время действующие правовые нормы слабо способствуют повышению конкурентоспособности продукции отечественных производителей современных информационных технологий, ее приоритетному использованию в разрабатываемых и модернизируемых информационных системах, сетях связи, закреплению квалифицированных специалистов по современным информационным технологиям в отечественной науке и промышленности.

Значительно более развиты правовые нормы, регулирующие отношения в области противодействия угрозам формированию и эффективному использованию российских информационных ресурсов. По данным вопросам Российской Федерацией заключено более 30 международных соглашений, интенсивно развивается национальное законодательство.

К числу основных недостатков нормативного правового обеспечения информационной безопасности Российской Федерации в рассматриваемой области в целом относятся:

- отсутствие комплексности в развитии международного сотрудничества по вопросам интеграции России в мировой информационный рынок, необходимых условий для доступа отечественных товаропроизводителей к современным информационным технологиям, недостаточное участие российских специалистов в фундаментальных и поисковых исследованиях, проводимых международными, в том числе европейскими, сообществами;
- неопределенность приоритетов развития отечественной электронной промышленности, информационной индустрии, механизмов государственной поддержки деятельности

производителей по выпуску конкурентоспособной продукции и ее продвижению на внутренний и внешний рынки;

- недостаточная правовая защищенность отечественных товаропроизводителей от недобросовестной конкуренции со стороны зарубежных участников информационного рынка;

- слабое развитие нормативной правовой базы, стимулирующей вовлечение государственных информационных ресурсов в эффективный хозяйственный оборот.

Основным источником права в области **противодействия угрозам безопасности информационных и телекоммуникационных систем** и информационных ресурсов России является федеральное законодательство, регулирующее отношения в области обеспечения безопасности, деятельности отдельных федеральных органов исполнительной власти, создания и использования средств защиты информации и их сертификации, деятельности государственной системой защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам, а также нормативные правовые акты субъектов Российской Федерации, направленные на обеспечение безопасности региональных информационных и телекоммуникационных систем и сетей связи.

Система международных договоров Российской Федерации в этой области состоит, в основном, из двусторонних и многосторонних договоров с государствами-участниками Содружества Независимых Государств в области защиты информации, обеспечения безопасности закрытой правительственной связи и использования аппаратуры шифрования, а также соглашения с Организацией Североатлантического договора о защите информации.

Перечисленные нормативные правовые акты создают определенную нормативную правовую базу обеспечения безопасности информационных и телекоммуникационных систем и сетей связи, российских информационных ресурсов. В то же время эта правовая база обладает рядом недостатков, к числу которых относятся:

- отсутствие законодательной базы для согласования законотворческой деятельности Российской Федерации и ее субъектов в рассматриваемой области;

- недостаточное правовое регулирование отношений в области развития технологического обеспечения информационной безопасности Российской Федерации;

- неурегулированность вопросов разграничения полномочий между федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации в области обеспечения безопасности информационных и телекоммуникационных систем и сетей связи;

- недостаточная эффективность правового регулирования ответственности за правонарушения в сфере обеспечения информационной безопасности.

-

5.3. Основные направления совершенствования нормативного правового обеспечения информационной безопасности РФ

Совершенствование нормативного правового обеспечения информационной безопасности Российской Федерации должно осуществляться по направлениям развития:

- общепризнанных принципов и норм международного права, международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российская Федерация;

- федерального законодательства, регулирующего отношения в данной области по предметам ведения Российской Федерации и совместного ведения Российской Федерации и ее субъектов;

- законодательства субъектов Российской Федерации, регулирующего отношения в рассматриваемой области по вопросам, отнесенным к предметам совместного ведения Российской Федерации и субъектов Российской Федерации, а также собственного правового регулирования субъектов Российской Федерации;

- нормативных правовых актов федеральных органов исполнительной власти, принимаемых в пределах их полномочий.

В рамках совершенствования нормативного правового обеспечения информационной безопасности Российской Федерации должны быть конкретизирован перечень объектов обеспечения безопасности и уточнены правовые механизмы регулирования отношений в области противодействия угрозам безопасности этих объектов.

Основными целями совершенствования системы общепризнанных принципов и норм международного права, системы международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российской Федерация, являются:

- создание комплексной системы международной информационной безопасности, предусматривающей координацию усилий всех членов мирового сообщества по противодействию наиболее опасным угрозам безопасности международной информационной сферы и информационной сферы каждой страны;

- развитие системы международных договоров по отдельным направлениям обеспечения информационной безопасности Российской Федерации.

Основными целями совершенствования федерального законодательства в области обеспечения информационной безопасности являются:

- повышение эффективности правового регулирования отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере;

- формирование комплексной системы согласованных нормативных правовых актов Российской Федерации, регулирующих отношения в рассматриваемой области и затрагивающих вопросы, отнесенные к ведению Российской Федерации и ее совместному ведению с субъектами Российской Федерации.

Основными целями совершенствования законодательства субъектов Российской Федерации в области информационной безопасности являются:

- формирование системы обеспечения информационной безопасности субъектов Российской Федерации как составной части единой системы обеспечения информационной безопасности Российской Федерации;

- согласование направлений развития региональных информационных инфраструктур, принципов и механизмов их взаимодействия с федеральной информационной инфраструктурой, сохранение и развитие единого информационного пространства Российской Федерации.

Основными целями совершенствования нормативных правовых актов федеральных органов исполнительной власти Российской Федерации в области информационной безопасности являются конкретизация правовых механизмов реализации норм международного права и национального законодательства.

Совершенствование нормативного правового обеспечения информационной безопасности Российской Федерации осуществляется на основе максимально возможного сохранения системы действующих нормативных правовых актов и основных механизмов регулирования общественных отношений в области противодействия угрозам интересам Российской Федерации в информационной сфере.

Противодействие этим угрозам предполагает создание системы эффективного взаимодействия общества и государства в целях предупреждения, выявления и пресечения правона-

рушений в области обеспечения информационной безопасности Российской Федерации на основе расширения участия общественных организаций в контроле за соблюдением международных договоров Российской Федерации и законодательства Российской Федерации в области защиты прав и свобод человека, установления порядка взаимодействия общественных организаций с федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации в целях обеспечения информационной безопасности России.

Совершенствование системы общепризнанных принципов и норм международного права, системы международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российская Федерация, должно осуществляться по следующим основным направлениям:

- закрепление права на безопасность функционирования глобальных информационно-телекоммуникационных систем и сетей связи, на сохранность передаваемой в них информации в качестве общепризнанной нормы международного права;
- создание международной системы обеспечения безопасности глобальных информационных и телекоммуникационных систем и сетей связи, включая предотвращение и разрешение конфликтных ситуаций, возникающих при использовании этих систем и сетей, защиту законных интересов человека и гражданина, связанных с безопасностью информационного обмена, охрану объектов интеллектуальной собственности, обеспечение неприкосновенности частной жизни, личной и семейной тайны, тайны сообщений в интенсивно развивающихся глобальных информационно-телекоммуникационных системах;
- предотвращение создания и использования средств нарушения нормального функционирования международных и национальных информационных и телекоммуникационных систем и сетей связи, а также несанкционированного доступа к информационным ресурсам;
- присоединение к международным договорам по тарифам и услугам в области телекоммуникаций, а также по борьбе с преступлениями в сфере высоких технологий;
- присоединение к Конвенции о международном праве опровержения (1953г.) и продвижение идеи присоединения к ней других государств;
- расширение участия российских научных организаций в фундаментальных и поисковых исследованиях, проводимых международными организациями.

Совершенствование федерального законодательства должно осуществляться по следующим направлениям:

- усиление гарантий конституционных прав и свобод граждан, реализуемых в информационной сфере;
- развитие правовых механизмов регулирования общественных отношений в области конституционных ограничений прав и свобод человека и гражданина, реализуемые в информационной сфере, в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- обеспечение государственной поддержки фундаментальных, поисковых и опытно-конструкторских работ в области создания конкурентоспособных средств информатизации, телекоммуникации и связи;
- стимулирование инвестиций в производство конкурентоспособных средств информатизации, телекоммуникации и связи, их продвижение на внутренний и мировой рынки;
- развитие системы обеспечения информационной безопасности Российской Федерации, прежде всего, за счет включения в нее органов государственной власти субъектов Российской Федерации, общественных объединений, организаций и граждан;
- создание системы государственного управления информационными ресурсами;

- совершенствование законодательства, регулирующего отношения в области международного информационного обмена;
- совершенствование законодательства по вопросам защиты государственной тайны, предотвращения несанкционированного доступа к другим охраняемым законом сведениям;
- совершенствование законодательства по вопросам защиты конфиденциальной информации;
- законодательное разграничение уровней правового регулирования проблем обеспечения информационной безопасности (федеральный уровень, уровень субъекта Федерации, уровень местного самоуправления).

Совершенствование законодательства субъектов Российской Федерации должно осуществляться по следующим направлениям:

приведение в соответствие с федеральным законодательством по вопросам, отнесенным к совместному ведению Российской Федерации и ее субъектов;

внесение изменений и дополнений в действующее законодательство субъектов Федерации в области обеспечения информационной безопасности для устранения противоречий нормам Конституции Российской Федерации, федеральному законодательству и международным соглашениям, к которым присоединилась Российская Федерация, а также конкретизация норм ответственности за правонарушения в данной области;

согласование усилий органов государственной власти субъектов Российской Федерации и федеральных органов государственной власти по решению проблем обеспечения безопасности региональных информационных и телекоммуникационных систем и информационных ресурсов;

поддержка отечественных товаропроизводителей конкурентоспособных средств информатизации, телекоммуникации и связи, содействие в продвижении их продукции на внутренний и мировой рынки;

повышение экономической эффективности использования региональных информационных ресурсов, введения их в хозяйственный оборот.

- нормативных правовых актов федеральных органов исполнительной власти, принимаемых в пределах их полномочий.

ТЕМА 6. ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

6.1. Виды информации и право на нее

Информация - сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком; сообщения, осведомляющие о положении дел, о состоянии чего-либо. Информацией называются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Научно-технический прогресс превращает информацию не только в исключительно ценный товар, но и в средство активного воздействия на общественное сознание.

Информатизация – это организационный социально - экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

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

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

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

Пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Право на информацию – одно из основных прав человека и гражданина. Согласно статье девятнадцать Всеобщей Декларации Прав Человека, каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

Статья десять Конвенции о защите прав человека и основных свобод гласит, что каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ.

Однако осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

В соответствии с Конституцией Российской Федерации каждому гарантируется право на информацию, то есть право свободно искать, получать и передавать информацию. Право на информацию является неотчуждаемым правом человека и гражданина.

Иностранные граждане и лица без гражданства пользуются в Российской Федерации правом на информацию наравне с гражданами Российской Федерации, кроме случаев, установленных федеральным законом или международным договором Российской Федерации.

Основными принципами реализации права на информацию являются:

- общедоступность и открытость информации;
- обеспечение безопасности личности, общества и государства;
- информированность граждан о деятельности органов и организаций;
- законность поиска, получения и передачи информации;
- предоставление достоверной информации;
- защита права на информацию.

Обеспечение конституционных прав граждан на информационную деятельность, включая право на получение достоверной информации, гарантии возможности свободно искать, получать, передавать, производить и распространять информацию в сочетании с обеспечением свободы слова, свободы прессы и других средств массовой информации является важнейшей составляющей информационной безопасности.

Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей, - не допускается. Создание и финансирование организаций, учреждений, органов или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, - не допускаются.

Категории информации.

1. Общедоступная

Информация, которая должна предоставляться свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных, предоставленных законом прав.

2. С ограниченным доступом:

а) Являющаяся объектом гражданских прав.

Информация, обладатели которой вправе предоставлять ее по своему усмотрению, в том числе на возмездной основе, самостоятельно определять порядок доступа к ней и не обязаны мотивировать свой отказ в ее предоставлении.

б) Конфиденциальная.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации в целях соблюдения интересов государства или прав и законных интересов их владельцев.

Виды информации, являющейся объектом гражданских прав:

- Произведения, являющиеся объектом авторского права;
- Информация, являющаяся объектом патентного права;
- Товарные знаки, знаки обслуживания и наименования мест происхождения товаров.

К конфиденциальной информации относится государственная тайна; служебная и коммерческая тайны. К этой категории также выделяют тайны, связанные с правом на неприкосновенность личной жизни: персональные данные; личная и семейная тайны; тайна записи актов гражданского состояния; медицинская тайна; тайна вероисповедания. Информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Кроме того, здесь выделяют и группу профессиональных тайн: адвокатская тайна; нотариальная тайна; журналистская тайна; тайна исповеди.

Федеральный закон «Об информации, информатизации и защите информации» запрещает к информации с ограниченным доступом относить:

- нормативные акты, устанавливающие правовой статус госорганов, органов местного самоуправления, организаций, общественных объединений и граждан;
- документы, содержащие информацию о деятельности госорганов и органов местного самоуправления, об использовании ими средств соответствующих бюджетов и иных фондов, формируемых за счет налогов и обязательных сборов;
- документы, необходимые для реализации прав, свобод и исполнения обязанностей граждан, находящиеся в открытых фондах библиотек и архивах или в открытых информационных системах госорганов, организаций и общественных объединений.

Основными методами регулирования отношений по поводу информации являются:

1. Гражданско-правовой (Право интеллектуальной собственности, авторское и патентное право). Его отличительными признаками являются диспозитивность, равноправие и координация воли субъектов правоотношений.

2. Государственно-правовой (законодательство о СМИ, законодательство об общедоступных государственных информационных ресурсах).

Здесь императивность на фоне недостаточного развития механизма санкционирования (поддержания действия) приводит к некоторой декларативности норм, устанавливающих права и обязанности субъектов правоотношений.

6.2. Организация доступа к информации и ограничение в праве на нее.

Доступ к информации обеспечивается органами и организациями путем опубликования или сообщения в иной форме сведений о своей деятельности, в том числе о своем правовом статусе.

Органы государственной власти и органы местного самоуправления публикуют принятые ими правовые акты в установленном законодательством порядке.

Органы и организации обязаны сообщать для всеобщего сведения ставшую им известной при осуществлении своей деятельности информацию если она может предотвратить угрозу жизни или здоровью граждан, если требуется пресечь сообщение недостоверной информации или если она имеет или может иметь общественно значимый характер.

Граждане и организации имеют право на бесплатный доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

Каждый имеет право непосредственно или через своих представителей обращаться в органы и организации с устной или письменной просьбой (запросом) об ознакомлении с интересующей его информацией, о получении соответствующих разъяснений или копий документов.

При этом граждане (наравне с другими пользователями) не обязаны обосновывать перед владельцами государственных информационных ресурсов необходимость получения запрашиваемой ими информации (исключение составляет информация с ограниченным доступом). Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов.

Порядок получения пользователем информации (место, время, ответственных должностных лиц, необходимые процедуры) определяет собственник или владелец информационных ресурсов. Такой порядок не должен противоречить действующему законодательству РФ.

Ответ на запрос о получении информации должен быть дан в возможно короткий срок, но не позднее чем через 30 дней после дня получения запроса, если иное не установлено федеральным законом. Если запрашиваемая информация не может быть предоставлена в указанный срок, обратившемуся за ее получением направляется письменное уведомление об отсрочке предоставления запрашиваемой информации. В уведомлении должны быть указаны причины отсрочки предоставления запрашиваемой информации.

Если орган или организация не обладают запрашиваемой информацией, они не позднее чем через семь дней после дня получения запроса обязаны сообщить об этом обратившемуся, а также предоставить ему наименование и адрес органа или организации, в том числе архива, которые, по имеющимся сведениям, обладают запрашиваемой информацией.

Ответ на запрос предоставляется, по желанию обратившегося, в устной или письменной форме. В ответе могут быть указаны орган, организация или лицо, располагающие более полной информацией по запросу.

Письменные запросы подлежат обязательной регистрации.

Органы и организации обязаны бесплатно предоставлять перечни имеющихся у них информации и услуг, связанных с ее получением.

Информация, затрагивающая права и свободы личности обратившегося, предоставляется бесплатно. За предоставление иной информации может взиматься плата, не превышающая расходы на ее предоставление.

Действие (бездействие) органов и организаций, их должностных лиц, нарушающее право на информацию, может быть обжаловано в суд.

Право на информацию может быть ограничено федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Так, Конституция РФ устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Каждому гарантируется свобода мысли и слова, однако не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства. Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны, а также для распространения передач, пропагандирующих порнографию, культ насилия и жестокости.

Запрещается использование в теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье. Запрещаются распространение в средствах массовой информации, а также в компьютерных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и т.д. Конституция гарантирует свободу массовой информации и запрещает цензуру.

Уголовный кодекс предполагает наказание за воспрепятствование законной профессиональной деятельности журналистов путем принуждения их к распространению либо к отказу от распространения информации.

Органы и организации отказывают в предоставлении информации по запросам, если запрашиваемая информация содержит сведения:

- составляющие государственную тайну;
- об осуществлении в установленном законом порядке оперативно-розыскной и следственной деятельности;
- о судебном рассмотрении гражданских и уголовных дел в случаях, когда разглашение этих сведений запрещено законом или может нарушить право человека на объективное судебное рассмотрение его дела, создать угрозу жизни или здоровью граждан;
- составляющие коммерческую или служебную тайну;

- о частной жизни другого лица без его согласия;
- доступ к которым ограничен федеральными законами.
-

6.3. Информационные ресурсы

Данный параграф основан на федеральном законе «Об информации, информатизации и защите информации».

Согласно закону, информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

Правовой режим информационных ресурсов определяется нормами, устанавливающими порядок документирования информации; право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах; категорию информации по уровню доступа к ней; порядок правовой защиты информации.

Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Информационные ресурсы могут быть и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.

Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо от их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона,

формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.

Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:

- назначить лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;
- устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;
- определять условия распоряжения документами при их копировании и распространении.

Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

- федеральные информационные ресурсы;
- информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации (далее - информационные ресурсы совместного ведения);
- информационные ресурсы субъектов Российской Федерации.

Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспечивают их использование в соответствии с установленной компетенцией.

Деятельность органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов «Информатика» («Информационное обеспечение»).

Организации, которые специализируются на формировании федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора, обязаны получить лицензию на этот вид деятельности в органах государственной власти. Порядок лицензирования определяется законодательством Российской Федерации.

Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию

органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство Российской Федерации.

Порядок и условия обязательного представления документированной информации доводятся до сведения граждан и организаций.

Порядок обязательного представления (получения) информации, отнесенной к государственной тайне, и конфиденциальной информации устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.

При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).

Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов с адресами их представления привлекаются к дисциплинарной ответственности вплоть до снятия с должности.

Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

6.4. Защита информации и прав субъектов в области информационных процессов и информатизации

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

Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации «О государственной тайне»;
- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании Федерального закона;
- в отношении персональных данных - Федеральным законом.

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

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

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

6.5. Права и обязанности субъектов в области защиты информации

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

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

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

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

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

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

Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

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

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

Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Поскольку перечни и списки сведений, составляющих государственную тайну, затрагивают порядок реализации права граждан на поиск и получение информации, в силу ч.3 ст. 10 Федерального закона «Об информации, информатизации и защите информации» они не могут быть засекречены, и любой гражданин вправе ознакомиться с ними в полном объеме.

Максимальный срок ограничения доступа к засекреченной информации составляет 30 лет, вопрос о продлении срока засекречивания рассматривается специальной межведомственной комиссией по защите государственной тайны.

Существует три степени ограничения доступа к сведениям, отнесенным к государственной тайне, обозначаемые соответственно грифами «особой важности», «совершенно секретно», «секретно». Установление иных грифов, равно как и использование перечисленных грифов для засекречивания не отнесенных к гостайне сведений, неправомерно.

Ответственность за сохранение в тайне засекреченных сведений несут только лица, которым они были предоставлены под условием их неразглашения после оформления соответствующего допуска. Факт отсутствия надлежаще оформленного допуска к таким сведениям является основанием для прекращения государственного преследования лица, распространившего их.

Обеспечивать режим конфиденциальности сведений следствия обязаны осуществляющие производство по уголовному делу работники правоохранительных органов, а также лица, присутствовавшие при производстве следственных действий, у которых в порядке ст. 139 УПК РСФСР отобрана подписка о недопустимости разглашения данных предварительного следствия с предупреждением об ответственности по ст. 310 УК РФ. Данные лица до прекращения предварительного расследования могут распространять эти сведения лишь с согласия следователя (дознателя), отобравшего у них подписку, или прокурора.

Законодательство предусматривает лишь один вид процессуальной судебной тайны - тайну совещания судей, предшествующего вынесению решения или приговора. В РФ действует принцип гласности судебного разбирательства. Закрытые судебные слушания допускаются в строго ограниченных законом случаях: в уголовном процессе - в целях предотвращения разглашения составляющих государственную тайну сведений, сведений об интимных сторонах жизни участвующих в деле лиц, по делам о половых преступлениях и преступлениях несовершеннолетних; (ст. 18 УПК РСФСР); в гражданском - в интересах охраны государственной тайны, в целях предотвращения разглашения сведений об интимных сторонах жизни участвующих в деле лиц, а также обеспечения тайны усыновления (ст. 9 ГПК РСФСР); в арбитражном - в предусмотренных федеральным законом о гостайне случаях, а также при удовлетворении ходатайства участвующего в деле лица, ссылающегося на необходимость сохранения коммерческой и иной охраняемой законом тайны (ст. 9 АПК РФ).

Коммерческой тайной является такая информация, которая имеет действительную или потенциальную коммерческую ценность (т.е. владелец информации, используя ее, может получать коммерческую выгоду (прибыль)).

Важным критерием отнесения информации к коммерческой тайне является ее неизвестность третьим лицам.

Ограничение доступа к ней возможно, например, путем установки паролей доступа к информации; охраны помещения, в котором находятся носители информации; отнесения сведений к коммерческой тайне и установления запрета на ее разглашение в должностных инструкциях, трудовом договоре, локальных нормативных актах и т.п.

Правом доступа к таким сведениям обладают лица, связанные с владельцем тайны трудовыми или иными договорными отношениями (работники и контрагенты в сделках), а также государственные органы и их должностные лица в силу своих полномочий (налоговые, судебно-следственные органы, органы валютного контроля, аудиторские организации и т.д.)

Указанные лица, разгласившие информацию, обязаны возместить ее владельцу убытки (включая упущенную выгоду), причиненные таким разглашением (ч.2 п.2 ст. 139 ГК РФ). Иные лица, получившие доступ к этим сведениям незаконно (путем хищения документов, подкупа, угроз и т.п.) в целях их разглашения или иного незаконного использования, несут уголовную ответственность по ч.1 ст. 183 УК РФ и также обязаны возместить убытки (исключая упущенную выгоду) (ч.2 п.2 ст. 139 ГК РФ). Уголовную ответственность по ч.2 ст. 183 УК РФ несет любое лицо, незаконно (без согласия владельца) разгласившее или использовавшее эти сведения из корыстной или иной личной заинтересованности и причинившее крупный ущерб.

Режим коммерческой тайны не должен распространяться на учредительные документы организации, а также документы, дающие право заниматься предпринимательской деятельностью, подтверждающие уплату налогов и сборов, и др. сведения. Полный перечень таких сведений утвержден постановлением Правительства РСФСР от 5 декабря 1991 г. № 35.

В соответствии со ст. 23 Конституции РФ, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну. Ч.1 ст. 24 Конституции РФ запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

П. 5 ст. 49 Закона РФ «О средствах массовой информации» устанавливает для журналиста одно исключение из закрепленного Конституцией общего правила, допуская распространение сведений о личной жизни гражданина без его согласия в целях защиты общественно значимых интересов.

В целях защиты неприкосновенности частной жизни законодательством введена тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Она гарантирована Конституцией РФ и может быть ограничена лишь на основании судебного решения (ч.2 ст. 23), поэтому любые третьи лица, в том числе и журналисты, несут в уголовную ответственность как за ознакомление с содержанием корреспонденции без согласия ее собственников, так и за разглашение этого содержания (ст. 138 УК РФ).

ТЕМА 7. ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

7.1. Интересы личности в информационной сфере.

На проблему информационной безопасности личности замыкаются все цивилизационные потери, политические провалы, культурные утраты, личностные сбои. Именно человек становится не только первой мишенью геополитической информационной войны, но и последним оплотом самосохранения цивилизации. И потому информационная безопасность личности – корневая проблема. Человек не должен терять культурную идентичность, свою особенность, своего “Я”, создающих особый колорит представителей той или иной цивилизации, культуры страны, региона, семьи.

Одним из главных социальных феноменов конца XX – начала XXI века является информационная сфера, представляющая собой область производства, поиска, получения, передачи и распространения информации как внутри страны, так и за рубежом. Среди характерных черт данного явления – стремительное увеличение информационных ресурсов, производимых человечеством. Оно сопровождается включением значительного числа трудоспособного населения в сферу интеллектуального труда, развитием интеллектуальной собственности, появлением новых информационных технологий. Все это не может пройти бесследно для человеческой личности.

Информационная революция в стране как прямое следствие реформаторских процессов способствовала не только значительному росту количества и качества информационной продукции, но и сопровождалась выбросом на “рынок новостей” избыточной, во многом искаженной и недостоверной информации.

Все это обостряет проблему обеспечения информационной безопасности личности и делает ее исключительно злободневной и актуальной.

Безопасность человека понимается нами как состояние защищенности его жизненно важных интересов, т.е. совокупности потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, от внутренних и внешних угроз.

В условиях современной России угрозы информационной безопасности личности можно было бы свести к трем основным группам.

К первой группе угроз, можно отнести те угрозы, которые связаны с развитием девиантного поведения личности. В результате неупорядоченности информационных потоков, особенно в нынешних российских СМИ, в значительной мере повышаются такие явления, как рост агрессивности среди молодежи; ослабление социального самоконтроля юношества, возникающего в результате противоречия между ранней физиологической зрелостью подростков и возросшим валом порнопродукции; резкая активация иррациональной сферы общественного сознания; усиление садо-мазохистских наклонностей в поведении молодых людей и т.д.

Ко второй группе относятся угрозы, связанные с вестернизацией сознания граждан Российской Федерации. И, наконец, к третьей группе угроз принадлежат угрозы, связанные с дестабилизацией социальной преемственности поколений. Как подтверждают исследования, отчуждение общества от позитивного исторического опыта – ныне один из основных принципов построения информационных потоков в современных российских СМИ демократической направленности.

Как отмечалось ранее в новой редакции Концепции национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 10 января 2000 г. № 24, интересы личности состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии.

Интересы человека, которые необходимо охранять в информационном обществе, заключаются прежде всего в реальном обеспечении конституционных прав и свобод человека и гражданина на доступ к открытой информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность, духовное и интеллектуальное развитие.

Наиболее опасным источником угроз этим интересам является существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг него индивидуального “виртуального информационного пространства”, а также возможности использования технологий воздействия на его психическую деятельность.

Важной особенностью образа жизни человека в информационном обществе является существенное сокращение “информационных” расстояний (времени доступа к требуемой информации), что ведет к появлению новых возможностей – как по формированию личности, так и по реализации ее потенциала. Человечество вплотную подходит к рубежу, за которым информационная инфраструктура становится, по существу, основным источником информации для человека, оказывает непосредственное влияние на его психическую деятельность, на формирование его социального поведения.

Направленность использования полученной информации и получаемые результаты определяются, прежде всего, личностью человека и его духовным потенциалом.

Сложность процедур, реализуемых в современных технологиях доступа к требуемым информационным ресурсам, критически увеличивает зависимость человека от других людей, осуществляющих разработку информационных технологий, определение алгоритмов поиска требуемой информации, ее предварительной обработки, приведения к виду, удобному для восприятия, доведение до потребителя. По существу, эти люди во многом формируют для человека информационный фон его жизни, определяют условия, в которых он живет и действует, решает свои жизненные проблемы. Именно поэтому представляется исключительно важным обеспечить безопасность взаимодействия человека с информационной инфраструктурой.

Другим опасным источником угроз интересам человека является использование во вред его интересам персональных данных, накапливаемых различными структурами, в том числе органами государственной власти, а также расширение возможности скрытого сбора информации, составляющей его личную и семейную тайну, сведений о его частной жизни.

Кроме того, безопасность человека представляет собой систему, входящей в качестве составной части в метасистему, которую на официальном уровне принято именовать национальной безопасностью Российской Федерации. Эта метасистема объединяет безопасность личности, общества и государства в различных сферах: политической, военной, экономической, экологической, информационной и других. Что касается информационной безопасности личности, то она является подсистемой безопасности личности и представляет собой состояние защищенности ее жизненно важных интересов от внутренних и внешних угроз в информационной сфере. При этом под внутренними угрозами понимаются условия и факторы, создающие опасность для информационных интересов, источники которых находятся внутри страны, а под внешними угрозами – те, которые исходят из-за рубежа.

Жизненно важные интересы человека в информационной сфере представляют собой совокупность информационных потребностей, удовлетворение которых надежно обеспечивает его существование и возможности прогрессивного развития. К их числу относятся потребности своевременно получать, производить, потреблять, перерабатывать, хранить, передавать и распространять информацию, необходимую для существования и прогрессивного развития человека, а также быть огражденным от ложной, дефектной, фальсифицированной и другой вредной информации, представляющей угрозу для его существования и прогрессивного развития. Удовлетворение этих потребностей является конституционным правом каждого человека и гражданина, при условии, что это право осуществляется законным способом. Воспрепятствование удовлетворению законных информационных интересов человека представляет собой угрозу его информационной безопасности.

Итак, к жизненно важным интересам личности относятся права и свободы человека и гражданина. В информационной сфере их основу составляют нормы Конституции РФ о праве каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23), а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23).

Центральным является понятие "частная жизнь" – та область жизнедеятельности человека, которая принадлежит только ему, а не обществу и государству, и поэтому, по общему правилу, не подлежит контролю с их стороны. Личная и семейная тайна являются частью единого понятия частной жизни. "Тайна" частной жизни определяется как скрываемые от других сведения о частной жизни. Тайна выражается в персонификации информации о личности. Так, никто не обязан сообщать о своем отношении к религии и не может подвергаться принуждению при определении своего отношения к религии, к исповеданию или отказу от исповедания религии, к участию или неучастию в богослужениях, других религиозных обрядах и церемониях, в деятельности религиозных объединений, в обучении религии.

Различие между личной и семейной тайной условно и проводится через принадлежность интересов одному или нескольким лицам. Если тайна принадлежит одному лицу – личная, если нескольким – семейная. В последнем случае круг лиц ограничивается наличием родственных связей.

Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.

Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использова-

ния информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицензирования определяется законодательством Российской Федерации. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 настоящего Федерального закона и законодательства о персональных данных.

Перечень конфиденциальных сведений в РФ включает:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
- сведения, составляющие тайну следствия и судопроизводства.
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Различают тайны двух видов: тайны личные – никому не доверяемые, и тайны профессиональные, в основе которых – личные, защищенные от разглашения запретами, адресованными тем, кому тайны по необходимости доверены (следователь, адвокат, врач, нотариус и т.д.).

Устранение угрозы от несанкционированного и неправомерного воздействия на персонифицированную информацию обеспечивается следующими правовыми мерами: установлением исчерпывающего перечня государственных органов, должностных лиц и частных организаций, которые в праве иметь в своем распоряжении информацию о частной жизни личности; запретом кому бы то ни было, кроме этих субъектов собирать, хранить и разглашать информацию о частной жизни граждан, в том числе и умерших; установления перечня сведений, составляющих информацию о частной жизни; предоставлением гражданину права отказаться сообщать факты о собственной частной жизни любой организации, за исключением случаев, предусмотренных законом; установлением правил использования и открытия личной информации, порядка ознакомления граждан с документами, касающимися их лично; формулированием условий, при которых некоторые документы с информацией о частной жизни не подлежат выдачи; установлением конкретных мер юридической ответственности за вторжение в частную жизнь посредством неправильного использования документов и ин-

формации органами государственной власти и управления, частными лицами и организациями.

Кроме того, граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.

Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации.

Субъекты, представляющие информацию о себе для комплектования информационных ресурсов имеют право бесплатно пользоваться этой информацией. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

Угрозы от воздействия ложной и недостоверной информации блокируются предоставлением правовой защиты таким личным благам, как честь и доброе имя.

Конституция РФ провозглашает недопустимость разглашения информации, которой обмениваются между собой люди. Вся эта информация не должна подвергаться цензуре. Защита предоставляется информации, передаваемой по любым техническим каналам связи. Работники организаций, обслуживающие эти каналы коммуникаций, должностные и иные официальные лица (следователи, понятые, присутствующие при выемке корреспонденции, и т.п.) несут ответственность за разглашение содержания корреспонденций.

Согласно ч. 2 ст. 23 Конституции РФ каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Данная норма отражает коммуникационный аспект частной жизни.

На основе соблюдения конституционных норм о неприкосновенности частной жизни и конфиденциальности корреспонденции должна строиться вся система нормативно-правового обеспечения безопасности в информационной сфере, поскольку права и свободы человека и гражданина имеют высший приоритет. Особенно осторожно при этом следует относиться к ограничению этих прав в правоохранных целях.

7.2. Профессиональные тайны как подсистема информационной безопасности личности

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки.

Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Врачебная тайна.

Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных частями третьей и четвертой настоящей статьи.

Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

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

Согласно постановлению Фонда социального страхования РФ от 17 мая 1995 г. № 25 при оформлении документов, удостоверяющих временную нетрудоспособность граждан, и других медицинских документов специальные печати или штампы учреждения, организации используются без указания его профиля.

Профессиональные тайны ЗАГСa и нотариата.

Сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат.

Руководитель органа записи актов гражданского состояния сообщает в орган социальной защиты населения, налоговый орган и орган Пенсионного фонда Российской Федерации в порядке, установленном нормативными правовыми актами Российской Федерации, сведения о государственной регистрации смерти.

Руководитель органа записи актов гражданского состояния обязан сообщить сведения о государственной регистрации акта гражданского состояния по запросу суда (судьи), органов прокуратуры, органов дознания или следствия либо Уполномоченного по правам человека в Российской Федерации и в других случаях, установленных федеральными законами.

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

Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

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.

Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Это относится к профессиональным тайнам средств массовой информации (СМИ).

Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая,

когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, признанного потерпевшим, без согласия самого несовершеннолетнего и (или) его законного представителя.

Распространение сообщений и материалов, подготовленных с использованием скрытой аудио- и видеозаписи, кино- и фотосъемки, допускается, если это не нарушает конституционных прав и свобод человека и гражданина; если это необходимо для защиты общественных интересов и приняты меры против возможной идентификации посторонних лиц; если демонстрация записи производится по решению суда.

Налоговая тайна.

Налоговую тайну составляют любые полученные налоговым органом, органами налоговой полиции, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:

- 1) разглашенных налогоплательщиком самостоятельно или с его согласия;
- 2) об идентификационном номере налогоплательщика;
- 3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;
- 4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам).

Налоговая тайна не подлежит разглашению налоговыми органами, органами налоговой полиции, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом.

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу производственной или коммерческой тайны налогоплательщика, ставшей известной должностному лицу налогового органа, органа налоговой полиции, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей.

Поступившие в налоговые органы, органы налоговой полиции, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа.

Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица по перечням, определяемым соответственно Министерством Российской Федерации по налогам и сборам, органами государственных внебюджетных фондов, Федеральной службой налоговой полиции Российской Федерации и Государственным таможенным комитетом Российской Федерации.

Утрата документов, содержащих составляющие налоговую тайну сведения, либо разглашение таких сведений влечет ответственность, предусмотренную федеральными законами.

Кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Это относится к банковской тайне. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиен-

тов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

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

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

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

Информация по операциям юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, и физических лиц предоставляется кредитными организациями в уполномоченный орган, осуществляющий 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."

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

ТЕМА 8. ЗАЩИТА ЛИЧНЫХ ИМУЩЕСТВЕННЫХ И НЕИМУЩЕСТВЕННЫХ ПРАВ ЛИЧНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право на имя, право авторства, иные личные неимущественные права и другие нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом. В случаях и в порядке, предусмотренных законом, личные неимущественные права и другие нематериальные блага, принадлежавшие умершему, могут осуществляться и защищаться другими лицами, в том числе наследниками правообладателя. В этой главе будут затронуты как вопросы защиты личных неимущественных благ, так и некоторые материальные права в части авторского права.

8.1. Честь и достоинство

Честь - это сопровождающееся положительной оценкой отражение качеств лица в общественном сознании (т.е. общественная оценка личности). Унижение чести предполагает, что истец ощущает изменение общественного мнения о себе в результате его дискредитации в глазах общества.

Достоинство есть ощущение человеком своей ценности как личности. Оно включает в себя осознание человеком своей абстрактной и конкретно-социальной ценности, а также ценности социальных групп, в которые он входит. Достоинство по определению может быть

только со знаком "плюс" - есть ли у данного лица те или иные положительные качества и что по поводу этого лица считает общественное мнение, не существенно.

Обладателем чести и достоинства может быть только физическое лицо.

Необходимо дифференцировать понятия "репутация" и "деловая репутация". Понятие репутации отсутствует в текстах закона, есть лишь понятие деловой репутации как нематериального права личности.

В статье 152 ГК РФ нет достаточной четкости в регламентации данного института. Поэтому в правоприменительной практике наблюдаются существенные расхождения в толковании этого понятия.

Так, Высший арбитражный суд России в своих постановлениях неоднократно подчеркивал, что понятие деловой репутации в гражданско-правовом смысле применимо только к физическим и юридическим лицам, участвующим в деловом обороте. По мнению арбитражных судов, это понятие имеет связь прежде всего с предпринимательской деятельностью. В свою очередь, Верховный суд РФ и вслед за ним суды общей юрисдикции, склонны отождествлять понятие деловой репутации не только с репутацией предприимчивости, но и с профессиональной, служебной репутацией гражданина или юридического лица.

Клевета и оскорбление - преступления, совершаемые с прямым умыслом: распространитель умышленно действует, желая опорочить или оскорбить человека, осознавая общественную опасность своих действий.

При клевете лицо, распространяющее порочащие сведения, заранее (заведомо) знает о том, что они ложные, но, несмотря на это, сознательно желает и принимает все возможные меры для ее распространения, понимая при этом, какой ущерб эти сведения могут нанести потерпевшему; желает наступления преступного результата - восстановления общественного мнения против фигуранта распространяемого сообщения. Для клеветы не имеет значения форма выражения измышлений. Она может быть как допустимой, так и неприличной.

Оскорбление характеризуется неприличностью формы. Оно может быть нанесено как в словесной форме (вербально), так и путем совершения непристойных действий. Оскорбление, как правило, вызывает личную обиду потерпевшего и может не сопровождаться изменением общественного мнения в отношении него.

Если распространяемая информация содержит в себе только отрицательную оценку личности либо каких-то отдельных ее качеств, но не содержит указаний на конкретный факт, конкретное обстоятельство, то распространение таковой должно рассматриваться как оскорбление. Если же в распространяемом сообщении будут указания на конкретные обстоятельства якобы совершенного фигурантом неблагоприятного поступка (если, например, указано, где совершено хищение, когда, какого именно имущества, с кем), при недоказанности этих сведений они рассматриваются как клевета.

Оскорбления могут быть нанесены и путем совершения неприличных действий. Оскорбляющими можно считать изображения конкретной личности, выполненные в неприличной форме. К оскорбляющим действиям следует относить повреждение и изменение внешней формы бюстов, скульптур здравствующих лиц, делающие эти бюсты и скульптуры неприличными как по форме, так и по содержанию. Оскорбление может быть нанесено гражданину и путем совершения в его отношении различного рода неприличных по своей форме и содержанию действий. В частности, к таким действиям относятся похлопывания по отдельным интимным частям человеческого тела, оголение отдельных его участков, неприличная мимика и т.д.

Если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.

Компенсация морального вреда - одна из мер восстановления нарушенных личных неимущественных благ, установленная законодательством. Статья 151 Гражданского кодекса

РФ определяет моральный вред как физические или нравственные страдания. Таковые может испытывать только живой человек. Юридическое же лицо - искусственное образование, не обладающее ни телом, ни сознанием, - испытывать какие-либо мучения неспособно "по определению".

При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинен вред.

Норма статьи 151 ГК РФ устанавливает право гражданина на компенсацию морального вреда. Однако пункт 7 следующей, 152-й статьи ГК РФ гласит, что правила о защите деловой репутации гражданина соответственно применяются к защите деловой репутации юридического лица. Учитывая, что право на компенсацию морального вреда является одним из элементов этих правил, получается, что на таковую вправе претендовать и юридическое лицо. Таким образом, коллизия двух норм очевидна.

Основные особенности гражданско-правовой защиты чести, достоинства и деловой репутации:

- на требования о защите личных неимущественных благ не распространяются сроки исковой давности (т.е. они могут быть предъявлены в любое время после публикации)
- бремя доказывания факта соответствия действительности распространенных сведений закон возлагает на ответчика (т.е. на распространителя) (ст. 152 ГК РФ);
- компенсация морального вреда осуществляется независимо от вины причинителя вреда в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию (ст. 1100 ГК РФ).

Признаки правонарушения, установленного ст. 152 ГК РФ:

- факт распространения;
- распространены именно сведения;
- сведения не соответствуют действительности;
- сведения относятся к истцу;
- сведения являются порочащими.

Отсутствие в распространенной информации хотя бы одного из этих признаков свидетельствует о том, что действия распространителя не образуют состава правонарушения, предусмотренного ст. 152 ГК РФ (т.е. имеются основания для отказа истцу в удовлетворении его требований).

Человеку от рождения или в силу закона принадлежат и иные неимущественные права: право на жизнь и здоровье, право на личную неприкосновенность, право на доброе имя, право на неприкосновенность частной жизни, личную и семейную тайну (см. ст. 150 ГК РФ). Перечень этих благ не является закрытым, закон защищает и другие нематериальные блага, прямо не указанные в этом перечне.

Единственный критерий, позволяющий разграничить действительные и мнимые нематериальные права (например, суд может быть поставлен перед необходимостью выяснять, существуют ли такие блага, как, например, "честь завода", "честь мундира", "честь города", "статус депутата", профессиональная, служебная репутация) - принадлежность таковых лицу от рождения или в силу закона.

8.2. Авторское право

Согласно статье 44 Конституции РФ каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом. В целом, отношения, связанные с авторским правом, регулируют Федеральным законом «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-І и гражданским кодексом.

В Федеральном законе определены следующие основные понятия.

Автор - физическое лицо, творческим трудом которого создано произведение. Автору в отношении его произведения принадлежат следующие личные неимущественные права:

- право признаваться автором произведения (право авторства);
- право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, то есть анонимно (право на имя);
- право обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
- право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Автор имеет право отказаться от ранее принятого решения об обнародовании произведения (право на отзыв) при условии возмещения пользователю причиненных таким решением убытков, включая упущенную выгоду. Если произведение уже было обнародовано, автор обязан публично оповестить о его отзыве. При этом он вправе изъять за свой счет из обращения ранее изготовленные экземпляры произведения. При создании служебных произведений положения настоящего пункта не применяются.

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

Автору в отношении его произведения принадлежат также имущественные права: исключительные права на использование произведения в любой форме и любым способом.

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

- воспроизводить произведение (право на воспроизведение);
- распространять экземпляры произведения любым способом: продавать, сдавать в прокат и так далее (право на распространение);
- импортировать экземпляры произведения в целях распространения, включая экземпляры, изготовленные с разрешения обладателя исключительных авторских прав (право на импорт);
- публично показывать произведение (право на публичный показ);
- публично исполнять произведение (право на публичное исполнение);
- сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения путем передачи в эфир и (или) последующей передачи в эфир (право на передачу в эфир);
- сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения по кабелю, проводам или с помощью иных аналогичных средств (право на сообщение для всеобщего сведения по кабелю);
- переводить произведение (право на перевод);
- переделывать, аранжировать или другим образом перерабатывать произведение (право на переработку).

Воспроизведение произведения - изготовление одного или более экземпляров произведения или его части в любой материальной форме, в том числе в форме звуко- и видеозаписи, изготовление в трех измерениях одного или более экземпляров двухмерного произведения и в двух измерениях - одного или более экземпляров трехмерного произведения; запись произведения в память ЭВМ также является воспроизведением.

Воспроизведение произведения - это повторение произведения в любой материальной форме. Воспроизведение есть не творческий, а механический процесс, не влекущий появления нового объекта авторского права. Творческий повтор не есть воспроизведение. Поэтому копирование живописного полотна (картины) от руки является не воспроизведением, а созданием нового объекта авторского права.

Изготовление на основе оригинального произведения или фонограммы копий (экземпляров) обычно не умаляет достоинств произведения (фонограммы), ибо, как правило, копия (экземпляр) полностью воспроизводит форму оригинала.

Однако в отношении произведений изобразительных искусств дело обстоит иначе. Копия из произведения не равноценна оригиналу. При копировании произведения изобразительного искусства теряется часть информации, содержащейся в оригинале произведения. Поэтому в этой сфере установлен разный правовой режим для оригинала и для копии.

Признаки объекта авторского права:

- 1) произведения науки, литературы и искусства;
- 2) являющиеся результатом творческой деятельности;
- 3) независимо от назначения и достоинства произведения, а также от способа его выражения.

Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено. Передача права собственности на материальный объект или права владения материальным объектом сама по себе не влечет передачи каких-либо авторских прав на произведение, выраженное в этом объекте.

Не являются объектами авторского права:

- официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы;
- государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки);
- произведения народного творчества;
- сообщения о событиях и фактах, имеющие информационный характер.

Произведения народного творчества не охраняются авторским правом вследствие отсутствия лица, которое может быть идентифицировано как автор.

События и факты, содержащиеся в информационных сообщениях, не получают охраны по авторскому праву в силу того, что являются содержательной частью сообщения, тогда как авторское право охраняет форму произведения, а не его содержание. Что касается самих сообщений, то они не охраняются авторским правом постольку, поскольку неоригинальны, представляют собой простое, механическое, нетворческое переложение событий и фактов. В случае, если форма выражения информационных сообщений является оригинальной, они являются объектом авторского права.

Использование произведения без согласия автора и без выплаты авторского вознаграждения возможно при наличии совокупности следующих условий:

- 1) отсутствие неоправданного ущерба нормальному использованию произведения;
- 2) соблюдение (отсутствие необоснованного ущемления) законных интересов автора;
- 3) обязательное указание имени автора, произведение которого используется, и источника заимствования.

Срок действия авторского права

- В течение всей жизни автора и 50 лет после его смерти, кроме случаев, предусмотренных настоящей статьей.

Право авторства, право на имя и право на защиту репутации автора бессрочны.

Авторское право на произведение, обнародованное анонимно или под псевдонимом, действует в течение 50 лет после даты его правомерного обнародования.

Авторское право на произведение, созданное в соавторстве, действует в течение всей жизни и 50 лет после смерти последнего автора, пережившего других соавторов.

Авторское право на произведение, впервые выпущенное в свет после смерти автора, действует в течение 50 лет после его выпуска.

Исчисление сроков начинается с 1 января года, следующего за годом, в котором имел место юридический факт, являющийся основанием для начала течения срока.

По истечении срока действия авторского права на произведения они переходят в общественное достояние, они могут свободно использоваться любым лицом без выплаты авторского вознаграждения при условии соблюдения права авторства, права на имя и права на защиту репутации автора.

Авторское право переходит по наследству.

Не переходят по наследству право авторства, право на имя и право на защиту репутации автора произведения. Наследники автора вправе осуществлять защиту указанных прав. Эти правомочия наследников сроком не ограничиваются. При отсутствии наследников автора защиту указанных прав осуществляет специально уполномоченный орган Российской Федерации.

Имущественные права могут передаваться только по авторскому договору. В устной форме он может быть заключен только в случаях использования произведения в периодической печати. Права, передаваемые по авторскому договору, считаются неисключительными, если в договоре прямо не предусмотрено иное. Авторский договор может заключаться только в отношении тех произведений, которые уже созданы, однако возможно также заключение авторского договора заказа, по которому автор обязуется создать произведение в соответствии с условиями договора и передать его заказчику.

Существенные условия авторского договора:

1) способы использования произведения (конкретные права, передаваемые по данному договору)

(Прямо не переданные по договору права на использование произведения считаются не переданными);

2) срок (Если условие о сроке передачи права отсутствует, по истечении 5 лет с даты заключения договора он может быть расторгнут автором с предварительным письменным уведомлением противоположной стороны за 6 месяцев до расторжения договора);

3) территория, на которые передается право

(Если условие о территории отсутствует, действие передаваемого по договору права ограничивается территорией РФ);

4) размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты (ст. 30-33 Закона об авторском праве).

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

Авторское право распространяется как на обнародованные произведения, так и на необнародованные произведения, существующие в какой-либо объективной форме:

- письменной (рукопись, машинопись, нотная запись и так далее);
- устной (публичное произнесение, публичное исполнение и так далее);
- звуко- или видеозаписи (механической, магнитной, цифровой, оптической и так далее);
- изображения (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фото-кадр и так далее);
- объемно-пространственной (скульптура, модель, макет, сооружение и так далее); в других формах.

- Объектами авторского права являются:
- литературные произведения (включая программы для ЭВМ);
- драматические и музыкально-драматические произведения, сценарные произведения;
- хореографические произведения и пантомимы;
- музыкальные произведения с текстом или без текста;
- аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения);
- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
- произведения декоративно-прикладного и сценографического искусства;
- произведения архитектуры, градостроительства и садово-паркового искусства;
- фотографические произведения и произведения, полученные способами, аналогичными фотографии;
- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;
- другие произведения.

К объектам авторского права также относятся:

- производные произведения (переводы, обработки, аннотации, рефераты, резюме, обзоры, инсценировки, аранжировки и другие переработки произведений наук, литературы и искусства);
- сборники (энциклопедии, антологии, базы данных) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Производные произведения и составные произведения охраняются авторским правом независимо от того, являются ли объектами авторского права произведения, на которых они основаны или которые они включают.

Не являются объектами авторского права:

- официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы;
- государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки);
- произведения народного творчества;
- сообщения о событиях и фактах, имеющие информационный характер.

Авторское право на произведение науки, литературы и искусства возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов: латинской буквы «С» в окружности: С; имени (наименования) обладателя исключительных авторских прав; года первого опубликования произведения.

При отсутствии доказательств иного автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения.

При опубликовании произведения анонимно или под псевдонимом (за исключением случая, когда псевдоним автора не оставляет сомнения в его личности) издатель, имя или наименование которого обозначено на произведении при отсутствии доказательств иного счи-

тается представителем автора в соответствии с настоящим Законом и в этом качестве имеет право защищать права автора и обеспечивать их осуществление. Это положение действует до тех пор, пока автор такого произведения не раскроет свою личность и не заявит о своем авторстве.

Авторское право на произведение, созданное совместным творческим трудом двух или более лиц (соавторство), принадлежит соавторам совместно независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение.

Часть произведения признается имеющей самостоятельное значение, если она может быть использована независимо от других частей этого произведения.

Каждый из соавторов вправе использовать созданную им часть произведения, имеющую самостоятельное значение, по своему усмотрению, если иное не предусмотрено соглашением между ними.

Право на использование произведения в целом принадлежит соавторам совместно.

Обладатели исключительных авторских и смежных прав вправе требовать от нарушителя:

- 1) признания прав;
- 2) восстановления положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушению;
- 3) возмещение убытков, включая упущенную выгоду;
- 4) взыскания дохода, полученного нарушителем вследствие нарушения авторских и смежных прав, вместо возмещения убытков;
- 5) выплаты компенсации в сумме от 10 до 50000 минимальных размеров оплаты труда, устанавливаемых законодательством Российской Федерации, определяемой по усмотрению суда или арбитражного суда, вместо возмещения убытков или взыскания дохода;
- 6) принятия иных предусмотренных законодательными актами мер, связанных с защитой их прав.

8.3. Доменные имена: проблемы правового регулирования

Отдельным параграфом в части авторского права нами вынесен вопрос о проблемах правового регулирования отношений, связанных с всемирной сетью.

Развитие информационных технологий в конце XX века привело к появлению новых форм и способов ведения хозяйственной деятельности, базирующихся на использовании возможностей глобальной сети "Интернет". Удельный вес так называемой интернет-коммерции в мировой экономике, включая и Россию, имеет тенденцию к возрастанию, в связи с этим возник ряд сложных проблем как в сфере публичного, так и частного права.

Особенную актуальность в последнее время приобретает вопрос о правовом статусе доменных имен, являющихся средством индивидуализации в сети "Интернет". Проблема доменных имен является новой для отечественной юридической науки и правоприменительной практики, чем и объясняется отсутствие на данный момент заметных научных работ в этой сфере. Законодательство России в настоящее время вообще не содержит нормативно-правовых актов, регулирующих отношения, возникающие в связи с регистрацией, использованием и оборотом доменных имен. Отсутствует законодательно определенная терминология и понятийный аппарат. Подобное состояние правового регулирования порождает неопределенность в сфере оборота доменных имен и судебной практике. В качестве примера можно привести решение Арбитражного суда г. Москвы по делу "Кодак Истман Компани" против предпринимателя без образования юридического лица о пресечении нарушения прав на товарный знак (о запрете ответчику использовать товарный знак "KODAK"TM в наименовании доменного имени). Суд в мотивировочной части решения определил, что оснований для удовлетворения иска не имелось, так как на день рассмотрения дела не существовало закона или иного правового акта, регулирующего взаимоотношения, связанные с наименованием домена.

Единственным источником непосредственного регулирования оборота доменных имен являются акты Российского Научно-Исследовательского Института развития общественных сетей. Последний создан в 1992 году, ныне действует как некоммерческая организация (организационно-правовая форма – учреждение) и осуществляет регистрацию доменов в зоне .ru и в этом качестве представлен в международном Центре по регистрации адресного пространства Интернет RIPE NCC (Голландия, Амстердам). Будучи некоммерческой организацией, РосНИИРОС не может создавать нормативно-правовые акты, тем не менее, понятийный аппарат и регламент этого учреждения могут послужить основой для будущих нормативных актов.

В конце 1999 года был подготовлен проект нормативного акта, регулирующего оборот доменных имен, однако Положение "О порядке выделения и использования доменных имен в российском сегменте сети "Интернет" (далее – Положение) так и не было утверждено. Среди положительных моментов в проекте Положения можно выделить то, что впервые предпринята попытка урегулировать оборот доменных имен второго уровня в зоне .ru

Проект включает систему терминов, например, определяет понятие доменного имени, IP-адреса, официального адреса и т.д.

Несмотря на наличие положительных сторон проекта, он содержит и ряд противоречий с действующим законодательством. Так, п. 2.1 проекта предусматривает, что доменное имя официального сайта в российском сегменте сети "Интернет" (в зоне .ru) является обязательным реквизитом и указывается во всех видах действующей отчетности для значительного числа юридических лиц, в том числе открытых акционерных обществ, СМИ, кредитных организаций, юридических лиц с участием иностранного капитала и многих других. Подобное требование не предусмотрено ни одним действующим законом, регулирующим соответствующие сферы хозяйственной деятельности. Кроме того, проект не решил основную проблему – о правовой природе доменного имени, что, как представляется, вообще невозможно в нормативном акте такого уровня.

Отвлекаясь от технической составляющей оборота доменных имен, в проблеме доменных имен можно выделить два основных направления.

Первым является вопрос о последствиях использования в доменном имени объектов интеллектуальной собственности, прежде всего фирменных наименований и товарных знаков. Как показала судебная практика, данная сторона проблемы вызывает определенные сложности, несмотря на наличие законодательства, посвященного охране фирменных наименований и товарных знаков.

Вторым - вопрос о правовой природе доменного имени и возможность отнесения его к объектам интеллектуальной собственности. Данная проблема достаточно сложна и заслуживает отдельного рассмотрения, поэтому отметим лишь наиболее важные положения.

Под объектом интеллектуальной собственности обычно в литературе понимается благо нематериальное, являющееся результатом интеллектуальной деятельности и на которое за достигнувшем его лицом или иным правообладателем признается исключительное право на его использование. Кроме того, к ним приравниваются средства индивидуализации – фирменные наименования, товарные знаки и другие. Необходимо отметить, что ст. 138 ГК РФ "Интеллектуальная собственность" содержит исчерпывающий перечень возможных средств индивидуализации, что открывает возможность дополнения традиционных объектов интеллектуальной собственности новыми. Представляется, что доменное имя, являясь нематериальным по своей сути, выполняет индивидуализирующую функцию в определенной области пространства в сети "Интернет" ("домен" как таковой). В этом смысле доменное имя близко к товарным знакам. Однако в настоящее время доменные имена не относятся к объектам интеллектуальной собственности, так как по ст. 138 ГК РФ исключительное право на тот или иной объект должно быть установлено законом. Как уже отмечалось, специальный закон о доменных именах отсутствует.

В заключение необходимо отметить, что в настоящее время имеется необходимость в принятии закона, регулирующего правовой режим доменных имен как средств индивидуали-

зации и объектов исключительных прав. Подобный нормативный акт мог бы войти в институт законодательства о средствах индивидуализации, дополнив тем самым подотрасль права интеллектуальной собственности.

ТЕМА 9. СМИ КАК ОБЪЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО ОБЩЕСТВА

9.1. Правовые основы СМИ

Средство массовой информации - форма периодического распространения массовой информации (предназначенных для неограниченного круга лиц сообщений и материалов). Таким образом, СМИ - объект, а не субъект права. Закон о СМИ, однако, зачастую недостаточно четко разводит эти два разных понятия, порой употребляя термин «СМИ» и для обозначения субъекта права. В основу настоящей главы положен Федеральный закон «О средствах массовой информации» от 27 декабря 1991 г. № 2124-I (с последующими изменениями).

Под массовой информацией понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Под средством массовой информации понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации.

Под периодическим печатным изданием понимается газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год.

Под продукцией средства массовой информации понимается тираж или часть тиража отдельного номера периодического печатного издания, отдельный выпуск радио-, теле-, кинохроникальной программы, тираж или часть тиража аудио- или видеозаписи программы.

Под распространением продукции средства массовой информации понимается продажа (подписка, доставка, раздача) периодических печатных изданий, аудио- или видеозаписей программ, трансляция радио, телепрограмм (вещание), демонстрация кинохроникальных программ.

Под редакцией средства массовой информации понимается организация, учреждение, предприятие либо гражданин, объединение граждан, осуществляющие производство и выпуск средства массовой информации.

Под главным редактором понимается лицо, возглавляющее редакцию (независимо от наименования должности) и принимающее окончательные решения в отношении производства и выпуска средства массовой информации.

Под журналистом понимается лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию.

Под издателем понимается издательство, иное учреждение, предприятие (предприниматель), осуществляющее материально-техническое обеспечение производства продукции средства массовой информации, а также приравненное к издателю юридическое лицо или гражданин, для которого эта деятельность не является основной либо не служит главным источником дохода.

Под распространителем понимается лицо, осуществляющее распространение продукции средства массовой информации по договору с редакцией, издателем или на иных законных основаниях.

Свобода массовой информации в Российской Федерации распространяется на поиск, получение, производство и распространение массовой информации, учреждение средств

массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации, не подлежат ограничениям, за исключением предусмотренных законодательством Российской Федерации о средствах массовой информации.

Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей, - не допускается.

Создание и финансирование организаций, учреждений, органов или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, - не допускаются.

Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны, а также для распространения передач, пропагандирующих порнографию, культ насилия и жестокости.

Запрещается использование в теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье.

Запрещается распространение в средствах массовой информации, а также в компьютерных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, за исключением рекламы наркотических средств и психотропных веществ, внесенных в списки II и III в соответствии с Федеральным законом «О наркотических средствах и психотропных веществах», в средствах массовой информации, рассчитанных на медицинских и фармацевтических работников, а также распространение иной информации, распространение которой запрещено федеральными законами.

9.2. Организация деятельности средств массовой информации

Порядок организации деятельности СМИ определяется главой 2 Закона о СМИ.

Учредителем (соучредителем) средства массовой информации может быть гражданин, объединение граждан, предприятие, учреждение, организация, государственный орган.

Не может выступать учредителем:

- гражданин, не достигший восемнадцатилетнего возраста, либо отбывающий наказание в местах лишения свободы по приговору суда, либо душевнобольной, признанный судом недееспособным;
- объединение граждан, предприятие, учреждение, организация, деятельность которого запрещена по закону;
- гражданин другого государства или лицо без гражданства, не проживающее постоянно в Российской Федерации.

Соучредители выступают в качестве учредителя совместно.

Редакция средства массовой информации осуществляет свою деятельность после его регистрации. Средство массовой информации считается зарегистрированным со дня выдачи свидетельства о регистрации. Зарегистрированное средство массовой информации не может быть повторно зарегистрировано в том же или ином регистрирующем органе. В случае установления судом факта повторной регистрации законной признается первая по дате регистрация. Смена учредителя, изменение состава соучредителей, а равно названия, языка, формы периодического распространения массовой информации, территории распространения его продукции допускается лишь при условии перерегистрации средства массовой информации. Перерегистрация средств массовой информации осуществляется в том же порядке, что и их регистрация.

Деятельность средства массовой информации может быть прекращена или приостановлена только по решению учредителя либо судом в порядке гражданского судопроизводства по иску регистрирующего органа или Министерства печати и информации Российской Федерации. Учредитель имеет право прекратить или приостановить деятельность средства массовой информации исключительно в случаях и порядке, предусмотренных уставом редакции или договором между учредителем и редакцией (главным редактором). Основанием для прекращения судом деятельности средства массовой информации являются неоднократные в течение двенадцати месяцев нарушения редакцией требований статьи 4 настоящего Закона, по поводу которых регистрирующим органом или Министерством печати и информации Российской Федерации делались письменные предупреждения учредителю и (или) редакции (главному редактору), а равно неисполнение постановления суда о приостановлении деятельности средства массовой информации.

Прекращение деятельности средства массовой информации влечет недействительность свидетельства о его регистрации и устава редакции.

Права и обязанности учредителя и редакции, предусмотренные Законом, возникают с момента регистрации средства массовой информации, а предусмотренные уставом редакции - с момента его утверждения. Учредитель, редакция, издатель, распространитель могут дополнительно установить на договорной основе взаимные права и обязанности. Положения устава и договоров не должны противоречить настоящему Закону и иным актам законодательства Российской Федерации.

Учредитель не вправе вмешиваться в деятельность средства массовой информации, за исключением случаев, предусмотренных Законом, уставом редакции, договором между учредителем и редакцией (главным редактором).

Учредитель может передать свои права и обязанности третьему лицу с согласия редакции и соучредителей. В случае ликвидации или реорганизации учредителя - объединения граждан, предприятия, учреждения, организации, государственного органа его права и обязанности в полном объеме переходят к редакции, если иное не предусмотрено уставом редакции.

Учредитель может выступать в качестве редакции, издателя, распространителя, собственника имущества редакции.

Редакция осуществляет свою деятельность на основе профессиональной самостоятельности.

Редакция может быть юридическим лицом, самостоятельным хозяйствующим субъектом, организованным в любой допускаемой законом форме. Если редакция зарегистрированного средства массовой информации организуется в качестве предприятия, то она подлежит также регистрации в соответствии с законодательством Российской Федерации о предприятиях и предпринимательской деятельности и помимо производства и выпуска средства массовой информации вправе осуществлять в установленном порядке иную, не запрещенную законом деятельность.

В течение двух лет со дня первого выхода в свет (в эфир) продукции средства массовой информации редакция освобождается от налоговых платежей.

Редакция может выступать в качестве учредителя средства массовой информации, издателя, распространителя, собственника имущества редакции.

Редакцией руководит главный редактор, который осуществляет свои полномочия на основе Закона, устава редакции, договора между учредителем и редакцией (главным редактором).

Главный редактор представляет редакцию в отношениях с учредителем, издателем, распространителем, гражданами, объединениями граждан, предприятиями, учреждениями, организациями, государственными органами, а также в суде. Он несет ответственность за выполнение требований, предъявляемых к деятельности средства массовой информации Законом о СМИ и другими законодательными актами Российской Федерации.

Иностранное юридическое лицо, а равно российское юридическое лицо с иностранным участием, доля (вклад) иностранного участия в уставном (складочном) капитале составляет 50 процентов и более, гражданин Российской Федерации, имеющий двойное гражданство, не вправе выступать учредителями теле-, видеопрограмм.

Иностранный гражданин, либо без гражданства и гражданин Российской Федерации, имеющий двойное гражданство, иностранное юридическое лицо, а равно российское юридическое лицо с иностранным участием, доля (вклад) иностранного участия в уставном (складочном) капитале которого составляет 50 процентов и более, не вправе учреждать организации (юридические лица), осуществляющие телевидение, зона уверенного приема передач которых охватывает половину и более половины субъектов Российской Федерации либо территорию, на которой проживает половина и более половины численности населения Российской Федерации.

Отчуждение акций (долей) учредителем теле-, видеопрограммы, в том числе после ее регистрации, организацией (юридическим лицом), осуществляющей (осуществляющим) телевидение, зона уверенного приема передач которой (которого) охватывает половину и более половины субъектов Российской Федерации либо территорию, на которой проживает половина и более половины численности населения Российской Федерации, повлекшее появление в их уставном (складочном) капитале доли (вклада) иностранного участия, составляющей 50 процентов и более, не допускается.

Издатель осуществляет свои права и несет обязанности на основе Закона о СМИ, Федерального закона «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», законодательства об издательском деле, предприятиях и предпринимательской деятельности.

Издатель может выступать в качестве учредителя средства массовой информации, редакции, распространителя, собственника имущества редакции.

При распространении сообщений и материалов информационного агентства другим средством массовой информации ссылка на информационное агентство обязательна.

Правила, установленные законом для периодических печатных изданий, применяются в отношении периодического распространения тиражом тысяча и более экземпляров текстов, созданных с помощью компьютеров и (или) хранящихся в их банках и базах данных, а равно в отношении иных средств массовой информации, продукция которых распространяется в виде печатных сообщений, материалов, изображений.

Правила, установленные настоящим Законом для радио- и телепрограмм, применяются в отношении периодического распространения массовой информации через системы телетекста, видеотекста и иные телекоммуникационные сети, если законодательством Российской Федерации не установлено иное.

Воспрепятствование осуществляемому на законном основании распространению продукции средств массовой информации со стороны граждан, объединений граждан, должностных лиц, предприятий, учреждений, организаций, государственных органов не допускается.

Распространение продукции средства массовой информации считается коммерческим, если за нее взимается плата. Продукция, предназначенная для некоммерческого распростра-

нения, должна иметь пометку «Бесплатно» и не может быть предметом коммерческого распространения.

Демонстрация видеозаписей программ в жилых помещениях, а равно снятие единичных копий с них, если при этом не взимается плата прямо или косвенно, не считается распространением продукции средства массовой информации в смысле настоящего Закона.

Розничная продажа, в том числе с рук, тиража периодических печатных изданий не подлежит ограничениям, за исключением предусмотренных настоящим Законом. Розничная продажа тиража периодических печатных изданий в местах, не являющихся общедоступными - помещениях и иных объектах, в отношении которых собственником или лицом, уполномоченным управлять его имуществом, установлен особый режим пользования, - допускается не иначе как с согласия указанных лиц.

Изъятие, а равно уничтожение тиража или его части допускается не иначе как по вступившему в силу решению суда.

Для средств массовой информации, специализирующихся на производстве продукции рекламного или эротического характера, устанавливается потиражный сбор, взимаемый в порядке, определяемом Правительством Российской Федерации.

Лицензия на вещание дает ее держателю право, используя технические средства эфирного, проводного или кабельного телерадиовещания, в том числе находящиеся в его собственности, осуществлять с соблюдением лицензионных условий распространение продукции средств массовой информации, зарегистрированных в соответствии с настоящим Законом.

В выдаче лицензии на вещание должно быть отказано, если отсутствует техническая возможность осуществлять вещание с заявленными характеристиками либо близкими к ним.

Создание искусственных помех, препятствующих уверенному приему радио-, телепрограмм, то есть распространению радио-, теле- и иных технических сигналов в полосе частот, на которых осуществляется вещание по лицензии, влечет ответственность в соответствии с законодательством Российской Федерации.

В целях обеспечения доказательств, имеющих значение для правильного разрешения споров, редакция радио-, телепрограммы обязана: сохранять материалы собственных передач, вышедших в эфир в записи; фиксировать в регистрационном журнале передачи, вышедшие в эфир. В регистрационном журнале указываются дата и время выхода в эфир, тема передачи, ее автор, ведущий и участники.

Сроки хранения материалов передач - не менее одного месяца со дня выхода в эфир; регистрационного журнала - не менее одного года с даты последней записи в нем.

Гражданам Российской Федерации гарантируется беспрепятственный доступ к сообщениям и материалам зарубежных средств массовой информации.

Ограничение приема программ непосредственного телевизионного вещания допускается не иначе как в случаях, предусмотренных межгосударственными договорами, заключенными Российской Федерацией.

Для распространения продукции зарубежного периодического печатного издания, то есть не зарегистрированного в Российской Федерации и имеющего место постоянного пребывания учредителя или редакции вне ее пределов, а равно финансируемого иностранными государствами, юридическими лицами или гражданами, необходимо получить разрешение Министерства печати и информации Российской Федерации, если порядок распространения не установлен межгосударственным договором, заключенным Российской Федерацией.

9.3. Отношения средств массовой информации с гражданами и организациями

Отношения СМИ с гражданами и организациями определяются главой 3 Закона о СМИ.

Согласно Закону, граждане имеют право на оперативное получение через средства массовой информации достоверных сведений о деятельности государственных органов и организаций, общественных объединений, их должностных лиц.

Государственные органы и организации, общественные объединения, их должностные лица предоставляют сведения о своей деятельности средствам массовой информации по запросам редакций, а также путем проведения пресс-конференций, рассылки справочных и статистических материалов и в иных формах.

Редакция имеет право запрашивать информацию о деятельности государственных органов и организаций, общественных объединений, их должностных лиц. Запрос информации возможен как в устной, так и в письменной форме. Запрашиваемую информацию обязаны предоставлять руководители указанных органов, организаций и объединений, их заместители, работники пресс-служб либо другие уполномоченные лица в пределах их компетенции.

Отказ в предоставлении запрашиваемой информации возможен, только если она содержит сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну. Уведомление об отказе вручается представителю редакции в трехдневный срок со дня получения письменного запроса информации. В уведомлении должны быть указаны причины, по которым запрашиваемая информация не может быть отделена от сведений, составляющих специально охраняемую законом тайну; должностное лицо, отказывающееся в предоставлении информации; дата принятия решения об отказе.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

Редакция обязана соблюдать права на используемые произведения, включая авторские права, издательские права, иные права на интеллектуальную собственность. Автор либо иное лицо, обладающее правами на произведение, может особо оговорить условия и характер использования предоставляемого редакции произведения.

Письмо, адресованное в редакцию, может быть использовано в сообщениях и материалах данного средства массовой информации, если при этом не искажается смысл письма и не нарушаются положения настоящего Закона. Редакция не обязана отвечать на письма граждан и пересылать эти письма тем органам, организациям и должностным лицам, в чью компетенцию входит их рассмотрение.

Никто не вправе обязать редакцию опубликовать отклоненное ею произведение, письмо, другое сообщение или материал, если иное не предусмотрено законом.

Распространение сообщений и материалов, подготовленных с использованием скрытой аудио- и видеозаписи, кино- и фотосъемки, допускается:

- 1) если это не нарушает конституционных прав и свобод человека и гражданина;
- 2) если это необходимо для защиты общественных интересов и приняты меры против возможной идентификации посторонних лиц;
- 3) если демонстрация записи производится по решению суда.

Гражданин или организация вправе потребовать от редакции опровержения не соответствующих действительности и порочащих их честь и достоинство сведений, которые были распространены в данном средстве массовой информации. Такое право имеют также законные представители гражданина, если сам гражданин не имеет возможности потребовать опровержения. Если редакция средства массовой информации не располагает доказательствами того, что распространенные им сведения соответствуют действительности, она обязана опровергнуть их в том же средстве массовой информации.

Если гражданин или организация представили текст опровержения, то распространению подлежит данный текст при условии его соответствия требованиям настоящего Закона. Редакция радио-, телепрограммы, обязанная распространить опровержение, может предоста-

вить гражданину или представителю организации, потребовавшему этого, возможность зачитать собственный текст и передать его в записи.

В опровержении должно быть указано, какие сведения не соответствуют действительности, когда и как они были распространены данным средством массовой информации.

Опровержение в периодическом печатном издании должно быть набрано тем же шрифтом и помещено под заголовком «Опровержение», как правило, на том же месте полосы, что и опровергаемое сообщение или материал. По радио и телевидению опровержение должно быть передано в то же время суток и, как правило, в той же передаче, что и опровергаемое сообщение или материал.

В течение месяца со дня получения требования об опровержении либо его текста редакция обязана в письменной форме уведомить заинтересованных гражданина или организацию о предполагаемом сроке распространения опровержения либо об отказе в его распространении с указанием оснований отказа.

В опровержении может быть отказано:

1) если опровергаются сведения, которые уже опровергнуты в данном средстве массовой информации;

2) если требование об опровержении либо представленный текст его поступили в редакцию по истечении одного года со дня распространения опровергаемых сведений в данном средстве массовой информации.

Гражданин или организация, в отношении которых в средстве массовой информации распространены сведения, не соответствующие действительности либо ущемляющие права и законные интересы гражданина, имеют право на ответ (комментарий, реплику) в том же средстве массовой информации.

Ответ на ответ помещается не ранее чем в следующем выпуске средства массовой информации. Данное правило не распространяется на редакционные комментарии.

9.4. Права и обязанности журналиста

Согласно главе 7 Закона о СМИ, журналист имеет право:

- искать, запрашивать, получать и распространять информацию;
- посещать государственные органы и организации, предприятия и учреждения, органы общественных объединений либо их пресс-службы;
- быть принятым должностными лицами в связи с запросом информации;
- получать доступ к документам и материалам, за исключением их фрагментов, содержащих сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну;
- копировать, публиковать, оглашать или иным способом воспроизводить документы и материалы;
- производить записи, в том числе с использованием средств аудио- и видеотехники, кино- и фотосъемки, за исключением случаев, предусмотренных законом;
- посещать специально охраняемые места стихийных бедствий, аварий и катастроф, массовых беспорядков и массовых скоплений граждан, а также местности, в которых объявлено чрезвычайное положение; присутствовать на митингах и демонстрациях;
- проверять достоверность сообщаемой ему информации;
- излагать свои личные суждения и оценки в сообщениях и материалах, предназначенных для распространения за его подписью;

- отказаться от подготовки за своей подписью сообщения или материала, противоречащего его убеждениям;

- снять свою подпись под сообщением или материалом, содержание которого, по его мнению, было искажено в процессе редакционной подготовки, либо запретить или иным образом оговорить условия и характер использования данного сообщения или материала в соответствии с частью первой статьи 42 настоящего Закона;

- распространять подготовленные им сообщения и материалы за своей подписью, под псевдонимом или без подписи.

Журналист пользуется также иными правами, предоставленными ему законодательством Российской Федерации о средствах массовой информации.

Аккредитованный журналист имеет право присутствовать на заседаниях, совещаниях и других мероприятиях, проводимых аккредитовавшими его органами, организациями, учреждениями, за исключением случаев, когда приняты решения о проведении закрытого мероприятия.

Журналист может быть лишен аккредитации, если им или редакцией нарушены установленные правила аккредитации либо распространены не соответствующие действительности сведения, порочащие честь и достоинство организации, аккредитовавшей журналиста, что подтверждено вступившим в законную силу решением суда.

Журналист обязан соблюдать устав редакции, с которой он состоит в трудовых отношениях; проверять достоверность сообщаемой им информации; удовлетворять просьбы лиц, предоставивших информацию, об указании на ее источник, а также об авторизации цитируемого высказывания, если оно оглашается впервые; сохранять конфиденциальность информации и (или) ее источника; получать согласие (за исключением случаев, когда это необходимо для защиты общественных интересов) на распространение в средстве массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей; при получении информации от граждан и должностных лиц ставить их в известность о проведении аудио- и видеозаписи, кино- и фотосъемки; ставить в известность главного редактора о возможных исках и предъявлении иных предусмотренных законом требований в связи с распространением подготовленного им сообщения или материала; отказаться от данного ему главным редактором или редакцией задания, если оно либо его выполнение связано с нарушением закона; предъявлять при осуществлении профессиональной деятельности по первому требованию редакционное удостоверение или иной документ, удостоверяющий личность и полномочия журналиста.

При осуществлении профессиональной деятельности журналист обязан уважать права, законные интересы, честь и достоинство граждан и организаций.

Государство гарантирует журналисту в связи с осуществлением им профессиональной деятельности защиту его чести, достоинства, здоровья, жизни и имущества как лицу, выполняющему общественный долг.

Не допускается использование установленных настоящим Законом прав журналиста в целях сокрытия или фальсификации общественно значимых сведений, распространения слухов под видом достоверных сообщений, сбора информации в пользу постороннего лица или организации, не являющейся средством массовой информации.

Запрещается использовать право журналиста на распространение информации с целью опорочить гражданина или отдельные категории граждан исключительно по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

9.5. Ответственность за нарушение законодательства о средствах массовой информации

Учредители, редакции, издатели, распространители, государственные органы, организации, учреждения, предприятия и общественные объединения, должностные лица, журналисты, авторы распространенных сообщений и материалов несут ответственность за нарушения законодательства Российской Федерации о средствах массовой информации.

Редакция, главный редактор, журналист не несут ответственности за распространение сведений, не соответствующих действительности и порочащих честь и достоинство граждан и организаций, либо ущемляющих права и законные интересы граждан, либо представляющих собой злоупотребление свободой массовой информации и (или) правами журналиста:

- 1) если эти сведения присутствуют в обязательных сообщениях;
- 2) если они получены от информационных агентств;
- 3) если они содержатся в ответе на запрос информации либо в материалах пресслужб государственных органов, организаций, учреждений, предприятий, органов общественных объединений;
- 4) если они являются дословным воспроизведением фрагментов выступлений народных депутатов на съездах и сессиях Советов народных депутатов, делегатов съездов, конференций, пленумов общественных объединений, а также официальных выступлений должностных лиц государственных органов, организаций и общественных объединений;
- 5) если они содержатся в авторских произведениях, идущих в эфир без предварительной записи, либо в текстах, не подлежащих редактированию в соответствии с настоящим Законом;
- 6) если они являются дословным воспроизведением сообщений и материалов или их фрагментов, распространенных другим средством массовой информации, которое может быть установлено и привлечено к ответственности за данное нарушение законодательства Российской Федерации о средствах массовой информации.

Ущемление свободы массовой информации, то есть воспрепятствование в какой бы то ни было форме со стороны граждан, должностных лиц государственных органов и организаций, общественных объединений законной деятельности учредителей, редакций, издателей и распространителей продукции средства массовой информации, а также журналистов, в том числе посредством:

- осуществления цензуры;
- вмешательства в деятельность и нарушения профессиональной самостоятельности редакции;
- незаконного прекращения либо приостановления деятельности средства массовой информации;
- нарушения права редакции на запрос и получение информации;
- незаконного изъятия, а равно уничтожения тиража или его части;
- принуждения журналиста к распространению или отказу от распространения информации;
- установления ограничений на контакты с журналистом и передачу ему информации, за исключением сведений, составляющих государственную, коммерческую или иную специально охраняемую законом тайну;
- нарушения прав журналиста, установленных настоящим Законом, - влечет уголовную, административную, дисциплинарную или иную ответственность в соответствии с законодательством Российской Федерации.

Злоупотребление свободой массовой информации влечет уголовную, административную, дисциплинарную или иную ответственность в соответствии с законодательством Российской Федерации.

Злоупотребление правами журналиста, либо несоблюдение обязанностей журналиста - влечет уголовную или дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

ТЕМА 10. РЕКЛАМА КАК СОСТАВЛЯЮЩАЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

10.1. Понятие рекламы

Согласно федеральному закону «О рекламе», положенному в основу данной главы, реклама – распространяемая в любой форме, с помощью любых средств информация о физическом или юридическом лице, товарах, идеях и начинаниях (рекламная информация), которая предназначена для неопределенного круга лиц и призвана формировать или поддерживать интерес к этим физическому, юридическому лицу, товарам, идеям и начинаниям и способствовать реализации товаров, идей и начинаний.

Понятийный аппарат Закона составляют следующие сведения:

Ненадлежащая реклама – это недобросовестная, недостоверная, неэтичная, заведомо ложная и иная реклама, в которой допущены нарушения требований к ее содержанию, времени, месту и способу распространения, установленных законодательством Российской Федерации. Контрреклама является опровержением ненадлежащей рекламы, распространяемое в целях ликвидации вызванных ею последствий.

Рекламодатель – юридическое или физическое лицо, являющееся источником рекламной информации для производства, размещения, последующего распространения рекламы.

Рекламопроизводитель – юридическое или физическое лицо, осуществляющее полное или частичное приведение рекламной информации к готовой для распространения форме.

Рекламораспространитель – юридическое или физическое лицо, осуществляющее размещение и (или) распространение рекламной информации путем предоставления и (или) использования имущества, в том числе технических средств радиовещания, телевизионного вещания, а также каналов связи, эфирного времени и иными способами.

Потребители рекламы – юридические или физические лица, до сведения которых доводится или может быть доведена реклама, следствием чего является или может являться соответствующее воздействие рекламы на них.

Реклама должна быть распознаваема без специальных знаний или без применения технических средств именно как реклама непосредственно в момент ее представления независимо от формы или от используемого средства распространения (ст. 5 Закона).

Использование в радио-, теле-, видео-, аудио- и кинопродукции, а также в печатной продукции нерекламного характера целенаправленного обращения внимания потребителей рекламы на конкретную марку (модель, артикул) товара либо на изготовителя, исполнителя, продавца для формирования и поддержания интереса к ним без надлежащего предварительного сообщения об этом (в частности, путем пометки «на правах рекламы») не допускается.

Если радио-, теле-, видео-, аудио- и кинопродукция, а также печатная продукция распространяются частями (сериями), сообщения о рекламе также должны повторяться соответственно количеству частей (серий).

Организациям средств массовой информации запрещается взимать плату за размещение рекламы под видом информационного, редакционного или авторского материала.

Реклама товаров, реклама о самом рекламодателе, если осуществляемая им деятельность требует специального разрешения (лицензии), но такое разрешение (лицензия) не получено, а также реклама товаров, запрещенных к производству и реализации в соответствии с законодательством Российской Федерации, не допускается.

Если деятельность рекламодателя подлежит лицензированию, в рекламе должны быть указаны номер лицензии, а также наименование органа, выдавшего эту лицензию.

Реклама товаров, подлежащих обязательной сертификации, должна сопровождаться пометкой «подлежит обязательной сертификации».

Использование в рекламе объектов исключительных прав (интеллектуальной собственности) допускается в порядке, предусмотренном законодательством Российской Федерации.

Реклама не должна побуждать граждан к насилию, агрессии, возбуждать панику, а также побуждать к опасным действиям, способным нанести вред здоровью физических лиц или угрожающим их безопасности.

Реклама не должна побуждать к действиям, нарушающим природоохранное законодательство.

Недобросовестной является реклама, которая:

- дискредитирует юридических и физических лиц, не пользующихся рекламируемыми товарами;
- содержит некорректные сравнения рекламируемого товара с товаром (товарами) других юридических или физических лиц, а также содержит высказывания, образы, порочащие честь, достоинство или деловую репутацию конкурента (конкурентов);
- вводит потребителей в заблуждение относительно рекламируемого товара посредством имитации (копирования или подражания) общего проекта, текста, рекламных формул, изображений, музыкальных или звуковых эффектов, используемых в рекламе других товаров, либо посредством злоупотребления доверием физических лиц или недостатком у них опыта, знаний, в том числе в связи с отсутствием в рекламе части существенной информации.

Недобросовестная реклама не допускается.

Недостовой является реклама, в которой присутствуют не соответствующие действительности сведения в отношении:

- таких характеристик товара, как природа, состав, способ и дата изготовления, назначение, потребительские свойства, условия применения, наличие сертификата соответствия, сертификационных знаков и знаков соответствия государственным стандартам, количество, место происхождения;
- наличия товара на рынке, возможности его приобретения в указанных объеме, периоде времени и месте;
- стоимости (цены) товара на момент распространения рекламы;
- дополнительных условий оплаты;
- доставки, обмена, возврата, ремонта и обслуживания товара;
- гарантийных обязательств, сроков службы, сроков годности;
- исключительных прав на результаты интеллектуальной деятельности и приравненных к ним средств индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг;
- прав на использование государственных символов (флагов, гербов, гимнов), а также символов международных организаций;
- официального признания, получения медалей, призов, дипломов и иных наград;
- предоставления информации о способах приобретения полной серии товара, если товар является частью серии;
- результатов исследований и испытаний, научных терминов, цитат из технических, научных и иных публикаций;
- статистических данных, которые не должны представляться в виде, преувеличивающем их обоснованность;

- ссылок на какие-либо рекомендации либо на одобрение юридических или физических лиц, в том числе на устаревшие;

- использования терминов в превосходной степени, в том числе путем употребления слов «самый», «только», «лучший», «абсолютный», «единственный» и тому подобных, если их невозможно подтвердить документально;

- сравнений с другим товаром (товарами), а также с правами и положением иных юридических или физических лиц;

- ссылок на какие-либо гарантии потребителю рекламируемых товаров;

- фактического размера спроса на товар;

- информации о самом рекламодателе.

Недостоверная реклама не допускается.

Неэтичной является реклама, которая:

- содержит текстовую, зрительную, звуковую информацию, нарушающую общепринятые нормы гуманности и морали путем употребления оскорбительных слов, сравнений, образов в отношении расы, национальности, профессии, социальной категории, возрастной группы, пола, языка, религиозных, философских, политических и иных убеждений физических лиц;

- порочит объекты искусства, составляющие национальное или мировое культурное достояние;

- порочит государственные символы (флаги, гербы, гимны), национальную валюту Российской Федерации или иного государства, религиозные символы;

- порочит какое-либо физическое или юридическое лицо, какую-либо деятельность, профессию, товар.

Неэтичная реклама не допускается.

Физическое или юридическое лицо, которому стало известно о производстве или о распространении рекламы, содержащей сведения, порочащие его честь, достоинство или деловую репутацию, вправе обратиться за защитой нарушенных прав соответственно в суд или в арбитражный суд в порядке, предусмотренном законодательством Российской Федерации, а также вправе требовать от рекламодателя опровержения такой рекламы тем же способом, каким она была распространена, если рекламодатель не выполняет это требование в добровольном порядке.

Заведомо ложной является реклама, с помощью которой рекламодатель (рекламопроизводитель, рекламораспространитель) умышленно вводит в заблуждение потребителя рекламы.

Заведомо ложная реклама не допускается.

Использование в радио-, теле-, видео-, аудио- и кинопродукции, а также в иной продукции и распространение иными способами скрытой рекламы, то есть рекламы, которая оказывает не осознаваемое потребителем воздействие на его восприятие, в том числе путем использования специальных видеовставок (двойной звукозаписи) и иными способами, не допускаются.

10.2. Особенности рекламы в радио- и телепрограммах

В радио- и телепрограммах не допускается прерывать рекламой и совмещать с рекламой, включая рекламу в виде наложений, в том числе способом «бегущей строки»:

- детские, образовательные и религиозные передачи;

- радиопостановки и художественные фильмы без согласия правообладателей;

- транслируемые в прямом эфире передачи, перечень которых установлен Федеральным законом «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»;
- иные передачи, продолжительность трансляции которых составляет менее чем 15 минут.

Иные передачи, продолжительность трансляции которых составляет более чем 15 минут, а также радиопостановки и художественные фильмы не могут совмещаться с рекламой чаще чем через каждые 15 минут или могут прерываться столько раз, сколько 15-минутных периодов включают эти передачи, радиопостановки и художественные фильмы.

При трансляции рекламы ее звук не может быть громче звука транслируемой программы.

При использовании рекламы в виде наложений, в том числе способом «бегущей строки», ее размер не должен превышать семи процентов площади кадра.

Распространение одной и той же по содержанию рекламы одного и того же товара или рекламы о рекламодателе не должно осуществляться более чем два раза общей продолжительностью не более чем 2 минуты в течение часа эфирного времени радио- и телепрограммы на одной частоте вещания.

В радио- и телепрограммах, не зарегистрированных в качестве специализирующихся на сообщениях и материалах рекламного характера, реклама не должна превышать 20 процентов эфирного времени.

В периодических печатных изданиях, не специализирующихся на сообщениях и материалах рекламного характера, реклама не должна превышать 40 процентов объема одного номера периодического печатного издания.

10.3. Особенности рекламы отдельных видов товара

Особенностями рекламы товаров определяются Законом о СМИ (глава 2), а также рядом других Федеральных законов, касающихся продажи отдельных видов товара (ФЗ «О рынке ценных бумаг» от 22 апреля 1996 г. № 39-ФЗ, ФЗ от 7 января 1999 г. № 18-ФЗ «О внесении изменений и дополнений в Федеральный закон «О государственном регулировании производства и оборота этилового спирта и алкогольной продукции», ФЗ «О лекарственных средствах» от 22 июня 1998 г. № 86-ФЗ и другие)

Реклама алкогольных напитков, табака и табачных изделий, распространяемая любыми способами, не должна:

- содержать демонстрацию процессов курения и потребления алкогольных напитков, а также не должна создавать впечатление, что употребление алкоголя или курение имеет важное значение для достижения общественного, спортивного или личного успеха либо для улучшения физического или психического состояния;
- дискредитировать воздержание от употребления алкоголя или от курения, содержать информацию о положительных терапевтических свойствах алкоголя, табака и табачных изделий и представлять их высокое содержание в продукте как достоинство;
- обращаться непосредственно к несовершеннолетним, а также использовать образы физических лиц в возрасте до 35 лет, высказывания или участие лиц, пользующихся популярностью у несовершеннолетних и лиц в возрасте до 21 года;
- распространяться в радио- и телепрограммах с 7 до 22 часов местного времени;
- распространяться в любой форме в радио- и телепередачах, при кино- и видеообслуживании, в печатных изданиях для несовершеннолетних;
- распространяться на первой и последней полосах газет, а также на первой и последней страницах и обложках журналов;

- распространяться в детских, учебных, медицинских, спортивных, культурных организациях, а также ближе 100 метров от них.

Распространение рекламы табака и табачных изделий во всех случаях должно сопровождаться предупреждением о вреде курения, причем в радио- и телепрограммах данному предупреждению должно быть отведено не менее чем три секунды эфирного времени, при распространении рекламы другими способами - не менее пяти процентов рекламной площади (пространства).

Реклама алкогольной продукции с содержанием этилового спирта более 15 процентов объема готовой продукции допускается только в организациях, осуществляющих деятельность по производству и обороту алкогольной продукции, с соблюдением требований, предусмотренных законодательством Российской Федерации о рекламе.

При рекламе алкогольной продукции с содержанием этилового спирта не более 15 процентов объема готовой продукции должно использоваться не менее половины рекламного времени (площади) для информации населения о вредных последствиях употребления алкогольных напитков и способах определения их фальсификации.

Реклама медикаментов, изделий медицинского назначения, медицинской техники при отсутствии разрешения на их производство и (или) реализацию, а также реклама методов лечения, профилактики, диагностики, реабилитации при отсутствии разрешения на оказание таких услуг, выдаваемого федеральным органом исполнительной власти в области здравоохранения, не допускается, в том числе и в случаях получения патентов на изобретения в указанной области.

Реклама лекарственных средств, отпускаемых по рецепту врача, а также реклама изделий медицинского назначения и медицинской техники, использование которых требует специальной подготовки, допускается только в печатных изданиях, предназначенных для медицинских и фармацевтических работников. В свободном показе может быть лишь реклама лекарственных средств, отпускаемых без рецепта врача. Реклама не должна подрывать репутацию предприятий - производителей лекарственных средств, веру потребителей в действие лекарственных средств. Реклама не должна создавать впечатление ненужности медицинских консультаций или хирургических операций. Реклама не должна содержать утверждений о том, что действие лекарственного средства гарантировано.

Реклама наркотических средств и психотропных веществ, внесенных в списки II и III, может осуществляться исключительно в специализированных печатных изданиях, рассчитанных на медицинских и фармацевтических работников.

Распространение в целях рекламы образцов лекарственных средств, содержащих наркотические средства или психотропные вещества, запрещается.

Не допускается реклама всех видов оружия, вооружения и военной техники, за исключением рекламы боевого и служебного оружия, вооружения и военной техники, внесенных в перечень продукции военного назначения, экспорт и импорт которой в Российской Федерации осуществляются по лицензиям, а также разрешенного гражданского оружия, в том числе охотничьего и спортивного.

Не допускается реклама разрешенного гражданского оружия, вооружения и военной техники, внесенных в перечень продукции военного назначения, экспорт и импорт которой в Российской Федерации осуществляются по лицензиям, если указанная реклама прямо или косвенно раскрывает технологию производства, способы боевого и специального применения оружия, вооружения и военной техники.

Распространение рекламы разрешенного гражданского оружия, в том числе охотничьего и спортивного, допускается только в периодических печатных изданиях, специализирующихся на распространении рекламы, а также в иных периодических печатных изданиях, предназначенных для пользователей разрешенного гражданского оружия, и в местах применения охотничьего и спортивного оружия.

Распространение рекламы разрешенного гражданского оружия в электронных средствах массовой информации допускается только после 22 часов местного времени.

Реклама боевого и служебного оружия, а также вооружения и военной техники, внесенных в перечень продукции военного назначения, экспорт и импорт которой в Российской Федерации осуществляются по лицензиям, допускается только в изданиях, указанных в Законе Российской Федерации «Об оружии», а также на специализированных выставках или на ярмарках-продажах, проводимых в порядке, устанавливаемом Правительством Российской Федерации.

При производстве, размещении и распространении рекламы финансовых (в том числе банковских), страховых, инвестиционных услуг и иных услуг, связанных с использованием денежных средств юридических и физических лиц, а также ценных бумаг не допускается:

- приводить в рекламе количественную информацию, не имеющую непосредственного отношения к рекламируемым услугам или ценным бумагам;
- гарантировать размеры дивидендов по простым именным акциям;
- рекламировать ценные бумаги до регистрации проспектов их эмиссий;
- представлять любого рода гарантии, обещания или предположения о будущей эффективности (доходности) деятельности, в том числе путем объявления роста курсовой стоимости ценных бумаг;
- умалчивать хотя бы об одном из условий договора, если в рекламе сообщается об условиях договора.

10.4. Защита несовершеннолетних при производстве, размещении и распространении рекламы

При производстве, размещении и распространении рекламы в целях защиты несовершеннолетних от злоупотреблений их легковерностью и отсутствием опыта не допускаются:

- дискредитация авторитета родителей и воспитателей, подрыв доверия к ним несовершеннолетних;
- внушение непосредственно несовершеннолетним, чтобы они убедили родителей или других лиц приобрести рекламируемые товары;
- привлечение внимания несовершеннолетних к тому, что обладание теми или иными товарами дает им какое-либо преимущество над другими несовершеннолетними, а также к тому, что отсутствие этих товаров дает обратный эффект;
- размещение в рекламе текстовой, визуальной или звуковой информации, показывающей несовершеннолетних в опасных местах и ситуациях;
- преуменьшение необходимого уровня навыков использования товара у несовершеннолетних. При этом в случае, если результаты использования товара показаны или описаны, реклама должна давать информацию о том, что реально достижимо для несовершеннолетних той возрастной группы, для которой предназначен товар;
- создание у несовершеннолетних нереального (искаженного) представления о стоимости (цене) товара для несовершеннолетних, в частности, путем применения слов «только», «всего» и тому подобных, а также путем прямого или косвенного указания на то, что рекламируемый товар доступен для любого семейного бюджета.

Текстовое, визуальное или звуковое использование образов несовершеннолетних в рекламе, не относящейся непосредственно к товарам для несовершеннолетних, не допускается.

10.5. Права и обязанности рекламодателей, рекламопроизводителей и рекламораспространителей

Рекламодатель, рекламопроизводитель и рекламораспространитель обязаны хранить материалы или их копии, содержащие рекламу, включая все вносимые в них последующие изменения, в течение года со дня последнего распространения рекламы.

Рекламопроизводитель и рекламораспространитель вправе требовать, а рекламодатель в этом случае обязан предоставлять документальные подтверждения достоверности рекламной информации.

Если деятельность рекламодателя подлежит лицензированию, то при рекламе соответствующего товара, а также при рекламе самого рекламодателя последний обязан предоставлять, а рекламопроизводитель и рекламораспространитель обязаны требовать предъявления соответствующей лицензии либо ее надлежаще заверенной копии.

Рекламопроизводитель обязан своевременно информировать рекламодателя о том, что соблюдение требований последнего при производстве рекламы может привести к нарушению законодательства Российской Федерации о рекламе.

Если рекламодатель, несмотря на своевременное и обоснованное предупреждение рекламопроизводителя, не изменит свое требование (требования) к рекламе, либо не представит по требованию рекламопроизводителя документальное подтверждение достоверности предоставляемой для производства рекламы информации, либо не устранит иные обстоятельства, которые могут сделать рекламу ненадлежащей, рекламопроизводитель вправе в установленном порядке расторгнуть договор и потребовать полного возмещения убытков, если договором не предусмотрено иное.

В случае установления факта нарушения законодательства Российской Федерации о рекламе нарушитель обязан осуществить контррекламу в срок, установленный федеральным антимонопольным органом (его территориальным органом), вынесшим решение об осуществлении контррекламы. При этом нарушитель несет расходы по контррекламе в полном объеме.

В случае, если контрреклама не осуществлена нарушителем в установленный срок, федеральный антимонопольный орган (его территориальный орган), принявший решение о проведении контррекламы, вправе принять решение о полном или о частичном приостановлении рекламы нарушителя до дня завершения распространения им контррекламы.

При этом орган, принявший решение о полном или о частичном приостановлении рекламы нарушителя, обязан незамедлительно поставить об этом в известность все стороны договоров с нарушителем на производство, размещение и распространение его рекламы.

Контрреклама осуществляется посредством того же средства распространения, с использованием тех же характеристик продолжительности, пространства, места и порядка, что и опровергаемая ненадлежащая реклама. Содержание контррекламы согласовывается с федеральным антимонопольным органом (его территориальным органом), который установил факт нарушения и принял соответствующее решение о его исправлении.

В отдельных случаях по решению федерального антимонопольного органа (его территориального органа), который принял решение о проведении контррекламы, допускается замена средства распространения, характеристик продолжительности, пространства, места и порядка осуществления контррекламы.

Рекламодатель несет ответственность за нарушение законодательства Российской Федерации о рекламе в части содержания информации, предоставляемой для создания рекламы, если не доказано, что указанное нарушение произошло по вине рекламопроизводителя или рекламораспространителя.

Рекламопроизводитель несет ответственность за нарушение законодательства Российской Федерации о рекламе в части оформления, производства, подготовки рекламы.

Рекламораспространитель несет ответственность за нарушение законодательства Российской Федерации о рекламе в части, касающейся времени, места и средств размещения рекламы.

Юридические лица или граждане (рекламодатели, рекламопроизводители и рекламораспространители) за нарушение законодательства Российской Федерации о рекламе несут гражданско-правовую ответственность в соответствии с законодательством Российской Федерации.

Лица, права и интересы которых нарушены в результате ненадлежащей рекламы, вправе обратиться в установленном порядке в суд, арбитражный суд с исками, в том числе с исками о возмещении убытков, включая упущенную выгоду, возмещении вреда, причиненного здоровью и имуществу, компенсации морального вреда, публичном опровержении ненадлежащей рекламы.

Истцы по искам о возмещении вреда, причиненного ненадлежащей рекламой здоровью, имуществу, чести, достоинству и деловой репутации, освобождаются от уплаты государственной пошлины.

ТЕМА 11. ГОСУДАРСТВЕННАЯ ТАЙНА – ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

11.1. Понятие государственной тайны, полномочия власти в области отнесения сведений к государственной тайне.

В основу данной главы положен Федеральный закон «О государственной тайне». Согласно п.1. ст. 2 данного закона государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Исполнение Закона Российской Федерации "О государственной тайне" организует правительство РФ. Оно же представляет на утверждение президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней; представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

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

В ст.2 Закона определены некоторые термины, составляющие сущность закона.

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

Система защиты государственной тайны определена как совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, состав-

ляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях.

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

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

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

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

11.2. Перечень сведений, составляющих государственную тайну

Согласно II разделу Закона государственную тайну составляют:

1) сведения в военной области:

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

- о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

- об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

- о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
- о методах и средствах защиты секретной информации;
- об организации и о фактическом состоянии защиты государственной тайны;
- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;
- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;
- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

11.3. Отнесение сведений к государственной тайне и их засекречивание

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

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии с положениями статей «Закона о государственной тайне» и законодательству Российской Федерации о государственной тайне.

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

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

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и 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. (ст. 7 Закона)

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

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно".

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с законом.

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

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

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее – собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом го-

сударственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены (ст. 12 Закона).

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

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

Помимо перечисленных реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и

порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

11.4. Рассекречивание сведений и их носителей

Рассекречивание сведений и их носителей - снятие ранее введенных в предусмотренном законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям (ст.13 Закона).

Основаниями для рассекречивания сведений являются:

- взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;
- изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

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

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

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

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

В исключительных случаях право продления первоначально установленных сроков засекречивания носителей сведений, составляющих государственную тайну, предоставляется руководителям государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.

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

Руководители государственных архивов Российской Федерации наделяются полномочиями по рассекречиванию носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах этих архивов, в случае делегирования им таких полномочий организацией - фондообразователем или ее правопреемником. В случае ликвидации организации - фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государственную тайну, рассматривается межведомственной комиссией по защите государственной тайны.

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации вправе обратиться в органы государственной власти, на предприятия, в учреждения, организации в том числе в государственные архивы, с запросом о рассекречивании сведений, отнесенных к государственной тайне.

Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, обязаны в течение трех месяцев рассмотреть его и дать мотивированный ответ по существу запроса. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с момента его поступления передается в орган государственной власти, наделенный такими полномочиями либо в межведомственную комиссию по защите государственной тайны о чем уведомляются граждане предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Уклонение должностных лиц от рассмотрения запроса по существу влечет за собой административную (дисциплинарную) ответственность в соответствии с действующим законодательством.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. При признании судом необоснованности засекречивания сведений эти сведения подлежат рассекречиванию в установленном Законом порядке.

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

Органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, обязаны принять меры по обеспечению защиты этих сведений и их носителей (ст. 19 Закона). При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:

- правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;
- органу государственной власти, в распоряжении которого в соответствии со статьей 9 Закона находятся соответствующие сведения;
- другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

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

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласия на частичные, временные ограничения их прав в Законом;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом;

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

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

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации.

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

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

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

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

Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.

Устанавливается три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Сроки, обстоятельства и порядок переоформления допуска граждан к государственной тайне устанавливаются нормативными документами, утверждаемыми Правительством Российской Федерации.

Порядок допуска должностных лиц и граждан к государственной тайне в условиях объявленного чрезвычайного положения может быть изменен Президентом Российской Федерации.

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

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

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

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

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

- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения Российской Федерации;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

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

- расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;
- однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;
- возникновения обстоятельств, являющихся согласно статье 22 настоящего Закона основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

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

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

Решение администрации о прекращении допуска должностного лица или гражданина к государственной тайне и расторжении на основании этого с ним трудового договора (контракта) может быть обжаловано в вышестоящую организацию или в суд.

11.6. Шпионаж и разглашение государственной тайны

Согласно статье 275 УК РФ государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации, - наказывается лишением свободы на срок от двенадцати до двадцати лет с конфискацией имущества или без таковой.

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

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказываются лишением свободы на срок от десяти до двадцати лет.

Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

ТЕМА 12. ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ – НОВЫЙ МЕТОД ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

12.1. Понятие электронной цифровой подписи

В условиях увеличившегося числа преступлений в информационной сфере, необходимы перемены в сфере информационных технологий. Одной из новых технологий, обеспечивающих безопасность информации, является электронная цифровая подпись. В данной главе рассмотрены важные аспекты проекта закона, предложенного правительству.

Для наилучшего понимания настоящей главы необходимо уделить внимание следующим понятиям.

Электронное сообщение – информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком.

Документ в электронной форме отображения (электронный документ) – электронное сообщение, имеющей атрибуты для идентификации его как документа.

Электронная цифровая подпись (ЭЦП) – последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа ЭЦП, которая позволяет пользователю открытого ключа ЭЦП, установить целостность и неизменность этой информации, а также владельца закрытого ключа ЭЦП.

Средство ЭЦП – совокупность программных и технических средств, реализующих функцию выработки и проверки ЭЦП.

Открытый ключ ЭЦП – общедоступная последовательность символов, предназначенная для проверки ЭЦП.

Закрытый ключ ЭЦП – последовательность символов, предназначенная для выработки ЭЦП и известная только правомочному лицу.

Пользователь открытого ключа ЭЦП – физическое или юридическое лицо, использующее открытый ключ ЭЦП.

Сертификат открытого ключа ЭЦП (сертификат ключа подписи) – документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭЦП определенному лицу.

Владелец сертификата ключа подписи (владелец сертификата) – физическое или юридическое лицо, на имя которого выдан сертификат ключа подписи, и которое владеет закрытым ключом ЭЦП, соответствующим открытому ключу, указанному в сертификате.

Центр по удостоверению подлинности ЭЦП (удостоверяющий центр) – юридическое лицо или обособленное подразделение юридического лица, обладающие полномочиями на удостоверение принадлежности конкретного открытого ключа ЭЦП владельцу сертификата.

Сертификат на средство ЭЦП – документ, выданный по правилам соответствующей системы сертификации, удостоверяющий соответствие этого средства специальным требованиям и гарантирующий в течение определенного срока действия возможность использования данного средства в качестве инструмента выработки и проверки ЭЦП.

Подтверждение подлинности ЭЦП – положительный результат проверки правильности ЭЦП, выработанной правомочным лицом из исходной информации путем применения принадлежащего ему закрытого ключа ЭЦП, полученный с использованием зарегистрированного и сертифицированного открытого ключа ЭЦП.

12.2. Принципы и условия использования электронной цифровой подписи

ЭЦП может признаваться равнозначной собственноручной подписи подписывающего лица и использоваться для подтверждения целостности и неизменности любой информации, передаваемой в виде электронных сообщений. Лицо может иметь неограниченное количество закрытых ключей ЭЦП, приобретенных им на законном основании. Все экземпляры электронного сообщения, подписанного ЭЦП, имеют силу оригинала. ЭЦП может использоваться физическими и юридическими лицами, органами государственной власти и органами местного самоуправления с соблюдением положений действующего законодательства.

Общий порядок ограничения сферы применения ЭЦП может устанавливаться федеральными законами. Ограничения использования ЭЦП в договорных отношениях могут устанавливаться соглашением сторон.

При соблюдении требований действующего законодательства и (или) соглашения сторон ЭЦП признается равнозначной собственноручной подписи физического лица, в том числе полномочного представителя юридического лица, если:

- она прошла проверку на подлинность при помощи открытого ключа ЭЦП, имеющего сертификат ключа подписи удостоверяющего центра, действующего по лицензии, или в порядке, предусмотренном соглашением сторон;
- подписавшее лицо правомерно владеет закрытым ключом, используемым для создания ЭЦП;
- сертификат ключа подписи является действующим на момент подписания.

Для использования ЭЦП подписывающим лицом и получателем электронного сообщения не требуется получения лицензии.

Деятельность по указанию услуг, связанных с формированием ЭЦП и ее проверки, подлежит лицензированию в порядке, установленном законодательством Российской Федерации.

Несовершеннолетние граждане имеют право на использование ЭЦП, получение сертификата ключа подписи и приобретение средств ЭЦП с соблюдением норм действующего законодательства.

Подписывающее лицо вправе передавать полномочия на подписание электронных сообщений с использованием своего закрытого ключа ЭЦП уполномоченному надлежащим образом представителю.

Сертификат ключа подписи, удостоверяющий юридическое лицо без указания имени должностного лица, уполномоченного на использование данного ключа, считается сертификатом удостоверяющим лицо, которое в силу закона или учредительных документов юридического лица действует от его имени.

Средства ЭЦП не относятся к средствам, обеспечивающим конфиденциальность информации. Создание ключей ЭЦП производится собственниками средств ЭЦП, если иной порядок не установлен законодательством Российской Федерации. Сертификация средств ЭЦП осуществляется в соответствии с законодательством о сертификации товаров и услуг. Сертификация средств ЭЦП осуществляется на основании лицензии, выдаваемой государственным лицензирующим органом. Обязательная сертификация средств ЭЦП устанавливается законодательством Российской Федерации.

Допускается использование несертифицированных средств ЭЦП. При этом владелец несертифицированных средств ЭЦП (владелец закрытого ключа) обязан заявить об отсутствии сертификации всем пользователям открытого ключа ЭЦП, создаваемой несертифицированным средством.

В противном случае владелец несертифицированных средств ЭЦП несет ответственность за убытки, понесенные пользователем открытого ключа, вследствие использования для его создания несертифицированного средства ЭЦП.

В случае использования заявленных несертифицированных средств ЭЦП риски убытков несут владелец закрытого ключа и пользователь открытого ключа ЭЦП.

Пользователь открытого ключа ЭЦП вправе обратиться к удостоверяющему центру, выдавшему сертификат ключа подписи, за подтверждением: информации, содержащейся в данном сертификате ключа подписи; подлинности ЭЦП. Владелец закрытого ключа ЭЦП не несет ответственность перед пользователем соответствующего открытого ключа за убытки, причиненные несанкционированным использованием закрытого ключа вследствие ненадлежащей охраны закрытого ключа. Владелец закрытого ключа ЭЦП обязан потребовать от удостоверяющего центра, выдавшего соответствующий сертификат ключа подписи, приостановить действие сертификата или аннулировать его, если он узнал или должен был разумно предполагать о возможном нарушении режима ограничения доступа к закрытому ключу.

Сертификат ключа подписи должен содержать следующие обязательные сведения: наименование юридического лица либо фамилию, имя и отчество или псевдоним физического лица – владельца закрытого ключа ЭЦП; открытый ключ ЭЦП; номер сертификата ключа подписи, дату начала и дату окончания срока его действия; наименование средств ЭЦП, с которыми можно использовать данный открытый ключ ЭЦП, номер сертификата на это средство и срок его действия, наименование и юридический адрес центра сертификации, выдавшего данный сертификат, номер лицензии этого центра и дату ее выдачи; наименование и юридический адрес удостоверяющего центра, выдавшего сертификат ключа подписи, номер лицензии и дата ее выдачи; наименование и юридический адрес государственного органа, уполномоченного удостоверить открытый ключ ЭЦП удостоверяющего центра, выдавшего сертификат ключа подписи; данные об ограничении вида или области применения ЭЦП; данные о полномочиях представителя владельца сертификата; данные, позволяющие идентифицировать общедоступный реестр владельцев сертификатов, в который внесен данный сертификат ключа подписи, и место опубликования этого реестра.

Удостоверяющим центром открытых ключей электронной цифровой подписи может быть юридическое лицо, созданное в соответствии с законодательством Российской Федерации, а также обособленное подразделение юридического лица, выполняющее все или часть функций юридического лица. Удостоверение открытых ключей ЭЦП может осуществляться в качестве единственного вида деятельности или наряду с иными видами деятельности юридического лица.

Удостоверяющий центр должен располагать финансовыми ресурсами (в том числе, собственным капиталом, заемными средствами и др.), достаточными для осуществления деятельности, включая возможную имущественную ответственность перед лицами, полагающимися на выданные им сертификаты ключа подписи, за убытки, понесенные указанными лицами вследствие недостоверности содержания сертификатов ключа подписи.

Удостоверяющий центр подтверждает принадлежность открытого ключа ЭЦП конкретному лицу посредством выдачи сертификата ключа подписи. Удостоверяющий центр вправе подтверждать подлинность открытого ключа ЭЦП.

Удостоверяющий центр, выдавая сертификат ключа подписи, принимает на себя следующие обязательства перед его владельцем:

действовать надлежащим образом в соответствии с положениями настоящего Федерального закона для приостановления действия или аннулирования сертификата ключа подписи;

уведомить владельца сертификата в течение разумного срока о всех известных удостоверяющему центру фактах, которые существенным образом сказываются на юридической силе выпущенного сертификата ключа подписи.

12.3 Обязательства владельца по принятии сертификата ключа подписи и защита персональных данных

Приняв сертификат ключа подписи, выданный удостоверяющим центром, его владелец принимает на себя следующие обязательства: гарантировать достоверность информации, предоставленной им в целях выдачи сертификата ключа подписи; законным образом владеть закрытым ключом, соответствующим открытому ключу ЭЦП, указанному в сертификате ключа подписи; обеспечить контроль использования закрытого ключа и предотвращение его раскрытия какому-либо лицу, не уполномоченному на создание ЭЦП, при условии соблюдения положений настоящего Федерального закона.

При принятии решения о прекращении деятельности по удостоверению открытых ключей ЭЦП юридическое лицо обязано заблаговременно проинформировать об этом решении орган, выдавший лицензию на указанную деятельность, уполномоченный государственный орган, выдавший сертификат ключа подписи этому удостоверяющему центру, а также всех владельцев сертификатов ключей подписи, выданных этим удостоверяющим центром.

Удостоверяющий центр обеспечивает защиту персональных данных владельца сертификата, содержащихся в документах, представленных заявителем, в соответствии с требованиями законодательства Российской Федерации, касающегося защиты персональных данных.

Раскрытие персональных данных владельцев сертификата ключа подписи удостоверяющим центром допускается только с их согласия либо по законному требованию правоохранительных органов. В случае, когда владелец закрытого ключа ЭЦП регистрируется под псевдонимом, удостоверяющий центр обязан сообщить правоохранительным органам по их законному требованию о тождественности псевдонима и владельца сертификата, при этом удостоверяющий центр обязан известить владельца сертификата о раскрытии псевдонима, если законодательством Российской Федерации не предусмотрено иное.

12.4. Использование электронной цифровой подписи в сфере государственного управления и корпоративных информационных системах

ЭЦП применяется органами государственной власти и органами местного самоуправления при передаче по информационным системам и хранении в электронных базах данных любых документов, издаваемых данным органом в соответствии с его компетенцией.

Органы государственной власти и органы местного самоуправления, направляющие электронные данные, подписанные ЭЦП, обязаны иметь сертификат ключа подписи, выданный в установленном порядке удостоверяющим центром, имеющим государственную лицензию.

Органы государственной власти и органы местного самоуправления принимают электронные сообщения, направленные в эти органы физическими и юридическими лицами и подписанные ЭЦП, только при наличии у этих лиц сертификата ключа подписи, выданного в соответствии с настоящим Федеральным законом удостоверяющим центром, имеющим государственную лицензию.

Условия использования ЭЦП органами государственной власти и органами местного самоуправления устанавливаются законодательством Российской Федерации.

Для удостоверения подлинности ЭЦП должностных лиц органов государственной власти и органов местного самоуправления создаются государственные удостоверяющие центры, выдающие сертификаты ключей подписи.

Законодательством Российской Федерации могут быть установлены дополнительные функции государственных удостоверяющих центров, в том числе создание ключей ЭЦП должностным лицам, использующим ЭЦП по своему статусу, и предоставление открытых ключей получателям сообщений, подписанных ЭЦП.

Использование ЭЦП в корпоративных информационных системах регламентируется внутренними нормативными документами системы, соглашением между участников системы или между владельцем системы и пользователями (клиентами).

Указанные нормативные документы или соглашения должны содержать положения о правах, обязанностях и ответственности лиц, использующих ЭЦП, а также о распределении рисков убытков при использовании недостоверной ЭЦП между участниками системы.

Электронная цифровая подпись, которая может быть проверена открытым ключом, имеющим иностранный сертификат ключа подписи, выданный государством, с которым есть договор о признании таких свидетельств или иной договор, обеспечивающий равноценную безопасность электронных сообщений, признается электронной цифровой подписью в соответствии с настоящим Федеральным законом.

В случае возникновения спора допускается представление суду электронных сообщений, подписанных ЭЦП и заверенных удостоверяющим центром в соответствии с настоящим Федеральным законом и изданными в его исполнение нормативными актами.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Копылов В.А. «Информационное право» Юрист. М., 1997
2. Рассолов М.М. «Информационное право» Юрист. М., 1999
3. Емельянов Г.В., Стрельцов А.А. «Информационная безопасность России. Основные понятия и определения». РАГС при Президенте РФ. М., 2000
4. Стрельцов А.А. «Правовое обеспечение информационной безопасности Российской Федерации как правовая категория». Проблемы информатизации №2, 2001
5. Всеобщая декларация прав человека от 10 декабря 1948 г.
6. Конституция Российской Федерации
7. Доктрина информационной безопасности Российской Федерации. Поручение Президента РФ от 9 сентября 2000 года, № Пр-1895
8. Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95г.
9. Федеральный закон «О средствах массовой информации» от 27 декабря 1991 г. № 2124-I (с последующими изменениями)
10. Федеральный закон "О государственной тайне" от 21.07.93 № 5485-1
11. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ
12. Гражданский кодекс РФ
13. Федеральный закон «О внесении изменений и дополнений в Закон РСФСР «О банках и банковской деятельности в РСФСР» от 3 февраля 1996 г. № 17-ФЗ
14. Налоговый кодекс Российской Федерации
15. Постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. № 35
16. Федеральный закон «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-I (с последующими изменениями)
13. Федеральный закон «О рекламе» от 18 июля 1995 г. № 108-ФЗ (с последующими изменениями)
14. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. N 1-ФЗ

Эдуард Николаевич Камышев

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ**

Учебное пособие

Редактор: Камышев Э.Н.

Печатается с оригинал-макета, предоставленного автором, на ризографе кафедры социологии, психологии и права Томского политехнического университета.

Тираж 50 экз.