

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

А.А. Парошин

Нормативно-правовые аспекты защиты информации

Учебное пособие

**Владивосток
Издательство Дальневосточного федерального университета
2010**

ББК 67.404.3я73

П 18

Парошин А.А.

П 18 Нормативно-правовые аспекты защиты информации: Учебное пособие / А.А. Парошин. – Владивосток: Изд-во Дальневост. федер. ун-та, 2010. – 116 с.

В настоящем учебном пособии собран материал, необходимый для самостоятельного освоения тем учебного курса «Технология защиты информации», связанных с нормативно-правовыми аспектами деятельности по защите информации.

В достижение поставленной цели изложенный материал снабжен ссылками на источники информации (24 ссылки на используемую литературу и более 470 ссылок на нормативно-правовые и нормативно-методические акты). Ссылки на нормативно-правовые и методические документы приводятся по состоянию на 15.02.2010.

Пособие предназначено для студентов естественнонаучных специальностей вузов в учебных планах которых предусмотрен указанный курс.

ББК 67.404.3я73

© А.А. Парошин, 2010

© Дальневосточный федеральный университет, 2010

Содержание

Принятые сокращения.....	6
Используемая литература	8
Введение	10
Часть Общая.....	11
Раздел I. Правовые основы	11
Глава 1. Основы теории права.....	11
1.1. Базовые понятия	11
1.2. Система права	12
1.3. Виды источников	13
Глава 2. Основы информационного права.....	15
2.1. Основной объект информационного права.....	15
2.2. Информационное общество	16
2.3. Дополнительные объекты информационного права.....	17
2.4. Предмет и метод отрасли	18
2.5. Источники отрасли.....	19
2.6. Система информационного права	19
Раздел II. Правовая идеология информационной безопасности.....	21
Глава 3. Правовые основы защиты информации	21
3.1. Характеристика деятельности по защите информации	21
3.2. Категории защищаемой информации	22
3.3. Связь информационной безопасности с другими отраслями права	24
Глава 4. Базовые источники информационной безопасности.....	25
4.1. Конституция РФ	25
4.2. Федеральный Закон «Об информации, информационных технологиях и о защите информации»	26
4.3. Статус концепций и доктрин.....	27
4.4. Перечень нормативно-правовых документов	27
4.5. Перечень международных декларативных документов	28
4.6. Перечень модельных (типовых) законов	29
4.7. Перечень национальных концепций РФ	32
Глава 5. Организационная структура государственной системы обеспечения информационной безопасности России	34
5.1. Система федеральных органов государственной власти	34
5.2. Компетенция органов государственной власти в области информационной безопасности	41
5.3. Перечень нормативно-правовых, нормативно-методических документов	43

Часть Специальная.....	46
Раздел III. Категории информации по режиму ограничения доступа и использования	46
Глава 6. Общедоступная информация	46
6.1. Право на информацию.....	46
6.2. Перечень международных правовых актов	47
6.3. Перечень национальных нормативно-правовых документов.....	49
6.4. Перечень нормативно-методических документов	53
Глава 7. Информация, относимая к коммерческой тайне, служебной тайне	54
7.1. Общие положения.....	54
7.2. Перечень нормативно-правовых документов, регламентирующих обработку и защиту информации, относимой к коммерческой тайне	56
7.3. Перечень нормативно-правовых документов, регламентирующих обработку и защиту служебной информации ограниченного распространения	56
7.4. Перечень нормативно-методических документов	57
Глава 8. Информация, относимая к профессиональной тайне.....	60
8.1. Общие положения.....	60
8.2. Перечень нормативно-правовых, нормативно-методических документов.....	61
Глава 9. Персональные данные	62
9.1. Общие положения.....	62
9.2. Перечень нормативно-правовых документов.....	63
9.3. Перечень нормативно-методических документов	64
Глава 10. Информация, относимая к государственной тайне в РФ	66
10.1. Общие положения	66
10.2. Перечень нормативно-правовых документов	67
Раздел IV. Институты права собственности и исключительных прав	69
Глава 11. Защита результатов интеллектуальной деятельности и средств индивидуализации 69	
11.1. Общие положения	69
11.2. Перечень нормативно-правовых документов.....	71
11.3. Перечень нормативно-методических документов	75
Раздел V. Правовое регулирование отношений, связанных с информационными технологиями 76	
Глава 12. Нормативно-правовое обеспечение в сфере связи и коммуникаций.....	76
12.1. Общие положения	76
12.2. Перечень нормативно-правовых документов.....	76
12.3. Перечень нормативно-методических документов	78
Глава 13. Государственное регулирование вопросов использования криптографических средств и ЭЦП.....	80
13.1. Общие положения	80

13.2.	Перечень нормативно-правовых документов	81
13.3.	Перечень нормативно-методических документов.....	81
Глава 14.	Лицензирование, сертификация и аттестация объектов информатизации и защиты информации	83
14.1.	Общие положения	83
14.2.	Перечень нормативно-правовых документов	85
14.3.	Перечень нормативно-методических документов.....	88
Раздел VI.	Правонарушения и ответственность в области эксплуатации информационных систем и информационной безопасности.....	90
Глава 15.	Виды и формы правонарушений и юридической ответственности	90
15.1.	Общее понятие юридической ответственности.....	90
15.2.	Гражданско-правовая ответственность	91
15.3.	Административная и дисциплинарная ответственность.....	92
15.4.	Уголовная ответственность	93
Глава 16.	Характеристика личности правонарушителя.....	95
Глава 17.	Юрисдикционные органы РФ, должностные лица и внутренние структуры предприятия	97
17.1.	Распределение компетенции	97
17.2.	Предварительное следствие и оперативно-розыскная деятельность.....	97
17.3.	Подразделение по борьбе с киберпреступностью в МВД России	99
17.4.	Подразделения защиты информации на предприятии, учреждении и организации.....	100
17.5.	Деятельность судов и прокуратуры	101
17.6.	Перечень национальных нормативно-правовых документов РФ.....	102
17.7.	Перечень нормативно-методических документов.....	103
Глава 18.	Международные аспекты обеспечения информационной безопасности.	
Международное сотрудничество.....		105
18.1.	Международное сотрудничество в борьбе с преступностью по линии ООН	105
18.2.	Инициативы Совета Европы	106
18.3.	Международное сотрудничество в борьбе с преступностью по линии неправительственных международных организаций.....	107
18.4.	Международное сотрудничество в борьбе с преступностью по линии Интерпола.....	108
18.5.	Структуры по реагированию на инциденты информационной безопасности	109
18.6.	Перечень международных договоров.....	110
18.7.	Перечень национальных нормативно-правовых актов	111
Алфавитный указатель юридических терминов		112
Электронные ресурсы с источниками информационного права		114

Принятые сокращения

CERT – Computer Emergency Response Team.

CSIRT – Computer Security Incident Response Team.

FIRST – Forum of Incident Response and Security Teams.

UNESCO – United Nations Educational, Scientific and Cultural Organization.

UNCITRAL – United Nations Commission on International Trade Law.

ВС – Верховный Совет.

ВАС – Высший Арбитражный Суд.

ВВУИО – Всемирной встречи на высшем уровне по вопросам информационного общества.

ВОИС – Всемирная организация интеллектуальной собственности.

ГД – Государственная Дума.

Гостайна – государственная тайна.

Гостехкомиссия – Государственная техническая комиссия при Президенте РФ.

ГФС – Государственная фельдъегерская служба.

ЕС – Европейский Союз (Европейское сообщество).

Зарег. – зарегистрировано.

ИБ – информационная безопасность.

ИКТ – информационные и коммуникационные технологии.

ИМПАКТ – Международное многостороннее партнерство против киберугроз МСЭ.

Интерпол – Международная организация уголовной полиции.

ИП – информационное право.

ИТ – информационные технологии.

МАУП – Международная ассоциация уголовного права.

МВД – Министерство внутренних дел.

МИД – Министерство иностранных дел.

Минздравсоцразвития – Министерство здравоохранения и социального развития.

Мининформсвязи – Министерство информационных технологий и связи.

Минкомсвязи – Министерство связи и массовых коммуникаций.

Минкультуры – Министерство культуры.

Минобороны – Министерство обороны.

Минюст – Министерство юстиции.

МКО – Международное криминологическое общество.

МНС – Министерство по налогам и сборам.

МОСЗ – Международное общество социальной защиты.

МСЭ – Международный союз электросвязи.

МУПФ – Международный уголовный и пенитенциарный фонд.

МЧС – Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

НЦБ – Национальное центральное бюро Интерпол.

ОБСЕ – Организация по безопасности и сотрудничеству в Европе.

ООН – Организация Объединенных Наций.

Пост. – постановление.

Пр-во – Правительство.

ПФ – Пенсионный Фонд.

РД – руководящий документ.

Росархив – Федеральное архивное агентство.

Росинформтехнологии – Федеральное агентство по информационным технологиям.

Роскомнадзор, Россвязькомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Роспатент – Федеральная служба по интеллектуальной собственности, патентам и товарным знакам.
Ростехрегулирование – Федеральное агентство по техническому регулированию и метрологии.
РСФСР – Российская Союзная Федеративная Социалистическая Республика.
РФ – Российская Федерация.
СВР – Служба внешней разведки.
СМИ – средства массовой информации.
СНГ – Содружество Независимых Государств.
СовБез – Совет Безопасности.
СССР – Союз Советских Социалистических Республик.
Ст. – статья.
Утв. – утвержден(ный), утверждение.
ФАПСИ – Федеральное агентство правительственной связи и информации.
ФАС – Федеральная антимонопольная служба.

ФЗ – Федеральный закон.
ФКЗ – Федеральный конституционный закон.
ФНС – Федеральная налоговая служба.
ФС – Федеральное Собрание.
ФСБ – Федеральная служба безопасности.
ФСО – Федеральная служба охраны.
ФСФР – Федеральная служба по финансовым рынкам.
ЦБ, Центробанк – Центральный Банк РФ, Банк России.
Центризбирком – Центральная избирательная комиссия.
ЭВМ – электронно-вычислительная машина.
ЭКОСОС – Экономический и Социальный Совет ООН.
ЭЦП – электронная цифровая подпись.
ЮНЕСКО – Организация Объединенных Наций по вопросам образования, науки и культуры (от англ. UNESCO).
ЮНСИТРАЛ – Комиссия Организации Объединенных Наций по праву международной торговли (от англ. UNCITRAL).

Используемая литература¹

1. Парошин А.А. Технология защиты информации: Программа курса – Владивосток: Изд-во Дальневост. Ун-та, 2010.
2. Стрельцов А.А. Государственная информационная политика: основы теории. М.: МЦНМО, 2010.
3. "Безопасность в электросвязи и информационных технологиях: Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи". Международный союз электросвязи. Женева, 2010.
4. Парошин А.А. Информационная безопасность: стандартизированные термины и понятия – Владивосток: Изд-во Дальневост. Ун-та, 2010.
5. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации (постатейный) – М.: Проспект, 2010.
6. Бачило И. Л. Информационное право – М.: Высшее образование, Юрайт-Издат, 2009.
7. "Понимание киберпреступности: Руководство для развивающихся стран". Международный союз электросвязи. Женева, апрель 2009.
8. Рассолов И.М. Право и Интернет. Теоретические проблемы – М.: Норма, 2009.
9. Витрук Н.В. Общая теория юридической ответственности. М.: Норма, 2009.
10. Родичев Ю.А. Информационная безопасность: Нормативно-правовые аспекты – СПб.: Питер, 2008.
11. Правовое обеспечение информационной безопасности: учебное пособие для студ. высших учеб. заведений/ Под ред. С.Я.Казанцева – М.: Издательский центр «Академия», 2008.
12. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студ. высших учеб. заведений/ Под ред. А.А. Стрельцова – М.: Издательский центр «Академия», 2008.
13. Дашян М.С. Право информационных магистралей (Law of information highways): Вопросы правового регулирования в сфере Интернет – М.: Волтерс Клувер, 2007.
14. Ковалева Н.Н. Информационное право России. – М.: Дашков и Ко, 2007.
15. Коротков А.В., Кристальный Б.В., Курносков И.Н. Государственная политика Российской Федерации в области развития информационного общества/ Под научн. ред. А.В.Короткова – М.: ООО "Трейн", 2007.
16. Мелехин А.В. Теория государства и права – М.: Маркет ДС, 2007.
17. Конявский В.А., Лопаткин С.В. Компьютерные преступления. В 2-х томах. Том 1 – М.: РФК-Имидж Лаб., 2006. 560 с.
18. Ищенко Е.П., Топорков А.А. Криминалистика: Учебник/ Под ред. Е.П. Ищенко – М.: КОНТРАКТ, ИНФРА-М, 2006.

¹ В списке не приводятся ссылки на нормативно-правовые акты и методические документы государственных органов, которые перечислены в тексте пособия.

19. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право/ Под ред. академика РАН Б.Н. Топорнина – СПб.: Издательство Р. Асланова "Юридический центр Пресс", 2005.
20. Копылов В.А. Информационное право: Учебник – М: Юристь, 2005.
21. Тропинина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Диссертация на соискание звания кандидата юридических наук. Владивосток, 2005.
22. Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право: Учебное пособие для студентов вузов, обучающихся по специальности 021100 "Юриспруденция" – М.: "ЮНИТИ-ДАНА", "Закон и право", 2004.
23. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы/ Под ред. В.А. Садовниченко и В.П. Шерстюка – М.: МЦНМО, 2002.
24. Бачило И.Л. Информационное право: основы практической информатики – М.: ИГиП РАН, 2001.

Введение

Основная цель настоящего пособия – изложение учебного и методического материала, необходимого для освоения следующих тем курса «Технология защиты информации»:

- Структура органов государственной власти РФ.
- Классификация защищаемой законом информации.
- Нормативно-правовое обеспечение защиты информации.
- Регуляторы в области защиты информации.
- Ответственность за нарушения законодательства РФ в сфере ИТ.

Систематическое изложение материала по указанным темам можно найти в литературе, приводимой в настоящем пособии.

В 1-м разделе пособия определяются базовые понятия теории права, необходимые для понимания последующего материала курса. Также в разделе приводятся базовые положения отрасли информационного права.

Во 2-м разделе описывается подотрасль информационной безопасности: дается определение основных категорий информации и информационной безопасности; проводится анализ базовых источников; описывается структура органов государственной власти РФ, регулирующих деятельность в области информационной безопасности и защиты информации.

Раздел 3 посвящен описанию нормативно-правового статуса различных категорий информации, охраняемой законодательством РФ.

В 4-5 разделах затронуты области государственного регулирования общественных отношений, смежных с отношениями в области информационной безопасности, в частности институты права собственности на информацию, исключительных прав на объекты интеллектуальной собственности и институты, регулирующие отношения в сферах информатизации.

Раздел 6 посвящен юридической ответственности за правонарушения в сфере информационной безопасности и защиты информации.

В пособии применяется сквозная нумерация источников правовых актов. В списке нормативно-правовые документы распределены по юридической силе; документы одного статуса – по дате принятия.

В пособии не включены ссылки на нормативно-правовые документы, изменяющие или уточняющие уже действующие; предполагается использование последних редакций действующих документов (со всеми вступившими в законную силу изменениями). Ссылки на нормативно-правовые и методические документы приводятся по состоянию на 15.02.2010.

Часть Общая

Раздел I. Правовые основы

Глава 1. Основы теории права

1.1. Базовые понятия

Право² есть система нормативного регулирования деятельности человека в государстве, определяемая следующими признаками:

1. Данная система регулирования основана на учете интересов различных слоев общества, их согласии и компромиссах.
2. Право есть мера, масштаб свободы и поведения человека.
3. Право обеспечивается государственной властью.
4. Нормативность есть исходное и основополагающее свойство права.
5. Право есть реально действующая система нормативной регуляции.
6. Право не тождественно закону.

В теории права соотношение категорий "право" и "законодательство" понимается неодинаково. Специфика права выражается в том, что это особое, обладающее объективными свойствами социальное явление. Право рассматривается как более широкая категория по отношению к законодательству.

Под **законодательством** в широком смысле понимают совокупность законов и подзаконных актов. Законодательство по уровню юридической силы делится на законы, нормативные указы главы государства и другие; а по сферам регулирования общественных отношений – на гражданское, трудовое, семейное и другие.

Закон в РФ – нормативно-правовой акт высшей (помимо конституции) юридической силы. Законы принимаются только Федеральным Собранием РФ; закон должен быть подписан Президентом РФ и опубликован.

Правовая норма – это общеобязательное правило поведения, установленное или санкционированное государством и им охраняемое. Особенно важно разграничение правовых норм по их роли в регулировании общественных отношений на *регулятивные* (правоустановительные), *правоохранительные* и *специализированные*.

Регулятивные нормы устанавливают юридические права и обязанности участников общественных отношений. Эти нормы рассчитаны на правомерное поведение людей и составляют большинство норм права

Правоохранительные нормы предусматривают меры государственного принудительного воздействия за совершение правонарушений. Они рассчитаны на неправомерное поведение людей и всегда содержат санкции. Взаимодействие регулятивных и правоохранительных норм заключается в том, что первые регулируют положительные действия людей, а вторые выражают отрицательную реакцию государства на их неправомерное поведение. Они направлены на охрану регулятивных норм и несут в себе государственное принуждение. Правоохранительные нормы

² Определения данной главы приводятся на основе учебника Мелехин А.В. Теория государства и права. М.: Маркет ДС, 2007 и материалов Википедии (ru.wikipedia.org).

направлены на регламентацию мер юридической ответственности, а также специфических государственно принудительных мер защиты субъективных прав.

Специализированные нормы содержат предписания, обеспечивающие понимание и действие как регулятивных, так и правоохранительных норм.

Реализация норм права физическим или юридическим лицом предполагает образование правоотношений.

Правоотношение в узком смысле является совокупностью персональных прав и обязанностей, возникших на основе норм права. Под правоотношением в широком смысле понимается общественное отношение, урегулированное правом (трудовое, гражданское, административное).

Правоотношения являются разновидностью общественных отношений (социальных отношений). **Общественные отношения** определяются как различные взаимодействия, урегулированные социальными нормами, между двумя или более людьми, каждый из которых имеет социальную позицию и осуществляет социальную роль.

К элементам структуры правоотношения относятся: *субъекты, содержание и объект правоотношения*.

Субъекты правоотношений – это отдельные люди или организации, которые в соответствии с нормой права наделены способностью быть участниками правоотношений. Субъектами правоотношений выступают право- и дееспособные физические лица, юридические лица и государство в целом.

Под социальным **содержанием правоотношения** понимается содержание фактического общественного отношения, т.е. деятельность, поведение участников отношения, осуществляемые в рамках их *субъективных прав и юридических обязанностей*, которые образуют юридическое содержание этого правоотношения.

Субъективное право – это установленная законом мера (вид, объем) возможного поведения конкретного субъекта права.

Юридическая обязанность – это установленная законом мера (вид, объем) должного поведения обязанного субъекта, которому оно должно следовать в интересах уполномоченной стороны под страхом государственного принуждения.

Объект правоотношений – это то, на что воздействуют юридические права и обязанности субъектов, т.е. волевое фактическое поведение участников правоотношений по осуществлению их прав и обязанностей. Иными словами – это блага, ценности, ради которых субъекты вступают в правоотношения. Так, в имущественных правоотношениях это действия, поведение сторон по выполнению прав и обязанностей, связанных с удовлетворением их материальных и культурных потребностей.

1.2. Система права

Отрасль права – эта систематизированная совокупность основных норм, образующих самостоятельную часть системы права, которые регулируют качественно своеобразный вид общественных отношений своим специфическим методом. Критериями деления права на отрасли являются предмет и метод правового регулирования.

Под **предметом правового регулирования** здесь понимается однородная и отделимая от других группа общественных отношений

Подотрасль права – это совокупность правовых норм, регулирующих общественные отношения определенного вида, которые составляют часть предмета правового регулирования отрасли права. Иными словами, это группа родственных институтов права в составе определенной отрасли права. Например, авторское и патентное право в гражданском праве. Внутри отраслей имеются правовые институты.

Правовой институт – это группа норм права, которые регулируют близкие по своему характеру и содержанию общественные отношения, отличающиеся существенными особенностями.

1.3. Виды источников

Источники права в юридическом смысле – форма выражения объективизации государственной воли, которой придается нормативный характер. Другими словами – это нормы, выраженные в какой-либо правовой форме. В теории выделяют четыре основные формы права:

- **нормативно-правовой акт** – это правовой акт, содержащий нормы права и направленный на урегулирование определенных общественных отношений. К их числу относятся: конституция, законы, подзаконные акты и т.п. Нормативный акт – одна из основных, наиболее распространенных и совершенных форм современного континентального права Германии, Франции, Италии, России и т.п.;
- **правовой обычай** – это исторически сложившееся правило поведения, содержащееся в сознании людей и вошедшее в привычку в результате многократного применения, приводящее к правовым последствиям вследствие санкционирования применения этого обычая государством. Санкционироваться применение правовых обычаев может ссылкой на него в нормативно-правовых актах, либо решением суда. В российской юридической системе роль правового обычая незначительна (например, согласно ст. 5 ГК РФ отдельные имущественные отношения могут регулироваться обычаями делового оборота, а правила погрузки-выгрузки судов обычаями портов);
- **юридический прецедент** – это судебное или административное решение по конкретному юридическому делу, которому придается сила нормы права и которым руководствуются при разрешении схожих дел. Во многих государствах публикуются судебные отчеты, из которых можно получить информацию о прецедентах. Признание прецедента источником права означает признание правотворческой функции суда. В России юридический прецедент официально не считается источником права, однако указания Высших судебных органов, формирующиеся на основании анализа судебной практики, считаются обязательными для исполнения всеми судами;
- **нормативный договор** – соглашение между правотворческими субъектами, в результате которого возникает новая норма права (например, Федеративный договор РФ 1992 г.; коллективный договор, который заключают между собой администрация предприятия и профсоюз).

В российском праве нормативно-правовой акт является основным источником права. Основные характеристики нормативно-правовых актов:

- 1) наиболее точно отражают содержание норм права;
- 2) наиболее оперативно позволяют изменять отраженные в них нормы;
- 3) доступны и удобны в использовании;
- 4) в масштабах страны составляют единую стройную соподчиненную систему.

Классификация нормативно-правовых актов по критерию юридической силы приводится в таблице ниже.

Таблица 1

Виды источников	Примеры
Основы государственного строя РФ	Конституция РФ; Законы РФ о принятии поправок к Конституции РФ; Акты Конституционного суда;
Международные правовые акты	Международные конвенции, соглашения, договоры; Директивы межправительственных международных организаций; Хартии, концепции;
Законы РФ	Федеральные конституционные законы; Кодифицированные федеральные законы; Федеральные законы; Законы СССР и РСФСР, приняты до вступления в силу Конституции РФ;
Федеральные нормативно-правовые акты	Внутригосударственные декларации, договоры и соглашения; Акты палат Федерального собрания РФ; Акты и Послания Президента РФ; Акты Правительства РФ; Акты федеральных министерств и иных федеральных органов исполнительной власти; Акты иных федеральных государственных органов (Центризбирком, Центробанк и т.п.);
Нормативно-правовые акты субъектов РФ	Основные законы (Конституции, или Уставы) субъектов РФ; Законы субъектов РФ; Акты высших должностных лиц и высшего исполнительного органа субъекта РФ; Акты иных государственных органов субъекта РФ;
Нормативно-правовые акты муниципальных образований	Уставы муниципальных образований; Акты представительного органа местного самоуправления; Акты главы местного самоуправления и исполнительно-распорядительных органов муниципального образования;
Локальные нормативные акты организаций	Коллективные договоры и соглашения; Приказы, распоряжения и иные внутренние нормативные документы.

Глава 2. Основы информационного права

2.1. Основной объект информационного права

Базовым объектом отрасли является *информация*. В понятие информации ученые разных научных подходов вкладывают различные значения. Мы будем придерживаться здесь подхода к анализу данного понятия предложенного А.А. Стрельцовым³. Постулируется, что информация представляет собой результат отражения движения объектов материального мира в системах живой природы. То есть понятие информации появляется только в жизнедеятельности живых организмов, не являясь абстрактным атрибутом материи.

Информация представляется в виде *сведений* об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством, либо *сообщений*, осведомляющих о положении дел, о состоянии чего-нибудь⁴.

Сведения представляют собой запечатленные в организме результаты отражения движения объектов материального мира. Они имеют духовный (идеальный, нематериальный) характер, объективны и инвариантны к субъекту восприятия. Предполагается что сведения не имеют физического носителя, не воспринимаются органами чувств и неуничтожаемы.

Сообщение представляет собой набор знаков, с помощью которого сведения могут быть переданы другому организму и восприняты им. Соответственно информация в виде сообщений субъективна, изменяема как в процессе передачи от организма к организму, так и в процессе восприятия и осознания получателем. Кроме этого, сообщения обладают свойством материальности (не хранятся без носителя) и, как следствие, свойствами копируемости и уничтожаемости.

Из всех форм представления информации наиболее выделяют «**Данные**». Под последними понимают представление информации в некотором формализованном виде, пригодном для передачи, интерпретации или обработки. Данные могут обрабатываться людьми или автоматическими средствами.

Основными свойствами информации являются:

1. Свойство физической неотчуждаемости информации. Оно основано на том, что знания не отчуждаемы от человека, их носителя. Исходя из этого, при передаче информации от одного лица к другому и юридического закрепления этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами.

2. Свойство обособляемое информации. Для включения в оборот информация всегда овеществляется в виде символов, знаков, волн, вследствие этого обособляется от ее производителя (создателя) и существует отдельно и независимо от него. Это подтверждает факт оборотоспособности информации как самостоятельного отдельного объекта правоотношений, в результате чего появляется возможность передачи информации в такой форме от одного субъекта к другому.

³ Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦНМО, 2002.

⁴ Ожегов С.И. Толковый словарь русского языка. М.: Оникс, Мир и Образование, 2010.

3. Свойство информационной вещи (информационного объекта). Это свойство возникает в силу того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя и проявляется как "двуединство" информации (ее содержания) и носителя, на котором эта информация (содержание) закреплена. Это свойство позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие двух институтов - института авторского права и института вещной собственности.

4. Свойство тиражируемое (распространяемости) информации. Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания. Одна и та же информация (содержание) может принадлежать одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации). Отсюда следует, что юридически необходимо закреплять объем прав по использованию информации (ее содержания) лицами, обладающими такой информацией (обладающими знаниями о содержании информации).

5. Свойство организационной формы. Информация, находящаяся в обороте, как правило, представляется в документированном виде, т.е. в форме документа. Это могут быть подлинник (оригинал) документа, его копия, массив документов на бумажном или электронном носителе (банк данных или база данных) тоже в виде оригинала или копии, библиотека, фонд документов, архив и т.п. Такое свойство дает возможность юридически закреплять факт "принадлежности" документа конкретному лицу, например, закрепив его соответствующей подписью в традиционном или в электронном виде (с помощью ЭЦП). Это свойство позволяет также относить к информационным вещам (информационным объектам) как отдельные документы, так и сложные организационные информационные структуры.

6. Свойство экзemplярности информации. Это свойство заключается в том, что информация распространяется, как правило, не сама по себе, а на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию. Понятие экзemplярности дает возможность учитывать документированную информацию и тем самым связывать содержательную сторону информации с ее "вещным" обрамлением, т.е. с отображением на носителе, вводить понятие учитываемой копии документа, а отсюда и механизма регистрации информации, в особенности учитывать обращение оригиналов (подлинников) документов. Экзemplярность информации уже сегодня активно реализуется при обращении информации ограниченного доступа.

Указанные юридические особенности и свойства должны учитываться при правовом регулировании информационных отношений.

2.2. Информационное общество

Учитывая глубину и размах технологических и социальных последствий компьютеризации и информатизации различных сфер общественной жизни и экономической деятельности, политологи предсказывают в ближайшее время новый этап развития современного общества в форме **информационного общества**, в которой главными продуктами производства становятся информация и знания.

Формирование информационного общества уже началось, некоторые страны и международные организации активно участвуют в этом⁵. Основные характеристики информационного общества можно легко проследить во всех сферах деятельности современного мира:

- Технологическая: ключевой фактор — информационные технологии, которые широко применяются в производстве, учреждениях, системе образования и в быту.
- Социальная: информация выступает в качестве важного стимулятора изменения качества жизни, формируется и утверждается «информационное сознание» при широком доступе к информации.
- Экономическая: информация составляет ключевой фактор в экономике в качестве ресурса, услуг, товара, источника добавленной стоимости и занятости.
- Политическая: свобода информации, ведущая к политическому процессу, который характеризуется растущим участием и консенсусом между различными классами и социальными слоями населения.
- Культурная: признание культурной ценности информации посредством содействия утверждению информационных ценностей в интересах развития отдельного индивида и общества в целом.

Соответственно информация стала жизненно необходимым фактором нормальной жизнедеятельности любого общества; решение вопросов информационной безопасности в настоящее время стало неотъемлемой частью обеспечения безопасности любой организации, общества, государства.

По мере формирования и развития информационного общества «деньги все в большей мере превращаются в информацию»: знание вытесняет труд (и ручной и механизированный) в стоимости товаров. Возникает новая дифференциация общества: деление «имущих и неимущих» по принципу лучшей информированности (а не только оснащенности ИТ, которые только создают для этого предпосылки). Информация начинает выступать как товар. В этой связи крайне востребовано становится институт права интеллектуальной собственности.

В настоящее время Законодательство РФ о праве интеллектуальной собственности отражено в Ч. 4 Гражданского кодекса РФ.

2.3. Дополнительные объекты информационного права

В качестве дополнительных объектов информационного права согласно ФЗ «Об информации, информационных технологиях и защите информации» могут выступать *информационные ресурсы, информационные технологии* (в том числе информационно-телекоммуникационные сети), *информационные системы*, а также *средства защиты информации и меры обеспечения информационной безопасности*.

Информационные ресурсы⁶ — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

⁵ Окинавская хартия глобального информационного общества. 22.07.2000.

⁶ Решение Коллегии Гостехкомиссии России № 7.2/02.03.01 «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

Документированная информация⁷ – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

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

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

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

Средство защиты информации⁸ – техническое, программное средство, вещество и (или) материал, предназначенный или используемый для защиты информации.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Меры обеспечения информационной безопасности⁹ – совокупность действий, направленных на разработку и (или) практическое применение способов и средств обеспечения информационной безопасности.

2.4. Предмет и метод отрасли

Основным предметом правового регулирования информационного права выступают **информационные отношения**, т.е. общественные отношения в информационной сфере, возникающие при осуществлении информационных процессов – процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации.

Под **методом правового регулирования** понимаются способы воздействия отрасли информационного права на информационные отношения. Многофункциональность и специфика информации приводят к необходимости применять в информационном праве по сути дела весь известный спектр методов правового регулирования в зависимости от вида и назначения информации.

В теории права существуют два основных метода правового регулирования общественных отношений: **императивный** (основан на использовании властеотношений и строгой связанности субъектов права правовыми рамками) и **диспозитивный** (основан на равенстве субъектов, их самостоятельности при вступлении в правоотношения, ответственности по своим обязательствам и т.п.). Способами воздействия на общественные отношения для императивного метода являются запрет и предписание, для диспозитивного – согласования, рекомендации.

⁷ ФЗ РФ от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

⁸ Государственный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).

⁹ Национальный стандарт РФ «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (ГОСТ Р 53114-2008).

В сфере правового регулирования существует деление и на такие два метода, как административно-правовой и гражданско-правовой (иногда их называют публично-правовой и частноправовой). Эти методы имеют особое значение для регулирования информационных отношений.

В целом **информационное право** представляет собой комплексную отрасль права, имеющую свой особый предмет правового регулирования – информационные отношения и использующую весь набор традиционных методов правового регулирования в пределах одной предметной отрасли¹⁰.

Информационное право, как и всякая иная отрасль права, проявляется в четырех свойственных юридическим знаниям формах. Имеются в виду такие формы, как: юридическая наука в области информационного права; информационное законодательство и связанная с ним правоприменительная практика; учебная дисциплина «Информационное право»; информационное правосознание.

2.5. Источники отрасли

В информационном праве в качестве источников рассматриваются международные и внутренние договоры РФ, система нормативных правовых актов начиная с федеральных законов и заканчивая локальными актами организаций.

Следует отметить, что нормы международных правовых актов действуют на территории России в виде норм международных договоров, ратифицированных РФ. Директивы межправительственных международных организаций, членом которых состоит, или к участию в которых стремится РФ, являются указанием к принятию в России национальных законов, исполняющих соответствующие нормы. Декларативные документы (хартии, концепции и т.п.) служат ориентиром в процессе законодательства или актуализации действующего национального законодательства.

Директивы Европейского Союза, принимаемые Европейским парламентом и Советом Европейского Союза, представляют собой удачный пример унификации (точнее, гармонизации) международного права в том смысле, что они обязывают государства-члены Европейского Союза привести свое внутреннее право в соответствие с предписаниями этих Директив в установленные сроки.

Кроме этого, необходимо знать, что Россия является юридическим правопреемником СССР (и РСФСР), поэтому внутренние нормативные акты и международные договора, принятые или подписанные от имени СССР (и РСФСР), и не отмененные прямым указанием на это в других нормативных актах (той же юридической силы), считаются действующими в настоящее время.

2.6. Система информационного права

Согласно предлагаемой классификации проблем информационного права, предложенной сектором информационного права Института государства и права Российской академии наук¹¹, можно выделить следующие направления отрасли:

¹⁰ Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право. М.: "ЮНИТИ-ДАНА", "Закон и право", 2004.

¹¹ Бачило И.Л. Информационное право: основы практической информатики. М.: ИГИП РАН, 2001.

1. **Решение общих организационных проблем** (государственная политика в области информации и информатизации, концепции и программы развития законодательства, номенклатура научных специальностей по информатике; органы гос. управления в области информации, информатизации).
2. **Информация. Информационные ресурсы.**
3. **Право на информацию.**
4. **Международный обмен информацией.**
5. **Информатизация.**
6. **СМИ. Телерадиовещание.**
7. **Информационная безопасность** (проблемы защиты открытой информации, охраны государственной тайны, обеспечения защиты информации ограниченного доступа, кроме государственной тайны, страхование информации, информационных ресурсов).
8. **Управление в области информации и информатизации.**
9. **Информационная деятельность. Информационные отношения.**
10. **Ответственность за правонарушения в области информации и информатизации.**

Однако, как указывается в последних учебниках по информационному праву¹², система отрасли в настоящее время окончательно не сформировалась. Определены несколько наиболее разработанных подотраслей и институтов отрасли, тогда как их список пока открыт, а структура в рамках отрасли до конца не сформирована.

ФЗ «Об информации, информационных технологиях и защите информации» выделяет следующие институты информационного права:

- **институт права собственности на информацию** (информация как объект гражданско-правовых отношений) (Ст. 5);
- **институт права на доступ к информации** (Ст. 8);
- **институт ограничения доступа к информации** (Ст. 9);
- **институт распространения информации**; статус общедоступной информации (Ст. 7,10);
- **институт предоставления информации**; информация, обязательная для предоставления и распространения (Ст. 10);
- **документирование информации** (Ст. 11);
- **институты государственного регулирования в сфере применения информационных технологий** (Ст. 12, 15);
- **информационные системы** как объект правового регулирования, порядок их создания и эксплуатации (Ст. 13, 14);
- **подотрасль защиты информации** (Ст. 16);
- **ответственность за правонарушения в сфере информации, информационных технологий и защиты информации** (Ст. 17).

В соответствии с этим, при написании настоящего пособия мы ориентировались на приведенную классификацию проблем и институтов отрасли, структурируя материал согласно наиболее проработанным областям законодательства РФ.

¹² Бачило И. Л. Информационное право. М.: Высшее образование, Юрайт-Издат, 2009.

Раздел II.

Правовая идеология информационной безопасности

Глава 3. Правовые основы защиты информации

3.1. Характеристика деятельности по защите информации

Определение понятия «защита информации» дается в Ст. 16 ФЗ «Об информации, информационных технологиях и защите информации»:

«**Защита информации** представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации».

Анализ Ст. 16 указанного Закона показывает, что:

- ✓ деятельность по защите информации применима ко всем категориям информации, описанной в Ст. 5 Закона. Для различных категорий информации содержание защиты (выбираемые способы защиты информации) будет различаться;
- ✓ выбираемые способы защиты информации применимы ко всем описанным ранее объектам информационного права;
- ✓ государственное регулирование отношений в сфере защиты информации осуществляется в двух формах: установление требований о защите информации и установление ответственности за нарушение информационного законодательства;
- ✓ основным субъектом информационного права, на которого возложена обязанность защиты информации, является обладатель информации;
- ✓ для защиты государственных информационных ресурсов и технологий федеральные органы исполнительной власти устанавливают обязательные для исполнения требования на обеспечение информационной безопасности этих ресурсов и технологий;
- ✓ федеральное законодательство может ограничивать использование в РФ определенных средств защиты информации и осуществление отдельных видов деятельности по защите информации для всех субъектов информационного права. Ограничения могут выражаться в форме прямых запретов или государственного контроля (например, лицензирование деятельности).

Информационная безопасность – Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности,

неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки¹³.

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

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

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К объектам физической защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Криптографическая защита информации – защита данных (информации) при помощи криптографического преобразования данных, т.е. при помощи шифрования и (или) выработки имитовставок.

Организационные меры обеспечения информационной безопасности – меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

3.2. Категории защищаемой информации

По критерию ограничения доступа к информации, согласно положениям Федерального закона N 149-ФЗ "Об информации, информационных технологиях и о защите информации", информацию можно разделить на:

- 1) общедоступную информацию;
- 2) конфиденциальную информацию;
- 3) информацию, относимую к гостайне.

¹³ Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий..

Конфиденциальная информация – это информация, не относимая к гостайне, доступ к которой ограничен федеральными законами. Среди конфиденциальной информации выделяют:

- 1) информацию, относимую к коммерческой тайне;
- 2) служебную информацию ограниченного распространения (для служебного пользования);
- 3) информацию, относимую к профессиональной тайне;
- 4) информацию, содержащую персональные данные.

Каждая из перечисленных категорий информации определяется и защищается правовыми нормами, источники которых можно рассматривать отдельно.

К деятельности по обеспечению информационной безопасности относят также защиту интеллектуальной собственности.

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

- 1) обеспечение связи и коммуникаций;
- 2) использования криптографических средств, в т.ч. шифрования и ЭЦП;
- 3) лицензирование, сертификация и аттестация объектов и средств защиты информации.

Кроме этого, к деятельности по защите информации относят механизмы применения мер ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации. Эта деятельность регулируется на государственном уровне.

Таким образом, при обзоре нормативно-правовых актов РФ предлагается отдельно рассматривать направления, регламентирующие деятельность в сфере обработки и защиты:

- 1) общедоступной информации;
- 2) информации, относимой к коммерческой тайне;
- 3) служебной информации ограниченного распространения;
- 4) информации, относимой к профессиональной тайне;
- 5) информации, содержащей персональные данные;
- 6) информации, относимой к гостайне;
- 7) объектов интеллектуальной собственности;
- 8) информации с использованием объектов связи и коммуникаций;
- 9) информации с использованием криптографических средств;
- 10) информации и объектов информатизации при необходимости лицензирования, сертификации и аттестации объектов и средств защиты информации;
- 11) в случаях нарушения законодательства РФ об информации, информационных технологиях и о защите информации.

3.3. Связь информационной безопасности с другими отраслями права

Базовыми отраслями, регулирующими право на информацию и предпосылки ограничения этого права являются конституционное право РФ и международное право, так как соответствующие нормы определяются Конституцией РФ, международными договорами.

Информационное право во многом берет свои методы из административного права. Это прямо указывается в ФЗ "Об информации, информационных технологиях и о защите информации", где (Ст. 16.2), в частности, определяется сфера государственного регулирования вопросов защиты информации. В нем обладатели информации, операторы обработки персональных данных и пр. субъекты ИП прямо обязываются обеспечивать необходимые меры по защите собственной информации.

Институты права на интеллектуальную собственность (в том числе в виде информационных ресурсов) регулируются гражданско-правовыми нормами, зафиксированными в Части 4 Гражданского кодекса РФ.

Институты ограничения доступа к информации базируются на определении конфиденциальной информации, к которой, относится служебная тайна, в том числе тайна следствия (предварительного и судебного) и судопроизводства (тайна заседания судей и присяжных). Регламент ограничения доступа к подобной информации регламентируют процессуальные институты: гражданский, административный, арбитражный процессы.

В списке объектов информации, относимых к профессиональной тайне весома роль объектов финансового права. Это банковская, аудиторская тайна, тайна страхования.

Для формирования комплекса организационных мер по обеспечению защиты всех типов информации могут привлекаться нормы предпринимательского, административного, трудового права.

Ответственность за нарушение информационного законодательства привлекает к регулированию как нормы базовых отраслей права (уголовного, административного, трудового), так и процессуальные отрасли (гражданского, уголовного процесса).

К сожалению, методы криминалистики ограниченно применимы к расследованию правонарушений в области ИБ из-за того, что процессуальные действия могут совершать только органы следствия и дознания, список которых определен законодательством РФ и строго ограничен.

Криминология, напротив, позволяет при помощи своего методологического аппарата провести анализ возникших ранее преступлений в сфере ИБ как отдельных, так и в совокупности, и разработать модель противодействия им в будущем.

Глава 4. Базовые источники информационной безопасности

4.1. Конституция РФ

Принципы защиты информации базируются на основополагающих международных нормах, конституционных принципах построения государственности России и излагаются в следующих статьях Конституции РФ:

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

Ст. 15:

1. Конституция РФ имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции РФ.

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

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

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

Ст. 23:

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

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

Ст. 24:

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

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

Ст. 29: Каждому гарантируется свобода мысли и слова.

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

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

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

5. Гарантируется свобода массовой информации. Цензура запрещается.

Ст. 44: Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

4.2. Федеральный Закон «Об информации, информационных технологиях и о защите информации»

В Ст. 1 Закона ограничивается его сфера применимости – это общественные правоотношения, связанные:

- с доступом к информации;
- с применением информационных технологий;
- с обеспечением защиты информации.

В Законе вводится официальное определение понятия информации: «**Информация** – сведения (сообщения, данные) независимо от формы их представления»; определяются принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации; говорится о возможности классификации информации по трем критериям:

- в зависимости от категории доступа к ней;
- в зависимости от порядка ее предоставления или распространения;
- в зависимости от ее содержания или обладателя.

В Законе определяются круг субъектов, способных быть обладателем информации (Ст. 6) – гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект РФ, муниципальное образование. Перед этим приводится определение понятия **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Определены **права обладателя информации**:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

- 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Владелец информации при осуществлении своих прав обязан:

- 1) соблюдать права и законные интересы иных лиц;
- 2) принимать меры по защите информации;
- 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Также Законом вводятся требования к владельцу информации при осуществлении его прав:

- 1) соблюдать права и законные интересы иных лиц;
- 2) принимать меры по защите информации;
- 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Законодательство РФ об информации, информационных технологиях и о защите информации основывается на Конституции РФ, международных договорах РФ и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

4.3. Статус концепций и доктрин

Кроме нормативно-правовых актов важную роль в формировании научного подхода и правового института информационной безопасности играют концептуальные документы, принимаемые на уровне Президента РФ, Правительства РФ и иных компетентных федеральных органов исполнительной власти России. Они определяют политику государства в развитии описываемых общественных отношений, формируют базис для принятия нормативно-правовых актов в соответствующей сфере деятельности.

К концептуальным документам можно отнести также хартии и декларации международных межправительственных организаций, которыми руководствуется РФ при формировании своей внешней и внутренней политики.

4.4. Перечень нормативно-правовых документов¹⁴

1. "Конституция РФ" (Принята всенародным голосованием 12.12.1993).
2. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

¹⁴ Здесь и далее список нормативных документов сформировался с использованием справочно-правовой системы «КонсультантПлюс», информационно-правовой системы «Гарант», Единого реестра правовых актов и других документов СНГ.

4.5. Перечень международных декларативных документов

3. "Всеобщая декларация прав человека" (Принята 10.12.1948 Генеральной Ассамблеей ООН).
4. Резолюция N 428 (1970) Консультативной ассамблеи Совета Европы "Относительно Декларации о средствах массовой информации и правах человека" (Принята 23.01.1970 на 21-ой сессии Консультативной ассамблеи Совета Европы).
5. "Декларация об основных принципах, касающихся вклада средств массовой информации в укрепление мира и Международного взаимопонимания, в развитие прав человека и борьбу против расизма и апартеида и подстрекательства к войне" (Принята ЮНЕСКО 28.11.1978).
6. "Международный кодекс рекламной практики" (Принят на 47-ой сессии Исполнительного совета Международной торговой палаты, 02.12.1986).
7. "Концепция межгосударственной подсистемы информационного обмена между Пограничными войсками государств-участников СНГ" (Утв. Решение Совета глав пр-в СНГ от 18.10.1996).
8. "Декларация о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы" (Принята в г.Нью-Йорке 09.12.1998 Резолюцией 53/144 на 85-ом пленарном заседании 53-ей сессии Генеральной Ассамблеи ООН).
9. "Декларация о европейской политике в области новых информационных технологий" (Принята в г. Будапеште 06.05.1999–07.05.1999 на 104-ой сессии Комитета министров СЕ).
10. "Концепция межгосударственной подсистемы информационного обмена между органами внутренних дел государств-участников СНГ" (Утв. Решение Совета глав пр-в СНГ от 04.06.1999).
11. "Концепция информационной безопасности государств-участников СНГ в военной сфере" (Утв. Решением Совета глав пр-в СНГ от 04.06.1999).
12. Окинавская хартия глобального информационного общества. 22.07.2000.
13. "Элементы для создания глобальной культуры кибербезопасности" (Утверждены резолюцией 57/239 Генеральной Ассамблеи ООН от 20.12.2002).
14. "Декларация о свободе обмена информацией в Интернете" (принята на 840 заседании Комитета министров СЕ 28.05.2003).
15. Хартия о сохранении цифрового наследия (Принята на 32-й Генеральной конференции ЮНЕСКО, Париж, Франция, октябрь 2003).
16. "Декларация принципов: Построение информационного общества – глобальная задача в новом тысячелетии" (Всемирная встреча на высшем

уровне по вопросам информационного общества WSIS-03/GENEVA/DOC/4-R. Женева, 12.12.2003).

17. "План действий" (Всемирная встреча на высшем уровне по вопросам информационного общества WSIS-03/GENEVA/DOC/5-R. Женева, 12.12.2003).
18. "Концепция Единого реестра правовых актов и других документов СНГ" (вместе с Положением о Едином реестре правовых актов и других документов СНГ) (Утв. Решение Совета глав пр-в СНГ от 15.09.2004).
19. "Декларация Комитета министров о правах человека и верховенстве права в Информационном Обществе" (принята Комитетом министров СЕ 13.05.2005).
20. "Тунисская программа для информационного общества" (Всемирная встреча на высшем уровне по вопросам информационного общества. WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунис, 15.11.2005).
21. "Тунисское обязательство" (Всемирная встреча на высшем уровне по вопросам информационного общества WSIS-05/TUNIS/DOC/7-R. Тунис, 18.11.2005).
22. "Концепция формирования национальных баз данных и организации межгосударственного обмена информацией по предупреждению и пресечению правонарушений в области интеллектуальной собственности" (утв. Решением Совета глав государств СНГ от 25.05.2006 № ЕРПА СНГ 3/20648).
23. "Глобальная программа кибербезопасности (ГПК) МСЭ" (Международный союз электросвязи. Женева, апрель 2008).
24. "Сеульская декларация по будущему интернет-экономики" (принята по итогам Министерской встречи ОЭСР 17-18 июня 2008 г., Сеул, Корея).
25. "Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности" (вместе с Комплексным планом мероприятий по реализации Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на период с 2008 по 2010 год) (утв. Решением Совета глав государств СНГ от 10.10.2008 N ЕРПА СНГ 2/208574).

4.6. Перечень модельных (типовых) законов

26. "Международный кодекс рекламной деятельности" Международной торговой палаты (ред. 1986).
27. "Типовой закон ЮНСИТРАЛ об электронной торговле" (Принят на 29-й сессии ЮНСИТРАЛ. Рекомендован Резолюцией 51/162 Генеральной Ассамблеи ООН от 16.12.1996).
28. Модельный закон "О доступе к экологической информации" (Принят в г. Санкт-Петербурге 06.12.1997 Пост. 10-7 на 10-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).

29. Модельный закон "Об оперативно-розыскной деятельности" (Принят в г. Санкт-Петербурге 06.12.1997 Пост. 10-12 на 10-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
30. Модельный закон "О стандартизации" (Принят в г. Санкт-Петербурге 06.12.1997 Пост. 10-16 на 10-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
31. Модельный закон "Об обеспечении единства измерений" (Принят в г. Санкт-Петербурге 15.06.1998 Постановлением 11-4 на 11-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
32. Модельный закон "О трансграничном спутниковом телевизионном и радиовещании и международном спутниковом информационном обмене" (Принят в г. Санкт-Петербурге 15.06.1998 Пост. 11-11 на 11-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
33. "Модельный библиотечный кодекс для государств-участников СНГ (часть вторая)" (Принят в г. Санкт-Петербурге 08.12.1998 Пост. 12-11 на 12-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
34. Модельный закон "Об архивах и архивном фонде" (Принят в г. Санкт-Петербурге 03.04.1999 Пост. 13-9 на 13-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
35. Модельный закон "О банковской тайне" (Принят в г. Санкт-Петербурге 16.10.1999 Пост. 14-7 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
36. Модельный закон "Об издательском деле" (Принят в г. Санкт-Петербурге 16.10.1999 Пост. 14-17 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
37. Модельный закон "О персональных данных" (Принят в г. Санкт-Петербурге 16.10.1999 Пост. 14-19 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
38. "Российский рекламный кодекс" Рекламного Совета России (2000).
39. Модельный закон "О научно-технической информации" (Принят в г. Санкт-Петербурге 13.06.2000 Пост. 15-10 на 15-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
40. Модельный закон "Об электронной цифровой подписи" (Принят в г. Санкт-Петербурге 09.12.2000 Пост. 16-10 на 16-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
41. "Типовой закон ЮНСИТРАЛ об электронных подписях" (Принят в г. Вене 05.07.2001 на 34-ой сессии ЮНСИТРАЛ).

42. Модельный закон "О международном информационном обмене" (Принят на 19-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ. Пост. № 19-7 от 26.03.2002).
43. Модельный закон "О государственной экспертизе" (Принят в г. Санкт-Петербурге 07.12.2002 Пост. 20-7 на 20-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
44. Модельный закон "О полиции (милиции)" (Принят в г. Санкт-Петербурге 07.12.2002 Пост. 20-12 на 20-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
45. Модельный закон "О реализации прав государства на объекты интеллектуальной собственности в сфере науки и технологий" (Принят в г. Санкт-Петербурге 07.12.2002 Пост. 20-13 на 20-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
46. Модельный закон "О государственных секретах" (Принят в г. Санкт-Петербурге 16.06.2003 Пост. 21-10 на 21-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
47. Модельный закон "О негосударственной (частной) охранной деятельности и негосударственной (частной) сыскной деятельности" (Принят в г. Санкт-Петербурге 16.06.2003 Пост. 21-11 на 21-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
48. Модельный закон "О телекоммуникациях" (Принят в г. Санкт-Петербурге 15.11.2003 Пост. 22-14 на 22-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
49. Модельный закон "О научной и научно-технической экспертизе" (Принят в г. Санкт-Петербурге 15.11.2003 Пост. 22-17 на 22-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
50. Модельный закон "О праве на доступ к информации" (Принят на 23-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (Пост. № 23-14 от 17.04.2004)).
51. Модельный закон "Об информатизации, информации и защите информации" (Принят в г. Санкт-Петербурге 18.11.2005 Пост. 26-7 на 26-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
52. Модельный закон "О прокуратуре" (Принят в г. Санкт-Петербурге 16.11.2006 Пост. 27-6 на 27-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
53. "Модельный информационный кодекс для государств - участников СНГ. Часть первая" (Принят в г. Санкт-Петербурге 03.04.2008 Пост. N 30-6 на 30-м Пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ).

54. Модельный закон "Об электронной торговле" (Принят в г. Санкт-Петербурге 25.11.2008 Пост. 31-12 на 31-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).

4.7. Перечень национальных концепций РФ

55. "Декларация прав и свобод человека и гражданина" (утв. Пост. ВС РФ от 22.11.1991 N 1920-1).

56. "Концепция государственной информационной политики РФ" (Одобрена на заседании Комитета по информационной политике и связи Государственной Думы ФС РФ 15.10.1998).

57. "Концепция правовой информатизации России" (утв. Указом Президента РФ от 28 июня 1993 г. N 966).

58. "Доктрина информационной безопасности РФ" (утв. Президентом РФ 09.09.2000 N Пр-1895).

59. "Стратегия развития информационного общества в РФ" (утв. Президентом РФ 07.02.2008 N Пр-212).

60. "Концепция внешней политики РФ" (утв. Президентом РФ 12.07.2008 N Пр-1440).

61. "Послание Президента РФ Федеральному Собранию" (Публикуется ежегодно, последнее от 12.11.2009).

62. "Стратегия национальной безопасности РФ до 2020 года" (утв. Указом Президента РФ от 12.05.2009 N 537).

63. "Военная доктрина РФ" (утв. Указом Президента РФ от 05.02.2010 N 146).

64. "Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года и План мероприятий по её реализации" (утв. Распоряжением Пр-ва РФ от 27.09.2004 N 1244-р).

65. "Концепция создания государственной системы изготовления, оформления и контроля паспортно-визовых документов нового поколения" (утв. Распоряжением Пр-ва РФ от 15.03.2005 N 277-р).

66. "Концепция создания системы персонального учета населения РФ" (утв. Распоряжением Пр-ва РФ от 09.06.2005 N 748-р).

67. "Концепция развития национальной системы стандартизации" (утв. Распоряжением Пр-ва РФ от 28.02.2006 N 266-р).

68. "Концепция региональной информатизации до 2010 года" (утв. Распоряжением Пр-ва РФ от 17.07.2006 N 1024-р).

69. "Концепция создания государственной автоматизированной системы информационного обеспечения управления приоритетными национальными проектами" (утв. Распоряжением Пр-ва РФ от 24.04.2007 N 516-р).

70. "Концепция формирования в РФ электронного правительства до 2010 года" (утв. Распоряжением Пр-ва РФ от 06.05.2008 N 632-р).
71. "Концепция долгосрочного социально-экономического развития РФ на период до 2020 года" (утв. Распоряжением Пр-ва РФ от 17.11.2008 N 1662-р).
72. "Концепция федеральной целевой программы "Развитие телерадиовещания в РФ на 2009-2015 годы" (утв. Распоряжением Пр-ва РФ от 21.09.2009 N 1349-р).
73. "Концепция информатизации судов общей юрисдикции и системы Судебного департамента" (Одобрена Советом судей РФ 29.10.99).
74. "Концепция информационной политики судебной системы" (утв. Пост. Совета судей РФ N 60 от 16.11.2001).
75. "Приоритетные проблемы научных исследований в области обеспечения информационной безопасности РФ" (утв. Исполняющим обязанности Секретаря Совета Безопасности РФ, председателя научного совета при Совете Безопасности РФ 07.03.2008).
76. "Концепция развития гражданского законодательства РФ" (одобрена решением Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства от 07.10.2009).

Глава 5. Организационная структура государственной системы обеспечения информационной безопасности России

5.1. Система федеральных органов государственной власти

Согласно конституционным основам государственного устройства России (ст. 10 Конституции РФ), «государственная власть в РФ осуществляется на основе разделения на *законодательную, исполнительную и судебную*». Верховное положение занимает **Законодательная власть**, поскольку именно она облекает в закон основные направления внутренней и внешней политики, обеспечивает верховенство закона в обществе. **Исполнительная власть** в лице своих органов занимается непосредственной реализацией правовых норм, принятых законодателем. **Судебная власть** призвана охранять право, правовые устои государственной и общественной жизни от любых нарушений, кто бы их ни совершал¹⁵.

Для дальнейшего понимания уточним понятия *государственных органов* и *органов государственной власти*. Согласно доктринальному толкованию¹⁶, это:

Государственный орган – это составная часть механизма государства, имеющая в соответствии с законом собственную структуру, строго определенные полномочия по управлению конкретной сферой общественной жизни и органически взаимодействующая с другими частями государственного механизма, образуя единое целое.

Органы государственной власти – понятие несколько уже, чем государственные органы. Органам государственной власти присуща компетенция осуществления властных полномочий. Например, Избирательные комиссии, являются государственным органом РФ, но не входят в состав органов государственной власти.

Среди органов государственной власти выделяют *правоохранительные органы* или *контрольно-надзорные органы*.

Правоохранительные органы (или **Регуляторы**) осуществляют постоянный повседневный надзор и контроль за правильной реализацией и применением норм права органами исполнительной власти, различными организациями, учреждениями, предприятиями, должностными лицами и гражданами. К контрольно-надзорным органам государственной власти относятся: Прокуратура РФ, Счетная палата РФ и другие органы государственной власти, осуществляющие контрольно-надзорные функции. Контрольно-надзорные органы государственной власти выявляют различные нарушения законности и правопорядка, применяют к правонарушителям соответствующие санкции или ставят перед компетентными органами вопрос об устранении допущенных нарушений законности и привлечении виновных лиц к юридической ответственности.

¹⁵ Бархатова Е.Ю. Комментарий к Конституции Российской Федерации (постатейный) – М.: Проспект, 2010.

¹⁶ Мелехин А.В. Теория государства и права: Учебник. М.: Маркет ДС, 2007.

На федеральном уровне к высшим органами, осуществляющими государственную власть РФ (ст. 11 Конституции РФ), относятся¹⁷:

Таблица 2

Ветвь власти	Законодательная	Исполнительная	Судебная
Функция	Правотворчество	Правоприменение	Правосудие
Представительные органы власти	Федеральное собрание (Совет Федераций и Государственная Дума)	Президент РФ, Правительство РФ	Конституционный суд РФ, Верховный суд РФ, Высший арбитражный суд РФ, Дисциплинарное судебное присутствие, Генеральная прокуратура РФ, Уполномоченный по правам человека в РФ

При каждом из высших органов законодательной и исполнительной ветвей федеральной власти существуют органы (комиссии, подразделения, отдельные структуры и т.п.), осуществляющие необходимые полномочия высших органов государственной власти в сфере информации, информационной безопасности.

Комитеты и комиссии Совета Федераций¹⁸

Таблица 3

Подведомственный орган	Компетенция
Комитет по обороне и безопасности СФ РФ	вопросы законодательного обеспечения в рамках своей компетенции
Комиссия по информационной политике СФ РФ	изучение и мониторинг информационной ситуации, а дальнейшее совершенствование законодательной базы в интересах большей ее ориентации на формирование единого информационного пространства, решение других вопросов информационной политики РФ

Комитеты и комиссии Государственной Думы¹⁹

Таблица 4

Подведомственный орган	Компетенция
Комитет по безопасности ГД РФ	законодательная, представительная и международная деятельность в сфере своей компетенции
Комитет по информационной политике, информационным технологиям и связи ГД РФ	законодательная, представительная и международная деятельность в сфере своей компетенции

¹⁷ www.gov.ru.

¹⁸ council.gov.ru.

¹⁹ www.duma.gov.ru.

Органы государственной власти, подведомственные Президенту РФ²⁰

Таблица 5

Подведомственный орган	Компетенция	Официальный сайт
Совет Безопасности РФ (СовБез России); Межведомственная комиссия по ИБ (в составе СовБеза)	является конституционным органом, осуществляющим подготовку решений Президента РФ в области обеспечения безопасности	scrf.gov.ru
Совет по развитию информационного общества в РФ	является совещательным органом при Президенте РФ, созданным для обеспечения взаимодействия федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, общественных объединений, научных и других организаций при рассмотрении вопросов, связанных с развитием информационного общества в РФ	
Федеральная служба по техническому и экспортному контролю (ФСТЭК России)	федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля	www.fstec.ru
Федеральная служба безопасности РФ (ФСБ России)	является федеральным органом исполнительной власти, в пределах своих полномочий осуществляющим государственное управление в области обеспечения безопасности РФ, защиты и охраны государственной границы РФ, охраны внутренних морских вод, территориального моря, исключительной экономической зоны, континентального шельфа РФ и их природных ресурсов, обеспечивающим информационную безопасность РФ и непосредственно реализующим основные направления деятельности органов федеральной службы безопасности, определенные законодательством РФ, а также координирующим контрразведывательную деятельность федеральных органов исполнительной власти, имеющих право на ее осуществление	www.fsb.ru
Служба внешней разведки РФ (СВР России)	является составной частью сил обеспечения безопасности и призвана защищать безопасность личности, общества и государства от внешних угроз. СВР осуществляет разведывательную деятельность в целях: - обеспечения Президента РФ, Федерального Собрания и Правительства РФ разведывательной информацией, необходимой им для принятия решений в политической, экономической, военно-стратегической, научно-технической и экологической областях;	svr.gov.ru

²⁰ www.kremlin.ru.

	<ul style="list-style-type: none"> - обеспечения условий, способствующих успешной реализации политики РФ в сфере безопасности; - содействия экономическому развитию, научно-техническому прогрессу страны и военно-техническому обеспечению безопасности РФ 	
Федеральная служба охраны РФ (ФСО России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны, президентской, правительственной и иных видов специальной связи и информации, предоставляемых федеральным органам государственной власти, органам государственной власти субъектов РФ и другим государственным органам	fso.gov.ru
Министерство внутренних дел (МВД России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, в том числе в сфере миграции	www.mvd.ru
Министерство обороны (Минобороны России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики, нормативно-правовому регулированию в области обороны, а также иные установленные федеральными конституционными законами, федеральными законами, актами Президента РФ и Правительства РФ функции в этой области	www.mil.ru
Министерство иностранных дел (МИД России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере международных отношений РФ	www.mid.ru
Министерство юстиции (Минюст России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, в том числе в сфере исполнения уголовных наказаний, регистрации некоммерческих организаций, включая отделения международных организаций и иностранных некоммерческих неправительственных организаций, общественные объединения, политические партии и религиозные организации, в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния, обеспечения установленного порядка деятельности судов и исполнения судебных актов и актов других органов, а также правоприменительные функции и функции по контролю и надзору в сфере регистрации некоммерческих организаций, включая отделения международных организаций и иностранных некоммерческих неправительственных организаций, общественные объединения, политические партии и религиозные организации, в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния	minjust.ru

Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики, нормативно-правовому регулированию, а также по надзору и контролю в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, обеспечения пожарной безопасности и безопасности людей на водных объектах	mchs.gov.ru
Государственная фельдъегерская служба РФ (ГФС России)	является федеральным органом исполнительной власти, осуществляющим специальные функции в сфере обеспечения федеральной фельдъегерской связи в РФ	
Межведомственная комиссия по защите государственной тайны	является коллегиальным органом, координирующим деятельность федеральных органов государственной власти и органов государственной власти субъектов РФ по защите гостайны в интересах разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о гостайне	
Межведомственная комиссия по вопросам предоставления правительственной и специальной связи	рассматривает обращения об обеспечении правительственной и специальной связью должностных лиц государственных органов, предприятий и организаций, поступившие в Администрацию Президента РФ, Аппарат Пр-ва РФ, ФСО РФ	

Органы государственной власти, подведомственные Правительству РФ²¹

Таблица 6

Подведомственный орган	Компетенция	Официальный сайт
Правительственная комиссия по федеральной связи и информационным технологиям	является координационным органом, образованным для обеспечения согласованных действий федеральных органов исполнительной власти в сфере развития и совершенствования федеральной связи и информационных технологий	minkomsvjaz.ru /ministry/2614/
Министерство связи и массовых коммуникаций РФ (Минкомсвязи России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним), электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи, массовых коммуникаций и средств массовой информации, в том числе электронных (включая развитие сети Интернет, систем телевизионного (в том числе цифро-	minsvyaz.ru

²¹ www.government.ru.

	вого) вещания и радиовещания и новых технологий в этих областях), печати, издательской и полиграфической деятельности, обработки персональных данных. Минкомсвязи РФ выступает в качестве почтовой администрации РФ и выполняет функции администрации связи РФ при осуществлении международной деятельности в области связи	
Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)	является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, а также функции по организации деятельности радиочастотной службы	www.rsoc.ru
Федеральное агентство по информационным технологиям (Росинформтехнологии)	является федеральным органом исполнительной власти, осуществляющим функции по управлению государственным имуществом и оказанию государственных услуг в сфере информационных технологий, в том числе в части использования информационных технологий для формирования государственных информационных ресурсов и обеспечения доступа к ним, а также уполномоченным федеральным органом исполнительной власти в области использования электронной цифровой подписи	mins-vyaz.ru/departments/rosinformtechnologii
Государственная комиссия по радиочастотам	является межведомственным координационным органом, действующим при Минкомсвязи РФ и осуществляющим на коллегиальной основе регулирование использования радиочастотного спектра в РФ	
Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент)	является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере правовой охраны и использования объектов интеллектуальной собственности, включая патенты и товарные знаки. Основными функциями Федеральной службы по интеллектуальной собственности, патентам и товарным знакам являются: а) обеспечение установленного Конституцией РФ, федеральными конституционными законами, федеральными законами и другими нормативными правовыми актами порядка предоставления в РФ правовой охраны объектам интеллектуальной собственности, а также порядка их использования; б) осуществление контроля и надзора за проведением экспертизы заявок на объекты интеллектуальной собственности и выдача охранных документов в установленном законодательством РФ порядке; в) регистрация прав на объекты интеллектуальной собственности, а также лицензионных договоров и договоров уступки прав в сфере интеллектуальной собственности и публикация сведений о зарегистрированных объектах ин-	www.fips.ru

	<p>теллектуальной собственности;</p> <p>г) осуществление контроля и надзора за соблюдением порядка уплаты патентных пошлин и регистрационных сборов;</p> <p>д) проведение аттестации и регистрация патентных поверенных РФ и осуществление контроля за выполнением ими требований, предусмотренных законодательством РФ</p>	
Федеральное агентство по техническому регулированию и метрологии (Ростехрегулирование)	является федеральным органом исполнительной власти, осуществляющим функции по оказанию государственных услуг, управлению государственным имуществом в сфере технического регулирования и метрологии	www.gost.ru
Министерство культуры РФ (Минкультуры России)	является федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики в сфере культуры, искусства, историко-культурного наследия, кинематографии, архивного дела, авторского права и смежных прав, а также по нормативно-правовому регулированию в сфере культуры, искусства, историко-культурного наследия (за исключением сферы охраны культурного наследия), кинематографии, архивного дела, авторского права и смежных прав (за исключением нормативно-правового регулирования осуществления контроля и надзора в сфере авторского права и смежных прав) и функции по управлению государственным имуществом и оказанию государственных услуг в сфере культуры и кинематографии	www.mkmk.ru
Федеральное архивное агентство (Росархив)	является федеральным органом исполнительной власти, осуществляющим функции по оказанию государственных услуг, управлению федеральным имуществом, а также правоприменительные функции в сфере архивного дела. Росархив в установленной сфере деятельности осуществляет: <ul style="list-style-type: none"> а) оказание государственных услуг в сфере архивного дела; б) государственный учет документов Архивного фонда РФ, ведение Государственного реестра уникальных документов Архивного фонда РФ; в) обеспечение соблюдения правил хранения, комплектования, учета и использования архивных документов 	archives.ru , rusarchives.ru
Федеральная антимонопольная служба (ФАС России)	является уполномоченным федеральным органом исполнительной власти, осуществляющим функции по принятию нормативных правовых актов и контролю за соблюдением антимонопольного законодательства, законодательства в сфере деятельности субъектов естественных монополий (в части установленных законодательством полномочий антимонопольного органа), рекламы, контролю за осуществлением иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства, а также по контролю в сфере размещения заказов на поставки това-	fas.gov.ru

	ров, выполнение работ, оказание услуг для федеральных государственных нужд (за исключением полномочий по контролю в сфере размещения заказов на поставки товаров, выполнение работ, оказание услуг по государственному оборонному заказу, а также в сфере размещения заказов на поставки товаров, выполнение работ, оказание услуг для федеральных государственных нужд, не относящихся к государственному оборонному заказу, сведения о которых составляют гостайну)	
Экспертный совет по авторским и смежным правам	является экспертным органом, призванным на основе взаимодействия Минкультуры РФ, заинтересованных органов государственной власти, организаций по управлению правами на коллективной основе, имеющих государственную аккредитацию, научных кругов и ведущих специалистов отрасли содействовать поиску оптимальных и эффективных решений для реализации Минкультуры РФ государственной политики и нормативно-правового регулирования сферы авторских и смежных прав	

5.2. Компетенция органов государственной власти в области информационной безопасности

Система обеспечения информационной безопасности РФ является частью системы обеспечения национальной безопасности страны²².

Система обеспечения информационной безопасности РФ строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов РФ.

Основными элементами организационной основы системы обеспечения информационной безопасности РФ являются:

Таблица 7

Орган государственной власти	Компетенция в области ИБ
Президент РФ	руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности РФ; санкционирует действия по обеспечению информационной безопасности РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности РФ; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации настоящей Доктрины
Палаты Федерального Собрания РФ	на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности РФ

²² "Доктрина информационной безопасности РФ" (утв. Президентом РФ 09.09.2000 N Пр-1895).

Правительство РФ	в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области
Совет Безопасности РФ	проводит работу по выявлению и оценке угроз информационной безопасности РФ, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности РФ, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности РФ, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области
Федеральные органы исполнительной власти	обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту РФ и в Правительство РФ
Межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ	решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности РФ
Органы исполнительной власти субъектов РФ	взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности РФ; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ
Органы местного самоуправления	обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности РФ
Органы судебной власти	осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ

5.3. Перечень нормативно-правовых, нормативно-методических документов

77. Федеральный конституционный закон от 21.07.1994 N 1-ФКЗ "О Конституционном Суде РФ".
78. Федеральный конституционный закон от 28.04.1995 N 1-ФКЗ "Об арбитражных судах в РФ".
79. Федеральный конституционный закон от 31.12.1996 N 1-ФКЗ "О судебной системе РФ".
80. Федеральный конституционный закон от 26.02.1997 N 1-ФКЗ "Об Уполномоченном по правам человека в РФ".
81. Федеральный конституционный закон от 17.12.1997 N 2-ФКЗ "О Правительстве РФ".
82. Федеральный конституционный закон от 23.06.1999 N 1-ФКЗ "О военных судах РФ".
83. Федеральный конституционный закон от 09.11.2009 N 4-ФКЗ "О Дисциплинарном судебном присутствии".
84. Федеральный закон от 17.01.1992 N 2202-1 "О прокуратуре РФ".
85. Закон РФ от 05.03.1992 N 2446-1 "О безопасности".
86. Федеральный закон от 03.04.1995 N 40-ФЗ "О Федеральной службе безопасности".
87. Федеральный закон от 10.01.1996 N 5-ФЗ "О внешней разведке".
88. Федеральный закон от 17.12.1998 N 188-ФЗ "О мировых судьях в РФ".
89. Федеральный закон от 24.07.2002 N 102-ФЗ "О третейских судах в РФ".
90. Указ Президента РФ от 20.01.1994 N 170 "Об основах государственной политики в сфере информатизации".
91. Указ Президента РФ от 08.11.1995 N 1108 "О Межведомственной комиссии по защите гостайны".
92. Указ Президента РФ от 29.01.2001 N 88 "О Межведомственной комиссии по вопросам предоставления правительственной и специальной связи".
93. Указ Президента РФ от 11.08.2003 N 960 "Вопросы Федеральной службы безопасности РФ".
94. Указ Президента РФ от 09.03.2004 N 314 "О системе и структуре федеральных органов исполнительной власти".
95. Указ Президента РФ от 07.06.2004 N 726 "Об утв. Положений о Совете Безопасности РФ и аппарате Совета Безопасности РФ, а также об изменении и признании утратившими силу отдельных актов Президента РФ".
96. Указ Президента РФ от 11.07.2004 N 865 "Вопросы Министерства иностранных дел РФ".

97. Указ Президента РФ от 11.07.2004 N 868 "Вопросы Министерства РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий".
98. Указ Президента РФ от 19.07.2004 N 927 "Вопросы Министерства внутренних дел РФ".
99. Указ Президента РФ от 07.08.2004 N 1013 "Вопросы Федеральной службы охраны РФ".
100. Указ Президента РФ от 13.08.2004 N 1074 "Вопросы Государственной фельдъегерской службы РФ".
101. Указ Президента РФ от 16.08.2004 N 1082 "Вопросы Министерства обороны РФ".
102. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю".
103. Указ Президента РФ от 06.10.2004 N 1286 "Вопросы Межведомственной комиссии по защите гостайны".
104. Указ Президента РФ от 13.10.2004 N 1313 "Вопросы Министерства юстиции РФ".
105. Указ Президента РФ от 12.05.2008 N 724 "Вопросы системы и структуры федеральных органов исполнительной власти".
106. Указ Президента РФ от 01.11.2008 N 1576 "О Совете при Президенте РФ по развитию информационного общества в РФ" (вместе с "Положением о Совете при Президенте РФ по развитию информационного общества в РФ").
107. Пост. Пр-ва РФ от 07.04.2004 N 177 "Вопросы Федерального архивного агентства".
108. Пост. Пр-ва РФ от 07.04.2004 N 178 "Вопросы Федеральной службы по интеллектуальной собственности, патентам и товарным знакам".
109. Пост. Пр-ва РФ от 16.06.2004 N 299 "Об утв. Положения о Федеральной службе по интеллектуальной собственности, патентам и товарным знакам".
110. Пост. Пр-ва РФ от 17.06.2004 N 290 "О Федеральном архивном агентстве".
111. Пост. Пр-ва РФ от 17.06.2004 N 294 "О Федеральном агентстве по техническому регулированию и метрологии".
112. Пост. Пр-ва РФ от 30.06.2004 N 319 "Об утв. Положения о Федеральном агентстве по информационным технологиям".
113. Пост. Пр-ва РФ от 30.06.2004 N 331 "Об утверждении Положения о Федеральной антимонопольной службе".

114. Пост. Пр-ва РФ от 02.07.2004 N 336 "Об утверждении Положения о Государственной комиссии по радиочастотам".
115. Пост. Пр-ва РФ от 28.03.2008 N 215 "О Правительственной комиссии по федеральной связи и информационным технологиям".
116. Пост. Пр-ва РФ от 29.05.2008 N 406 "О Министерстве культуры РФ".
117. Пост. Пр-ва РФ от 02.06.2008 N 418 "О Министерстве связи и массовых коммуникаций РФ".
118. Пост. Пр-ва РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций").
119. Приказ Минкультуры РФ от 22.09.2009 N 650 "О создании Экспертного совета по авторским и смежным правам" (вместе с "Положением об Экспертном совете по авторским и смежным правам") (Зарег. в Минюсте РФ 25.11.2009 N 15311).

Часть Специальная

Раздел III. Категории информации по режиму ограничения доступа и использования

Глава 6. Общедоступная информация

6.1. Право на информацию

Общедоступная информация определяется в ФЗ РФ «Об информации, информационных технологиях и защите информации» как «общеизвестные сведения и иная информация, доступ к которой не ограничен».

Принципами правового регулирования отношений в сфере информации, информационных технологий и защиты информации являются:

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

Правовое регулирование отношений в сфере оборота общедоступной информации определяется контролем за деятельностью, связанной с обращением информации. Так выделяют общественные отношения в сфере:

1. средств массовой информации и рекламы;
2. информационных ресурсов (архивные, музейные, библиотечные фонды);
3. информационных систем федерального, регионального, муниципального уровня;
4. доступа к информации (обязательной к обнародованию или предоставлению по запросам граждан, компетентных органов);
5. международного обмена информацией.

6.2. Перечень международных правовых актов

120. Соглашение ЮНЕСКО "О содействии распространению в международном плане Наглядно-звуковых материалов образовательного, научного и культурного характера"; Протокол о подписании и документ о передаче на хранение засвидетельствованной копии в соответствии со статьей IV упомянутого Соглашения («Бейрутское соглашение») (10.12.1948).
121. Пересмотренная рекомендация ЮНЕСКО "О международной стандартизации статистики и распространения книг, газет и периодических изданий" (01.11.1958).
122. Конвенция ЮНЕСКО "О международном обмене изданиями" (03.12.1958).
123. "Конвенция об обмене официальными изданиями и правительственными документами между государствами" (Принята в г. Париже 03.12.1958 на 10-ой сессии Генеральной конференции ЮНЕСКО. СССР ратифицировал Конвенцию (Указ Президиума ВС СССР от 11.09.1962 N 461-VI). Конвенция вступила в силу для СССР 08.10.1963).
124. Рекомендация ЮНЕСКО "О международной стандартизации библиотечной статистики" (13.11.1970).
125. Рекомендация N 748 (1975) Парламентской ассамблеи Совета Европы "О роли национального вещания и управлении им" (Вместе с "Проектом минимальных требований к национальному вещанию") (Принята 23.01.1975 на 26-ой сессии Парламентской ассамблеи СЕ).
126. Рекомендация ЮНЕСКО "О международной стандартизации статистики в области радио и телевидения" (22.11.1976).
127. Пересмотренная рекомендация ЮНЕСКО "О международной стандартизации статистики в области образования" (27.11.1978).
128. Рекомендация ЮНЕСКО "Об охране и сохранении движущихся изображений" (27.10.1980).
129. Резолюция N 820 (1984) Парламентской ассамблеи СЕ "Об отношениях парламентов государств со средствами массовой информации" (Принята 07.05.1984 на 36-ой сессии Парламентской ассамблеи СЕ).
130. "Европейская конвенция о трансграничном телевидении" (ETS N 132) (Вместе с "Арбитражем") (Страсбург, 05.05.1989. Россия подписала Конвенцию 04.10.2006 (Распоряжение Пр-ва РФ от 26.07.2006 N 1060-р). Конвенция не вступила в силу для России в настоящее время).
131. "Соглашение об обмене экономической информацией" (Заклучено государствами-участниками СНГ в г. Минске 26.06.1992. Соглашение вступило в силу в день его подписания).

132. "Соглашение о сотрудничестве в области информации" (Заключено государствами-участниками СНГ в г. Бишкеке 09.10.1992. Соглашение вступило в силу в день его подписания).
133. "Соглашение об обмене информацией в области внешнеэкономической деятельности" (Заключено государствами-участниками СНГ в г. Москве 24.09.1993. Соглашение вступило в силу в день его подписания).
134. "Соглашение об обмене правовой информацией" (Вместе с "Тематическим перечнем нормативно-правовых актов, подлежащих межгосударственному обмену") (Заключено государствами-участниками СНГ в г. Москве 21.10.1994. Соглашение вступило в силу в день его подписания).
135. "Соглашение о свободном доступе и порядке обмена открытой научно-технической информацией государств-участников СНГ" (Заключено в г. Москве 11.09.1998. Россия утвердила Соглашение (Пост. Пр-ва РФ от 26.10.1999 N 1196). Соглашение вступило в силу для России 08.11.1999).
136. "Соглашение об информационном сотрудничестве в области экологии и охраны окружающей природной среды" (Заключено в г. Москве 11.09.1998. Россия утвердила Соглашение (Пост. Пр-ва РФ от 07.12.1998 N 1445). Соглашение вступило в силу для России 17.03.2003).
137. Рекомендация ЮНЕСКО "О развитии и использовании многоязычия и всеобщем доступе к киберпространству" (2003).
138. "Соглашение о принципах и формах взаимодействия государств-участников СНГ в области использования архивной информации" (Минск, 04.06.1999. Соглашение вступило в силу для России 23.02.2000).
139. "Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств-участников СНГ в сфере информатизации" (Вместе с "Базовым перечнем приоритетных направлений...", "Порядком формирования и реализации межгосударственных программ...") (Москва, 24.12.1999. Россия утв. Соглашение (Пост. Пр-ва РФ от 28.05.2002 N 356). Соглашение вступило в силу для России 10.06.2002)
140. Директива N 2000/31/ЕС Европейского парламента и Совета Европейского Союза «О некоторых правовых аспектах услуг информационного общества» (Принята Европейским союзом 08.08.2000).
141. "Европейская конвенция о правовой защите услуг, предполагающих ограниченный доступ". ETS N 178. (Страсбург, 24.01.2001. Россия подписала Конвенцию 07.11.2002. Конвенция не вступила в силу для России в настоящее время).
142. "Конвенция об информационном и правовом сотрудничестве, касающемся "Информационных общественных услуг" (ETS N 180) (Заключена в г. Москве 04.10.2001. Россия не участвует).

143. "Соглашение об обмене материалами национальных информационных агентств государств–участников СНГ" (Ялта, 18.09.2003. Соглашение вступило в силу для России 03.03.2006).
144. "Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств-участников СНГ" (Принято в г. Санкт-Петербурге 14.04.2005 Пост. 25-8 на 25-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ).
145. "Конвенция ООН об использовании электронных сообщений в международных договорах" (Принята в г. Нью-Йорке 23.11.2005 Резолюцией 60/21 на 53-ем пленарном заседании 60-ой сессии Генеральной Ассамблеи ООН) (Россия подписала Конвенцию 25.04.2007. Конвенция не вступила в силу для России в настоящее время).
146. "Соглашение об обмене информацией в сфере борьбы с преступностью" (Принято в г. Астана 22.05.2009 на заседании Совета глав правительств СНГ).
147. "Соглашение о сотрудничестве по организации межгосударственного обмена информацией и формированию национальных баз данных авторского права и смежных прав" (Принято в г. Ялта 20.11.2009 на заседании Совета глав правительств СНГ).

6.3. Перечень национальных нормативно-правовых документов

148. Федеральный конституционный закон от 28.06.2004 N 5-ФКЗ "О референдуме РФ".
149. Закон РФ от 27.12.1991 N 2124-1 "О средствах массовой информации".
150. Федеральный закон от 14.06.1994 N 5-ФЗ "О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания".
151. Федеральный закон от 29.12.1994 N 77-ФЗ "Об обязательном экземпляре документов".
152. Федеральный закон от 29.12.1994 N 78-ФЗ "О библиотечном деле".
153. Федеральный закон от 13.01.1995 N 7-ФЗ "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации".
154. Федеральный закон от 15.07.1995 N 101-ФЗ "О международных договорах РФ".
155. Федеральный закон от 26.05.1996 N 54-ФЗ "О Музейном фонде РФ и музеях в РФ".
156. Федеральный закон от 12.06.2002 N 67-ФЗ "Об основных гарантиях избирательных прав и права на участие в референдуме граждан РФ".

157. Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в РФ".
158. Федеральный закон от 21.07.2005 N 94-ФЗ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".
159. Федеральный закон от 13.03.2006 N 38-ФЗ "О рекламе".
160. Федеральный закон от 02.05.2006 N 59-ФЗ "О порядке рассмотрения обращений граждан РФ".
161. Федеральный закон от 29.11.2007 N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в РФ".
162. Федеральный закон от 22.12.2008 N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в РФ".
163. Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления".
164. Указ Президента РФ от 20.03.1993 N 377 "О гарантиях информационной стабильности и требованиях к телерадиовещанию" (Вместе с «Минимальным стандартом требований к телерадиовещанию»).
165. Указ Президента РФ от 05.12.1993 N 2093 "О мерах по защите свободы массовой информации в РФ".
166. Указ Президента РФ от 31.12.1993 N 2334 "О дополнительных гарантиях прав граждан на информацию".
167. Указ Президента РФ от 20.01.1994 N 170 "Об основах государственной политики в сфере информатизации".
168. Указ Президента РФ от 17.02.1995 N 161 "О гарантиях права граждан на охрану здоровья при распространении рекламы".
169. Указ Президента РФ от 24.11.1995 N 1178 "О мерах по обеспечению открытости и общедоступности нормативных актов".
170. Указ Президента РФ от 23.05.1996 N 763 "О порядке опубликования и вступления в силу актов Президента РФ, Пр-ва РФ и нормативных правовых актов федеральных органов исполнительной власти".
171. Указ Президента РФ от 10.08.2000 N 1486 "О дополнительных мерах по обеспечению единства правового пространства РФ".
172. Указ Президента РФ от 11.03.2003 N 308 "О мерах по совершенствованию государственного управления в области безопасности РФ".
173. Пост. Пр-ва РФ от 11.12.1994 N 1370 "Об утв. Положения о Российском государственном историческом архиве".
174. Пост. Пр-ва РФ от 11.12.1994 N 1371 "Об утв. Положения о Российском государственном архиве древних актов".

175. Пост. Пр-ва РФ от 03.05.1995 N 448 "О мерах по совершенствованию взаимодействия Правительства РФ со средствами массовой информации".
176. Пост. Пр-ва РФ от 12.01.1996 N 11 "Об улучшении информационного обеспечения населения РФ".
177. Пост. Пр-ва РФ от 24.03.1997 N 334 "О Порядке сбора и обмена в РФ информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера".
178. Пост. Пр-ва РФ от 27.07.1998 N 844 "О формировании единого производственно-технологического комплекса государственных электронных средств массовой информации" (вместе с "Уставом федерального государственного унитарного предприятия "Всероссийская государственная телевизионная и радиовещательная компания").
179. Пост. Пр-ва РФ от 11.01.2000 N 26 "О федеральной системе каталогизации продукции для федеральных государственных нужд".
180. Пост. Пр-ва РФ от 29.11.2000 N 904 "Об утв. Положения о порядке ведения федерального регистра нормативных правовых актов субъектов РФ".
181. Пост. Пр-ва РФ от 28.01.2002 N 65 "О федеральной целевой программе "Электронная Россия (2002-2010 годы)".
182. Пост. Пр-ва РФ от 03.12.2002 N 859 "Об обязательном экземпляре изданий" (вместе с "Правилами доставки обязательного платного экземпляра изданий в Центральный коллектор научных библиотек", "Перечнем изданий, обязательный платный экземпляр которых доставляется в Центральный коллектор научных библиотек для распределения между библиотечно-информационными организациями").
183. Пост. Пр-ва РФ от 03.12.2002 N 860 "Об утв. Правил распределения обязательного бесплатного экземпляра, состоящего из комбинированных документов, а также обязательного экземпляра, содержащего аналогичную, зафиксированную на различных носителях информацию".
184. Пост. Пр-ва РФ от 15.08.2003 N 500 "О федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию".
185. Распоряжение Пр-ва РФ от 20.02.2006 N 229-р "Об официальном сайте РФ для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для федеральных государственных нужд".
186. Пост. Пр-ва РФ от 18.05.2006 N 298 "О создании системы мониторинга использования информационных технологий в деятельности федеральных органов государственной власти".
187. Пост. Пр-ва РФ от 27.12.2006 N 807 "Об утв. Положения о ведении реестров государственных или муниципальных контрактов, заключенных по

итогах размещения заказов, и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования официальным сайтом в сети Интернет, на котором размещаются указанные реестры".

188. Пост. Пр-ва РФ от 10.03.2007 N 147 "Об утв. Положения о пользовании официальными сайтами в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами".
189. Пост. Пр-ва РФ от 25.12.2007 N 931 "О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям"
190. Распоряжение Пр-ва РФ от 27.02.2008 N 236-р "О перечне товаров (работ, услуг), размещение заказов на поставки (выполнение, оказание) которых осуществляется путем проведения аукциона".
191. Пост. Пр-ва РФ от 18.08.2008 N 620 "Об условиях предоставления в обязательном порядке первичных статистических данных и административных данных субъектам официального статистического учета".
192. Пост. Пр-ва РФ от 15.06.2009 N 478 "О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет" (вместе с "Концепцией единой системы информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет", "Правилами размещения в федеральных государственных информационных системах "Сводный реестр государственных и муниципальных услуг (функций)" и "Единый портал государственных и муниципальных услуг (функций)" сведений о государственных и муниципальных услугах (функциях)").
193. Пост. Пр-ва РФ от 24.11.2009 N 953 "Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти" (вместе с "Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства РФ в сети Интернет").

6.4. Перечень нормативно-методических документов

194. "Положение по созданию и сопровождению официальных Интернет-сайтов судов общей юрисдикции РФ" (утв. Пост. Президиума Верховного Суда РФ от 24.11.2004).
195. Приказ Мининформсвязи РФ от 19.03.2007 N 36 "Об утв. перечня представляемых сведений об использовании информационных технологий в деятельности федеральных органов государственной власти и Порядка представления их в электронном виде" (Зарег. в Минюсте РФ 18.04.2007 N 9298).
196. Приказ Мининформсвязи РФ от 11.03.2008 N 32 "Об утв. Положения об общероссийском государственном информационном центре" (Зарег. в Минюсте РФ 21.03.2008 N 11394).

Глава 7. Информация, относимая к коммерческой тайне, служебной тайне

7.1. Общие положения

В соответствии с указом Президента РФ "Об утверждении Перечня сведений конфиденциального характера", к сведениям конфиденциального характера относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные).
2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью (профессиональная тайна).
5. Сведения, связанные с коммерческой деятельностью (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них (ноу-хау).

Существуют следующие признаки отнесения сведений к служебной тайне:

- 1) сведения, содержащие служебную информацию о деятельности государственных органов или подведомственных им предприятий, организаций, запрет на распространение которых установлен законом или диктуется служебной необходимостью;
- 2) сведения, являющиеся конфиденциальной информацией для других лиц, но ставшие известными представителям государственных органов в силу исполнения ими служебных обязанностей.

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

Критерии охраноспособности информации, составляющей служебную тайну:

- 1) информация, составляющая собственную служебную информацию о деятельности самого органа власти;
- 2) охраноспособная конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну, тайну частной жизни – "чужая тайна";
- 3) сведения, не являющиеся гостайной и не подпадающие под перечень сведений, доступ к которым не может быть ограничен;
- 4) получена информация в силу исполнения служебных обязанностей.

Объекты служебной тайны:

1. Военная тайна.
2. Тайна следствия.
3. Судебная тайна (тайна совещания судей и присяжных).
4. Налоговая тайна.
5. Таможенная тайна.

Обычно на документы, относящиеся к служебной тайне, наносится гриф «Для служебного пользования».

ФЗ РФ "О коммерческой тайне" выделяет следующие признаки относимости информации к коммерческой тайне:

- информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- отсутствует свободный доступ к информации;
- обладатель информации принимает меры к охране ее конфиденциальности.

Коммерческая тайна (ФЗ РФ от 29.07.2004 N 98-ФЗ) – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

К коммерческой тайне не могут быть отнесены следующие сведения:

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

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

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

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

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

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

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

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

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

Для введения в режима коммерческой тайны в организации в обязательном порядке должно быть выполнено:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации.

При этом гриф коммерческой тайны должен содержать следующие сведения:

- для юридических лиц – полное наименование и место нахождения;
- для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.

Информация, относимая к коммерческой тайне, может категоризироваться локальными нормативными актами организации (по аналогии со степенями секретности). Соответственно могут использоваться несколько грифов, например: «Конфиденциально», «Строго конфиденциально».

7.2. Перечень нормативно-правовых документов, регламентирующих обработку и защиту информации, относимой к коммерческой тайне

197. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне".

198. Указ Президента РФ от 06.03.1997 N 188 "Об утв. Перечня сведений конфиденциального характера".

199. Пост. Пр-ва РСФСР от 05.12.1991 N 35 "О перечне сведений, которые не могут составлять коммерческую тайну".

7.3. Перечень нормативно-правовых документов, регламентирующих обработку и защиту служебной информации ограниченного распространения

200. "Соглашение об информационном обеспечении системы управления и защите секретов Объединенных Вооруженных Сил СНГ и Вооруженных сил государств-участников Соглашения" (Заключено в г. Ташкенте 15.05.1992. Соглашение вступило в силу в день его подписания).

201. "Соглашение об организации информационного взаимодействия в Объединенных Вооруженных Силах СНГ и Вооруженных Силах государств-участников Соглашения" (Москва, 13.11.1992).

202. "Соглашение между Пр-вом РФ и Пр-вом Украины о сотрудничестве в области технической защиты информации" (Киев, 14.06.1996).

203. "Соглашение между Пр-вом РФ и Пр-вом Республики Белоруссия о сотрудничестве в области защиты информации" (Москва, 09.071997).
204. "Уголовно-процессуальный кодекс РФ" от 18.12.2001 N 174-ФЗ.
205. "Арбитражный процессуальный кодекс РФ" от 24.07.2002 N 95-ФЗ.
206. "Гражданский процессуальный кодекс РФ" от 14.11.2002 N 138-ФЗ.
207. "Таможенный кодекс РФ" от 28.05.2003 N 61-ФЗ.
208. Федеральный закон от 17.12.1994 N 67-ФЗ "О федеральной фельдъегерской связи".
209. Федеральный закон от 27.05.1996 N 57-ФЗ "О государственной охране".
210. Федеральный закон от 21.07.1997 N 114-ФЗ "О службе в таможенных органах РФ".
211. Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе РФ".
212. Пост. Пр-ва РФ от 03.11.1994 N 1233 "Об утв. Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти".
213. Пост. Пр-ва РФ от 22.09.2009 N 754 "Об утверждении Положения о системе межведомственного электронного документооборота".
214. Распоряжение Пр-ва РФ от 02.10.2009 N 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти».
215. Приказ МНС РФ от 03.03.2003 N БГ-3-28/96 "Об утв. Порядка доступа к конфиденциальной информации налоговых органов" (Зарег. в Минюсте РФ 26.03.2003 N 4335).

7.4. Перечень нормативно-методических документов

216. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». (Гостехкомиссия России, 1992).
217. РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». (Гостехкомиссия России, 1992).
218. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». (Гостехкомиссия России, 1992).

219. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». (Гостехкомиссия России, 1992).
220. РД «Защита от несанкционированного доступа к информации. Термины и определения». (Гостехкомиссия России, 1992).
221. РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». (Гостехкомиссия России, 1997).
222. РД «Защита информации. Специальные защитные знаки. Классификация и общие требования». (Гостехкомиссия России, 1997).
223. РД «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей». (утв. приказом Гостехкомиссии России от 04.06.1999 N 114).
224. РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». (утв. приказом Гостехкомиссии России от 19.06.2002 N 187) (часть 1, 2, 3).
225. РД «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности». (Гостехкомиссия России, 2003).
226. РД «Безопасность информационных технологий. Руководство по регистрации профилей защиты». (Гостехкомиссия России, 2003).
227. РД «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты». (Гостехкомиссия России, 2003).
228. РД «Руководство по разработке профилей защиты и заданий по безопасности». (Гостехкомиссия России, 2003).
229. РД «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», (Гостехкомиссия России, 2002).
230. РД «Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации». (Гостехкомиссия России, 2002).
231. РД «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам». (Гостехкомиссия России, 2002).

232. РД «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах». (Гостехкомиссия России, 2002).
233. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (Для служебного пользования) (утв. приказом Гостехкомиссии России от 30.08.2002 N 282).
234. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну» (утв. Зам. директора ФСТЭК России 25.12.2006).
235. «Базовая модель угроз безопасности информации в ключевых системах информационной структуры» (Для служебного пользования) (утв. зам. директора ФСТЭК России 18.05.2007).
236. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (Для служебного пользования) (утв. Зам. директора ФСТЭК России 18.05.2007).
237. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (Для служебного пользования) (утв. Зам. директора ФСТЭК России 18.05.2007).
238. «Положение о Реестре ключевых систем информационной инфраструктуры» (Для служебного пользования) (утв. приказом ФСТЭК России №74 от 04.03.2009. Зарег. в Минюсте России 07.04.2009).

Глава 8. Информация, относимая к профессиональной тайне

8.1. Общие положения

Профессиональная тайна определяется тремя признаками.

- 1) Профессиональная принадлежность.
- 2) Конфиденциальная информация добровольно доверяется лицу, исполняющему соответствующие профессиональные обязанности, по выбору владельца этой информации.
- 3) У лица, к которому поступает такая информация, возникает обязанность обеспечить ее сохранность.

Профессиональная тайна (ФЗ РФ от 26.01.1996 N 14-ФЗ) – защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой. Распространение этой информации может нанести ущерб доверителю, но при этом информация не является государственной или коммерческой тайной.

Критерии охраноспособности:

- 1) Информация стала известной в силу профессиональных обязанностей.
- 2) Держатель не состоит на государственной, муниципальной службе.
- 3) Запрет на распространение установлен законом.
- 4) Не относится к государственной, коммерческой тайне.

Объекты информации, составляющей профессиональную тайну:

1. Врачебная тайна.
2. Тайна связи.
3. Нотариальная тайна.
4. Адвокатская тайна.
5. Тайна страхования.
6. Тайна исповеди.
7. Аудиторская тайна
8. Журналистская тайна.
9. Тайна усыновления.
10. Банковская тайна.

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

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

8.2. Перечень нормативно-правовых, нормативно-методических документов

239. "Семейный кодекс РФ" от 29.12.1995 N 223-ФЗ.
240. "Гражданский кодекс РФ (часть вторая)" от 26.01.1996 N 14-ФЗ.
241. Федеральный закон от 02.12.1990 N 395-1 "О банках и банковской деятельности".
242. "Основы законодательства РФ о нотариате" (утв. ВС РФ 11.02.1993 N 4462-1).
243. "Основы Законодательства РФ об охране здоровья граждан" (утв. ВС РФ 22.07.1993 N 5487-1).
244. Федеральный закон от 11.01.1995 N 4-ФЗ "О Счетной палате Российской Федерации".
245. Федеральный закон от 02.08.1995 N 122-ФЗ "О социальном обслуживании граждан пожилого возраста и инвалидов".
246. Федеральный закон от 26.09.1997 N 125-ФЗ "О свободе совести и о религиозных объединениях".
247. Федеральный закон от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в РФ".
248. Федеральный закон от 10.07.2002 N 86-ФЗ "О Центральном банке РФ (Банке России)".
249. Федеральный закон от 24.04.2008 N 48-ФЗ "Об опеке и попечительстве".
250. Федеральный закон от 30.12.2008 N 307-ФЗ "Об аудиторской деятельности".
251. Письмо ЦБ РФ от 30.06.2003 N 99-Т "О предоставлении сведений, составляющих банковскую тайну".

Глава 9. Персональные данные

9.1. Общие положения

Базовым национальным нормативным актом, регламентирующим отношения в сфере хранения и обработки персональных данных является ФЗ РФ «О персональных данных». В нем даются основные определения:

персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

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

В Законе определяются принципы обработки персональных данных:

- 1) законности целей и способов обработки персональных данных и добросовестности;
- 2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- 3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Также в Законе оператор персональных данных обязывается зарегистрировать созданные им информационные системы персональных данных и выполнять требования на защиту персональных данных:

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

Правительство РФ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных

данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

В законе указывается требование об обязательном уведомлении оператором уполномоченного органа до начала обработки персональных данных. Этим органом является Роскомнадзор, который ведет единый государственный реестр РФ информационных систем персональных данных.

Регуляторами в сфере защиты персональных данных являются следующие государственные органы:

- Роскомнадзор (является основным проверяющим органом);
- ФСТЭК России (привлекается к проверке систем защиты ПДн);
- ФСБ России, 8-й Центр (привлекается к проверке в случае наличия в системе криптографических средств защиты информации и систем обнаружения атак).

9.2. Перечень нормативно-правовых документов

252. "Конвенция о защите физических лиц при автоматизированной обработке персональных данных". ETS N 108 (Страсбург 28.01.1981. Россия подписала Конвенцию 07.11.2001. Конвенция не вступила в силу для России к настоящему времени).
253. Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза "О защите личности в отношении обработки персональных данных и свободном обращении этих данных" (Принята ЕС 24.10.1995).
254. Директива N 2002/58/ЕС Европейского парламента и Совета Европейского Союза "Относительно обработки личных данных и защите личной тайны в сфере электронных коммуникаций" (Директива о тайне и электронных коммуникациях) (Принята ЕС 12.07.2002).
255. Федеральный закон от 15.11.1997 N 143-ФЗ "Об актах гражданского состояния".
256. Федеральный закон от 25.07.1998 N 128-ФЗ "О государственной дактилоскопической регистрации в РФ".
257. Федеральный закон от 08.08.2001 N 129-ФЗ "О государственной регистрации юридических лиц и индивидуальных предпринимателей".
258. Федеральный закон от 10.01.2003 N 20-ФЗ "О Государственной автоматизированной системе РФ "Выборы".
259. Федеральный закон от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных".
260. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

261. Указ Президента РФ от 30.05.2005 N 609 "Об утв. Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела".
262. Пост. Пр-ва РФ от 25.12.1998 N 1543 "Об утверждении Положения о направлении материальных носителей, содержащих дактилоскопическую информацию, в органы внутренних дел".
263. Пост. Пр-ва РФ от 06.04.1999 N 386 "Об утверждении перечня должностей, на которых проходят службу граждане РФ, подлежащие обязательной государственной дактилоскопической регистрации".
264. Пост. Пр-ва РФ от 17.11.2007 N 781 "Об утв. Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".
265. Пост. Пр-ва РФ от 06.07.2008 N 512 «Об утв. требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
266. Пост. Пр-ва РФ от 15.09.2008 N 687 "Об утв. Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

9.3. Перечень нормативно-методических документов

267. Пост. Центризбиркома РФ от 23.07.2003 N 19/137-4 "О Положении об обеспечении безопасности информации в Государственной автоматизированной системе РФ "Выборы".
268. Пост. Центризбиркома РФ от 28.02.2007 N 200/1255-4 "Об Инструкции по размещению данных Государственной автоматизированной системы РФ "Выборы" в сети Интернет".
269. Приказ ФСТЭК РФ N 55, ФСБ РФ N 86, Мининформсвязи РФ N 20 от 13.02.2008 "Об утв. Порядка проведения классификации информационных систем персональных данных" (Зарег. в Минюсте РФ 03.04.2008 N 11462).
270. "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. зам. директора ФСТЭК России 14.02.2008).
271. "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. зам. директора ФСТЭК России 15.02.2008).
272. "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. зам. директора ФСТЭК России 15.02.2008).
273. "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных

системах персональных данных" (утв. зам. директора ФСТЭК России 15.02.2008).

274. "Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации" (утв. руководством 8 Центра ФСБ России 21.02.2008 N 149/54-144).
275. "Типовые требования по организации и обеспечению функционирования шифровальных, предназначенных для обеспечения безопасности персональных данных" (утв. руководством 8 Центра ФСБ России 21.02.2008 N 149/6/6-622).
276. Приказ Россвязькомнадзора от 17.07.2008 N 08 "Об утв. образца формы уведомления об обработке персональных данных".
277. Пост. Центризбиркома РФ от 19.11.2008 N 138/1019-5 "О Порядке использования Государственной автоматизированной системы РФ "Выборы" при подготовке и проведении выборов в органы местного самоуправления поселений и внесении изменений в Инструкцию по размещению данных Государственной автоматизированной системы РФ "Выборы" в сети Интернет".
278. Приказ Роскомнадзора от 01.12.2009 N 630 "Об утверждении Административного регламента проведения проверок Роскомнадзором при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных" (Зарег. в Минюсте РФ 28.01.2010 N 16095).
279. Пост. Центризбиркома РФ от 29.12.2009 N 187/1312-5 "О Положении об организации единого порядка использования, эксплуатации и развития Государственной автоматизированной системы РФ "Выборы" в избирательных комиссиях и комиссиях референдума".
280. Приказ ФСТЭК РФ от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных" (Зарег. в Минюсте РФ 19.02.2010 N 16456).

Глава 10. Информация, относимая к государственной тайне в РФ

10.1. Общие положения

Общественные отношения, связанные с отнесением информации к гостайне, а также с операциями по доступу, обработке и рассекречиванию подобной информации, регламентируются ФЗ РФ «О государственной тайне». В нем даются базовые определения:

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

система защиты государственной тайны – совокупность органов защиты гостайны, используемых ими средств и методов защиты сведений, составляющих гостайну, и их носителей, а также мероприятий, проводимых в этих целях;

средства защиты информации (относимой к гостайне) – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих гостайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации»;

а также классифицируется информация по отнесению ее к сведениям гостайны.

Перечень сведений, относимых к гостайне, утверждается Указом Президента РФ. В Законе определяется, что не подлежат засекречиванию следующие сведения:

1. Сведения о чрезвычайных происшествиях, катастрофах, угрожающих безопасности и здоровью граждан.
2. Сведения о состоянии экологии, здравоохранения, демографии, образования, культуры, сельского хозяйства и преступности.
3. Сведения о привилегиях, компенсациях, льготах, предоставляемых всем субъектам.
4. Сведения о фактах нарушения прав и свобод человека и гражданина.
5. Сведения о ресурсах золотого запаса и государственных валютных резервов.
6. Сведения о состоянии здоровья высших должностных лиц.
7. Сведения о фактах нарушения здравоохранения органами государственной власти и должностными лицами.

Определены **Степени секретности** засекречиваемой информации:

1. Особая важность – сведения, разглашение которых может нанести ущерб интересам РФ.
2. Совершенно секретно – сведения, разглашение которых может нанести ущерб министерствам и ведомствам.
3. Секретно – сведения, разглашение которых может нанести ущерб предприятиям, учреждениям, организациям. Следует отметить, что до 1991 г. такого рода сведения относились к служебной тайне.

Необходимо отметить, что многие документы, регламентирующие защиту информации, относимой к гостайне, сами имеют грифы секретности.

Регуляторами в сфере контроля защиты гостайны являются следующие государственные органы: ФСБ, ФСТЭК, СВР, межведомственная комиссия по защите гостайны.

10.2. Перечень нормативно-правовых документов

281. "Соглашение между РФ и Республикой Беларусь о взаимном обеспечении защиты гостайны РФ и государственных секретов Республики Беларусь" (Заключено в г. Минске 20.01.2003. Соглашение вступило в силу 25.01.2004).
282. Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне".
283. Указ Президента РФ от 30.11.1995 N 1203 "Об утв. Перечня сведений, отнесенных к гостайне".
284. Указ Президента РФ от 6 октября 2004 г. N 1286 "Вопросы межведомственной комиссии по защите гостайны".
285. Распоряжение Президента РФ от 16.04.2005 N 151-рп "О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к гостайне".
286. Пост. Пр-ва РФ от 20.02.1995 N 170 "Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР".
287. Пост. Пр-ва РФ от 15.04.1995 N 333 ("О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих гостайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите гостайны").
288. Пост. Пр-ва РФ от 04.09.1995 N 870 "Об утв. Правил отнесения сведений, составляющих гостайну, к различным степеням секретности".
289. Пост. Пр-ва РФ от 02.08.1997 N 973 "Об утв. Положения о подготовке к передаче сведений, составляющих гостайну, другим государствам или Международным организациям".
290. Пост. Пр-ва РФ от 22.08.1998 N 1003 "Об утв. Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к гостайне".
291. Пост. Пр-ва РФ от 02.04.2002 N 210 "Об утв. списка стратегических видов полезных ископаемых, сведения о которых составляют гостайну".
292. Пост. Пр-ва РФ от 23.07.2005 N 443 "Об утв. Правил разработки перечня сведений, отнесенных к гостайне".

293. Пост. Пр-ва РФ от 31.07.2007 N 491 "Об утв. Положения о ведении реестра государственных или муниципальных контрактов, в которые включаются сведения, касающиеся размещения заказов и составляющие гостайну".
294. Пост. Пр-ва РФ от 24.12.2007 N 928 "О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в РФ, сведений, составляющих гостайну".
295. Пост. Пр-ва РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к гостайне".

Раздел IV. Институты права собственности и исключительных прав

Глава 11. Защита результатов интеллектуальной деятельности и средств индивидуализации

11.1. Общие положения

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

В последнем говорится (п. 1 Ст. 1225): «**Результатами интеллектуальной деятельности** и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

- 1) произведения науки, литературы и искусства;
- 2) программы для электронных вычислительных машин (программы для ЭВМ);
- 3) базы данных;
- 4) исполнения;
- 5) фонограммы;
- 6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- 7) изобретения;
- 8) полезные модели;
- 9) промышленные образцы;
- 10) селекционные достижения;
- 11) топологии интегральных микросхем;
- 12) секреты производства (ноу-хау);
- 13) фирменные наименования;
- 14) товарные знаки и знаки обслуживания;
- 15) наименования мест происхождения товаров;
- 16) коммерческие обозначения».

При защите интеллектуальных прав выделяют следующие институты гражданского права:

1. Авторское право;
2. Права, смежные с авторским;
3. Патентное право;
4. Право на селекционное достижение;
5. Право на топологии интегральных микросхем;
6. Право на секрет производства (ноу-хау);
7. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий;

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

В каждом из перечисленных выше правовых институтов определяются собственные объекты защиты прав. Приведем их на примере авторского права (Ст. 1259 Гражданского кодекса РФ):

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

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

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

2. К объектам авторских прав относятся:

1) производные произведения, то есть произведения, представляющие собой переработку другого произведения;

2) составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

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

4. Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 настоящего Кодекса.

5. Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования.

6. Не являются объектами авторских прав:

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

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

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

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

7. Авторские права распространяются на часть произведения, на его название, на персонаж произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора и отвечают требованиям, установленным пунктом 3 настоящей статьи».

С целью учета объектов, относимых к интеллектуальной собственности, в качестве меры государственного контроля предусмотрено ведение единых государственных реестров таких объектов. Подобные реестры отдельно ведутся для изобретений РФ, полезных моделей РФ, промышленных образцов РФ, охраняемых селекционных достижений, товарных знаков и знаков обслуживания РФ, наименование (места происхождения товара) и т.д.

Регуляторами по защите авторских, патентных и иных смежных с ними прав в РФ являются Роспатент, Экспертный совет по авторским и смежным правам, ФАС России.

11.2. Перечень нормативно-правовых документов

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

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

298. "Всемирная конвенция об авторском праве" (Женева, 06.09.1952. Пересмотрена в Париже 24.07.1971. Вступила в силу для СССР 27.05.1973).

299. "Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций" (Рим, 26.10.1961. Вступила в силу для РФ 26.05.2003).

300. "Конвенция, учреждающая Всемирную организацию интеллектуальной собственности" (Стокгольм, 14.07.1967. Вступила в силу для СССР 26.04.1070).
301. "Договор о патентной кооперации" (Подписан в г. Вашингтоне 19.06.1970. Договор подписан СССР 23.12.1970 с оговоркой и заявлением, ратифицирован (Указ Президиума ВС СССР от 23.12.1977 N 6758-IX). Ратификационная грамота СССР была сдана на хранение Генеральному директору ВОИС 29.12.1977. Договор вступил в силу для СССР 29.03.1978).
302. "Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм" (Женева, 29.10.1971. Вступила в силу для РФ 13.03.1995).
303. "Найробский договор об охране олимпийского символа" (Подписан в г. Найроби 26.09.1981. Договор вступил в силу для России 17.04.1986).
304. Директива N 87/54/ЕС Европейского парламента и Совета Европейского Союза "О правовой охране топографий полупроводниковых продуктов" (Принята ЕС 16.12.1986).
305. Директива N 91/10/ЕС Европейского парламента и Совета Европейского Союза "О правах на аренду, заем и другие смежные права, авторские права в области интеллектуальной собственности".
306. Директива N 91/83/ЕС Европейского парламента и Совета Европейского Союза "О координации определенных постановлений в отношении авторских и смежных прав при передаче через спутники и по кабельным сетям".
307. Директива N 91/250/ЕС Европейского парламента и Совета Европейского Союза "О правовой охране компьютерных программ" (Брюссель, 14.05.1991).
308. Директива N 92/100/ЕС Европейского парламента и Совета Европейского Союза "По вопросам охраны прав проката и использования, а также ряда иных прав, смежных с авторским правом, в сфере интеллектуальной собственности" (Принята ЕС 19.11.1992).
309. Директива N 93/83/ЕС Европейского парламента и Совета Европейского Союза "О согласовании ряда правил, касающихся охраны авторского права и смежных прав в сфере спутникового вещания и кабельной ретрансляции" (Принята ЕС 27.09.1993).
310. Соглашение стран СНГ от 24.09.1993 "О сотрудничестве в области охраны авторского права и смежных прав" (Вступило в силу для России с 06.05.1995).
311. "Договор о законах по товарным знакам" (Вместе с "Инструкцией к Договору...", <Типовыми международными бланками>) (Подписан в г. Женеве 27.10.1994. Россия приняла решение принять Договор (Постановление

Пр-ва РФ от 01.12.1997 N 1503). Договор вступил в силу для России 11.05.1998).

312. Директива N 93/98/ЕС Европейского парламента и Совета Европейского Союза "О согласовании сроков защиты авторских и смежных прав" (Принята ЕС 29.10.1993).
313. Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) (ВТО, Уругвайский раунд многосторонних торговых переговоров, 15.04.1994. Соглашение имеет обязательную силу для всех членов ВТО. РФ членом ВТО не является).
314. "Евразийская патентная конвенция" (Заключена в г. Москве 09.09.1994. Россия ратифицировала конвенцию – ФЗ от 01.06.1995 N 85-ФЗ. Конвенция вступила в силу для России 27.09.1995).
315. Директива N 96/9/ЕС Европейского парламента и Совета Европейского Союза "О правовой охране баз данных" (Принята ЕС 11.03.1996).
316. "Договор ВОИС по авторскому праву" (Вместе с "Согласованными заявлениями в отношении Договора ВОИС по авторскому праву") (Принят 20.12.1996 Дипломатической конференцией. Россия приняла решение о присоединении к Договору (Распоряжение Пр-ва РФ от 21.07.2008 N 1052-р). Договор вступил в силу для России 05.02.2009).
317. "Договор ВОИС по исполнениям и фонограммам" (Вместе с "Согласованными заявлениями в отношении Договора...") (Принят 20.12.1996 Дипломатической конференцией. Россия приняла решение о присоединении к Договору с оговоркой и заявлением (Распоряжение Пр-ва РФ от 14.07.2008 N 998-р). Договор не вступил в силу для России в настоящее время).
318. "Соглашение между Российским агентством по патентам и товарным знакам и Международным бюро ВОИС о выполнении Российским агентством по патентам и товарным знакам функций Международного поискового органа и Органа международной предварительной экспертизы в соответствии с Договором о патентной кооперации" (Вместе с "Языками", "Объектами, не исключаемыми из поиска или экспертизы", "Пошлинами и тарифами", "Языками переписки") (Женева, 01.10.1997. Соглашение вступило в силу 01.01.1998).
319. "Соглашение о мерах по предупреждению и пресечению использования ложных товарных знаков и географических указаний" (Минск, 04.06.1999. Россия утвердила Соглашение (Пост. Пр-ва РФ от 15.10.2001 N 726). Соглашение вступило в силу для России 05.11.2001).
320. "Договор о патентном праве" (PLT) (Вместе с "Инструкцией к Договору о патентном праве", "Согласованными заявлениями дипломатической конференции...") (Принят в г. Женеве 01.06.2000 на Дипломатической конференции по принятию Договора о патентном праве. Россия приняла реше-

ние о присоединении к Договору с оговоркой (Распоряжение Пр-ва РФ от 09.02.2009 N 137-р). Договор не вступил в силу для России).

321. "Европейская конвенция о защите культурного наследия в форме аудиовидео произведений" (ETS N 183) (Заключена в г. Страсбурге 08.11.2001. Россия не участвует).
322. "Соглашение между Правительством РФ и Европейским сообществом о сотрудничестве в области науки и технологий" (Вместе с "Отличительными чертами плана по распоряжению технологиями", "Принципами распределения прав на интеллектуальную собственность") (Брюссель, 16.11.2000. Соглашение вступило в силу 10.05.2001 и действовало до 31.12.2002. Действие Соглашения продлено на основании статьи 1 Соглашения от 06.11.2003).
323. "Сингапурский договор о законах по товарным знакам" (Принят в г. Сингапуре 27.03.2006 на Дипломатической конференции по принятию Пересмотренного договора о законах по товарным знакам. Россия подписала Договор 26.03.2007 (Распоряжение Правительства РФ от 24.03.2007 N 352-р), ратифицировала (Федеральный закон от 23.05.2009 N 98-ФЗ). Договор вступил в силу для России 18.12.2009).
324. Директива N 2008/95/ЕС Европейского парламента и Совета Европейского Союза "О сближении законодательств государств-членов в отношении товарных знаков и знаков обслуживания" (Вместе с "Таблицей соответствия") (Страсбург, 22.10.2008).
325. "Гражданский Кодекс РФ (часть четвертая)" от 18.12.2006 N 230-ФЗ.
326. "Основы законодательства Российской Федерации о культуре" (утв. ВС РФ 09.10.1992 N 3612-1).
327. Федеральный закон от 26.07.2006 N 135-ФЗ "О защите конкуренции".
328. Федеральный закон от 30.12.2008 N 316-ФЗ "О патентных поверенных".
329. Указ Президента РФ от 07.10.1993 N 1607 "О государственной политике в области охраны авторского права и смежных прав".
330. Указ Президента РФ от 05.12.1998 N 1471 "О мерах по реализации прав авторов произведений, исполнителей и производителей фонограмм на вознаграждение за воспроизведение в личных целях аудиовизуального произведения или звукозаписи произведения".
331. Пост. Пр-ва РФ от 17.05.1996 N 614 "О ставках вознаграждения исполнителям за некоторые виды использования исполнения (постановки)".
332. Пост. Пр-ва РФ от 02.09.1999 N 982 "Об использовании результатов научно-технической деятельности".

333. Пост. Пр-ва РФ от 07.05.2006 N 276 "Об упорядочении функций федеральных органов исполнительной власти в области авторского права и смежных прав".
334. Пост. Пр-ва РФ от 29.12.2007 N 992 "Об утв. Положения о государственной аккредитации организаций, осуществляющих коллективное управление авторскими и смежными правами".
335. Пост. Пр-ва РФ от 22.04.2009 N 342 "О некоторых вопросах регулирования закрепления прав на результаты научно-технической деятельности".

11.3. Перечень нормативно-методических документов

336. Приказ Минобрнауки РФ от 12.12.2007 N 346 "Об утв. Административного регламента исполнения Роспатентом государственной функции по осуществлению ведения реестров зарегистрированных объектов интеллектуальной собственности, публикации сведений о зарегистрированных объектах интеллектуальной собственности, поданных заявках и выданных по ним патентах и свидетельствах, о действии, прекращении действия и возобновлении действия правовой охраны в отношении объектов интеллектуальной собственности, передаче прав на охраняемые объекты, об официальной регистрации объектов интеллектуальной собственности" (Зарег. в Минюсте РФ 30.05.2008 N 11785).
337. Приказ Минобрнауки РФ от 29.10.2008 N 324 "Об утв. Административного регламента исполнения Роспатентом государственной функции по организации приема заявок на государственную регистрацию программы для ЭВМ и заявок на государственную регистрацию базы данных, их рассмотрения и выдачи в установленном порядке свидетельств о государственной регистрации программы для ЭВМ или базы данных" (Зарег. в Минюсте РФ 17.12.2008 N 12893).
338. Приказ Роспатента от 26.02.2009 N 32 "Об утв. Положения об официальных изданиях Роспатента".

Раздел V. Правовое регулирование отношений, связанных с информационными технологиями

Глава 12. Нормативно-правовое обеспечение в сфере связи и коммуникаций

12.1. Общие положения

Причина включения регламентирующих документов в области связи и коммуникаций в данное пособие – тесная связь данных требований с формированием систем защиты информации, обрабатываемой с помощью объектов, сетей и средств связи, в том числе Интернет.

Основными методами контроля со стороны государства за развитием отрасли (связи) является стандартизация и лицензирование деятельности.

Регулирующими органами в сфере связи являются ФСБ РФ, ФСО РФ, ФСТЭК, Роскомнадзор.

В соответствии с ФЗ РФ «О Связи», «деятельность юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи осуществляется только на основании лицензии». Лицензионным органом в области услуг связи является Минкомсвязи РФ.

12.2. Перечень нормативно-правовых документов

339. "Брюссельская конвенция о распространении несущих программы сигналов, передаваемых через спутники" (Заключена в г. Брюсселе 21.05.1974. СССР присоединился к Конвенции (Указ Президиума ВС СССР от 12.08.1988 N 9388-XI). Вступила в силу для СССР 20.01.1989).
340. "Устав Международного союза электросвязи" (Женева, 22.12.1992. Устав вступил в силу для России 01.08.1995 (ФЗ от 30.03.1995 N 37-ФЗ)).
341. "Конвенция Международного союза электросвязи" (Женева, 22.12.1992. Конвенция вступила в силу для России 01.08.1995).
342. Директива N 97/13/ЕС Европейского Парламента и Совета Европейского Союза (лицензии в области связи).
343. Директива N 97/33/ЕС Европейского Парламента и Совета Европейского Союза (взаимодействие через открытые сети).
344. Директива N 2000/31/ЕС Европейского Парламента и Совета Европейского Союза "О некоторых правовых аспектах услуг информационного общества, в том числе электронной коммерции на внутреннем рынке" (Директива об электронной коммерции) (Принята ЕС 8.06.2000).
345. Директива N 2002/58/ЕС Европейского парламента и Совета Европейского Союза "О защите тайны и электронных коммуникациях" (Принята ЕС 12.07.2002).

346. "Соглашение между Правительством РФ и Международным союзом электросвязи об учреждении в РФ Зонального представительства Международного союза электросвязи" (Женева, 15.12.2003. Соглашение временно применялось с даты его подписания. Соглашение вступило в силу 20.02.2006 (ФЗ от 10.01.2006 N 17-ФЗ)).
347. Федеральный закон от 07.07.2003 N 126-ФЗ "О связи".
348. Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена".
349. Пост. Пр-ва РФ от 12.10.2004 N 539 "О порядке регистрации радиоэлектронных средств и высокочастотных устройств".
350. Пост. Пр-ва РФ от 13.07.2004 N 350 "Об утв. Правил распределения и использования ресурсов нумерации единой сети электросвязи РФ".
351. Пост. Пр-ва РФ от 02.03.2005 N 110 "Об утв. Порядка осуществления государственного надзора за деятельностью в области связи".
352. Пост. Пр-ва РФ от 28.03.2005 N 161 "Об утверждении Правил присоединения сетей электросвязи и их взаимодействия".
353. Пост. Пр-ва РФ от 01.04.2005 N 175 "Об утв. Правил осуществления радиоконтроля в РФ".
354. Пост. Пр-ва РФ от 15.04.2005 N 222 "Об утв. Правил оказания услуг телеграфной связи".
355. Пост. Пр-ва РФ от 15.04.2005 N 221 "Об утв. Правил оказания услуг почтовой связи".
356. Пост. Пр-ва РФ от 18.05.2005 N 310 "Об утв. Правил оказания услуг местной, внутризонавой, междугородной и международной телефонной связи".
357. Пост. Пр-ва РФ от 25.05.2005 N 328 "Об утв. Правил оказания услуг подвижной связи".
358. Пост. Пр-ва РФ от 23.01.2006 N 32 "Об утв. Правил оказания услуг связи по передаче данных".
359. Пост. Пр-ва РФ от 22.02.2006 N 103 "Об утв. Правил подготовки и использования ресурсов единой сети электросвязи РФ в целях обеспечения функционирования сетей связи специального назначения".
360. Распоряжение Пр-ва РФ от 19.07.2006 N 1032-р "Об организации подключения к сети Интернет за счет средств федерального бюджета государственных образовательных учреждений субъектов РФ и муниципальных образовательных учреждений, реализующих общеобразовательные про-

граммы начального общего, основного общего и среднего (полного) общего образования".

361. Пост. Пр-ва РФ от 10.09.2007 N 575 "Об утв. Правил оказания телематических услуг связи".
362. Пост. Пр-ва РФ от 27.09.2007 N 612 "Об утв. Правил продажи товаров дистанционным способом".
363. Распоряжение Пр-ва РФ от 18.10.2007 N 1447-р "О приобретении для образовательных учреждений программ, входящих в стандартный (базовый) пакет программного обеспечения и дополнительный пакет специализированного программного обеспечения, а также о внедрении системы исключения доступа к Интернет-ресурсам, несовместимым с задачами образования и воспитания учащихся".
364. Пост. Пр-ва РФ от 18.05.2009 N 424 "Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям".

12.3. Перечень нормативно-методических документов

365. РД "Телематические службы" (утв. Приказом Минкомсвязи РФ N 175 от 23.07.2001).
366. Письмо Министерства образования и науки РФ от 10.11.2006 N АС-1299/03 "О реализации контентной фильтрации доступа образовательных учреждений, подключаемых к сети Интернет в рамках приоритетного национального проекта "Образование".
367. Приказ Мининформсвязи РФ от 02.07.2007 N 73 "Об утв. Правил применения автоматизированных систем расчетов" (Зарег. в Минюсте РФ 13.07.2007 N 9828).
368. Приказ Мининформсвязи РФ от 27.09.2007 N 113 "Об утв. Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования" (Зарег. в Минюсте РФ 22.10.2007 N 10380).
369. Приказ Мининформсвязи РФ от 09.01.2008 N 1 "Об утв. требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации" (Зарег. в Минюсте РФ 23.01.2008 N 10993).
370. Приказ ФСО РФ от 07.08.2009 N 487 "Об утверждении Положения о сегменте информационно-телекоммуникационной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов РФ" (Зарегистрировано в Минюсте РФ 04.09.2009 N 14705).

371. Приказ Минкомсвязи РФ от 25.08.2009 N 104 "Об утв. Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования" (Зарег. в Минюсте РФ 25.09.2009 N 14874).

Глава 13. Государственное регулирование вопросов использования криптографических средств и ЭЦП

13.1. Общие положения

В большинстве развитых стран мира распространение криптографических средств регулируется на уровне государства. В России обязательному федеральному контролю и лицензированию подлежит деятельность, связанная с разработкой, производством, продажей и использованием средств криптографической защиты информации.

В настоящее время на основе несимметричных криптографических алгоритмов строится система электронной цифровой подписи (ЭЦП) и связанный с ней электронный (защищенный) документооборот. ФЗ РФ «Об информации, информационных технологиях и о защите информации» вводит понятие «подписанного электронного документа»:

электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается **электронным документом**, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Правовую основу использования электронной подписи определяет ФЗ РФ «Об электронной цифровой подписи». Там определяется понятие ЭЦП, а также нормы регулирования общественных отношений по созданию, проверке и использованию ЭЦП в РФ.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Сертификаты ЭЦП должны выпускаться Удостоверяющими центрами. Для внутрикорпоративного использования разрешается создавать собственные Удостоверяющие центры. **Удостоверяющим центром**, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, обладающее необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей. При создании ключей ЭЦП для использования в инфор-

мационной системе общего пользования должны применяться только сертифицированные средства ЭЦП.

Регуляторами в области применения криптографических средств в РФ являются ФСБ России, СВР России, Росинформтехнологии.

13.2. Перечень нормативно-правовых документов

372. Директива N 99/93/ЕС Европейского парламента и Совета Европейского Союза «По структуре для электронных подписей в европейском сообществе» (Принята Европейским союзом 13.12.99).
373. Федеральный закон от 10.01.2002 N 1-ФЗ "Об электронной цифровой подписи".
374. Указ Президента РФ от 03.04.1995 N 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации".

13.3. Перечень нормативно-методических документов

375. Приказ ФАПСИ от 13.06.2001 N 152 "Об утв. Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих гостайну" (Зарег. в Минюсте РФ 06.08.2001 N 2848).
376. Приказ МНС РФ от 02.04.2002 N БГ-3-32/169 "Об утв. Порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи" (Зарег. в Минюсте РФ 16.05.2002 N 3437).
377. Приказ ФСФР РФ от 10.11.2004 N 04-910/пз "Об удостоверяющих центрах".
378. Приказ ФСБ РФ от 09.02.2005 N 66 "Об утв. Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (Зарег. в Минюсте РФ 03.03.2005 N 6382).
379. Приказ ФНС РФ от 13.06.2006 N САЭ-3-27/346@ "Об организации сети доверенных удостоверяющих центров" (вместе с "Положением о сети доверенных удостоверяющих центров ФНС").
380. Распоряжение Правления ПФ РФ от 11.10.2007 N 190р "О внедрении защищенного электронного документооборота в системе индивидуального (персонифицированного) учета для целей обязательного пенсионного страхования" (вместе с "Регламентом обмена документами индивидуального (персонифицированного) учета страховых взносов по телекоммуникационным каналам связи в системе электронного документооборота ПФ РФ с внешними организациями", "Регламентом обеспечения безопасности

информации при защищенном обмене электронными документами в системе электронного документооборота ПФ РФ по телекоммуникационным каналам связи").

381. Приказ Минкомсвязи РФ от 23.03.2009 N 41 "Об утв. Требований к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра". (Зарег. в Минюсте РФ 24.04.2009 N 13831).
382. Приказ ФНС РФ от 02.07.2009 N ММ-7-6/353@ "Об утверждении Требований к сертификату ключа подписи и списку отозванных сертификатов для обеспечения единого пространства доверия сертификатам ключей ЭЦП".
383. Приказ Минкомсвязи РФ от 10.07.2009 N 92 "Об утв. Административного регламента предоставления Росинформтехнологиями государственной услуги по подтверждению подлинности ЭЦП уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей" (Зарег. в Минюсте РФ 02.10.2009 N 14953).
384. Приказ Минздравсоцразвития РФ от 27.11.2009 N 926н "О порядке формирования, использования, хранения, приема и передачи документов в электронной форме в ПФ РФ" (Зарег. в Минюсте РФ 31.12.2009 N 15913).

Глава 14. Лицензирование, сертификация и аттестация объектов информатизации и защиты информации

14.1. Общие положения

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

- лицензирование;
- техническое регулирование;

Дадим определения этих базовых понятий:

лицензирование (ФЗ РФ от 08.08.2001 N 128-ФЗ) – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании;

техническое регулирование (ФЗ РФ от 27.12.2002 N 184-ФЗ) – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.

Согласно ФЗ РФ «О лицензировании отдельных видов деятельности», к лицензируемым видам деятельности относятся такие виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства.

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

технический регламент (ФЗ РФ от 27.12.2002 N 184-ФЗ) – документ, который принят международным договором РФ, ратифицированным в порядке, установленном законодательством РФ, или межправительственным соглашением, заключенным в порядке, установленном законодательством РФ, или федеральным законом, или указом Президента РФ, или постановлением Пр-ва РФ, или нормативным правовым актом федерального органа исполнительной власти по техническому регулирова-

нию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации);

стандарт (ФЗ РФ от 27.12.2002 N 184-ФЗ) – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

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

- защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- охраны окружающей среды, жизни или здоровья животных и растений;
- предупреждения действий, вводящих в заблуждение приобретателей;
- обеспечения энергетической эффективности.

Для оценки соответствия объектов защиты (продуктов, товаров, услуг) требованиям технических регламентов, положениям стандартов проводится подтверждение соответствия. **Подтверждение соответствия** (ФЗ РФ от 27.12.2002 N 184-ФЗ) – это документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

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

- принятия декларации о соответствии;
- обязательной сертификации.

Сертификация (ФЗ РФ от 27.12.2002 N 184-ФЗ) – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Декларация о соответствии (ФЗ РФ от 27.12.2002 N 184-ФЗ) – документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

Основными регулирующими органами по лицензированию в области защиты информации являются ФСТЭК России, ФСБ России, СВР России. Деятельность по из-

готовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей – Роскомнадзор. Деятельность по предоставлению услуг в области ЭЦП лицензируется федеральным агентством Росинформтехнологии.

Органом по стандартизации и техническому регулированию является Ростехрегулирование.

14.2. Перечень нормативно-правовых документов

385. Федеральный закон от 08.08.2001 N 128-ФЗ "О лицензировании отдельных видов деятельности".
386. Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании".
387. Указ Президента РФ от 09.01.1996 N 21 "О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации".
388. Пост. Пр-ва РФ от 15.04.1995 N 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих гостайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите гостайны".
389. Пост. Пр-ва РФ от 26.06.1995 N 608 "О сертификации средств защиты информации".
390. Пост. Пр-ва РФ от 01.07.1996 N 770 "Об утв. Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в РФ и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности".
391. Пост. Пр-ва РФ от 10.03.2000 N 214 "Об утв. Положения о ввозе в РФ и вывозе из РФ специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию".
392. Пост. Пр-ва РФ от 15.07.2002 N 526 "Об утв. Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных

для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность".

393. Пост. Пр-ва РФ от 15.08.2003 N 500 "О федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию".
394. Пост. Пр-ва РФ от 10.11.2003 N 677 "Об общероссийских классификаторах технико-экономической и социальной информации в социально-экономической области" (вместе с "Положением о разработке, принятии, введении в действие, ведении и применении общероссийских классификаторов технико-экономической и социальной информации в социально-экономической области").
395. Распоряжение Пр-ва РФ от 06.11.2004 N 1421-р "Об утв. Программы разработки технических регламентов".
396. Пост. Пр-ва РФ от 18.02.2005 N 87 "Об утв. перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий".
397. Пост. Пр-ва РФ от 29.03.2005 N 165 "Об утв. Правил аккредитации органов по сертификации, испытательных лабораторий (центров), проводящих сертификационные испытания средств связи".
398. Пост. Пр-ва РФ от 13.04.2005 N 214 "Об утв. Правил организации и проведения работ по обязательному подтверждению соответствия средств связи".
399. Пост. Пр-ва РФ от 12.01.2006 N 8 "Об утв. Правил проведения торгов (аукциона, конкурса) на получение лицензии на оказание услуг связи".
400. Пост. Пр-ва РФ от 26.01.2006 N 45 "Об организации лицензирования отдельных видов деятельности".
401. Пост. Пр-ва РФ от 28.04.2006 N 252 "О лицензировании деятельности по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин (программ для ЭВМ), баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу ФЗ или договора)".
402. Пост. Пр-ва РФ от 15.08.2006 N 504 "О лицензировании деятельности по технической защите конфиденциальной информации".
403. Пост. Пр-ва РФ от 31.08.2006 N 532 "О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации".
404. Пост. Пр-ва РФ от 29.12.2007 N 957 "Об утв. Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (крипто-

графическими) средствами" (вместе с "Положением о лицензировании деятельности по распространению шифровальных (криптографических) средств", "Положением о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств", "Положением о лицензировании предоставления услуг в области шифрования информации", "Положением о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем").

405. Пост. Пр-ва РФ от 18.05.2009 N 414 "Об утв. Положения о государственной аккредитации образовательных учреждений ФСБ РФ и ФСО РФ, реализующих образовательные программы, содержащие сведения, составляющие гостайну, и о внесении изменения в пункт 2 Положения о государственной аккредитации образовательных учреждений и научных организаций".
406. Пост. Пр-ва РФ от 25.06.2009 N 532 "Об утв. перечня средств связи, подлежащих обязательной сертификации".
407. Пост. Пр-ва РФ от 10.09.2009 N 723 "О порядке ввода в эксплуатацию отдельных государственных информационных систем" (вместе с "Положением о регистрации федеральных государственных информационных систем").
408. Пост. Пр-ва РФ от 17.10.2009 N 822 "Об утв. Положения об особенностях стандартизации оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих гостайну или относимых к охраняемой в соответствии с законодательством РФ иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют гостайну, а также процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения указанной продукции".
409. Пост. Пр-ва РФ от 17.10.2009 N 837 "Об утв. Положения о лицензировании образовательной деятельности образовательных учреждений, находящихся в ведении ФСБ РФ и ФСО РФ и реализующих образовательные программы, содержащие сведения, составляющие гостайну".
410. Пост. Пр-ва РФ от 01.12.2009 N 982 "Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии".
411. Пост. Пр-ва РФ от 03.02.2010 N 49 "О лицензировании образовательной деятельности образовательных учреждений органа внешней разведки

Минобороны РФ, реализующих военные профессиональные образовательные программы, содержащие сведения, составляющие гостайну" (вместе с "Положением о лицензировании образовательной деятельности образовательных учреждений органа внешней разведки Минобороны РФ, реализующих военные профессиональные образовательные программы, содержащие сведения, составляющие гостайну").

412. Приказ ФСБ РФ от 27.02.2009 N 75 "Об утв. Административного регламента ФСБ РФ по исполнению государственной функции по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих гостайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите гостайны" (Зарег. в Минюсте РФ 06.04.2009 N 13686).

14.3. Перечень нормативно-методических документов

413. "Положение о государственном лицензировании деятельности в области защиты информации" (утв. Решением Гостехкомиссии России и ФАПСИ от 27.04.1994 N 10).

414. Порядок проведения сертификации продукции в РФ (Утв. пост. Госстандарта России от 21.09. 1994 № 15. Зарег. в Минюсте РФ 05.04.1995 № 286. Зарег. в Госреестре Госстандарта России 10.04.1995 РОСС RU . 0001.010107).

415. "Положение по аттестации объектов информатизации по требованиям безопасности информации" (утв. председателем Гостехкомиссии России от 25.11.1994).

416. "Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации" (утв. председателем Гостехкомиссии России 25.11.1994).

417. "Типовое положение об испытательной лаборатории" (утв. председателем Гостехкомиссии России 25.11.1994).

418. "Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации" (утв. председателем Гостехкомиссии России 25.11.1994).

419. "Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации" (утв. председателем Гостехкомиссии России 25.11.1994).

420. "Положение о сертификации средств защиты информации по требованиям безопасности информации" (утв. Приказом председателя Гостехкомиссии России от 27.10.1995 N 199).

421. Правила применения знака соответствия при обязательной сертификации продукции. (Утв. пост. Госстандарта России от 25.07.1996 № 14. Зарег.

в Минюсте РФ 01.08.1996 № 1138. Зарег. в Госреестре Госстандарта России 30.08.1996 РОСС RU . 0001.000123).

422. Правила сертификации работ и услуг в РФ (Утв. о пост. Госстандарта России от 05.08.1997 № 17. Зарег. Министерством в Минюсте РФ 03.04.1998 № 1502. Зарег. в Госреестре Госстандарта России 18.06.1998 РОСС RU 0001 010134).
423. Положение о системе сертификации ГОСТ Р (Пост. Госстандарта России от 17.03.1998 № 11 . Зарег. в Минюсте РФ 29.04.1998 №1520. Зарег. в Госреестре Госстандарта России 30.04.1998 РОСС RU 0001 010001).
424. Система сертификации ГОСТ Р. Правила по проведению добровольной сертификации продукции (работ, услуг) на соответствие требованиям государственных стандартов (Утв. пост. Госстандарта России от 29.06.1998 № 50).
425. Система сертификации ГОСТ Р. Положение о знаке системы сертификации ГОСТ Р при добровольной сертификации продукции (работ, услуг) (Утв. пост. Госстандарта России от 29.06.1998 №50).
426. Система сертификации ГОСТ Р. Формы основных документов, применяемых в Системе (Утв. пост. Госстандарта России от 17.03.1998 № 12).
427. Правила по сертификации. Оплата работ по сертификации продукции и услуг (Утв. пост. Госстандарта РФ 23.08.1999, № 44. Зарег. в Госреестре Госстандарта России РОСС RU 0001.00ДД01. Зарег. в Минюсте РФ 29.12.1999 № 2031).
428. Приказ ФСБ РФ от 13.11.1999 N 564 "Об утв. Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих гостайну, и о ее знаках соответствия" (Зарег. в Минюсте РФ 27.12.1999 N 2028).
429. Правила по проведению сертификации в РФ (Утв. пост. Госстандарта России от 10 мая 2000 г. № 26. Зарег. в Минюсте РФ 27.06.2000 № 2284).
430. Приказ Мининформсвязи РФ от 20.09.2004 N 14 "О форме декларации о соответствии средств связи" (Зарег. в Минюсте РФ 28.09.2004 N 6044).

Раздел VI. Правонарушения и ответственность в области эксплуатации информационных систем и информационной безопасности

Глава 15. Виды и формы правонарушений и юридической ответственности

15.1. Общее понятие юридической ответственности

Юридической ответственностью называют применение к лицу, совершившему правонарушение, мер государственного принуждения, предусмотренных санкцией нарушенной нормы, в установленном для этого процессуальном порядке.

Основными признаками юридической ответственности являются:

- 1) наличие неблагоприятных последствий для нарушителя;
- 2) государственно-правовое принуждение;
- 3) осуждение правонарушителя и его субъекта со стороны общества и государства.

Традиционным в научной и учебной литературе является признание следующих видов юридической ответственности: *гражданско-правовой, материальной, дисциплинарной, административной и уголовной*, соответствующих таким отраслям права, как гражданское, трудовое, административное и уголовное²³.

Правонарушение представляет собой противоправное деяние юридическое определение (квалификация) которого содержится в законе.

К правонарушениям относят деликты (гражданско-правовые проступки), административные и дисциплинарные проступки, преступления (уголовное правонарушение).

Юрисдикционный процесс есть система органически взаимосвязанных процессуальных действий, процессуальных форм и средств, направленных на установление правонарушения и назначения меры юридической ответственности правонарушителя. Юрисдикционный процесс чаще всего выступает как судебный процесс, как судопроизводство. Однако судебный процесс может включать и элементы внесудебного процесса.

Административно-судебный процесс включает как процессуальную деятельность судей в рамках судопроизводства, так и процессуальную деятельность административных органов и должностных лиц по разрешению административных дел.

В уголовный процесс наряду с судопроизводством входит предварительное расследование преступлений, осуществляемое компетентными органами дознания и предварительного расследования.

²³ Витрук Н.В. Общая теория юридической ответственности. М.: НОРМА, 2009.

Санкции делятся на два основных вида в соответствии со способом, каким они служат охране правопорядка:

- правосстановительные санкции, которые направлены на устранения непосредственного вреда, причиненного правопорядку;
- штрафные, карательные санкции, которые имеют цель воздействия на нарушителя в целях общей и частной превенции правонарушений.

Правосстановительные санкции предусмотрены нормами Гражданского Кодекса РФ (гражданско-правовая ответственность), Трудового Кодекса РФ (материальная ответственность).

Штрафы и иные карательные санкции определены нормами Уголовного Кодекса РФ (уголовная ответственность), Кодекса РФ об административных правонарушениях (административная ответственность), Трудовым Кодексом РФ (дисциплинарная ответственность).

Санкции, относящиеся к различным видам ответственности не исключают одна другую и могут назначаться в комплексе.

15.2. Гражданско-правовая ответственность

Основными правонарушениями в гражданской и трудовой сферах деятельности, затрагивающими область информационной безопасности, являются нарушения прав собственности (в т.ч. и интеллектуальной), режимов защиты информации, ограниченной к распространению и т.п.

Гражданско-правовая ответственность возникает из юридических фактов нарушения договорных отношений, либо из нарушений обязательных норм гражданского права РФ (деликтные обязательства). В своем содержании гражданско-правовая ответственность главным образом состоит в восстановлении нарушенного права (состояния), в заглаживании нанесенного в результате неправомерного действия вреда, возмещении ущерба в натуре либо в виде компенсации.

Материальная ответственность — возмещение имущественного вреда, нанесенного в результате неправомерных действий в процессе выполнения лицом своих служебных обязанностей. Материальная ответственность регламентируется нормами трудового права, применяется только к физическим лицам (работникам), характеризуется:

- 1) наличием трудовых отношений между работником и работодателем;
- 2) конкретизацией формы материальной ответственности работника в трудовом договоре или в заключаемом в письменной форме соглашении;
- 3) наличием ущерба, причиненного работником работодателю в результате его виновного противоправного поведения (действий или бездействия).

Гражданскому процессу известно несколько самостоятельных производств, выделенных ранее действовавшим Гражданско-процессуальным Кодексом РСФСР: исковое производство (ст. ст. 113 - 230); производство по делам, возникающим из ад-

министративно-правовых отношений (ст. ст. 231 - 244); дела особого производства (ст. ст. 245 - 281).

15.3. Административная и дисциплинарная ответственность

Административным правонарушением признается противоправное, виновное (умышленное или неосторожное) действие либо бездействие физического или юридического лица, за которое законодательством РФ предусмотрена административная ответственность.

В сфере ИБ административная ответственность устанавливается следующими статьями Кодекса РФ об административных правонарушениях по соответствующим направлениям: нарушение авторских и смежных прав, изобретательских и патентных прав (Ст. 7.12), правонарушения в области защиты информации (Ст. 13.6, 13.11, 13.12, 13.13, 13.14), и т.д.

Административная ответственность представляет собой государственное осуждение поведения правонарушителя, выражающее в наступлении для него отрицательных последствий в виде санкций (административных наказаний). Кодексом РФ об административных правонарушениях установлены следующие виды **административных наказаний**:

- 1) предупреждение;
- 2) административный штраф;
- 3) возмездное изъятие орудия совершения или предмета административного правонарушения;
- 4) конфискация орудия совершения или предмета административного правонарушения;
- 5) лишение специального права, предоставленного физическому лицу;
- 6) административный арест;
- 7) административное выдворение за пределы РФ иностранного гражданина или лица без гражданства;
- 8) дисквалификация;
- 9) административное приостановление деятельности.

Дисциплинарная ответственность заключается в наложении на виновное лицо дисциплинарного взыскания властью руководителя. Дисциплинарная ответственность подразделяется на общую (трудовая дисциплинарная ответственность) и специальную (основана на учебной, служебной, воинской, иной профессиональной дисциплине).

Меры дисциплинарной ответственности при общей ответственности – это дисциплинарные взыскания, определенные в Трудовом Кодексе РФ (замечание, выговор, увольнение по соответствующим основаниям). При специальной дисциплинарной ответственности меры устанавливаются в соответствующих локальных (внутренних) нормативных документах – уставах, положениях, т.п. Например, ФЗ «О статусе военнослужащих» предусматривает следующие дисциплинарные взыскания для военнослужащих: выговор; строгий выговор; лишение очередного увольнения

из расположения воинской части или с корабля на берег; лишение нагрудного знака отличника; предупреждение о неполном служебном соответствии; снижение в воинской должности; снижение в воинском звании на одну ступень; снижение в воинском звании на одну ступень со снижением в воинской должности; досрочное увольнение с военной службы в связи с невыполнением условий контракта; отчисление из военного образовательного учреждения профессионального образования; отчисление с военных сборов; дисциплинарный арест.

Особенностью административного законодательства является то, что оно создается из нормативных актов органов государственной власти двух уровней – федеральной и субъектов РФ. Однако в нормах субъектов РФ допускается использовать только две меры административной ответственности: предупреждение и штраф.

Второй особенностью административного законодательства является то, что для некоторых категорий субъектов (например, для военнослужащих) административная ответственность заменяется дисциплинарной.

В соответствии с действующим законодательством существуют два основных вида обычного производства по делам об административных правонарушениях:

- 1) административно-судебное по правилам Кодекса РФ об административных правонарушениях;
- 2) административно-арбитражное по правилам, установленным Арбитражно-процессуальным Кодексом РФ.

Наряду с указанным выше обычным производством существует непроцессуальное производство по делам об административных правонарушениях. Согласно ст. 28.6 Кодекса РФ об административных правонарушениях назначение административного наказания без составления протокола происходит в относительно упрощенной процедуре, что обуславливается, во-первых, самим характером совершенного правонарушения, его очевидностью и бесспорностью, во-вторых, отсутствием спора и согласием правонарушителя понести административное наказание. Должностное лицо согласно закону констатирует факт правонарушения на месте его совершения и принимает решение о наложении административного наказания, а правонарушитель, как правило, тут же исполняет принятое решение (уплачивает штраф).

15.4. Уголовная ответственность

Преступлением признается виновно совершенное общественно-опасное деяние, запрещенное Уголовным Кодексом РФ под угрозой наказания.

За последние 10 - 15 лет в международной юридической практике сформировалось новое понятие - "*киберпреступность*", под которым понимается преступность в традиционном смысле слова, которая имеет место в киберпространстве (в том числе Интернет) ²⁴.

²⁴ Дашян М.С. Право информационных магистралей (Law of information highways): Вопросы правового регулирования в сфере Интернет. М.: Волтерс Клувер, 2007.

Киберпреступление – это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству²⁵.

К киберпреступлениям относят деяния, квалифицирующиеся статьями Уголовного Кодекса РФ по соответствующим направлениям: нарушение основных прав человека (Ст. 137, 138, 140), нарушение авторских, смежных, патентных прав (Ст. 146, 147), нарушение режима коммерческой или иной тайны (Ст. 183), преступления в сфере компьютерной информации (Ст. 272, 273, 274), нарушение режима государственной тайны (Ст. 275, 276, 283, 284).

Уголовная ответственность является формой негативной реакции общества на противоправное поведение и заключается в применении к лицу, совершившему преступление, физических, имущественных и моральных лишений, призванных предотвратить совершение новых преступлений. Уголовная ответственность применяется только к физическим лицам за совершенное преступление. Порядок ее осуществления определяется уголовным, уголовно-процессуальным и уголовно-исполнительным законодательством. Ряд принципов уголовной ответственности закреплен в международных договорах и в конституционном законодательстве.

Уголовное наказание – мера государственного принуждения, назначаемая по приговору суда. Видами уголовных наказаний являются:

- 1) штраф;
- 2) лишение права занимать определенные должности или заниматься определенной деятельностью;
- 3) лишение специального, воинского или почетного звания, классного чина и государственных наград;
- 4) обязательные работы;
- 5) исправительные работы;
- 6) ограничение по военной службе;
- 7) ограничение свободы;
- 8) арест;
- 9) содержание в дисциплинарной воинской части;
- 10) лишение свободы на определенный срок;
- 11) пожизненное лишение свободы;
- 12) смертная казнь.

²⁵ Тропинина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Диссертация на соискание звания кандидата юридических наук. Владивосток, 2005.

Глава 16. Характеристика личности правонарушителя

Криминалистика в сфере ИТ-преступлений выделяет следующие группы преступников²⁶:

а) хакеры - лица, рассматривающие меры защиты информационных систем как личный вызов и взламывающие их с целью получения контроля за информацией независимо от ее ценности;

б) шпионы - лица, взламывающие защиту информационных систем для получения информации, которую можно использовать в целях политического влияния;

в) террористы - лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать и в целях политического влияния;

г) корпоративные налетчики - служащие компании, взламывающие компьютеры конкурентов для экономического влияния;

д) воры, вторгающиеся в информационные системы для получения личной выгоды;

е) вандалы - лица, взламывающие системы с целью их разрушения;

ж) нарушители правил пользования ЭВМ, совершающие противоправные действия из-за недостаточного знания техники и порядка пользования информационными ресурсами;

з) лица с психическими аномалиями, страдающие новым видом заболеваний - информационными болезнями или компьютерными фобиями.

С точки зрения процесса обеспечения информационной безопасности активов организации правонарушителей обычно разделяют на внутренних (инсайдеры) и внешних.

Внутренние правонарушители – это обычно работники организации, либо лица, связанные с организацией какими-либо договорными отношениями. Доступ к активам организации им предоставляется санкционировано, а нарушения чаще всего совершаются через превышение полномочий, нарушение внутренних правил организации. В качестве санкций к инсайдерам чаще применяют дисциплинарную, материальную ответственность, регламентируемую нормами трудового права. При наличии договорных отношений возможно применение гражданско-правовой ответственности.

Внешних нарушителей привлечь к ответственности несколько сложнее. В первую очередь из-за того, что большая часть атак является удаленными и производится через глобальные сети. При этом задача идентификации нарушителя и сбора доказательств преступления становится нетривиальной. Однако, при успешном выполнении этой задачи к правонарушителям потенциально возможно применение

²⁶ Ищенко Е.П., Топорков А.А. Криминалистика: Учебник/ под ред. Е.П. Ищенко. М.: КОНТРАКТ, ИНФРА-М, 2006.

как административных и уголовных санкций, так и (при наличии материального ущерба) предъявление гражданско-правовых исков.

Согласно классификации потенциальных субъектов преступлений в сфере компьютерной информации, выделяются 4 группы личностей²⁷:

«В России, как показывает статистика и проведенные отечественными специалистами исследования, до 20% от общего числа компьютерных преступников олицетворяют собой некий стереотип. В соответствии с ним компьютерный преступник – это гражданин страны примерно 18-20 лет, выросший в российской семье со средним достатком, обладающий неряшливой прической, в очках, молчаливый, замкнутый и рассеянный, увлеченный компьютерной техникой и игнорирующий события в окружающем мире.

Остальные 80% компьютерных преступников либо полностью, либо частично отличаются от приведенного описания, и их можно подразделить на группы следующим образом. Около 20% технократов, то есть людей, буквально «молящихся» на компьютер и электронную технику в целом, о которых иногда говорят «не от мира сего». Порядка 40% «крепкого середнячка», знающего свое дело, но «звезд с неба не хватающего». И примерно 20% «компьютерной элиты», представляющей собой законченный продукт рыночных отношений, знающим себе и своим знаниям истинную цену.

Последняя и частично вторая группа превратили свое увлечение в доходное дело, обладают не только общими знаниями в области информационных технологий, но и специальными навыками и наработками в плане обращения со средствами вычислительной техники, программным обеспечением, компьютерными системами и сетями, которые позволяют им преодолевать защиту компьютерных систем».

²⁷ Коняевский В.А., Лопаткин С.В. Компьютерные преступления. В 2-х томах. Том 1 – М.: РФК-Имидж Лаб., 2006. Стр. 47.

Глава 17. Юрисдикционные органы РФ, должностные лица и внутренние структуры предприятия

17.1. Распределение компетенции

Меры юридической ответственности, перечисленные в Главе 15, обеспечиваются деятельностью компетентных правоохранительных органов и должностных лиц.

Последние можно разделить на:

1. Органы международных организаций.
2. Национальные государственные органы.
3. Внутренние структуры организации по обеспечению законности и безопасности.

Основная компетенция в контроле за соблюдением законодательства, обеспечением защиты прав и поддержанием правопорядка лежит на государственных органах исполнительной и судебной власти.

Задачей органов международных организаций является помощь в гармонизации национальных законодательств, реагировании на инциденты и правонарушения, помощь в расследовании преступлений транснационального характера.

Задача внутренних структур безопасности организации – поддержка законности и защиты объектов частного права, а так же реагирование на правонарушения, помощь в подборе доказательств правонарушений в области публичных отношений.

17.2. Предварительное следствие и оперативно-розыскная деятельность

Предварительное следствие проводится в обязательном порядке для расследования преступлений.

Одной из основных задач предварительного следствия является сбор доказательств совершенного преступления. Основной проблемой сбора доказательств является обеспечение оперативности действий.

Проводить предварительное расследование в форме следствия или дознания (в рамках своей компетенции) могут только следователи и дознаватели Следственного комитета при прокуратуре РФ, органов ФСБ России, органов внутренних дел РФ, органов по контролю за оборотом наркотических средств и психотропных веществ, органов Федеральной службы судебных приставов, таможенных органов РФ, органов государственного пожарного надзора федеральной противопожарной службы. В последнее время ведутся активные споры о необходимости создания единого Следственного комитета, чьей исключительной компетенцией будет являться проведение предварительного расследования.

Следователь (дознаватель) при проведении предварительного расследования использовать следующий набор следственных действий:

1. личный обыск,
2. выемка предметов и документов,

3. освидетельствование,
4. осмотр трупа, эксгумация,
5. допрос,
6. очная ставка,
7. опознание,
8. предъявление для опознания людей и предметов,
9. проверка показаний на месте,
10. следственный эксперимент,
11. производство судебной экспертизы,
12. арест имущества,
13. осмотр и обыск места происшествия, местности, жилища, иного помещения, предметов и документов,
14. наложение ареста на почтово-телеграфные отправления, их осмотр и выемка
15. контроль и запись переговоров,
16. получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Все следственные действия проводятся согласно процедурам, определенным Уголовно-процессуальным Кодексом РФ. Проведение последних пяти следственных действий производится только на основании судебного решения.

Исключительная компетенция органов дознания – это полномочия по осуществлению **оперативно-розыскной деятельности**, под которой понимается проведение специальных разведывательных, по своей сущности непроцессуальных мероприятий, связанных с использованием специальных, преимущественно негласных тактических и технических средств, направленных на получение информации о преступлении, лице, его совершившем, и об источниках доказательств. Эта деятельность основывается на ФЗ от 12.08.1995 "Об оперативно-розыскной деятельности".

Оперативно-розыскные мероприятия по своему «арсеналу средств» несколько шире процессуальных следственных действий предварительного следствия и включают:

1. Опрос.
2. Наведение справок.
3. Сбор образцов для сравнительного исследования.
4. Проверочная закупка.
5. Исследование предметов и документов.
6. Наблюдение.
7. Отождествление личности.
8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
9. Контроль почтовых отправлений, телеграфных и иных сообщений.
10. Прослушивание телефонных переговоров.
11. Снятие информации с технических каналов связи.
12. Оперативное внедрение.
13. Контролируемая поставка.

14. Оперативный эксперимент.

Законом предусмотрены ограничения по использованию оперативно-розыскных мероприятий с целью обеспечения при их проведении соблюдения законности и защиты конституционных прав граждан. Проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения.

Возможности обеспечения и сбора доказательств с помощью средств ИТ и Интернет, а также процессуальный статус доказательств, полученных таким способом, подробно описаны в специальной юридической литературе²⁸.

17.3. Подразделение по борьбе с киберпреступностью в МВД России

В 1998 году в структуре МВД России было создано специальное подразделение по борьбе с преступлениями в области информационных технологий²⁹. В 2001 году в Министерстве внутренних дел РФ произошли организационно-штатные изменения, и подразделение по борьбе с преступлениями в информационной среде было реорганизовано в **Управление «К» МВД России**, а территориальные подразделения - в подразделения «К». Такая аббревиатура сохраняется и в настоящее время.

Основные направления работы Управления «К» МВД России

1. Борьба с преступлениями в сфере компьютерной информации:

- выявление и пресечение фактов неправомерного доступа к компьютерной информации;
- борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;
- противодействие мошенническим действиям с использованием возможностей электронных платежных систем;
- борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно - телекоммуникационных сетях, включая сеть Интернет:

- выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

²⁸ Вайшнурс А.А. Обеспечение и сбор доказательств с помощью Интернета. Процессуальный статус доказательств, полученных с помощью Интернета// Вестник ВАС РФ. 2003. N 3. С. 124.

²⁹ <http://www.mvd.ru/struct/upravleniek/10000288/>

- противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий. Борьба с изготовлением и распространением нелицензионного программного обеспечения для ЭВМ (на машинных носителях информации, через информационно-телекоммуникационные сети).

5. Борьба с международными преступлениями в сфере информационных технологий:

- противодействие преступлениям в сфере информационных технологий, носящим международный характер;

- взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Управление «К» МВД России активно взаимодействует с правоохранительными органами иностранных государств как на двусторонней, так и многосторонней основе (ООН, «восьмерка», СНГ, СЕ, ЕС, ШОС, АТР и др.).

17.4. Подразделения защиты информации на предприятии, учреждении и организации

Задачами управления предприятия является обеспечение экономической безопасности (в т.ч. в информационном плане), обеспечение объектно-пропускного режима, обеспечение режима защиты коммерческой и (или) служебной тайны, защиты гостайны, поддержание системы обеспечения информационной безопасности компьютерной сети (автоматизированной системы) предприятия и системы менеджмента информационной безопасности.

Эти задачи могут выполняться как собственными подразделениями предприятия, так и передаваться на аутсорсинг сторонним компаниям или специально организованным дочерним компаниям (корпоративным структурам). В последнем случае актуальным становится исполнение норм законодательства о частной детективной и охранной деятельности, норм и требований регуляторов по лицензированию деятельности по защите информации.

Одной из важных задач обеспечения информационной безопасности, выполняемой внутренними подразделениями предприятий, является поддержание связи с провайдерами связи, компетентными государственными органами и органами межправительственных международных организаций, компетентных в расследовании, предотвращении киберпреступлений. Это делается по следующим причинам:

- 1) необходимость подключения компетентных государственных органов для возбуждения уголовного дела и проведения соответствующего расследования при наличии достаточных оснований;
- 2) минимизация ущерба от зафиксированной сетевой атаки или ее оперативное предотвращение;
- 3) получение оперативной компетентной помощи в разрешении инцидента ИБ, выходящего за рамки одной организации.

17.5. Деятельность судов и прокуратуры

Судебная защита нарушенных прав в сфере ИБ обычно применяется при наличии материального ущерба вследствие правонарушений, связанных с ИТ.

Судам подведомственно рассмотрение уголовных дел, гражданско-правовых споров и некоторых категорий административных дел. Кроме этого, Конституционный суд разрешает дела о соответствии нормативных актов Конституции РФ, разрешает споры о компетенции между органами государственной власти.

Основными задачами системы правосудия являются³⁰:

1. Восстановление нарушенных прав.
2. Защиты прав и свобод личности.
3. Содействие укреплению законности и предупреждению правонарушений.

Эти задачи осуществляются в процессуальном порядке и их результат отражается в актах реализации правосудия. В этих актах могут быть:

- a) восстановительно-компенсационные меры;
- b) карательно-штрафные санкции;
- c) решение о признании нормативных актов (или отдельных норм) недействительными (недействительными);
- d) признание юридического факта.

Прокуратура РФ - единая федеральная централизованная система органов, осуществляющих от имени РФ надзор за соблюдением Конституции РФ и исполнением законов, действующих на территории РФ.

Основные задачи Прокуратуры РФ³¹:

1. Координация деятельности по борьбе с преступностью.
2. Участие в правотворческой деятельности.
3. Проведение антикоррупционной экспертизы нормативных правовых актов.
4. Рассмотрение и разрешение в органах прокуратуры заявлений, жалоб и иных обращений.

Прокуроры осуществляют свои задачи в форме надзора и участия в рассмотрении дел судами в случаях, предусмотренных процессуальным законодательством РФ. В порядке надзора мерами прокурорского реагирования являются:

- a) опротестование противоречащих закону актов;
- b) обращение в суд за защитой прав и охраняемых законом интересов граждан, общества и государства;

³⁰ www.supcourt.ru

³¹ www.genproc.gov.ru

- с) возбуждение производства об административном правонарушении;
- д) внесение представления об устранении нарушений закона в орган, общественную, политическую организацию или должностному лицу, полномочным устранить нарушение закона;
- е) объявление предостережения о недопустимости нарушения закона.

Кроме этого, прокурор вправе:

- ф) по предъявлении служебного удостоверения беспрепятственно входить на территории и в помещения государственных органов, и органов местного самоуправления, иметь доступ к их документам и материалам, проверять исполнение законов в связи с поступившей в органы прокуратуры информацией о фактах нарушения закона;
- г) требовать от руководителей и других должностных лиц указанных органов представления необходимых документов, материалов, статистических и иных сведений; выделения специалистов для выяснения возникших вопросов; проведения проверок по поступившим в органы прокуратуры материалам и обращениям, ревизий деятельности подконтрольных или подведомственных им организаций;
- h) вызывать должностных лиц и граждан для объяснений по поводу нарушений законов;
- и) освобождать своим постановлением лиц, незаконно подвергнутых административному задержанию на основании решений несудебных органов.

В составе органов Прокуратуры РФ действует Следственный комитет.

17.6. Перечень национальных нормативно-правовых документов РФ

- 431. "Гражданский кодекс РФ (часть вторая)" от 26.01.1996 N 14-ФЗ.
- 432. "Уголовный кодекс РФ" от 13.06.1996 N 63-ФЗ.
- 433. "Кодекс РФ об административных правонарушениях" от 30.12.2001 N 195-ФЗ.
- 434. "Трудовой кодекс РФ" от 30.12.2001 N 197-ФЗ.
- 435. Закон РФ от 18.04.1991 N 1026-1 "О милиции".
- 436. Закон РФ от 11.03.1992 N 2487-1 "О частной детективной и охранной деятельности в РФ".
- 437. Федеральный закон от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности".
- 438. Федеральный закон от 27.05.1998 N 76-ФЗ "О статусе военнослужащих".
- 439. Федеральный закон от 25.07.2002 N 114-ФЗ "О противодействии экстремистской деятельности".
- 440. Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе РФ".

441. Федеральный закон от 06.03.2006 N 35-ФЗ "О противодействии терроризму".
442. Указ Президента РФ от 01.09.1995 N 891 "Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств".
443. Указ Президента РФ от 10.11.2007 N 1495 "Об утверждении общевоинских уставов Вооруженных Сил РФ" (вместе с "Уставом внутренней службы Вооруженных Сил РФ", "Дисциплинарным уставом Вооруженных Сил РФ", "Уставом гарнизонной и караульной служб Вооруженных Сил РФ").
444. Пост. Пр-ва РФ от 14.08.1992 N 587 "Вопросы негосударственной (частной) охранной и негосударственной (частной) сыскной деятельности".
445. Пост. Пр-ва РФ от 27.08.2005 N 538 "Об утв. Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность".

17.7. Перечень нормативно-методических документов

446. Инструктивные указания Госарбитража СССР от 29.06.1979 N И-1-4 "Об использовании в качестве доказательств документов, представленных с помощью электронно-вычислительной техники".
447. ГОСТ 6.10.4-84 "Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения".
448. Информационное письмо Президиума ВАС РФ от 25.12.1998 N 37 "Обзор практики рассмотрения споров, связанных с применением законодательства о рекламе".
449. Информационное письмо Президиума ВАС РФ от 23.09.1999 N 46 "Обзор практики разрешения арбитражными судами споров, связанных с защитой деловой репутации".
450. Информационное письмо Президиума ВАС РФ от 28.09.1999 N 47 "Обзор практики рассмотрения споров, связанных с применением Закона Российской Федерации "Об авторском праве и смежных правах".
451. Пост. Пленума ВАС РФ от 27.01.2003 N 2 "О некоторых вопросах, связанных с введением в действие Кодекса РФ об административных правонарушениях".
452. Пост. Пленума Верховного Суда РФ от 18.11.2004 N 23 "О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем".

453. Пост. Пленума Верховного Суда РФ от 24.03.2005 N 5 "О некоторых вопросах, возникающих у судов при применении Кодекса РФ об административных правонарушениях".
454. Пост. Пленума Верховного Суда РФ от 24.02.2005 N 3 "О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц".
455. Пост. Пленума Верховного Суда РФ от 19.06.2006 N 15 "О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах".
456. Пост. Пленума Верховного Суда РФ от 26.04.2007 N 14 "О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака".
457. Пост. Пленума Верховного Суда РФ N 5, Пленума ВАС РФ N 29 от 26.03.2009 "О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса РФ".
458. Приказ МВД РФ N 786, Минюста РФ N 310, ФСБ РФ N 470, ФСО РФ N 454, ФСКН РФ N 333, ФТС РФ 971 от 06.10.2006 "Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола" (Зарег. в Минюсте РФ 03.11.2006 N 8437).
459. Пост. Пленума Верховного Суда РФ от 26.04.2007 N 14 "О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака".
460. Приказ Мининформсвязи РФ от 16.01.2008 N 6 "Об утв. Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть I. Общие требования" (Зарег. в Минюсте РФ 31.01.2008 N 11057).
461. Приказ Мининформсвязи РФ от 19.05.2009 N 65 "Об утв. Требований к сетям и средствам почтовой связи для проведения оперативно-розыскных мероприятий" (Зарег. в Минюсте РФ 06.07.2009 N 14209).

Глава 18. Международные аспекты обеспечения информационной безопасности. Международное сотрудничество

18.1. Международное сотрудничество в борьбе с преступностью по линии ООН

Организация Объединенных Наций создана в октябре 1945 г. По Уставу на нее возложена ответственность за международное сотрудничество между государствами по всем актуальным проблемам. Непосредственно вопросами сотрудничества стран в борьбе с преступностью занимается один из органов ООН — **Экономический и Социальный Совет (ЭКОСОС)**, в структуре которого в 1950 г. был учрежден Комитет экспертов по предупреждению преступности и обращению с правонарушителями. В 1971 г. он был преобразован в Комитет по предупреждению преступности и борьбе с ней, в 1993 г. — в Комиссию по предупреждению преступности и уголовному правосудию.

Комиссия (комитет) представляет ЭКОСОС рекомендации и предложения, направленные на более эффективную борьбу с преступностью и гуманное обращение с правонарушителями. Генеральная Ассамблея ООН возложила на этот орган функцию подготовки один раз в 5 лет конгрессов ООН по предупреждению преступности и обращению с правонарушителями. Конгрессы ООН играют основную роль в разработке международных правил, стандартов и рекомендаций по предупреждению преступности и уголовному правосудию. К настоящему времени было проведено 9 конгрессов.

Генеральная ассамблея ООН в своей резолюции № 56/183 от 21.12.2001 приняла решение о проведении **Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО)**. ВВУИО прошла в 2 этапа в Женеве и Тунисе, в 2003 и 2005 годах. Базовыми руководящими документами, принятыми на первом этапе встречи были: Декларация принципов и План действий Информационного общества. На втором этапе были приняты: Тунисское обязательство и Тунисская программа для информационного общества.

Во время второго этапа ВВУИО, прошедшей в Тунисе в 2005 году, **Международному союзу электросвязи (МСЭ)** было поручено взять на себя руководство, в качестве единственной содействующей организации, по Направлению деятельности С5 “Укрепление доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ)”.

Кроме этого, МСЭ недавно была утверждена и обнародована в рамках Всемирных форумов по политике в области электросвязи «**Глобальная программа кибербезопасности**». Программа состоит из 7 целей, распределенных по 5-ти основным направлениям действия (стратегическим принципам):

1. Правовые меры.
2. Технические и процедурные меры.
3. Организационные структуры.
4. Создание потенциала.
5. Международное сотрудничество.

В документе указывается, что Глобальная программа кибербезопасности МСЭ объединит существующие инициативы, а также партнеров, для того, чтобы предложить глобальные стратегии по решению современных проблем в борьбе с киберпреступностью и поддержанию кибермира.

В качестве ведущего учреждения ООН в области информационно-коммуникационных технологий, определенного ведущей содействующей организацией по Направлению деятельности С5 ВВУИО "Укрепление доверия и безопасности при использовании ИКТ", а также в рамках Глобальной программы кибербезопасности МСЭ и **Международное многостороннее партнерство против киберугроз (ИМПАКТ)** первыми приступили к развертыванию решений и услуг, предназначенных для борьбы с киберугрозами во всемирном масштабе, совместно с Государствами-Членами МСЭ и ведущими мировыми партнерами, представляющими отрасль и научное сообщество.

ИМПАК³² – первая государственно-частная организация, задуманная для обеспечения взаимодействия частных секторов экономики и ученых сообществ всех государств с целью противостояния киберугрозам. Международный экспертный совет, в состав которого входят ведущие специалисты промышленных предприятий и учебных заведений, дает рекомендации ИМПАК по основным вопросам, координируя повседневную деятельность его правления и международного секретариата.

Глобальный центр реагирования ИМПАКТ был определен в качестве глобальной платформы для системы раннего предупреждения и главного центра ресурсов борьбы с киберугрозами для мирового сообщества, который предоставляет услуги по реагированию в чрезвычайных ситуациях, а также механизмы совместного использования знаний в безопасной среде.

Кроме того, на национальном уровне будут создаваться специализированные организационные структуры для борьбы с кибератаками. Для этих целей МСЭ и ИМПАКТ разработали стратегию реализации с помощью программы "CIRT-Lite" национальных групп реагирования на компьютерные инциденты (CIRT), которые будут функционировать в качестве надежных центральных координационных пунктов для связи в пределах страны, обеспечивая системы контроля и оповещения и услуги по реагированию на инциденты. Это предлагаемое решение интегрируется в уже созданный для стран Глобальный центр реагирования и будет соответствовать передовому международному опыту.

18.2. Инициативы Совета Европы

Совет Европы выступил флагманом в формировании унифицированного подхода к законотворчеству разных стран через рамочные международные акты в сфере борьбы с преступностью в Интернет. Конвенция СЕ о киберпреступности стала первой попыткой выработать единое законодательство в области борьбы с преступлениями в компьютерных сетях.

³² Абукабар Ш. ИМПАК – первое в мире государственно-частное партнерство для борьбы с киберугрозами// Электронный журнал ENас. 2009, № 2. URL: polis.osce.org/library/view?item_id=3633&attach_id=2757.

Совет Европы работал над Конвенцией о киберпреступности на протяжении четырех лет. В период с 1997 г. по 2000 г. Комитет экспертов СЕ провел десять пленарных заседаний и пятнадцать совещаний открытой рабочей группы. Конвенция была открыта для подписания государствами на церемонии подписания 23 ноября 2001 г. в Будапеште, в ходе которой 30 стран подписали это соглашение, включая 4 страны, не входящие в СЕ: Канада, Япония, ЮАР и США. На данный момент 47 стран подписали и 30 стран ратифицировали Конвенцию о киберпреступности. В настоящее время Конвенция признана важнейшим международным инструментом в борьбе с киберпреступностью и поддерживается различными международными организациями.

В 2003 г. к Конвенции был подготовлен первый дополнительный протокол. В него были включены вопросы уголовного преследования за расизм и распространение ксенофобных материалов, так как при обсуждении Конвенции некоторые страны выразили озабоченность, что если в Конвенцию будут включены положения, нарушающие свободу самовыражения, то они не смогут ее подписать. На данный момент Дополнительный протокол подписан 34 странами и 18 из них ратифицирован.

Советом Европы ежегодно с 2007 года проводится Конференция по борьбе с киберпреступностью, призванная внести свой вклад в укрепление взаимодействия между государственным и частным секторами в вопросах борьбы с преступлениями, совершаемыми с использованием Интернета.

18.3. Международное сотрудничество в борьбе с преступностью по линии неправительственных международных организаций

В числе субъектов работы по международному сотрудничеству в борьбе с преступностью необходимо выделить неправительственные организации: **Международная ассоциация уголовного права (МАУП)**, **Международное криминологическое общество (МКО)**, **Международное общество социальной защиты (МОСЗ)** и **Международный уголовный и пенитенциарный фонд (МУПФ)**.

Международная ассоциация уголовного права основана в 1924 г. Она изучает преступность, ее причины и средства борьбы с ней, занимается сравнительными уголовно-правовыми исследованиями, организует проведение международных конгрессов по проблемам уголовного права, консультирует ООН, ЮНЕСКО и другие международные организации.

Международное криминологическое общество основано в 1934 г. и непосредственно занимается обеспечением сотрудничества в борьбе с преступностью. Оно объединяет национальные институты и специалистов по криминологии. МКО имеет консультативный статус ЭКОСОС, ООН и ЮНЕСКО. МКО изучает причины преступности на международном уровне, организует криминологические конгрессы, семинары, коллоквиумы, публикует их материалы, оказывает содействие национальным криминологическим институтам, учреждает и назначает стипендии и премии для стимулирования криминологической науки. Аналогичную работу по своему профилю проводят МОСЗ и МУПФ.

18.4. Международное сотрудничество в борьбе с преступностью по линии Интерпола

Особое место в международном сотрудничестве занимает Международная организация уголовной полиции (**Интерпол**), которая была создана в 1923 г. в Вене вначале как международная комиссия уголовной полиции. Из неправительственной организации Интерпол превратился в межправительственную и в настоящее время объединяет более 170 государств. Высшим органом Интерпола является Генеральная ассамблея, сессии которой проходят один раз в год. Исполнительный комитет формируется из представителей регионов. Постоянно действующим аппаратом является секретариат. Для научной проработки документов существует институт советников.

В отличие от других международных организаций Интерпол имеет национальные центральные бюро (НЦБ) в каждой стране. Согласно уставу Интерпол обеспечивает и развивает взаимное сотрудничество органов уголовной полиции в рамках действующих в их странах законов, создает и развивает учреждения, которые могут способствовать предупреждению уголовной преступности. Основная его работа - организация сотрудничества по конкретным уголовным делам путем приема, анализа и передачи информации от НЦБ и для них. Каждое НЦБ поддерживает постоянные связи со своими правоохранительными органами, а на международном уровне - с НЦБ других стран и с Генеральным секретариатом Интерпола.

Ядром деятельности Интерпола является I-24/7 – глобальная система полицейской коммуникации, позволяющая странам-участницам обмениваться служебной информацией и получать оперативный доступ к важнейшим базам данных³³. В Интерполе используется система цветового кодирования международных уведомлений о поиске, аресте или данных о лицах, скрывающихся от правосудия, и других преступниках. Кроме того, она применяется для распространения сведений о новых планах и методах работы и служит в качестве системы раннего оповещения. В настоящее время с помощью сети I-24/7 осуществляются связи НЦБ всех стран-участниц. Планируется расширить прямой доступ к ней всем действующим отделам по борьбе с киберпреступностью, что позволит им пользоваться «Руководством по расследованию преступлений в области информационных технологий», разработанным Интерполом.

В рамках Глобальной инициативы безопасности (Global Security Initiative), выдвинутой Интерполом, была разработана новая «киберинициатива». В настоящее время осуществляется ее реализация. Программа содержит пять направлений деятельности:

1. Потенциальные возможности криминалистики в расследовании преступлений.

³³ Отупаль Б. Киберугрозы и ответные меры Интерпола [Электронный документ]// Электронный информационный бюллетень Сyбex по борьбе с киберпреступностью — ENAC, 2009, № 3, Стр. 18-21. URL: http://polis.osce.org/library/view?item_id=3634&attach_id=2797 (дата обращения 06.12.2010).

2. Обучение и развитие.
3. Комплексное информирование о киберпреступлениях (выпуск информационных бюллетеней, своевременное предупреждение, уведомления).
4. Партнерство государства и частного сектора.
5. Исследование новых технологий.

Работа по реализации «киберинициатив» будет производиться в тесном сотрудничестве с другими организациями, в частности Международным многосторонним партнерством против киберпреступности (IMPACT), Международной организацией по работе с компьютерными доказательствами (International Organization on Computer Evidence, IOCE), Ассоциацией по расследованию преступлений в сфере высоких технологий (High Tech Crime Investigation Association, HTCIA), Центром по борьбе с киберпреступлениями при образовательско-исследовательской сети совершенствования (2Centr), научным сообществом и частным бизнесом.

Интерпол был одной из первых международных организаций, которая провела встречу экспертов по теме киберпреступности. Она состоялась в 1995 г. в Лионе (Франция)³⁴. С того времени Интерпол приложил много усилий, чтобы помочь полиции и другим правоохранительным органам всего мира упрочить свои возможности в противодействии киберпреступности. Для достижения этой цели Интерполом была создана система контрольных пунктов (Interpol National Central Reference Points, NCRP), смысл работы которой состоит в оказании помощи участникам организации на постоянной основе. Сейчас NCRP насчитывает более 100 пунктов во всем мире. Цель этой структуры – дать возможность органам полиции мгновенно найти нужных специалистов в другой стране и незамедлительно получить помощь в касающихся компьютеров расследованиях и в сборе доказательств.

18.5. Структуры по реагированию на инциденты информационной безопасности

Компьютерная группа реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT), другие названия: Команда компьютерной безопасности по реагированию на инциденты (Computer Security Incident Response Team, CSIRT), или Компьютерная команда экстренной готовности (Computer Emergency Readiness Team) — названия экспертных групп, которые занимаются инцидентами в компьютерной и интернет-безопасности. Название CERT является историческим обозначением первой группы в университете Карнеги—Меллона. Аббревиатуру CERT подхватили другие команды во всём мире. В англоязычных странах мира некоторые команды взяли название CSIRT. История CERT тесно связана с борьбой против сетевых червей. Когда прибывают новые технологии, её использование невозможно в следующем - IBM VNET была закрыта из-за первого червя. Червь попал в сеть Интернета 3 ноября 1988 года, когда так называемый червь Морриса парализовал ра-

³⁴ Вердельо П. Киберпреступления и электронные доказательства их совершения [Электронный документ] // Электронный информационный бюллетень Cybex по борьбе с киберпреступностью — ENAC, 2009, № 1, Стр. 1-6. URL: http://polis.osce.org/library/view?item_id=3628&attach_id=2739 (дата обращения 01.12.2010).

боту интернет-узлов. Это привело к формированию первого Computer Emergency Response Team в университете Карнеги — Меллона по контракту пр-ва США.

При массовом развитии в области использования информационных и коммуникационных технологий в последующие годы, теперь общий термин "CERT/CSIRT" относится к важной части структуры большинства крупных организаций.

Международными координационными центрами CERT являются CERT/CC (www.cert.org) и FIRST (www.first.org).

В ЕС большинство групп CERT были локально созданы университетами и крупными ИТ-компаниями. Большинство стран-членов ЕС не имеют национального координационного центра и сотрудничают через общеевропейский TF-CSIRT (Task Force - Collaboration Security Incident Response Teams). Есть около 100 команд CERT, аккредитованных на TF-CSIRT в 2006 году. TF-CSIRT также запускает FIRST (Forum of Incident Response and Security Teams) для совещаний по вопросам команд CERT.

RU-CERT (www.cert.ru) – российский центр реагирования на компьютерные инциденты. Основная задача центра - снижение уровня угроз информационной безопасности для пользователей российского сегмента сети Интернет. В этих целях RU-CERT оказывает содействие российским и зарубежным юридическим и физическим лицам при выявлении, предупреждении и пресечении противоправной деятельности, имеющей отношение к расположенным на территории Российской Федерации сетевым ресурсам.

RU-CERT осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории РФ. Для реализации поставленных задач RU-CERT взаимодействует с ведущими российскими ИТ компаниями, субъектами оперативно-розыскной деятельности, органами государственной власти и управления РФ, зарубежными центрами реагирования на компьютерные инциденты и другими организациями, осуществляющими свою деятельность в области компьютерной и информационной безопасности.

RU-CERT входит в состав международных объединений CSIRT/CERT центров (FIRST, Trusted Introducer) и, официально в рамках данных объединений, выполняет функции контактной стороны в РФ.

18.6. Перечень международных договоров

462. "Европейская конвенция о выдаче" от 13.12.1957 (Конвенция ратифицирована РФ – ФЗ от 25.10.1999 N 190-ФЗ. Конвенция вступила в силу для России 28.10.1999).
463. "Европейская конвенция о взаимной правовой помощи по уголовным делам" от 20.04.1959 (СЕД N 30) (Конвенция ратифицирована РФ – ФЗ от 25.10.1999 N 193-ФЗ. Конвенция вступила в силу для России 28.10.1999).
464. "Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам" (Минск, 22.01.1993. Россия ратифи-

цировала Конвенцию (ФЗ от 04.08.1994 N 16-ФЗ). Конвенция вступила в силу для России 10.12.1994).

465. "Договор между РФ и США о взаимной правовой помощи по уголовным делам" (Подписан в г. Москве 17.06.1999. Россия ратифицировала договор – ФЗ от 03.11.2000 N 133-ФЗ. Договор вступил в силу 31.01.2002).
466. "Соглашение о сотрудничестве по пресечению правонарушений в области интеллектуальной собственности" (Москва, 06.03.1998. Соглашение вступило в силу для России 12.11.2001).
467. "Конвенция Организации Объединенных Наций против транснациональной организованной преступности" (Принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН).
468. "Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации" (Минск, 01.06.2001. Россия ратифицировала Соглашение с оговоркой (ФЗ от 01.10.2008 N 164-ФЗ). Соглашение вступило в силу для России 17.10.2008).
469. "Конвенция о преступности в сфере компьютерной информации" (ETS N 185) (Будапешт, 23.11.2001. Россия приняла решение подписать Конвенцию с заявлением (Распоряжение Президента РФ от 15.11.2005 N 557-рп). Последнее утратило силу (Распоряжение Президента РФ от 22.03.2008 N 144-рп)).
470. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (ETS N 189. Страсбург, 28.01.2003).
471. Конвенция ООН об использовании электронных сообщений в международных договорах (Нью-Йорк, 23.11.2005. Россия приняла решение подписать Конвенцию. (Распоряжение Пр-ва РФ от 27.12.2006 N 1821-р)).
472. Рамочное решение Совета ЕС 2005/222/ПВД от 24.02.2005 об атаках на информационные системы. (опубликовано в официальном журнале ЕС № L 69/67 от 16.03.2005).
473. Директива Европарламента и Совета Европы № 2006/24/ЕС от 15.03.2006 [Электронный документ]. (опубликовано в официальном журнале ЕС № L 105/54 от 13.04.2006).

18.7. Перечень национальных нормативно-правовых актов

474. Указ Президента РФ от 30.07.1996 N 1113 "Об участии РФ в деятельности Международной организации уголовной полиции - Интерпола".
475. Пост. Пр-ва РФ от 14.10.1996 N 1190 "Об утверждении Положения о Национальном центральном бюро Интерпола".

Алфавитный указатель юридических терминов

Административная ответственность.....	92	Комитет по информационной политике, информационным технологиям и связи ГД РФ.....	35
Административное наказание.....	92	Комитет по обороне и безопасности СФ РФ	35
Административное правонарушение	92	Коммерческая тайна	55
Всемирная встреча на высшем уровне по вопросам информационного общества	105	Компьютерная группа реагирования на чрезвычайные ситуации	109
Глобальная программа кибербезопасности	105	Контрольно-надзорные органы	34
Государственная комиссия по радиочастотам	39	Конфиденциальная информация	23
Государственная тайна.....	66	Криптографическая защита информации	22
Государственная фельдъегерская служба РФ	38	Лицензирование	83
Государственный орган.....	34	Материальная ответственность	91
Гражданско-правовая ответственность...91		Межведомственная комиссия по вопросам предоставления правительственной и специальной связи	38
Данные	15	Межведомственная комиссия по защите государственной тайны.....	38
Декларация о соответствии	84	Межведомственная комиссия по ИБ (в составе СовБеза)	36
Диспозитивный метод правового регулирования.....	18	Международное многостороннее партнерство против киберугроз	106
Дисциплинарная ответственность	92	Международный союз электросвязи	105
Документированная информация	18	Меры дисциплинарной ответственности 92	
Закон	11	Меры обеспечения информационной безопасности	18
Законодательная власть.....	34	Метод правового регулирования	18
Законодательство	11	Министерство внутренних дел.....	37
Законодательство РФ об информации, информационных технологиях и о защите информации	27	Министерство иностранных дел	37
Защита информации	21	Министерство культуры РФ.....	40
Императивный метод правового регулирования.....	18	Министерство обороны.....	37
Интерпол	108	Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.....	38
Информационная безопасность	21	Министерство связи и массовых коммуникаций РФ	38
Информационная система	18	Министерство юстиции	37
Информационная система персональных данных	62	Наказание административное	92
Информационное общество	16	Наказание уголовное	94
Информационное право	19	Нормативно-правовой акт	13
Информационно-телекоммуникационная сеть.....	18	Нормативный договор	13
Информационные отношения	18	Обладатель информации	26
Информационные ресурсы	17	Общедоступная информация	46
Информационные технологии	18	Общественные отношения	12
Информация	15, 26	Объект	12
Информация документированная.....	18	Объекты авторских прав	70
Информация конфиденциальная	23	Объекты информации, составляющей профессиональную тайну	60
Информация общедоступная.....	46	Объекты служебной тайны	54
Исполнительная власть	34	Оперативно-розыскная деятельность	98
Источники права	13	Оператор персональных данных	62
Киберпреступление	94		
Комиссия по информационной политике СФ РФ.....	35		
Комитет по безопасности ГД РФ	35		

Организационные меры обеспечения информационной безопасности 22	Сообщение 15
Организация Объединенных Наций 105	Специализированные нормы 12
Органы государственной власти 34	Способ защиты информации 18
Основные свойства информации 15	Средства защиты информации (относимой к гостайне) 66
Ответственность административная 92	Средство защиты информации 18
Ответственность дисциплинарная 92	Стандарт 84
Ответственность материальная 91	Степени секретности 66
Ответственность уголовная 94	Субъективное право 12
Ответственность юридическая 90	Субъекты 12
Отрасль права 12	Судебная власть 34
Персональные данные 62	Тайна коммерческая 55
Подотрасль права 13	Тайна профессиональная 60
Подтверждение соответствия 84	Тайна служебная 54
Права обладателя информации 26	Техническая защита информации 22
Правительственная комиссия по федеральной связи и информационным технологиям .. 38	Технический регламент 83
Право 11	Техническое регулирование 83
Правовая защита информации 22	Уголовная ответственность 94
Правовая норма 11	Уголовное наказание 94
Правовой институт 13	Удостоверяющий центр 80
Правовой обычай 13	Управление «К» МВД России 99
Правонарушение 90	Федеральная антимонопольная служба 40
Правоотношение 12	Федеральная служба безопасности РФ 36
Правоохранительные нормы 11	Федеральная служба охраны РФ 37
Правоохранительные органы 34	Федеральная служба по интеллектуальной собственности, патентам и товарным знакам 39
Предварительное следствие 97	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций 39
Предмет правового регулирования 13	Федеральная служба по техническому и экспортному контролю 36
Преступление 93	Федеральное агентство по информационным технологиям 39
Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации 46	Федеральное агентство по техническому регулированию и метрологии 40
Прокуратура РФ 101	Федеральное архивное агентство 40
Профессиональная тайна 60	Физическая защита информации 22
Регулятивные нормы 11	Экономический и Социальный Совет .. 105
Регуляторы 34	Экспертный совет по авторским и смежным правам 41
Результаты интеллектуальной деятельности 69	Электронная цифровая подпись 80
Санкции 91	Электронное сообщение 80
Сведения 15	Электронный документ 80
Сертификация 84	Юридическая обязанность 12
Система защиты государственной тайны 66	Юридическая ответственность 90
Служба внешней разведки РФ 36	Юридический прецедент 13
Служебная тайна 54	Юрисдикционный процесс 90
Совет Безопасности РФ 36	
Совет по развитию информационного общества в РФ 36	
Содержание правоотношения 12	

Электронные ресурсы с источниками информационного права

№	Организация	Описание	Ссылка
1.	ООО "НПП "Гарант-Сервис"	Информационно-справочная база законодательства РФ	www.garant.ru
2.	ЗАО "Консультант Плюс"	Информационно-справочная база законодательства РФ	www.cons-plus.ru
3.	Консорциум "Кодекс"	Информационно-справочная база законодательства РФ	www.kodeks.net
4.	Организация Объединенных Наций (ООН)	Официальный сайт	www.un.org/ru/
5.	Международный союз электросвязи	Официальный сайт	www.itu.int/ru/
6.	ЮНЕСКО	Официальный сайт	www.unesco.ru
7.	Совет Европы	Официальный сайт. Информационный офис в России	www.coe.int www.coe.ru
8.	Группа восьми (G8)	Информационный центр G8 Университета Торонто	www.g8.utoronto.ca
9.	Интерпол	Официальный сайт	www.interpol.int
10.	Организация по безопасности и сотрудничеству в Европе (ОБСЕ)	Официальный сайт. (ОБСЕ издает электронный информационный бюллетень Сувех по борьбе с киберпреступностью)	www.osce.org/ru/
11.	Бюро по демократическим институтам и правам человека ОБСЕ	База международных правовых актов и внутреннего законодательства стран ОБСЕ	www.legislationline.org/ru
12.	Организация по Экономическому Сотрудничеству и Развитию (ОЭСР)	Официальный сайт	www.oecd.org
13.	Форум Азиатско-тихоокеанского экономического сотрудничества (АТЭС)	Официальный сайт	www.apec.org
14.	МОО "Информация для всех"	База открытых договоров и концепций международных межправительственных организаций	www.ifap.ru/ofdocs/
15.	Исполнительный комитет СНГ	Единый реестр правовых актов СНГ	www.cis.minsk.by

16.	Органы государственной власти России	Информация об органах федеральной власти РФ и органах власти субъектов РФ	www.gov.ru
17.	Судебная система РФ	Государственная автоматизированная система Российской Федерации «Правосудие»	www.sudrf.ru
18.	Управление «К» МВД России	Информация об Управлении «К» на официальном сайте МВД России	www.mvd.ru/ struct/upravleniek/
19.	Государственная публичная научно-техническая библиотека России	Электронный каталог с выходными данными всех издаваемых в России книг и журналов	www.gpntb.ru
20.	Федеральное агентство по техническому регулированию и метрологии	Каталог актуальных стандартов ГОСТ	www.gost.ru/wps/portal/ pages.CatalogOfStandarts/
21.	Научный центр правовой информации при Министерстве юстиции РФ	Полнотекстовая база данных по действующему законодательству РФ «Эталон»; Подсистема «Федеральный регистр» Единой системы информационно-телекоммуникационного обеспечения; Автоматизированная информационная система «Учет некоммерческих и религиозных организаций»	www.scli.ru/bd/
22.	Министерство связи и массовых коммуникаций РФ	Государственные услуги. Справочно-информационный портал	www.gosuslugi.ru

Учебное издание

Парошин Алексей Анатольевич

Нормативно-правовые аспекты защиты информации

Учебное пособие

В авторской редакции

Компьютерный набор и верстка А.А. Парошин

Технический редактор А.К. Мухаматинова

Подписано в печать 08.12.2010

Формат 60x84 $\frac{1}{16}$. Усл. печ. л. 7,25; уч-изд. л. 5,47

Издательство Дальневосточного федерального университета

690950, г. Владивосток, ул. Октябрьская, 27

Отпечатано средствами копировально-множительной
техники ИМиКН ДВФУ

690950, г. Владивосток, ул. Октябрьская, 27