# Правовое обеспечение информации и функционирования корпоративных информационных систем в Российской Федерации

Степанова Галина Ананьевна

**Аннотация**: в статье определяется понятие информации и формы её существования. Рассматриваются структура правовой защиты и правовые режимы доступа к информации, а так же законодательный и локальный уровни правового обеспечения информации и функционирования корпоративных информационных систем в РФ.

## 1. Общие положения

Информация определяется как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1]. Объектом правового регулирования могут быть конкретные формы существования информации:

- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- правовая защита информации — законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Интерес к вопросам защиты информации повышается, что связано с возрастанием роли информационных ресурсов в конкурентной борьбе, расширением использования сетей, а, следовательно, и несанкционированного доступа к хранимой и передаваемой информации. Правовая защита информации как ресурса признана на международном, государственном уровне и регулируется соответствующими законодательными и

правовыми нормами государств и внутренними регламентами организаций разработчиков/пользователей. Структура правовой защиты показана на рис.1.

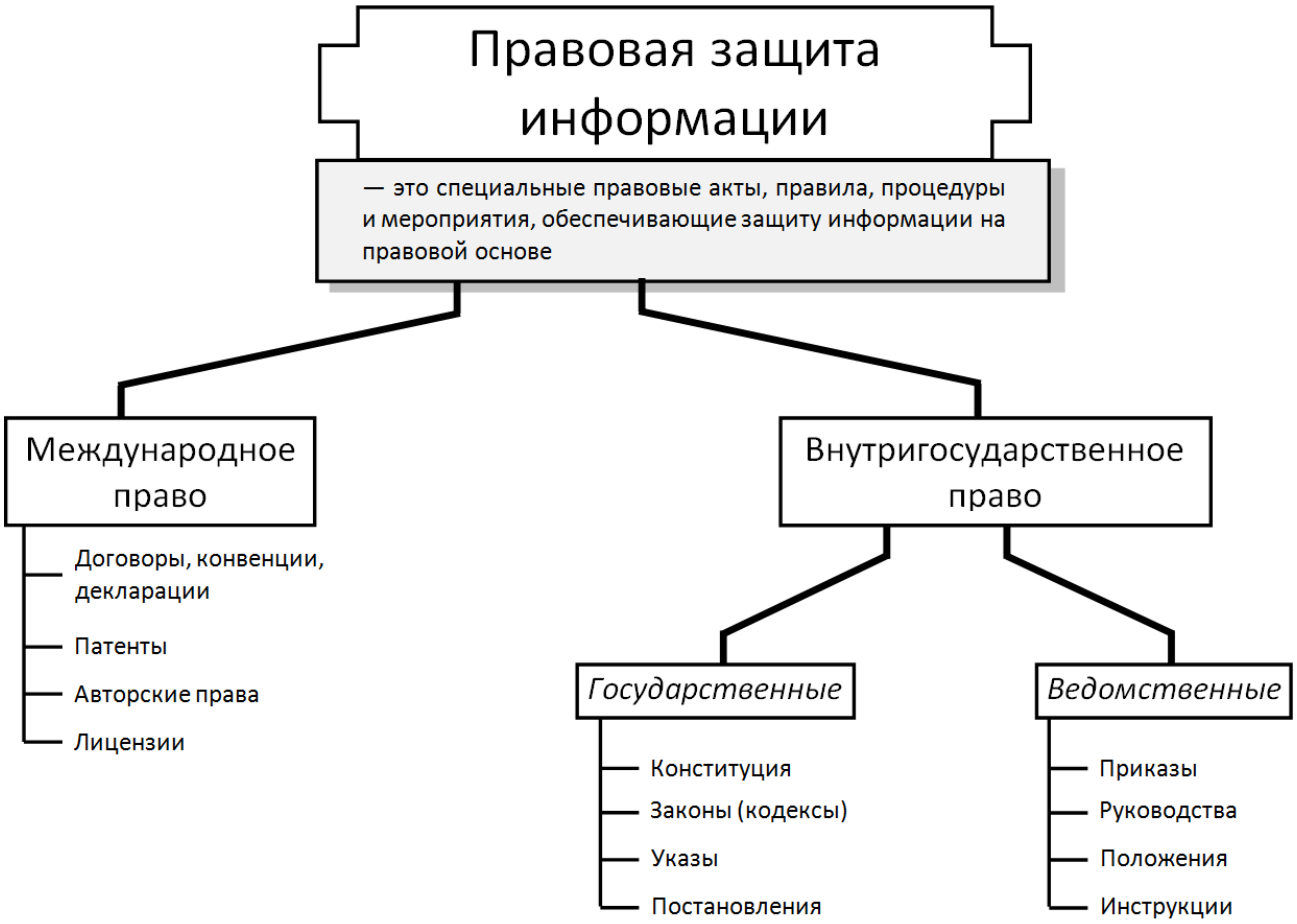


**Рис.1.** *Структура правовой защиты*

На стадии накопления и преобразования информации и формирования информационных ресурсов действует соответствующий раздел информационного права (правового обеспечения), включающий следующие направления:

- общие вопросы информационного законодательства;
- правовая информация;
- персональные данные;
- библиотечное дело;
- статистическая информация;
- международный обмен информацией;
- архивы.

Множество информационных объектов информационного права подразделяется на две категории – общедоступные и с ограниченным доступом. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не может быть ограничен в соответствии с действующим законодательством (например, информация о состоянии окружающей среды, деятельности государственных органов и т.п.). В свою очередь, информация с ограниченным доступом считается конфиденциальной, включая государственную, служебную, профессиональную (банковская, нотариальная и т.п.), коммерческую тайны, персональные данные и другие виды тайн.

Информация из любой области знаний и деятельности в принципе является открытой и общедоступной, если законодательством не предусмотрено ограничение доступа к ней в установленном порядке. Законами РФ определены режимы доступа к информационным ресурсам и порядок их использования (рис.2).


**Рис.2.** *Правовые режимы доступа к информации*

Обладателем информации в Российской Федерации могут выступать как физические и юридические лица, так и субъекты РФ, муниципальные образования и Российская Федерация. Обладатель вправе самостоятельно разрешать или ограничивать доступ к своей информации. Информационные системы (ИС) по масштабу подразделяются на следующие группы:

- одиночные;
- групповые;
- корпоративные.

Одиночные ИС реализуются на автономном персональном компьютере. Такая система может содержать несколько простых приложений, связанных общим информационным фондом, и рассчитана на работу одного пользователя или группы пользователей, разделяющих по времени одно рабочее место. Подобные приложения создаются с помощью так называемых настольных или локальных систем управления базами данных (СУБД). Среди локальных СУБД наиболее известными являются Clarion, Clipper, FoxPro, Paradox, dBase и Microsoft Access.

Групповые ИС ориентированы на коллективное использование информации членами рабочей группы и чаще всего строятся на базе локальной вычислительной сети. При разработке таких приложений используются серверы баз данных (называемые также SQL-серверами) для рабочих групп. Существует довольно большое количество различных SQL-серверов, как коммерческих, так и свободно распространяемых. Среди них наиболее известны такие серверы баз данных, как Oracle, DB2, Microsoft SQL Server, InterBase, Sybase, Informix.

Корпоративные ИС (КИС) ориентированы на крупные компании и могут поддерживать территориально разнесенные узлы или сети. В основном они имеют иерархическую структуру из нескольких уровней. Для таких систем характерна архитектура клиент-сервер со специализацией серверов или же многоуровневая архитектура. При разработке таких систем могут использоваться те же серверы баз данных, что и при разработке групповых информационных систем. Однако в крупных информационных системах наибольшее распространение получили серверы Oracle, DB2 и Microsoft SQL Server.

Правовое обеспечение функционирования информационных систем – совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации. Главной целью правового обеспечения функционирования информационных систем, в том числе и корпоративных, является укрепление законности использования информационных ресурсов, обеспечение информационной безопасности отдельных граждан, предприятий, организаций и в целом национальной безопасности страны. Регулирует отношения, возникающие при:

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

Правовое обеспечение функционирования информационных систем в Российской Федерации осуществляется путем законодательной поддержки на государственном уровне (законодательный уровень) и на уровне договорных отношений разработчика и заказчика в рамках заключаемых договоров на разработку и создание информационных систем (локальный уровень). Исходя из чего, в правовом обеспечении функционирования информационных систем в РФ можно выделить:

- общую часть, регулирующую функционирование любой информационной системы (законодательный уровень);
- локальную часть, регулирующую функционирование конкретной системы при разработке информационных систем (локальный уровень) - договорной уровень; внутренние нормативные акты организации (стандарты и регламенты разработчика/пользователя ИС).

В состав правового обеспечения законодательного уровня входят: Конституция РФ, законы, указы, постановления государственных органов власти, приказы, инструкции и другие нормативные документы министерств, ведомств, организаций, местных органов власти [2].

Правовое обеспечение этапов разработки информационной системы (локальный уровень) включает нормативные акты, связанные с договорными отношениями разработчика и заказчика ИС и правовым регулированием отклонений от договора; внутренние стандарты, а также регламенты информационной безопасности организации. Регулирование вопросов правового обеспечения этапов разработки и функционирования информационной системы (локальный уровень) включает в том числе:

- статус информационной системы;
- права, обязанности и ответственность персонала;
- правовые положения отдельных видов процесса управления;
- порядок создания и использования информации и другие.

На отношения в информационной сфере локального уровня распространяются нормы административного, гражданского, уголовного, трудового законодательства РФ.

## 2.Законодательный уровень правового обеспечения информации и функционирования корпоративных информационных систем в РФ

В таблице 1 приведены статьи из Конституции Российской Федерации о нормах, связанных с информацией.

**Таблица 1**. *Нормы, связанные с информацией*

| Номер статьи Конституции РФ | Содержание статьи Конституции РФ |
|---|---|
| Статья 15 | 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. |
| Статья 24 | Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. |
| Статья 29 п.4 | Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом. |
| Статья 44 | Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом. |

Условная классификация национальных правовых актов в информационной сфере приведена в таблице 2. Следует использовать в работе нижеуказанные ФЗ и нормативные акты в последней их редакции.

**Таблица 2**. Законодательство РФ в информационной сфере

| Область правового регулирования | Основные законодательные акты |
|---|---|
| Основы информационной безопасности | ▪ «Доктрина информационной безопасности Российской Федерации». (№Пр.1895 от 09.09.2000 г.).<br>▪ ФЗ «Об информации, информационных технологиях и |

| Область правового регулирования | Основные законодательные акты |
|---|---|
| | защите информации» № 149-ФЗ от 27.07.2006 г. |
| Обеспечение электронного документооборота | ▪ ФЗ «Об электронной подписи» №63-ФЗ от 23.06.2016 г.<br>▪ Гражданский кодекс РФ. Часть 4. |
| Правовые режимы доступа к информации, различные виды тайн | ▪ ФЗ «О государственной тайне» (№5485-1 от 21.07.93 г.).<br>▪ ФЗ «О коммерческой тайне» (№98-ФЗ от 29.07.2004 г.).<br>▪ ФЗ «О персональных данных» (№152-ФЗ от 27.07.2006 г.).<br>▪ ФЗ «О банках и банковской деятельности» от 02.12.1990 г. N 395-1.<br>▪ Таможенный, налоговый, гражданский, уголовный, административный, трудовой кодексы РФ, указы Президента РФ, утверждающие перечни сведений конфиденциального характера и сведений, отнесенных к государственной тайне, архивное законодательство РФ. ФЗ от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации". |
| Производство и использование систем защиты информации | ▪ ФЗ «О федеральных органах правительственной связи и информации» ФОПСИИ.<br>▪ ФЗ «О лицензировании отдельных видов деятельности».<br>▪ Постановления Правительства РФ о сертификации средств защиты информации и лицензировании деятельности в области защиты информации. |
| Защита авторских и имущественных прав разработчиков информационных систем | ▪ Гражданский кодекс РФ. Часть 4. |

Характеристика основных национальных правовых актов РФ в информационной сфере приведены в таблицах 3 и 4.

**Таблица 3.** *ФЗ «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006 г.*

| Объекты регулирования | Принципы правового регулирования | Законодательная база правового регулирования | Ответственность за правонарушения |
|---|---|---|---|

| Объекты регулирования | Принципы правового регулирования | Законодательная база правового регулирования | Ответственность за правонарушения |
|---|---|---|---|
| Регулирует:<br><br>▪ отношения, связанные с реализацией конституционного права на информацию;<br>▪ отношения, связанные с применением информационных технологий;<br>▪ отношения, связанные с обеспечением защиты информации. | ▪ свобода поиска, получения, передачи, производства и распространения информации любым законным способом [3];<br>▪ установление ограничений доступа к информации только федеральными законами [3];<br>▪ открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами [3];<br>▪ равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации [3];<br>▪ обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации [3];<br>▪ достоверность информации и своевременность ее предоставления;<br>▪ неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия [4];<br>▪ недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий | Первая группа:<br><br>▪ Конституция Российской Федерации;<br>▪ Международные договоры РФ;<br>▪ Федеральные законы и другие нормативные акты, регулирующие отношения по использованию информации федеральных законов.<br><br>Вторая группа:<br><br>▪ Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации.<br>▪ Закон РФ от 27 декабря 1991 г. N 2124-I "О средствах массовой информации".<br><br>Третья группа:<br><br>▪ Законодательство об архивном деле в РФ. | Дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством РФ. |

| Объекты регулирования | Принципы правового регулирования | Законодательная база правового регулирования | Ответственность за правонарушения |
|---|---|---|---|
| | для создания и эксплуатации государственных информационных систем не установлена федеральными законами. | | |

**Таблица 4.** *ФЗ «О персональных данных» №152-ФЗ от 27.07.2006 г.*

| Объекты регулирования | Принципы правового регулирования | Законодательная база правового регулирования | Ответственность за правонарушения |
|---|---|---|---|
| Регулируются: отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами местного самоуправления, иными муниципальными органами юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных | ▪ законность целей и способов обработки персональных данных и добросовестности;<br>▪ соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;<br>▪ соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;<br>▪ достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;<br>▪ недопустимость объединения созданных | ▪ Конституция Российской Федерации;<br>▪ Международные договоры РФ, в т.ч. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.);<br>▪ ФЗ «О персональных данных» (№152-ФЗ от 27.07.2006 г.). и нормативные акты к нему. | ▪ Дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством РФ [5].<br>▪ Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с |

| Объекты регулирования | Принципы правового регулирования | Законодательная база правового регулирования | Ответственность за правонарушения |
|---|---|---|---|
| без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным. | для несовместимых между собой целей баз данных информационных систем персональных данных. | | настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков. |

Кроме того, порядок использования информационных технологий и средств защиты информации в процессе создания информационных ресурсов в Российской Федерации регламентируется:

- Национальными стандартами – ФСТЭК России (ГОСТы) и сертификатами ФСБ. Для государственных учреждений соблюдение этих стандартов обязательно, для коммерческих организаций – носит рекомендательный характер. Тем не менее, ведущие российские компании-потребители склонны прислушиваться к требованиям государства, в том числе и в вопросах защиты своей информации. Указанные стандарты сейчас используются практически во всех крупных организациях, а также в средних и мелких, для которых политики информационной безопасности и системы защиты информации разрабатывались специализированным компаниям.

- Международными стандартами. На сегодня востребованы в России международные стандарты безопасности (ISO 17799, 27001, 13335 и 15408), приняты их российские аналоги (ГОСТ Р ИСО/МЭК 17799-2005, ГОСТ Р ИСО/МЭК 27001-2007, ГОСТ Р ИСО/МЭК ТО 13335-5-2006, ГОСТ Р ИСО/МЭК 15408-2002).
- Отраслевыми стандартами. Кроме нормативных документов, регулирующих использование решений в области информационной безопасности, в РФ существуют отраслевые стандарты. В частности, при построении информационных систем в финансовой сфере применяются стандарты Центрального Банка России «Обеспечение информационной безопасности организаций банковской системы РФ» (СТО БР ИББС-1.0-2006), информационные системы топливно-энергетического комплекса требуют ссылки на ОСТы Газпрома и т.д.
- Внутренними стандартами и регламентами безопасности организации. Российские компании, заинтересованные в повышении эффективности своей работы и снижении издержек, ориентируясь на мировой опыт, разрабатывают внутренние нормативы, регламентирующие организацию информационных процессов и обеспечение их безопасности. Польза от внутренних стандартов и регламентов безопасности наиболее очевидна в крупных и территориально-распределенных организациях.

Нарушение требований законодательства РФ в области информационных ресурсов и информационных технологий влечет за собой административную, гражданско-правовую и уголовную ответственность как отдельных физических лиц и работников организаций, так и организаций разработчиков/пользователей информационных систем (юридических лиц).

Иерархия соблюдения нормативных правовых актов, стандартов и регламентов в области информационной безопасности в РФ показана на рис.3.

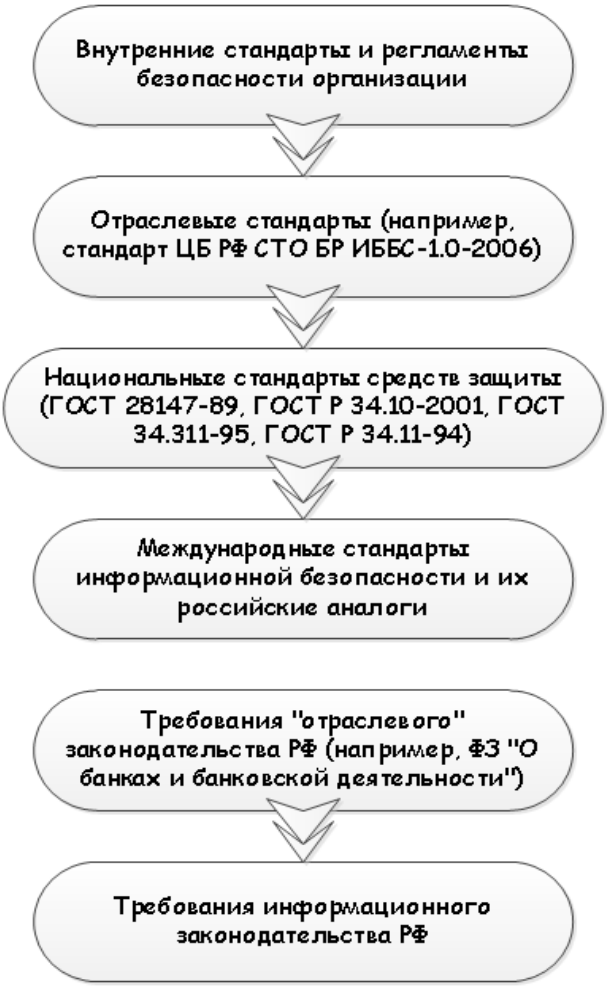


**Рис.3.** *Иерархия стандартов и регламентов информационной безопасности*

## 2.1. Административная ответственность в информационной сфере

Определена гл. 13 «Административные правонарушения в области связи и информации» КоАП РФ:

- ст. 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- ст. 13.12. Нарушение правил защиты информации;
- ст. 13.13. Незаконная деятельность в области защиты информации;
- ст. 13.14. Разглашение информации с ограниченным доступом и др.

За совершение административных правонарушений в информационной сфере установлены и применяются, как правило, следующие виды административных наказаний:

- предупреждение;
- административный штраф;
- приостановление деятельности на определенный срок;
- конфискация орудия совершения или предмета административного правонарушения.

Административно-правовые санкции установлены, кроме того (гл. 5 КоАП) «Административные правонарушения, посягающие на права граждан»), за нарушение конституционных прав граждан в информационной сфере (ст. 29 Конституции РФ).

## 2.2.Гражданско-правовая ответственность в информационной сфере

Меры гражданско-правовой ответственности предусмотрены в порядке и положениях ГК РФ и информационного законодательства, так согласно п.3 ст. 969 ГК РФ определяет, что компенсация морального вреда осуществляется в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию. Компенсация морального вреда выплачивается в денежной форме. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Гражданско-правовую ответственность за правонарушения информационного законодательства можно разделить на договорную и внедоговорную. Договорная ответственность возникает при нарушении условий договора, в которых предусмотрены санкции прямо не обеспеченные нормами законодательства.

Внедоговорная ответственность возникает при причинении личности потерпевшего или его имуществу вреда, который не связан с исполнением договорных обязательств.

## 2.3.Уголовная ответственность за преступления в информационной сфере

Уголовная ответственность в информационной сфере может наступить в случаях, предусмотренных Уголовным кодексом РФ. Уголовная ответственность является важным элементом в системе мер правового обеспечения информационной

безопасности, зашиты прав граждан, общества и государства в информационной сфере. Действующее законодательство содержит группу норм, предусматривающих уголовную ответственность за информационные преступления. В действующем Уголовном кодексе РФ из всего объема информационных отношений, подлежащих специальной охране, выделены отношения, возникающие в области компьютерной информации, объединены в главе 28 УК РФ, где содержатся нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие ответственность за их совершение. Такие нормы появились в российском законодательстве впервые. К уголовно наказуемым отнесены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

Уголовная ответственность за преступления в сфере компьютерной информации и информационных систем (Уголовный кодекс РФ (гл. 28):

- неправомерный доступ к компьютерной информации (ст. 272);
- создание, использование и распространение вредоносных программ для ЭВМ (ст. 273);
- нарушение правил эксплуатации ЭВМ, систем или сетей ЭВМ (ст. 274).

Практически все подобные преступления относятся к преступлениям средней тяжести, т.е. их максимальная наказуемость в виде лишения свободы не превышает 5 лет. Исключением является лишь создание, использование и распространение вредоносных программ для ЭВМ, повлекшее по неосторожности тяжкое последствие, которое наказывается лишением свободы на срок от 3 до 7 лет и поэтому относится к тяжким преступлениям. Уголовная ответственность предусмотрена также и за сбор и использование сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), нарушение авторских и смежных прав (ст. 146 и 180 УК РФ).

## 3. Локальный уровень правового обеспечения информации и функционирования корпоративных информационных систем в РФ

Локальный уровень правового обеспечения функционирования корпоративных информационных систем представлен двумя группами документов:

- внутренние стандарты и регламенты информационной безопасности организации;

- нормативные акты, связанные с договорными отношениями разработчика и заказчика информационных систем и правовым регулированием отклонений от договора.

Обеспечение информационной безопасности организации может быть регламентировано следующими документами:

- регламент обеспечения информационной безопасности. Включает формулировку целей и задач обеспечения информационной безопасности, перечень внутренних регламентов по средствам защиты информации и положение об администрировании распределенной информационной системы компании. Доступ к регламенту ограничен руководством организации и руководителем отдела автоматизации;
- регламенты технического обеспечения защиты информации. Документы являются конфиденциальными, доступ ограничен сотрудниками отдела автоматизации и вышестоящим руководством;
- регламент администрирования распределенной системы защиты информации. Доступ к регламенту ограничен сотрудниками отдела автоматизации, отвечающими за администрирование информационной системы и вышестоящим руководством. Основная цель всех предпринимаемых мероприятий в области обеспечения информационной безопасности заключается в защите интересов организации, так или иначе связанных с информационными ресурсами, которыми оно располагает.

Правовое обеспечение договорных взаимоотношений разработчика и заказчика информационных систем регулируется гражданским законодательством РФ (ГК РФ) и внутренними регламентами организации.

Правовое регулирование договоров по купле/продаже, созданию и сопровождению информационных систем осуществляется путем регламентирования порядка заключения договоров, исполнения сторонами принятых на себя обязательств, а также ответственности за неисполнение и/или ненадлежащее исполнение таких обязательств.

В соответствии со ст. 422 ГК РФ Договор должен соответствовать обязательным для сторон правилам, установленным законом и иными правовыми актами (императивным нормам), действующим в момент его заключения. После того как стороны определили свои обязательства, оговариваются меры, которые может предпринять каждая из сторон для защиты своих интересов, если другая не

выполнила своих обязательств. Когда речь идет о последствиях нарушения договора, в первую очередь имеют в виду предусмотренные законом меры ответственности. Общие положения об ответственности содержатся в гл. 25 ГК РФ. Они должны применяться с учетом положений ст. 15 ГК РФ о возмещении убытков и ст. 330—333 ГК РФ о неустойке. Закон предусматривает гражданско-правовую ответственность за неисполнение или ненадлежащее исполнение обязательств в виде:

- возмещения убытков;
- уплаты неустойки;
- уплаты процентов за пользование чужими денежными средствами.

Рассмотрение споров по договорам, в том числе в сфере купли/продажи, созданию и сопровождению информационных систем между юридическими и физическими лицами, в соответствии с гражданским законодательством РФ возможно двумя способами:

- досудебным порядком;
- судебным порядком.

В случае не урегулирования спора в досудебном (претензионном) порядке спор разрешается в арбитражном суде по месту нахождения ответчика.

Кроме того, порядок заключения, сопровождения и сдачи работ по договорам купли/продажи информационных систем; созданию, сопровождению и пользованию ИС может/должен регламентироваться внутренними локальными правовыми актами организации в виде приказов, положений, регламентов и других внутренних распорядительных документов, которые подлежит обязательному исполнению сотрудниками/работниками организации разработчика/пользователя ИС.

## Литература

1. Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. - М: Юрайт, 2017. – 326 с.
2. В. М. Елин. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. – М: Московский институт государственного управления и права, 2016. - 184 с.
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ст. 3, п. 1 - 5. - URL: http://ivo.garant.ru/#/document/12148555/paragraph/26.

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ст. 3, п. 7. - URL: http://ivo.garant.ru/#/document/12148555/paragraph/32.
5. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" - URL: http://ivo.garant.ru/#/document/12148567.

## Выходные данные статьи

Степанова Г.А. Правовое обеспечение информации и функционирования корпоративных информационных систем в РФ // Корпоративные информационные системы. – 2019. – №4(8). – С. 33-49. – URL: https://corpinfosys.ru/archive/issue-8/74-2019-8-erplaw.

## Об авторе



**Степанова Галина Ананьевна** – эксперт по бухгалтерскому и налоговому учетам, а также МСФО. Принимала участие в проектах по слиянию и ликвидации структурных подразделений с точки зрения Российского учета, а также внедрения и автоматизации работы предприятия на основе продуктов 1С. Имеет более чем 25-и летний опыт работы в нефтяных и горнодобывающих компаниях. Электронная почта: mail@corpinfosys.ru