Модуль 3
ИНФОРМАЦИОННАЯ ЭТИКА И ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1
ИНФОРМАЦИОННАЯ ЭТИКА И ПРАВО

Информационная безопасность

Безопасность — это не только наука, которую надо изучать, не только мастерство, секреты которого надо постигать, но это и культура, которую надо воспитывать.

Безопасность является той сферой, с которой любой человек сталкивается на протяжении всей жизни, в той или иной форме, на том или ином участке профессиональной деятельности. Организация защиты не может быть уделом только профессионалов. Те, кто выступает в качестве пользователей, исполнителей, носителей защищаемых сведений, в отношении которых осуществляется физическая охрана, должны разбираться в вопросах безопасности не хуже тех, кто ее обеспечивает.[1]

В.Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность. По С.Ожегову, безопасность — это «состояние, при котором не угрожает опасность, есть защита от опасности». Сегодня появилось множество других определений безопасности, авторы которых исходят из разных критериев. Также полагают, что «безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно

обусловленными инновациями и свободное, соответствующее собственной природе и ею определяемое функционирование».

Начнем изучение этой темы с определений в терминологии информационной безопасности.

Информационная безопасность — механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

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

Исходя из Доктрины информационной безопасности Российской Федерации, следует, что:

- Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.
- Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.
- Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению инфор-

мационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.

Основными составляющими и аспектами информационной безопасности (которые не следует отождествлять с информационной безопасностью в целом) являются:

- Защита информации (в смысле охраны персональных данных);
- Компьютерная безопасность или безопасность данных;
- Защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий;
- Информационно-психологическая удовлетворенность потребностей граждан и защищенность от негативных информационно-психологических и информационно-технических воздействий.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что ***информационная безопасность*** есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Угрозы информационной безопасности

Под ***угрозой (threat)*** понимаются характеристики, свойства системы и окружающей среды, которые в соответствующих условиях могут вызвать появление опасного события.

Угроза — это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации *угрозы* называется ***атакой***, а тот, кто предпринимает такую попытку, — ***злоумышленником***. Потенциальные злоумышленники называются ***источниками угрозы***.

Существует три разновидности угроз:

1. ***Угроза нарушения конфиденциальности*** заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к

другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. ***Угроза нарушения целостности,*** которая включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации — это существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства — достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т. е. ее неискаженности.

3. ***Угроза отказа служб,*** возникающая всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации — свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Исходя из Доктрины информационной безопасности Российской Федерации, угрозы информационной безопасности Российской Федерации подразделяются на **следующие виды**:

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

- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Уровни информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих **уровней:**

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Направления защиты компьютерной информации

Основными целями и направлениями защиты данных провозглашаются предотвращение потери и искажения данных, несанкционированного использования, угрозы безопасности человеку и государству, защита прав субъектов информатизации. Защита должна производиться как в интересах держателей информации (собственников, владельцев, пользователей), так и людей, имеющих непосредственное отношение к ним (авторов, пациентов медицинских учреждений, коммерсантов и т. д.).

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

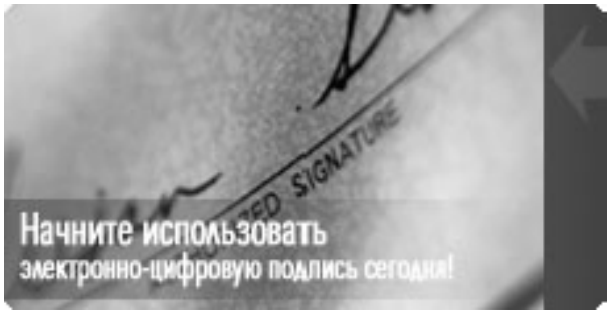
Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы.

Электронно-цифровая подпись

Электронно-цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов. Они могут использоваться при необходимости контроля с целью удостоверения, кто подписал электронный документ, а также при проверке, было ли содержание подписанного документа изменено. Рассмотрим подробнее нормативный документ об электронно-цифровой подписи. 10 января 2002 года Президентом был подписан закон «Об электронной цифровой подписи» номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года). Его роль поясняется в статье 1:

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.



Закон вводит следующие основные понятия (Статья 3):

- ***Электронный документ*** — документ, в котором информация представлена в электронно-цифровой форме.

- ***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.
- ***Владелец сертификата ключа подписи*** — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- ***Средства электронной цифровой подписи*** — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.
- ***Сертификат средств электронной цифровой подписи*** — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- ***Закрытый ключ электронной цифровой подписи*** — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- ***Открытый ключ электронной цифровой подписи*** — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

- ***Сертификат ключа подписи*** — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.
- ***Подтверждение подлинности электронной цифровой подписи в электронном документе*** — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.
- ***Пользователь сертификата ключа подписи*** — физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.
- ***Информационная система общего пользования*** — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.
- ***Корпоративная информационная система*** — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Согласно Закону, **электронная цифровая подпись в электронном документе равнозначна собственноручной подписи** в документе на бумажном носителе при одновременном соблюдении следующих **условий**:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет **сведения**, которые должен содержать **сертификат ключа подписи**:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Цифровые подписи могут применяться для любой формы документа, обрабатываемого электронным способом, например, при подписи электронных платежей, денежных переводов, контрактов и соглашений. Цифровые подписи могут быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой — для проверки подписи (открытый ключ). Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой имеющий к нему доступ может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Кроме того, очень важна защита целостности открытого ключа, которая обеспечивается при использовании сертификата открытого ключа

Следует уделять внимание выбору типа и качеству используемого алгоритма подписи и длине ключей. Необходимо, чтобы криптографические ключи, используемые для цифровых подписей, отличались от тех, которые используются для шифрования. При использовании цифровых подписей необходимо учитывать требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу.

Может потребоваться наличие специальных контрактов или других соглашений, чтобы поддерживать использование цифровых подписей в случаях, когда законодательство в отношении цифровых подписей недостаточно развито. Необходимо воспользоваться консультацией юриста в отношении законов и нормативных актов, которые могут быть применимыми в отношении предполагаемого использовании организацией цифровых подписей.

Тема 3.2
ОСНОВНЫЕ ЗАКОНЫ РОССИИ В ОБЛАСТИ КОМПЬЮТЕРНОГО ПРАВА

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Самое важное (и, вероятно, самое трудное) на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом развития современного общества, в частности, информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это может привести к снижению информационной безопасности.

Законодательство в сфере информационной безопасности в Российской Федерации начало развиваться только в начале девяностых годов прошлого столетия. Ряд законодательных актов довольно долго действовал в старых редакциях, часть документов утратили свою самостоятельность и были включены в Гражданский кодекс РФ. В рамках данной темы дается возможность проследить судьбу некоторых актуальных документов.

Одним из основных законов Российской Федерации является **Конституция**, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, 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. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 — право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации*.

В **Уголовном кодексе Российской Федерации** Глава 28 носит название «Преступления в сфере компьютерной информации», которая содержит три статьи:

- Статья 272. Неправомерный доступ к компьютерной информации;
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 272 УК РФ описывает ситуации неправомерного доступа к охраняемой законом компьютерной информации лицом или группами лиц, повлекшие за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Здесь описаны штрафные и уголовные меры за содеянное.

Статья 273 УК РФ знакомит с мерами пресечения действий в отношении создания программ для ЭВМ или внесения изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т. д.

Статья 138 УК РФ защищает конфиденциальность персональных данных и предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи интересны руководящие документы, выпущенные Федеральной службой по

техническому и экспортному контролю Российской Федерации, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно можно выделить документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В информационном обществе нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) — доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных) может представлять угрозу национальной безопасности (в том числе информационной безопасности), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Предлагаем ознакомиться с некоторыми важными нормативно-правовыми документами в области информационных технологий и информационной безопасности более подробно.

Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992г. № 3523—1). Закон «Об авторском праве и смежных правах» (от 09.07.1993г. № 5351—1 с последующим изменением и дополнением). Четвертая часть Гражданского кодекса РФ (от 18.12.2006г № 230-ФЗ). Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от 18.12.2006г. № 231-ФЗ)

Два важных документа — Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. № 3523—1) и Закон «Об авторском праве и смежных правах» (от 09.07.1993г. № 5351—1) были введены в действие с целью регулирования правовых норм в отношении авторского права и охране программ для ЭВМ. Законы работали самостоятельно до 1 января 2008 года, в связи с введением в действие ФЗ «О введении в действие части четвертой гражданского кодекса РФ» (от 18.12.2006 г. № 231-ФЗ).

Четвертая часть гражданского кодекса РФ (от 18.12.2006 г. № 230-ФЗ), в текстах которого прописаны нормы правовой охраны программ для ЭВМ и баз данных, затрагивает права на результаты интеллектуальной деятельности и средства индивидуализации (к которым и относятся программы для ЭВМ и базы данных); авторское право; права, смежные с авторскими; патентное право и т. д. Отсюда можно узнать, как используется авторское право, как оно действует, какие есть ограничения в использовании авторских прав, как составляются договора и документы по авторскому праву и охране программ для ЭВМ, какие санкции могут применяться относительно неправомерного использования авторского права и т. д.

Закон «О государственной тайне» (от 21.07.1993г. № 5485—1 с последующим изменением и дополнением)

Рассмотрим подробнее закон «О государственной тайне» (от 21.07. 1993г. № 5485—1 с последующим изменением и дополнением). Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О государственной тайне» (с изменениями и дополнениями от 6 октября 1997 года). В нем ***гостайна*** определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Согласно данному Закону, ***средства защиты информации*** — это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О Безопасности» и включает в себя настоящий закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Федеральный закон «О связи» (от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением)

Данный Федеральный закон впервые был принят в редакции от 16.02.1995г. за номером 15-ФЗ. В настоящее время имеют дело с редакцией от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением. Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Целями настоящего Федерального закона являются:

- создание условий для оказания услуг связи на всей территории Российской Федерации;

- содействие внедрению перспективных технологий и стандартов;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российским радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Статья 63 «Тайна связи» Главы 9 «Защита прав пользователей услугами связи» затрагивает проблему конфиденциальности передаваемой информации операторами связи.

Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006г. № 149-ФЗ)

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В настоящее время его название видоизменено и звучит следующим образом — «Об информации, информационных технологиях и защите информации». Закон в обновленном виде действует с 27 июля 2006г. за номером 149-ФЗ.

Настоящий Федеральный закон регулирует отношения, возникающие при:

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

В нем даются основные определения и намечаются направления развития законодательства в данной области.

Приведем основные определения согласно статье 2:

1) **информация** — сведения (сообщения, данные) независимо от формы их представления;

2) **информационные технологии** — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) **информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) **информационно-телекоммуникационная сеть** — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) **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;

6) **доступ к информации** — возможность получения информации и ее использования;

7) **конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) **предоставление информации** — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) **распространение информации** — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) **электронное сообщение** — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) **документированная информация** — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию — или в установленных, законодательством Российской Федерации случаях ее материальный носитель;

12) **оператор информационной системы** — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации прописаны в статье 3. Правовое регулирование отношений, возни-

кающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 16 носит название «Защита информации» и затрагивает следующие аспекты:

1. 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.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

А Статья 17 предусматривает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Исходя из того, что практические умения и навыки по указанным выше вопросам представляется целесообразным формировать в условиях, приближенных к жизненным, наиболее подходящим средством для этого являются ситуационные задачи, т. е. задачи, которые формулируются в виде описания жизненных ситуаций.

Для закрепления вышеизложенного материала предлагается проанализировать эти ситуации, выявить в них моменты правонарушений, обосновав выдержками из упомянутых выше нормативных документов, и по необходимости сделать выводы.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 3

Ситуационные задачи

Задача 1. Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Животные Крайнего Севера». Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.06 оформили свое авторство на данную информационную систему. В марте 2006 г. данный программный продукт был выпущен под авторством гражданина Андреева.

Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Решение. В данной ситуации есть нарушение авторского права граждан Серебренникова и Семенова, так как налицо факт выпуска программы для ЭВМ под чужим именем, что противоречит ст. 20 закона «О правовой охране программ для ЭВМ и баз данных».

Задача 2. Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю. Правомерно ли это?

Решение. Действия указанного лица в данной ситуации квалифицируются как противоправные на основании ст. 272, п. 2 УК РФ, так как очевиден факт превышения служебных полномочий и неправомерный доступ к компьютерной информации.

Задача 3. Определите, будет ли электронная подпись равнозначной собственноручной подписи, если подтверждена подлинность электронной цифровой подписи в электронном документе.

Решение. Электронная подпись не будет равнозначной собственноручной подписи только лишь при подтверждении подлинности электронной цифровой подписи в электронном документе, так как на основании ст. 4, п. 1 закона «Об электронной цифровой подписи» этого условия недостаточно.

Задача 4. Гражданин В. А. Мельников, автор и правообладатель электронной энциклопедии «Вокруг света», планировал сотрудничать с компанией «Видеотех», занимающейся тиражированием программных продуктов. Экземпляр электронной энциклопедии был передан в компанию для ознакомления. При этом договор о передаче компании «Видеотех» имущественных прав на программу составлен не был. В. А. Мельников предъявил судебный иск к компании «Видеотех», которая осуществила выпуск данного программного продукта. Какое решение вынесет суд и почему?

Решение. В данной ситуации суд вынесет решение в пользу гражданина Мельникова, так как имеет место быть нарушение его авторского права. Такое решение будет вынесено на основании соответствующей статьи ГК РФ, ввиду того, что налицо факт выпуска программы для ЭВМ без разрешения правообладателя.

Задача 5. Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки различным организациям на общую сумму 670 000 рублей.

Решение. Судебный иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им данной компании денежной компенсации будет удовлетворен, так как действия гражданина Р. И. Сизова в данной ситуации квалифицируются как противоправные на основании ст. 273, п. 2 УК РФ, ввиду того, что налицо распространение, вредоносных программ для ЭВМ, которое привело к тяжким последствиям.

Вопросы

1. Зачем нужны законодательные акты в информационной сфере?
2. Какой закон регламентирует права авторов программ и баз данных?
3. Какой закон регламентирует вопросы защиты информационных ресурсов? На какой закон вы сошлетесь, если вам будет нанесен ущерб путем использования информации, касающейся вашей частной жизни?
4. Какие действия уголовный кодекс классифицирует как преступления в компьютерной информационной сфере?
5. Появилось ли у вас желание после прочтения этого параграфа заняться производством и распространением компьютерных вирусов?
6. Какими положениями определяется правовой режим информационных ресурсов?

7. Какое условие является обязательным для включения информации в информационные ресурсы?
8. Когда документ приобретает юридическую силу?
9. Чем может подтверждаться юридическая сила документа, помимо собственноручной подписи?
10. Какими могут быть информационные ресурсы?
11. При каких условиях физические, юридические лица могут быть собственниками информационных ресурсов?
12. При каких условиях РФ и субъекты РФ могут быть собственниками информационных ресурсов?
13. При каких условиях государство имеет право выкупа документированной информации у физических и юридических лиц?
14. Имеет ли право собственник информационных ресурсов, принадлежащих к государственной тайне, распоряжаться ими? Если да, то на каких условиях?
15. Создает ли право собственности на средство обработки информации право собственности на информационные ресурсы?
16. Как подразделяются государственные информационные ресурсы?
17. По какой статье финансируется деятельность по формированию, накоплению и использованию информационных ресурсов?
18. Какие противоправные действия с компьютерной информацией со стороны граждан РФ отражены в УК РФ?
19. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный гражданином РФ, в результате которого произошли уничтожение, блокирование, модификация и (или) копирование информации?
20. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный гражданином РФ, в результате которого произошел сбой в работе ЭВМ, системы ЭВМ или их сети?
21. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный по предварительному сговору граждан РФ, в результате которого произошли уничтожение, блокирование, модификация и (или) копирование информации?
22. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный по предварительному сговору граждан РФ, в результате которого произошел сбой в работе ЭВМ, системы ЭВМ или их сети?

Используемые литература и ресурсы

1. Доктрина информационной безопасности Российской Федерации. (Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895) [Электронный ресурс]. — URL: http://www.scrf.gov.ru/documents/5.html

2. Галатенко В.А. Основы информационной безопасности. Дистанционный курс (с)INTUIT.ru: Интернет-Университет Информационных Технологий — дистанционное образование, 2003—2008 [Электронный ресурс]. — URL: http://www.intuit.ru/

3. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие, изд. 3-е, испр., доп. — М.: ФОРУМ, 2008. — 432 с.: ил. — (Профессиональное образование).

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. изд. 3-е — М.: Академический Проект — 2006. — 544 с.

5. Федеральный закон «Об электронной цифровой подписи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=72518;div=LAW;mb=LAW;opt=1;ts=AB736230098ADC672E8227AAFB97B9A8

6. Электронно-цифровая подпись — Что это такое? [Электронный ресурс]. — URL: http://www.digitalsign.ru/

7. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000 Information technology — Code of practice for information security management (IDT) Издание официальное. Москва. Стандартинформ, 2006.

8. ГОСТ Р 50922—2006 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения — сайт Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02-4212-8D58-3F1D91F314A0

9. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. — М.: Финансы и статистика, 2005. — 176 с.

10. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие — М.: Инфра-М, 2001. — 301 с.

11. Безбогов, А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. — Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. — 196 с.

12. Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=83483;fld=134;dst=100052

13. Федеральный закон «О государственной тайне» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=89782

14. Федеральный закон «О связи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=76690

15. Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=61798

16. Федеральный закон «О безопасности» [Электронный ресурс]. — URL: http://base.garant.ru/10136200.htm

17. Уголовный кодекс Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=93431

18. Конституция Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=2875

19. Официальный сайт Федеральной службы по техническому и экспортному контролю [Электронный ресурс]. — URL: http://www.fstec.ru/_razd/_ispo.htm

20. Блохина Е.В. Лекция по теме: «Правовые основы использования Интернет-ресурсов. Авторские права. Поиск информации в Интернете» [Электронный ресурс]. — URL: http://festival.1september.ru/articles/412857/

21. Расторгуев С.П. Основы информационной безопасности // Информатика и образование. — 2007. — № 8.

22. Семенова З.В. Углубленное изучение темы «Защита данных в информационных системах» // Информатика и образование. — 2004. — № 1.

23. Черкашина И. Ф. Изучение темы «Информационная безопасность» в курсе информатики // Информатика и образование. — 2007. — № 9.

24. Бачило И.Л. О законодательстве в информационной сфере отношений. [Электронный ресурс]. — URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/a11ec0af30c1cc6ec3256c4f00312cfb

25. Ефимова Л. Проблемы правовой защиты детей от информации, приносящей вред их здоровью и развитию, распространяемой в сети Интернет [Электронный ресурс]. — URL: http://www.medialaw.ru/publications/zip/156—157/1.htm