М.Т. ТУАЕВА

ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНОЕ ПОСОБИЕ

Владикавказ, 2021

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РСО-АЛАНИЯ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ВЛАДИКАВКАЗСКИЙ ТОРГОВО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНОЕ ПОСОБИЕ

Владикавказ
2021

Одобрено
предметно - цикловой комиссией математических и естественнонаучных дисциплин

Протокол № 3
От « 18 » ноября 2021г.

Председатель _____
И.С. Пархоменко

Составитель _____
М.Т. Туаева

Согласовано
Методист _____
З.А. Дзантиева

Утверждаю
Заместитель директора по УР
_____ И.М. Дзуцева
« 19 » ноября 2021 г.

Содержание

Введение 3
1. Основные права граждан, касающиеся вопросов обработки информации 5
2. Информация и ее свойства 8
3. Классификация информации по возможности доступа 12
4. Классификация информации с точки зрения возможности распространения 16
5. Информационные технологии и информационные системы 18
6. Ответственность 25
Вопросы для самоконтроля 27
Литература 30

Введение

Примечательная особенность нынешнего периода – переход общества от индустриального типа к информационному, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами являются материальные и нематериальные факторы, способствующие экономической деятельности, которыми располагает общество, и при необходимости, используемые для достижения какой-либо цели хозяйственной деятельности. Существуют такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому.

Но в современном мире появилось такое понятие как «информационные ресурсы». Они являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и обратить ее в наличность с пользой, продав кому-нибудь, или, что еще хуже, уничтожить. Собственная информация для производителя представляет большую ценность, поскольку получение или создание информации представляет собой трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимой пользой. В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

В пособии рассмотрены основные права граждан, касающиеся вопросов обработки информации; свойства информации как объекта защиты; классификация информации по возможности доступа и с точки зрения возможности распространения; понятия и классификации информационных технологий и информационных систем; виды ответственности, которые могут повлечь нарушения требований федерального законодательства в сфере обработки и защиты информации.

1. Основные права граждан, касающиеся вопросов обработки информации

Основные права и свободы граждан Российской Федерации закреплены в Конституции нашей страны. В том числе в ней введены базовые положения, касающиеся вопросов обработки и защиты информации. Так часть 4 статьи 29 устанавливает, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым **законным** способом.

Обратим внимание, что такая формулировка неявно содержит определенную проблему. Раскрывая приведенное ранее положение Конституции на практическом уровне, мы сталкиваемся с необходимостью описания либо всех законных, либо всех «незаконных» способов «обработки» информации. С технической точки зрения реализуемы (и получили широкое распространение) оба подхода. Первый из них получил название «запрещено все, что не разрешено», второй – «разрешено все, что не запрещено». С юридической же точки зрения существенным преимуществом пользуется второй подход, что приводит к определенному состязанию. Зная описание «незаконных» способов обработки информации (ввиду общедоступности правовых актов), «злоумышленник» получает возможность искать способы достижения своих целей, не попадающие под известные ему описания.

Обеспечение безопасности информации при этом во многом состоит в создании таких условий, при которых злоумышленник будет вынужден добиваться своих целей, используя явно описанные «незаконные» способы обработки информации.

Руководствуясь принципом, что свобода одного человека заканчивается там, где начинается свобода другого, мы можем понимать защиту информации, как создание определенных «барьеров», столкновение с которыми должно явно свидетельствовать, что реализация желаемых действий, включающая преодоление таких «барьеров», ведет к нарушению закона.

В уже упомянутой нами 29 статье Конституции также вводится первый встретившийся нам вид защищаемой информации – государственная тайна. Исторически это самый древний и во многом самый защищаемый вид информации.

Кроме государственной тайны в 23 и 24 статьях Конституции фактически вводится второй вид защищаемой информации – персональные данные. Так в 23 статье устанавливается, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а в 24 статье, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Положения Конституции Российской Федерации конкретизируются в федеральных законах (включая кодексы), в указах Президента Российской Федерации и постановлениях Правительства Российской Федерации, а также в ведомственных правовых, нормативных и методических документах.

Основным федеральным законом, регулирующим сферу обработки информации, является федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Указанный федеральный закон регулирует отношения, возникающие при:

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

С точки зрения защиты информации основными принципами правового регулирования, установленными рассматриваемым законом, являются:

- Свобода поиска, получения, передачи, производства и распространения информации любым **законным** способом.
- Обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.
- Установление ограничений доступа к информации только федеральными законами.
- Достоверность информации и своевременность ее предоставления.

- Неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Федеральный закон «Об информации, информационных технологиях и о защите информации» вводит определения базовых понятий в сфере обработки и защиты информации, которые используются во всем правовом поле Российской Федерации.

2. Информация и ее свойства

Очевидно, что основным понятием в рассматриваемой сфере является понятие «Информация». Согласно 149-му Федеральному закону:

Определение 1. Информация – это сведения (сообщения, данные) независимо от формы их представления.

Обратим внимание, что это определение является очень общим. Оно не требует, чтобы сведения были каким-либо образом структурированы, были зафиксированы на каком-либо носителе и т. п.

Следует особо подчеркнуть независимость сведений от формы представления. Говоря о формах представления информации, мы обычно понимаем, что информация может быть записана от руки на листочке (например, имя, адрес и телефон нового знакомого), напечатана на бумажном носителе (например, в книгах, брошюрах, на листовках, плакатах), представлена в виде файлов различных форматов в наших компьютерах, планшетах, смартфонах и т. п.

Кроме того, информацией можно обмениваться. Мы общаемся друг с другом, говорим и слышим, показываем и видим, пишем электронные сообщения и прикладываем к ним фотографии, читаем эти сообщения. Во всех этих процессах информация передается по «каналам связи» и может быть представлена в виде акустических, оптических, радио или электромагнитных сигналов.

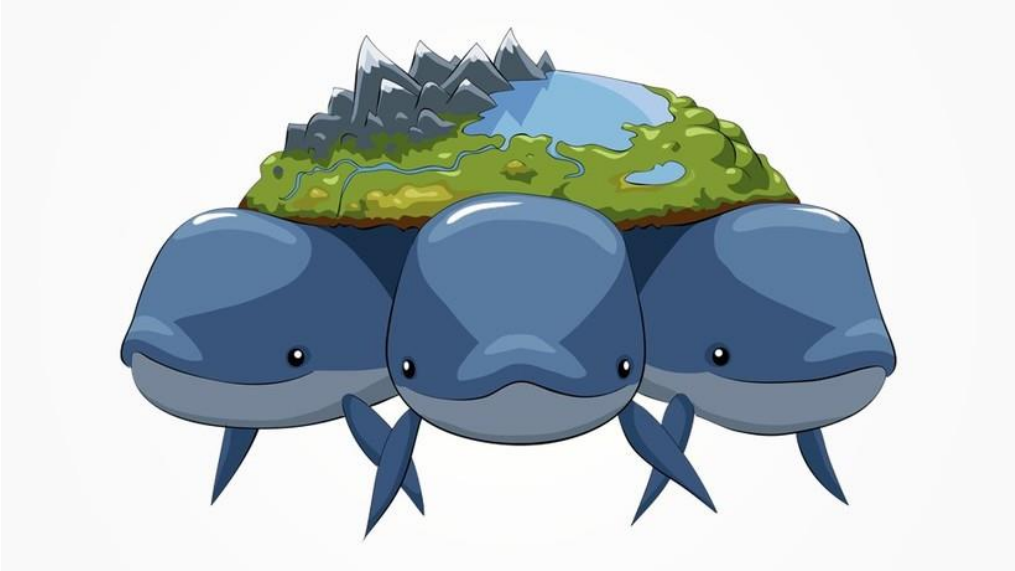
Если еще немного углубиться, то говоря, что «файлы с информацией обрабатываются на компьютере», мы понимаем компьютер как законченное целое. На самом деле он является сложной системой, состоящей из множества различных элементов, некоторые из которых могут выступать как «приемниками», так и «передатчиками» информации. Кроме того, для взаимодействия между элементами компьютера существуют особые «каналы связи» (например, шины) внутри компьютера.

Таким образом, «файлы с информацией, обрабатываемые на компьютере» на самом деле могут храниться на жестком диске в форме особым образом намагниченной области, могут находиться в оперативной памяти, передаваться по каналам материнской платы и обрабатываться процессором в виде электромагнитных сигналов. Более того, в процессе обработки информации различные элементы компьютера формируют

электромагнитные поля, которые также будут являться носителями (обрабатываемой) информации.

Отметим, что, с точки зрения данного выше определения понятия «информация», наши мысли также являются информацией. При этом, с одной стороны, человек как носитель мыслей может рассматриваться в качестве объекта защиты. С другой стороны, нарушитель, не обладая техническими средствами, может подсмотреть информацию, или подслушать. Поскольку защита человека реализуется скорее в правовом, организационном и физическом смысле, а наше пособие в большей степени ориентировано на вопросы технической защиты информации, то мы скорее рассматриваем человека как нарушителя, а не объект защиты.

При работе с информацией мы предъявляем к ней определенные требования. Например, мы можем предъявлять требования к форме ее представления, объему данных, новизне и так далее. С точки зрения информационной безопасности выделяются три основных свойства безопасности информации («Три кита»): **конфиденциальность, целостность** и **доступность.**



Определение 2. Конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Другими словами, конфиденциальность понимается как некоторое ограничение, наложенное на информацию ее владельцем. Каждый, кто желает получить такую информацию, должен согласиться с тем условием, что он не может своим собственным решением передать такую

(конфиденциальную) информацию третьим лицам, а должен предварительно получить согласие обладателя на передачу или обеспечить получение третьей стороной информации непосредственно у обладателя.

Согласитесь, что если мы доверяем кому-то напечатать наши фотографии, то мы (по крайней мере в некоторых случаях) хотим быть уверенными в том, что завтра не найдем эти фотографии в сети Интернет. Или, вряд ли мы будем рады, если обнаружим в сети Интернет данные своей банковской карты или копию медицинской книжки.

Не менее значимой характеристикой информации является **целостность**. Каждый из нас, положив в карман 1000 рублей, надеется их там обнаружить. В данном случае информация, которой являются сведения о номинале купюры, неразрывно связана с физическим носителем – то есть собственно купюрой. Ситуация существенно усложняется, если связь информации с «носителем» утрачивается или полностью исчезает.

Например, мы положили на банковский счет 100.000 рублей (будем считать, что процентная ставка не отрицательная) и не предпринимали никаких действий по снятию средств. Согласитесь, что все мы надеемся через какое-то время обнаружить на счету как минимум 100.000, и 10.000 нас явно расстроят. При этом доступные нам на банковском счете средства представляют собой записи в некоторой базе данных, значения которых можно изменять. Естественно, к данным нашего банковского счета можем иметь доступ не только мы, но и сотрудники банковской организации, а также, возможно, лица, обслуживающие автоматизированную банковскую систему, и аудиторы.

Действия со счетом могут быть санкционированными (например, мы переводим денежные средства с одного счета на другой, оператор просматривает информацию нашего счета при проведении операции) и несанкционированными (например, стороннее лицо осуществляет перевод денежных средств с нашего счета, но без нашего ведома). Если мы можем противостоять несанкционированным изменениям информации, то говорят, что мы обеспечиваем ее **целостность.**

Определение 3. Целостность информации – это состояние информации, при котором отсутствует любое ее изменение или изменение осуществляется только преднамеренно субъектами, имеющими необходимые права.

И последнее основное свойство безопасности – **доступность.**

Каждый из нас хотя бы один раз оказывался в ситуации, при которой информация необходима нам немедленно. Например, нам требуется связаться с родственником, попавшим в сложную жизненную ситуацию, или срочно необходимо оплатить покупку. Доступность информации оказывается критичной во многих ситуациях, требующих немедленного реагирования, например, в случае работы станка, обрабатывающего сложную деталь и получающего управляющие команды в режиме реального времени, или в случае игры на бирже, при которой необходимо как можно более оперативно реагировать на изменяющуюся ситуацию.

Определение 4. Доступность информации – это состояние информации, при котором лицу, обладающему правом доступа к информации и выполнившему все необходимые условия для получения доступа к информации и ее использованию, не может быть отказано в доступе.

Обратим внимание на ограничения, приведенные в определении.

Во-первых, доступность информации гарантируется только лицу, которое легитимно обращается к информации, то есть имеет право получить запрашиваемую информацию. Можно сказать, что одной из задач защиты информации является создание таких условий, при которых время получения информации при несанкционированном обращении должно стремиться к бесконечности.

Во-вторых, даже если Вы обладаете правом на получение информации, одного желания ее получить недостаточно. Требуется также соблюдение всех необходимых условий.

Например, для получения информации о банковском счете мы должны не просто обратиться к автоматизированной банковской системе посредством приложения «клиент-банк», но и должны предъявить определенную информацию, идентифицирующую нас в этой системе (обычно логин, пароль и одноразовый код, приходящий по альтернативному каналу связи и подтверждающий наше знание об этом канале и владение определенным устройством). Или для закрытия нашего счета в банке необходимо не только прийти в банк, но и подтвердить нашу личность, предъявив паспорт и, возможно, другие документы.

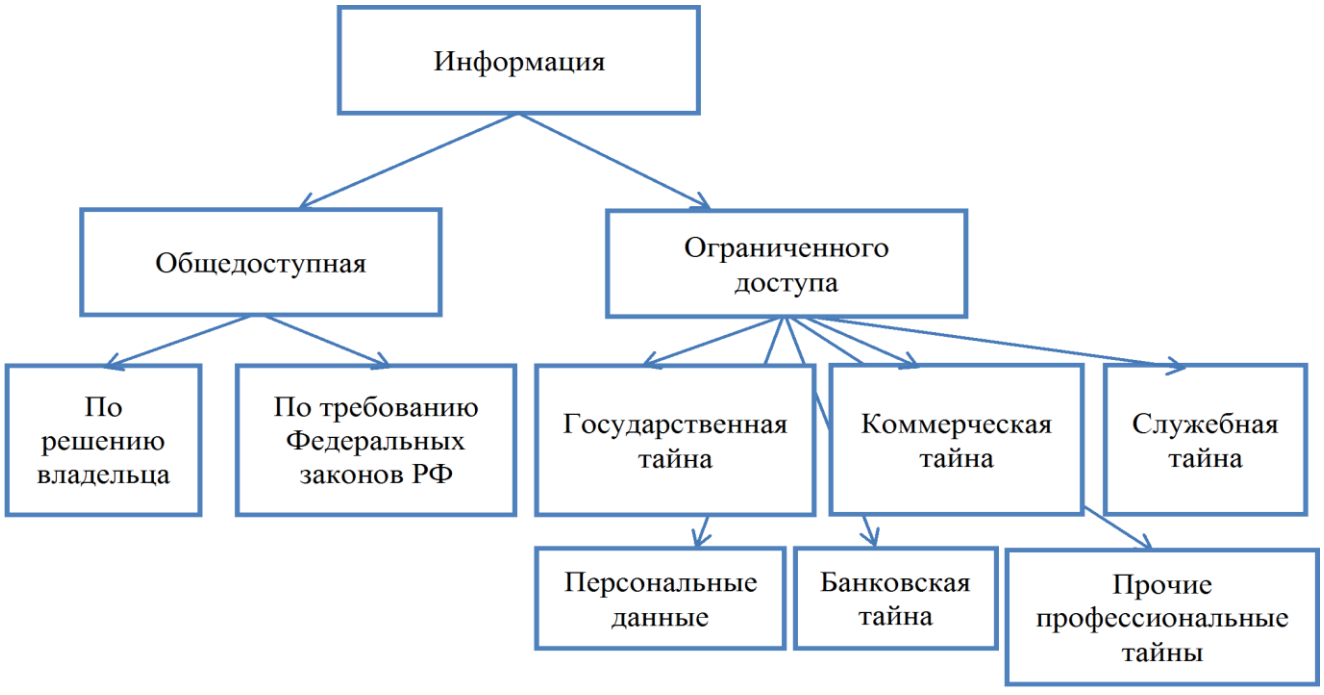
3. Классификация информации по возможности доступа

Как мы уже знаем, не ко всякой информации мы можем получить доступ. Например, мы можем получить доступ к состоянию своего банковского счета, но не можем получить доступ к банковскому счету стороннего лица.

В нашем законодательстве в зависимости от **категории доступа** выделяют **общедоступную** информацию и информацию, **доступ к которой ограничен федеральными законами** (информацию **ограниченного доступа**).

Как следует из названия, к общедоступной информации доступ может получить каждый. Для получения доступа к информации **ограниченного доступа** необходимо удовлетворять определенным требованиям (например, быть ее обладателем или входить в круг лиц, имеющих право доступа к такой информации).

К общедоступной информации относятся общеизвестные сведения (например, правила сложения и умножения целых чисел) и иная информация, доступ к которой не ограничен (например, список книг в общественной библиотеке). Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.



Особо выделяется ряд сведений, доступ к которым в соответствии с нашим законодательством нельзя ограничивать. Примерами таких сведений выступают:

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина;
- информация о деятельности государственных органов и органов местного самоуправления;
- информация о состоянии окружающей среды;
- сведения об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информация, накапливаемая в открытых фондах библиотек, музеев и архивов (в том числе оцифрованная).

При этом необходимо отметить особую роль сведений, составляющих государственную тайну. Как мы помним, существование государственной тайны – особого вида защищаемой информации закреплено в Конституции Российской Федерации, и отношения, связанные с обработкой государственной тайны, регулируются отдельным законом.

Поэтому не стоит удивляться тому, что, например, ограничен доступ к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, составляющим государственную тайну, или к архивным фондам документов, содержащих сведения, составляющие государственную тайну.

Ограничить доступ к произвольной информации, исходя только из своего желания, нельзя. Ограничение доступа к отдельным видам информации устанавливается федеральными законами. Примеров таких законов достаточно много. Помимо трех законов, непосредственно посвященных особым видам информации ограниченного доступа: государственной тайне, коммерческой тайне и персональным данным, существует множество законов, вводящих различные профессиональные тайны.

Для иллюстрации широты охвата, приведем далеко неполный перечень таких тайн: налоговая тайна, банковская тайна, тайна страхования, тайна ломбарда, адвокатская тайна, тайна завещания, тайна следствия, тайна совещания судей, врачебная тайна, тайна связи, тайна усыновления и тайна исповеди. При этом следует отметить, что многие из перечисленных тайн также являются персональными данными.

Обратим внимание на следующее важное положение: соблюдение конфиденциальности информации является обязательным в том случае, если доступ к ней ограничен федеральными законами.

В связи с этим представляет интерес вопрос о статусе «информации для служебного пользования» (или служебной информации ограниченного распространения). До сих пор на некоторых документах можно встретить метку «для служебного пользования», что должно предупреждать о наличии в документе конфиденциальной информации, предназначенной для ознакомления или использования только в служебных целях.

Однако федерального закона «О служебной информации» не существует. Он разрабатывался параллельно с Федеральным законом «О персональных данных» в 2008 году, но не был принят Государственной Думой. На текущий момент документом, определяющим порядок обработки и защиты служебной информации ограниченного распространения является Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности», статус которого ниже, чем статус федерального закона. Поэтому правовой статус документов, имеющих метку «для служебного пользования» во многом является дискуссионным.

Заметим также, что конфиденциальность не является единственным свойством информации, которое необходимо обеспечить, поэтому существуют достаточно много видов информации, требующих защиты, но не требующих ограничения доступа. В частности, защиты требуют открытые и общедоступные ресурсы (например, официальные сайты органов государственной власти и организаций), сведения, влияющие на работу автоматизированных систем управления технологическими процессами (например, сведения о температуре окружающей среды или давлении) и другая информация.

Если доступ к информации ограничивается, значит это кому-нибудь нужно. В первую очередь, ограничение доступа к информации призвано обеспечить преимущество одних лиц перед другими, основывающееся на возможности использования такой информации. Здесь возникает один из

главных субъектов (российского законодательства) в сфере обработки и защиты информации – владелец или обладатель информации.

Определение 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.

Обладателями информации могут выступать: физические лица, юридические лица, а также Российская Федерация, субъект Российской Федерации или муниципальное образование. В трех последних случаях право разрешать или ограничивать доступ к информации реализуется органами государственной власти и местного самоуправления, на которые возложены соответствующие полномочия.

Обладатель информации реализует всю полноту прав в ее отношении. В частности, он имеет права на использование информации по своему усмотрению (в том числе на уничтожение информации, ее дарение, продажу и т. п.), на ограничение доступа к информации, на защиту (законными способами) своих прав на информацию в случае их нарушения. При этом обладатель информации обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, а также ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

4. Классификация информации с точки зрения возможности распространения

Классифицируя информацию по порядку доступа, мы смотрим на нее с точки зрения получателя. Теперь мы рассмотрим вопрос о классификации информации с точки зрения источника. Для начала отметим, что наше законодательство выделяет два формата передачи информации: **предоставление** и **распространение.**

Определение 6. Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Определение 7. Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Обратим внимание, что это достаточно важно, поскольку многие вопросы об ответственности сформулированы в терминах только одного формата передачи информации и вопрос об ответственности применительно ко второму формату является дискуссионным. Например, в пункте 1 статьи 242 «Незаконные изготовление и оборот порнографических материалов или предметов» состав преступления сформулирован следующим образом:

Незаконные изготовление и (или) перемещение через Государственную границу Российской Федерации в целях **распространения**, публичной демонстрации или рекламирования либо **распространение**, публичная демонстрация или рекламирование порнографических материалов или предметов.

Итак, в зависимости от порядка распространения (предоставления) выделяют следующие виды информации:

- Свободно распространяемая информация (например, перечень книг в публичной библиотеке);
- Информация, предоставляемая по соглашению лиц, участвующих в определенных отношениях (например, произведения, защищенные авторским правом);
- Информация, подлежащая предоставлению или распространению (например, сведения о золотовалютных резервах Российской Федерации);

- Информация, распространение которой в Российской Федерации ограничивается или запрещается.

Например, на территории Российской Федерации запрещается распространение:

- Информации, направленной на пропаганду войны.
- Информации, направленной на разжигание национальной, расовой или религиозной ненависти и вражды.
- Информации, за распространение которой предусмотрена уголовная или административная ответственность (например, государственная тайна).

5. Информационные технологии и информационные системы

Информационные технологии

Следующим важным понятием, определение которому дано в федеральном законе «Об информации, информационных технологиях и о защите информации» является понятие «информационные технологии».

Определение 8. Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Это определение также является достаточно общим. В рамках данного определения информационными технологиями оказываются, например, чтение газет объявлений, формирование библиотек (бумажных и электронных книг), распространение листовок, рассылка электронных писем, хранение информации в центрах обработки данных, обработка видео на компьютере, общение через смс и сервисы обмена мгновенными сообщениями, передача информации по спутниковым каналам связи и многое-многое другое.

Информационные системы

Как мы уже знаем, информация не существует сама по себе. С одной стороны, обязательно должен существовать носитель информации. С другой стороны, должны быть определены информационные технологии, которые позволяют работать с информацией на таком носителе. В

противном случае, само по себе существование информации без возможности ее использования (применения) может не оказывать на нас никакого влияния.

При этом можно привести примеры ситуаций, при которых информация (вместе с носителем) существует, но технологий, позволяющих извлечь эту информацию и работать с ней, еще не существует. Например, можно считать, что наша Вселенная является «носителем» информации о самой себе. Поэтому открытие нового физического закона, по сути, является актом извлечения существовавшей на «носителе» информации, которую до этого момента не могли извлечь.

Другим примером является невозможность (по крайней мере, на текущий момент) чтения человеческих мыслей, если только человек сам их не воспроизводит. Поэтому студентам приходится доказывать преподавателям, что они что-то знают путем непосредственного воспроизведения своих мыслей.

Итак, с учетом сказанного, введем в рассмотрение еще одно важное понятие – «информационная система».

Определение 9. Информационная система (ИС) – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационную систему можно рассматривать как основной «строительный» элемент и «учетную единицу» в сфере информатизации и информационных технологий. Можно сказать, что нас окружают информационные системы, это не только широко известные Портал государственных услуг, Единая государственная информационная система в сфере здравоохранения или Единый государственный реестр записей актов гражданского состояния, но и информационные системы предприятий – кадровые или бухгалтерские информационные системы, системы управления предприятием (ERP) или системы управления взаимоотношениями с клиентами (CRM). Более того, у каждого из нас есть, как минимум одна своя информационная система, например, телефонный справочник друзей и знакомых.

Вернемся к определению информационной системы. Обратим внимание, что приведенное определение уже не подразумевает рассмотрение любой информации независимо от формы ее представления.

Согласно 1260 статьи Четвертой части Гражданского кодекса Российской Федерации **базой данных** является представленная в **объективной форме** (соответственно субъективные мысли человека не попадают под определение) совокупность самостоятельных материалов (например, статей, расчетов и т. п.), **систематизированных** таким образом, чтобы эти материалы могли быть **найдены и обработаны с помощью электронной вычислительной машины**.

Соответственно, говоря об информационной системе, мы подразумеваем не только применение компьютеров для обработки информации, но и обязательно определенные свойства самой обрабатываемой информации, а именно пригодность для обработки с помощью компьютера (объективную форму) и наличие определенной структуры (системности).

Несмотря на вышесказанное, под приведенное определение информационной системы попадает все еще очень широкий класс объектов. Например, в состав информационной системы могут входить базы данных с системами управления, такие как Oracle, MS SQL или MySQL, а могут электронные таблицы Excel. Более того, структурированная таблица в файле формата Microsoft Word также может рассматриваться в качестве базы данных и вместе с программным обеспечением и компьютером, на котором хранится файл, она формирует информационную систему.

Круг возможных технических средств, входящих в состав информационной системы также очень широк. Примерами технических средств являются серверы, персональные компьютеры, ноутбуки и планшеты, смартфоны, коммутационное оборудование, принтеры, веб-камеры и многое другое.

Таким образом, примерами информационных систем могут являться и упорядоченный перечень слушателей этого курса в файле формата Microsoft Word на рабочем компьютере преподавателя, и система управления университетом, включающая серверы, рабочие места пользователей – сотрудников университета и, уже упомянутый, Портал государственных услуг, в состав которого входят несколько центров обработки данных, а круг пользователей потенциально не ограничен.

Принято выделять три вида информационных систем.

К первому виду относятся государственные информационные системы, созданные на основании федеральных законов, законов субъектов

Российской Федерации или на основании правовых актов государственных органов. По масштабу государственные информационные системы делятся на региональные, территориально расположенные в одном субъекте Российской Федерации, и федеральные, территориально расположенные в нескольких субъектах Российской Федерации или на территории всей Российской Федерации.

Ко второму виду относятся муниципальные информационные системы, созданные на основании решения органа местного самоуправления. Такие информационные системы обычно расположены в пределах одного города или района субъекта Российской Федерации.

Все остальные информационные системы относятся к третьему виду – иные информационных систем. Такими информационными системами являются информационные системы предприятий и организаций, частные информационные системы независимо от их территориального размещения. Например, информационные системы ПАО «Газпром», социальная сеть ВКонтакте и наш телефонный справочник в телефоне относятся к иным информационным системам.

Обратим внимание, что, несмотря на правовое закрепление приведенной классификации, существуют альтернативные взгляды на то, что считать государственными информационными системами. Например, в одном из основных альтернативных подходов предлагается считать государственными все информационные системы, создание которых финансировалось (или финансируется) из бюджетов федерального и регионального уровней, при этом наличие правовых актов не считается первостепенным.

Поскольку информационная система содержит в своем составе технические средства, а также программное обеспечение, реализующее информационные технологии, то кто-то должен поддерживать их в работоспособном состоянии, обновлять, модернизировать, заменять и т. п. Лицо, обслуживающее информационную систему, принято называть **оператором информационной системы**. Это второй по важности (после обладателя информации) субъект в сфере информатизации и информационных технологий. Приведем формальное определение.

Определение 10. Оператор информационной системы – это гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Обладатель информации и оператор информационной системы могут находиться в различных отношениях. Эти роли могут совпадать или быть различными. К примеру, мы являемся обладателем информации в нашем смартфоне и одновременно оператором телефонного справочника. С другой стороны, мы можем являться обладателями информации, но поручить ее эксплуатацию центру обработки данных, который будет выступать в данном случае в роли оператора.

Более того, роли обладателя и оператора могут быть распределены между несколькими лицами. Например, технические средства центра обработки данных может арендовать организация, которая развернет на них информационную инфраструктуру социальной сети, к которой уже будут подключаться пользователи – обладатели «страниц» в этой социальной сети.

Необходимо отметить, что могут возникать и достаточно парадоксальные ситуации. Например, как обладатель информации, размещаемой на нашей странице в социальной сети, мы можем разрешать и ограничивать доступ к ней, но владелец самой социальной сети также может ограничить доступ к нашей странице и размещенной на ней информации, в том числе и нам самим.

То же самое может произойти во втором приведенном примере, в ситуации, при которой центр обработки данных (например, за неуплату) может ограничить доступ к информации ее обладателю. Поэтому в общем случае определение того, у кого в конкретный момент времени может

оказаться больше прав на информацию (и ресурсов на их реализацию) у обладателя или у оператора, может оказаться достаточно трудной задачей.

В случаях, при которых роль оператора информационной системы не определена явно (например, она может быть прописана в нормативных документах, являющихся основанием для создания информационной системы), оператором информационной системы считается **собственник технических средств**, которые используются для обработки содержащейся в базах данных информации, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Обладатель информации и оператор информационной системы в случаях, если это установлено законодательством Российской Федерации, обязаны принимать **правовые**, **организационные** и **технические** меры по защите информации, направленные на:

- предотвращение неправомерного (несанкционированного) доступа к информации, результатом которого может стать уничтожение, модификация, блокирование, копирование, предоставление или распространение информации, а также любые другие неправомерные действия в ее отношении;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию прав доступа к информации.

В случаях, установленных законодательством Российской Федерации, обладатель информации и оператор информационной системы обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим прав доступа к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации.

На настоящий момент в правовой и нормативной базе Российской Федерации можно выделить следующие основные виды защищаемой информации и основные виды защищаемых информационных систем (объекты защиты):

- государственная тайна;
- персональные данные;
- коммерческая тайна;
- информация для служебного пользования (смотри замечание о статусе этого вида конфиденциальной информации в разделе «Классификация информации по возможности доступа и возможности распространения»);
- объекты критической информационной инфраструктуры;
- государственные информационные системы;
- информационные системы персональных данных;
- автоматизированные системы управления технологическими процессами;
- открытые и общедоступные информационные ресурсы.

По каждому представленному в предыдущем списке объекту защиты существует своя «ветвь» в законодательстве Российской Федерации, в которую в том числе входят ведомственные правовые и нормативные документы Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, устанавливающие требования к составу и содержанию мер по защите информации.

6. Ответственность

Нарушение требований федерального законодательства в сфере обработки и защиты информации может повлечь различные виды ответственности. Внутри организаций и предприятий может предусматриваться **дисциплинарная ответственность** (например, лишение премии, выговор или увольнение). Серьезные проступки могут оказаться составом **административного** правонарушения или даже **уголовного** преступления.

Основными **нормативными актами,** определяющими ответственность в сфере защиты информации, являются: Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) и Уголовный кодекс Российской Федерации (УК РФ).

Приведем примеры положений этих документов.

В соответствии с частью 2 статьи 13.12 Кодекса Российской Федерации об административных правонарушениях:

Использование несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

В соответствии со статьей 137 Уголовного кодекса Российской Федерации:

Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой

информации наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

В соответствии со статьей 272 Уголовного кодекса Российской Федерации:

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Отметим, что кроме КоАП РФ и УК РФ, ответственность в области обработки и защиты информации могут определять и другие правовые документы. Например, в соответствии со статьей 81 Трудового кодекса Российской Федерации:

Работодатель может в одностороннем порядке расторгнуть трудовой договор в случае, если сотрудник разгласил охраняемую законом тайну, ставшую известной работнику в связи с исполнением им трудовых обязанностей.

Вопросы для самоконтроля

1. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?

☐ Право на неприкосновенность личной и семейной тайны.
☐ Право на обработку любой информации любым возможным способом.
☐ Запрет на обработку информации о частной жизни лица без его согласия.
☐ Право на получение гражданами допуска к государственной тайне.

2. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации?

☐ Информация для служебного пользования.
☐ Персональные данные.
☐ Государственная тайна.
☐ Врачебная тайна.

3. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» информация – это:

☐ Любые данные, представленные на материальном носителе.
☐ Сведения (сообщения, данные), независимо от формы их представления.
☐ Не энергия и не материя.
☐ Сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

4. Что из перечисленного можно рассматривать как базу данных в соответствии с законодательством Российской Федерации?

☐ EXCEL таблицу с упорядоченной и структурированной информацией.
☐ Файл формата DOC, в котором создан список слушателей этой программы.
☐ Картотеку регистратуры учреждения здравоохранения.
☐ Все перечисленные.

5. Целостность информации – это:

☐ Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

☐ Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

☐ Возможность получения информации и ее использования.

6. На территории Российской Федерации запрещено распространение:

☐ Информации, которая направлена на пропаганду войны.

☐ Коммерческой тайны.

☐ Информации, которая направлена на разжигание религиозной ненависти.

☐ Персональных данных.

7. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных – это:

☐ Обладатель информации.

☐ Оператор информационной системы.

8. Если не определено иного, оператором информационной системы является:

☐ Обладатель информации.

☐ Собственник используемых для обработки содержащейся в базах данных информации технических средств.

☐ Лицо, определяющее цели обработки информации и осуществляющее обработку информации.

9. Не может быть ограничен доступ:

☐ К информации о состоянии окружающей среды.

☐ К информации, хранящейся в открытых фондах библиотек.

☐ К персональным данным государственных гражданских служащих.

☐ К сведениям о золотовалютных запасах Российской Федерации.

10. Какую ответственность может повлечь нарушение требований Федеральных законов:

☐ Уголовную.
☐ Дисциплинарную.
☐ Административную.
☐ Гражданско-правовую.
☐ Все перечисленные.

Литература

1) Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 2021.

2) Гражданский кодекс Ч. №4 Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (18 декабря 2006 года N 230-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_64629/).

3) Доктрина информационной безопасности Российской Федерации (утв. утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.) (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html).

4) Постановление Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» (в ред. от 27.12.2012 г.) // Собрание законодательства Российской Федерации. 2008 г. N 28. Ст. 3384.

5) Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. 2012 г. N 45. Ст. 6257.

6) Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета. 2013 г. N 208.

7) Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения» (в ред. от 30.10.2018) (https://www.garant.ru/products/ipo/prime/doc/71652212/#review).

8) Трудовой кодекс РФ – глава 14 «Защита персональных данных работника» (от 30.12.2001 N 197-ФЗ (ред. от 28.06.2021) (http://www.consultant.ru/document/cons_doc_LAW_34683/aa501d1bd2f6e341d0d0aaf21bf5e694cfb4f28e/).

9) Уголовный кодекс Российской Федерации №63-ФЗ от 13.06.1996 (ред. от 05.04.2021) // Собрание законодательства РФ. 1996. №25. Ст. 2954.

10) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм. и доп. от 02.06.2021) // (https://base.garant.ru/12148567/).

11) Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (ред. от 12.03.14 г.) (http://yconsult.ru/zakony/zakon-rf-98-fz/).

12) Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации» (http://base.garant.ru/12148555/).

13) Федеральный закон от 06 апреля 2011 №63 «Об электронной подписи» (с изменениями на 23.06.16 г.) (http://docs.cntd.ru/document/902271495).

14) Баскаков А.В., Остапенко А.Г., Щербаков В.Б. Политика информационной безопасности как основной документ организации // Информация и безопасность. – 2016. - №2. – С. 43-47.

15) Борисова К.В., Кудашкин Я.В. Международная информационная безопасность как основополагающий фактор национальной безопасности// Сборник научных трудов. Национальная безопасность: противодействие экстремизму и терроризму и перспективы преодоления глобальных проблем. – 2016. – С. 68-73.

16) Галушкин А. А. К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. – 2015. - №2. – С. 8.

17) Камалова Г.Г. Вопросы ограничения доступа к информации в системе государственного управления// Вестник Удмуртского университета. – 2015. - №6. – С. 91-104.

18) Кирильчук С.П., Наливайченко Е.В. Обеспечение информационной безопасности предприятий. Международный научный журнал «Символ науки», № 3, 2015.

19) Юсупов Р.М., Шишкин В.М. Информационная безопасность, кибербезопасность и смежные понятия // Информационное противодействие угрозам терроризма – 2016. - №1. – С. 27-35.

Для заметок