

*Невский Д.О.,
Студент
2 курс, ИГСУ РАНХиГС
Россия, г. Москва*

**ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ**

***Аннотация:** в статье рассматриваются основные положения, касающиеся информации, информационных технологий и защиты информации, установленные Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Анализируется понятийный аппарат. Дается краткая характеристика указанных терминов.*

***Ключевые слова:** данные, защита информации, информационные технологии, информация, сведения, сообщения.*

***Annotation:** The article discusses the main provisions concerning information, information technology, and information protection, established by Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technology, and Information Protection." The conceptual framework is analyzed. A brief description of these terms is given.*

***Keywords:** data, information protection, information technology, information, information, messages.*

Основы государственного регулирования в данной сфере содержатся в Федеральном законе от 27 июля 2006 г. № 149-ФЗ "Об информации,

информационных технологиях и о защите информации" (далее - Закон об информации)[3].

Закон об информации регулирует сферу взаимодействий, связанных с реализацией прав на поиск, получение, передачу, создание и распространение сведений, использованием цифровых инструментов, а также обеспечением сохранности данных. При этом из его действия исключены отношения, касающиеся охраны интеллектуальной собственности и приравненных к ней средств идентификации.

Необходимость принятия нового базового нормативного акта в этой области обусловлена потребностью в приведении к единообразию как терминологических, так и содержательных подходов к регулированию информационных связей, устранении существующих правовых лакун и адаптации российского законодательства к международным стандартам в данной сфере.

Данный закон приводит систему понятий и регуляторные механизмы в соответствие с актуальными практиками использования информационных технологий. Он устанавливает правовой статус различных видов данных, фиксирует нормы, касающиеся создания и функционирования информационных систем, а также общие требования к работе информационно-телекоммуникационных сетей. Кроме того, документ определяет ключевые принципы регулирования общественных отношений, которые связаны с обращением информации.

Законодательно закрепляется принцип, согласно которому каждый имеет право свободно искать, получать, передавать, создавать и распространять данные любыми законными методами. Вместе с тем предусматривается, что ограничения доступа к информации могут вводиться исключительно на основании федеральных законов.

В тексте закона содержатся нормы, направленные на противодействие недобросовестному использованию или злоупотреблению возможностями

средств распространения сведений, когда пользователям навязываются нежелательные данные. В частности, информация должна содержать достоверные указания на своего владельца или иного распространителя, причем в таком виде и объеме, которые позволяют однозначно установить личность этого лица. Если для распространения данных используются методы, позволяющие идентифицировать получателя (например, почтовые отправления или электронные сообщения), то распространитель обязан предоставить получателю возможность отказаться от получения такой информации.

Законом устанавливаются основные правила и способы защиты прав на информацию, а также самой информации через принятие правовых, организационных и технических (включая программно-аппаратные) мер. Права владельца данных, содержащихся в базах данных информационных систем, подлежат охране независимо от авторских и иных прав на эти базы данных.

Отдельно закрепляется прямой запрет на требование от гражданина предоставления сведений о его частной жизни, включая данные, составляющие личную или семейную тайну, а также на получение таких сведений без его согласия. Исключения допускаются лишь в случаях, прямо предусмотренных федеральными законами.

Закон об информации закрепляет понятие "информация". Согласно закону, под информацией понимаются любые сведения, сообщения или данные, вне зависимости от способа их представления. Действующее законодательство оперирует гораздо более обширным определением информации, нежели предыдущий Закон[4]. Напомним, прежний закон трактовал информацию как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления". Существенное расширение понятия в обновленном акте объясняется тем, что прежняя, формально-юридическая трактовка не давала однозначного ответа на ряд

важных вопросов. В частности, оставалась неясность, следует ли относить к категории информации вымышленные явления и процессы, к примеру, те, что представлены в литературных произведениях. Также не было ясности относительно информации, касающейся будущего, то есть сведений о событиях и явлениях, которые еще не произошли и не стали фактическими[8]. Понятие информации находит применение в различных отраслях права, включая административное (например, при работе уполномоченных органов антимонопольной службы) и уголовное, когда речь идет о привлечении к ответственности, как, скажем, по статье 237 Уголовного кодекса Российской Федерации[1].

Понятие информации исследуется и в научной литературе. К примеру, выделяют следующие определения информации:

- информация есть знания, переданные кем-то другим или приобретенные путем собственного исследования или изучения;
- информация - это сведения, содержащиеся в данном сообщении и рассматриваемые как объект передачи, хранения и обработки;
- информация - это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему наших чувств;
- информацией являются все те данные о внешнем мире, которые мы получаем как путем непосредственного воздействия на наши органы чувств окружающих предметов и явлений, так и опосредованным путем через книги, газеты, рассказы других людей;
- информацией называется всякое сообщение или передача сведений о чем-либо, что заранее не было известно[6, С.52].

Если попытаться разделить это определение на категорию и отличительные признаки, задача окажется невыполнимой. Следовательно, данное определение нельзя признать удачным. По сути, оно лишь приравнивает друг к другу термины "информация", "сведения", "сообщения"

и "данные" в рамках российского законодательства, не раскрывая сути ни одного из них.

Всё, что существует в правовом поле, включая само право, представляет собой информацию. Денежные средства — тоже информация. Юридические факты — информация. Даже юридические лица, если заглянуть вперёд, являются информацией. Мы обмениваемся этими понятиями, фиксируем их в письменной форме и оперируем ими как объектами, которые называют идеальными (от слова "идея"). Антропологи утверждают, что способность создавать идеальные объекты и действовать на основе представлений о них — ключевое преимущество человека. Именно благодаря этому качеству человек стал царём природы: ни стадные животные, ни высокоразвитые виды, такие как слоны или дельфины, не способны на подобное.

Отдельный индивид может умереть, утратить память или покинуть сообщество, однако информация, накопленная обществом в виде социальных норм (право, мораль) или "мемов" (сказки, легенды, прочие тексты), сохраняется до тех пор, пока существует само общество. Как в коллективном сознании, так и в сознании каждого человека сведения постоянно упорядочиваются, проходя, как минимум, четыре этапа: данные, информация, знания и мудрость. Для каждого этапа люди и общество применяют свои методы работы.

Данные представляют собой разрозненные сведения. Они могут поступать из разнообразных источников — к примеру, из наших наблюдений, из сетей операторов связи или из банковских информационных систем. Когда эти разрозненные элементы связываются между собой, возникает собственно информация: то, что мы можем искать и находить, используя связи между отдельными составляющими.

Информация структурируется и организуется в массивы или формы представления данных: библиотеки, порталы данных, инфографику и прочее. Организованная, помещённая в контекст информация превращается в знание.

Знания становятся объектом анализа. Результат анализа знаний — мудрость, которая даёт нам возможность принимать решения. Пока знания не трансформируются в мудрость, то есть пока мы не проанализируем их и не осознаем для себя, мы не способны использовать их для принятия решений.

Определение информационных технологий также дано в Законе об информации: информационные технологии — это процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации, а также способы реализации этих процессов и методов.

Данное определение пригодно для квалификации понятия "информационные технологии" (ИТ):

— квалификационная принадлежность ИТ: во-первых, это процессы и методы, во-вторых, это способы;

— квалификационным признаком, который отличает процессы (методы, способы), относимые к ИТ, от прочих, является их связь с информацией (её поиском, сбором, хранением, обработкой, предоставлением, распространением), а способы относятся к процессам и методам работы с информацией.

Если кратко, ИТ — это процессы, методы и способы взаимодействия с информацией. Например, технология больших данных представляет собой процесс извлечения информации из больших объёмов неструктурированных данных на основе определённых методов. При этом способом реализации этих процессов и методов служит использование разнообразной компьютерной техники — от серверов до маршрутизаторов и смартфонов.

В определении информационной системы способы уже не относятся к информационным технологиям: там речь идёт об информационных технологиях и технических средствах. В таком узком понимании ИТ — это процессы и методы работы с информацией.

Основным видом технических средств, используемых для работы с информацией, являются электронно-вычислительные машины (ЭВМ).

Законодательство не уточняет, что именно под этим подразумевается. Более того, в разных нормативных актах встречаются различные термины, означающие примерно одно и то же: компьютер, компьютерная техника, средства вычислительной техники. Формально под эти понятия подпадает огромное количество устройств — от персональных компьютеров до цифровых датчиков (так называемый "Интернет вещей"); все они являются разновидностями компьютеров, оснащённых процессором, операционной системой, памятью и программами.

Согласно ч. 4 ст. 6 Закона об информации обладатель информации обязан принимать меры по ее защите.

К числу таких мер относятся правовые, организационные и технические. Их целью является: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализация права на доступ к информации (ч. 1 ст. 16 Закона об информации).

Обладателями подлежащей защите информации являются организации и физические лица, Российская Федерация, субъект РФ, муниципальное образование (ч. 1 ст. 6 Закона об информации)[5].

Защите информации посвящена лишь одна статья Закона об информации. Несмотря на её небольшой объём, из неё ясно: защита информации подразумевает не только ограничение, но и обеспечение доступа к ней. Право на доступ включает право на получение и использование полной и актуальной информации.

Из Закона об информации также следует, что государственное регулирование в сфере защиты информации осуществляется через установление требований к её защите, а также ответственности за нарушение

законодательства об информации, информационных технологиях и защите информации.

При создании и эксплуатации государственных информационных систем методы и способы защиты информации должны соответствовать установленным требованиям.

Действительно, некоторые законы устанавливают конкретные требования к защите информации. Например, статья 19 Федерального закона "О персональных данных"[2] гласит, что безопасность персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах;

2) применением организационных и технических мер, необходимых для выполнения требований к защите, исполнение которых обеспечивают установленные Правительством Российской Федерации уровни защищённости;

3) использованием средств защиты информации, прошедших процедуру оценки соответствия;

4) оценкой эффективности мер до ввода системы в эксплуатацию;

5) учётом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа и принятием мер;

7) восстановлением модифицированных или уничтоженных данных;

8) установлением правил доступа и обеспечением регистрации всех действий;

9) контролем за мерами и уровнем защищённости.

Эти пункты можно рассматривать как требования к защите информации. Однако далее в той же статье говорится, что Правительство РФ, с учётом возможного вреда, объёма данных, вида деятельности и актуальности угроз, устанавливает уровни защищённости и требования к их обеспечению.

Почему нельзя установить единые требования для всех? Это вытекает из базовой для теории информации теоремы Гёделя о неполноте: любая формальная система либо неполна, либо противоречива. Если система полна — она противоречива; если непротиворечива — то неполна[7]. Так и с требованиями к защите информации: невозможно сразу установить их для всех систем и случаев. Поэтому приходится дифференцировать их, используя подход, основанный на выявлении и предотвращении угроз.

Под угрозами безопасности информации понимается совокупность условий и факторов, создающих опасность несанкционированного (в том числе случайного) доступа, результатом которого могут быть уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия. Проще говоря, угроза — это возможные неприятности или действия злоумышленника, которые нужно предвидеть и к которым следует подготовиться.

Однако более эффективная система защиты информации строится не на угрозах, а на рисках. Представляется, что под риском причинения вреда (ущерба) понимается вероятность наступления событий, следствием которых может стать вред охраняемым законом ценностям. Риски добавляют к угрозам оценку вероятности. Всегда есть риск падения метеорита или ядерного взрыва. Подход, основанный только на моделировании угроз, требует защиты от них. Подход, основанный на оценке рисков, учитывает вероятность события и требует соотносить затраты на защиту с величиной риска.

Ещё более совершенным инструментом является концепция встроенной приватности, или приватности по умолчанию (privacy by design/default) Анны Кавукиан. Согласно ей, информационные системы и бизнес-процессы уже на этапе проектирования должны учитывать интересы приватности и не допускать смешения контекстов использования информации[7].

Разрабатывая информационные системы и организуя бизнес-процессы, следует ставить во главу угла потребности и цели пользователя. При этом

необходимо находить баланс между обеспечением конфиденциальности данных и достижением коммерческих задач, стремясь к взаимовыгодному решению (стратегия "выигрыш-выигрыш"). По умолчанию информация о пользователе должна быть скрыта, но сами информационные процессы в системе должны отличаться ясностью и прозрачностью. Такой подход, наряду с обеспечением безопасности данных на всех этапах их обработки, гарантирует пользователю чувство защищенности.

Список использованных источников и литературы:

1. Уголовный кодекс РФ от 13 июня 1996 г. N 63-ФЗ // Собрание законодательства Российской Федерации. 1996. N 25. ст. 2954.
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006. N 31. (часть I). ст. 3451.
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // Собрание законодательства РФ. 2006. N 31 (1 ч.). ст. 3448.
4. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" // Собрание законодательства Российской Федерации. 1995. N 8. ст. 609 (утратил силу).
5. Иванова С.В. Защита информации // СПС "КонсультантПлюс". 2026.
URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=116025#fYrqALVuGvgV2Adq>.
6. Мелик-Гайказян И.В., Мелик-Гайказян М.В., Тарасенко В.Ф. Методология моделирования нелинейной динамики сложных систем. М., 2001 ст. 52.
7. Дмитрик Н.А. Правовая информатика. М., 2022 // СПС "Гарант".
URL: <https://base.garant.ru/76873824>.

8. Чурилов А.Ю. Комментарий к Федеральному закону от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (постатейный). М., 2024 // СПС "КонсультантПлюс".
URL:<https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CMB&n=19163#LcDsALVgayrStyRI1>