РОССИЙСКАЯ АКАДЕМИЯ НАУК

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ, НАУКИ И ТЕХНОЛОГИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ (ВИНИТИ)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. № 4 Москва 2001

ОБЩИЙ РАЗДЕЛ

УДК 002:004.056.5](470)

А. В. Нестеров

Некоторые соображения по поводу "Доктрины информационной безопасности РФ"

Понятие "информация" стало фигурировать не только в научно-технической литературе, в правовых документах, но и в таких глобальных документах, как "Доктрина информационной безопасности", что требует дальнейшего изучения этого понятия,

Публикация "Доктрины информационной безопасности РФ" (далее Доктрина), представляющей собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ, является существенным шагом на пути дальнейшей информатизации нашего общества [1].

Данная Доктрина служит основой для совершенствования правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ.

В Доктрине было дано новое определение информационной сферы, которая представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

В этом определении уже вторично после закона РФ "Об информации, информатизации и защите информации" была сделана корректировка понятия информационной сферы и убрано слово "(среда)", которое, как уже отмечалось в [2], не является тождественным понятию "сфера".

Большим продвижением вперед стало включение в информационную сферу системы регулирования возникающих в этой сфере общественных отношений, о чем также отмечалось в [3].

Изменились функции субъектов информационной сферы, в частности, к ним относятся сбор, формирование, распространение и использование информации. Напомним, что в федеральном зако-

не РФ "Об участии в международном информационном обмене" в эти функции входили: создание, преобразование и потребление информации.

В Доктрине отмечено, что информационная сфера является системообразующим фактором жизни общества. Основополагающим понятием Доктрины является информационная безопасность РФ, под которой понимается состояние защищенности ее национальных интересов в информационной сфере.

С целью обеспечения информационной безопасности РФ предлагается усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов.

Под формированием информации, на наш взгляд, следует понимать действия, направленные на организацию операций с уже собранной информацией для подготовки ее к распространению или использованию.

Авторы Доктрины совершенно правильно включили в эту фразу слово "сохранение", так как в предыдущих законодательных актах этому понятию не уделялось внимания.

В Доктрине закреплено, что человек (гражданин) как потребитель (пользователь) информации вправе свободно искать, получать, передавать, производить и распространять информацию любым законным способом. К сожалению, эти информационные действия не увязаны с функциями субъектов информационной сферы, а также с информационными действиями, описанными в законе РФ "Об информации...", в частности, это — создание, обработка, накопление, хранение, поиск, распространение и потребление информации.

Несомненным достоинством Доктрины является включение положения об укреплении механизма правового регулирования отношений в области охраны интеллектуальной собственности.

В Доктрине выделены виды угроз информационной безопасности РФ, среди которых упомянуты манипулирование информацией (дезинформация, сокрытие или искажение информации). Как уже было отмечено в [2 и 3], к сожалению, до сих пор не получили развития исследования таких свойств информации, как некачественная, недостоверная и ложная информация, упомянутые в законах РФ. Аналогичная ситуация характерна для Доктрины, так как в ней нет расшифровки вышеуказанных понятий. Наши соображения по поводу несанкционированного использования информации приведены в [2].

Из последнего определения информационной сферы можно сделать вывод, что в ней есть субъекты, которые собирают, формируют и распространяют информацию, и есть субъекты, которые используют информацию. В соответствии с Гражданским кодексом РФ (ГК РФ) информация является объектом гражданских прав, а стало быть у нее могут быть авторы, владельцы, которые могут устанавливать на нее ограничения и запреты. Кроме того, в информационной сфере имеется система регулирования возникающих при этом общественных отношений, которая также может вводить ограничения и запреты на оборот информации, в частности, на информацию, содержащую государственную тайну.

В связи с тем, что у информации может быть не только владелец, но и автор, на некоторые информационные продукты распространяются действия закона об авторском праве и законов, охраняющих интеллектуальную собственность, что вводит ограничение на оборот некоторых видов информации.

В Доктрине только упоминается понятие "информационного рынка", а этой теме необходимо уделять самое серьезное внимание [4], кроме того, отмечается неразвитость институтов гражданского общества, недостаточность разработанности нормативной правовой базы, регулирующей отношения в информационной сфере.

В качестве методов обеспечения информационной безопасности в Доктрине предлагается разработка и принятие нормативных правовых документов, устанавливающих ответственность лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну.

В качестве мер противодействия предусматривается создание систем и средств предотвращения несанкционированного доступа к информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также перехвата информации при ее передаче.

К сожалению, эти два метода обеспечения информационной безопасности слабо увязаны между собой, так как получается, что за противоправное (несанкционированное) разрушение информации ответственности не должно быть предусмотрено.

В соответствии со ст. 272 Уголовного кодекса РФ (УК РФ) — Неправомерный доступ к компьютерной информации — подразумевается ответственность за неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

К охраняемой законом информации относят только ту, которая упоминается в законодательстве РФ. Закон РФ "О государственной тайне" охраняет информацию, содержащую государственную тайну, закон РФ "Об информации..." охраняет конфиденциальную информацию, а ГК РФ охраняет информацию, содержащую служебную и коммерческую тайны, и наконец, Конституция РФ закрепила, что любой гражданин имеет право на личную, семейную тайну, защиту своей чести и доброго имени, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Основная часть ответственности за преступления в информационной сфере регламентируется в УК РФ.

Понятие "доступ к информации" в УК РФ комментируется как возможность ознакомления с информацией, т. е. возможность восприятия, снятия, копирования и т. п. Однако к преступлению по ст. 272 УК РФ относят только материальный состав,

т. е. реальное наступление последствий. Если зрительное восприятие информации с экрана компьютера не приводит к материальному ущербу, например, к разглашению или тиражированию информации, то и не должно возникать санкций.

Ст. 273 и 274 УК РФ хотя и касаются вредоносных программ и правил эксплуатации ЭВМ, на самом деле также напрямую связаны с незаконным обращением компьютерной информации, так как вредоносные программы и программы, с помощью которых эксплуатируются ЭВМ, представляют собой компьютерную информацию.

В УК РФ отмечены следующие операции с компьютерной информацией: уничтожение, блокирование, модификация либо копирование.

Ранее было отмечено, что доступ подразумевает в том числе копирование. Рассмотрим более подробно уничтожение, блокирование и модификацию. Комментарий ст. 272 под "уничтожением" подразумевает физическое уничтожение экземпляра информации, т. е. уничтожение носителя с информацией либо стирание информации на носителе, при этом в данной статье не указано, что делать в случае, если при этом остается резервная копия этой информации. Разъяснение комментария ст. 272 по поводу блокирования информации, т. е. ограничения доступа в пользовании этой информацией владельцем, дает основание полагать, что уничтожение, если оно уничтожает не только конкретную информацию, но и все ее копии, является собственно уничтожением, а в общем случае уничтожение является блокированием, так как при копировании резервной копии возможно восстановление информации. Модификация подразумевает изменение информации в неприемлемом для владельца варианте.

Кроме законодательных актов существуют ГОСТы, которые также являются обязательными при защите информации [5–8]. Однако Доктрина слабо увязана положениями этих ГОСТов.

Под "защитой информации" [5] понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Под "утечкой информации" [5] понимается неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками. Под "несанкционированным доступом" [5] понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Под "разглашением защищаемой информации" [5] подразумевается несанкционированное доведение защищаемой информации до потребителей, не имеющих прав доступа к этой информации.

В связи с тем, что в понятие "защита информации" входит безопасность, целостность и сохранность информации, эти понятия являются базовыми для информационной сферы. Информация является не материальным, а материализованным объектом, поэтому под целостностью информации, на наш взгляд, надо понимать неприкосновенность информации, что подразумевает невозможность любого несанкционированного отражения информации, т. е., другими словами, информацию нельзя видеть или чувственно воспринимать любому субъекту, не имеющему на это полномочий. Под сохранностью информации необходимо понимать невозможность любого несанкционированного отображения информации, в том числе копирования.

В соответствии со ст. 20 закона РФ "Об информации...", к целям защиты информации относят предотвращение утечки, хищения, утраты, искажения, подделки информации, а также предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации. Из последнего видно, что возможны санкционированные действия по уничтожению, модификации, искажению (исправлению), копированию и блокированию (защите) информации.

Несанкционированные действия с информацией могут быть произведены в виде непреднамеренного случайного воздействия из внутренней среды или внешнего окружения (неквалифицированные действия персонала, отключение электропитания, стихийные бедствия) или в виде преднамеренного вмешательства (целенаправленные действия персонала, внешних субъектов, посредников, обработчиков информации).

В результате случайного воздействия информация может быть утрачена, недоступна, испорчена, а в случае преднамеренного несанкционированного вмешательства может быть уничтожена, блокирована, искажена (подделана), похищена, скопирована, подвергнута утечке, модифицирована (нарушение авторских и исключительных прав). В связи с этим под понятие "санкционированная обработка информации" попадают следующие операции: блокировка (защита), уничтожение (стирание), копирование, модификация и преобразование. Модификацией информации считаются такие ее изменения, которые требуют разрешения автора, собственника этой информации. Преобразованием информации считаются такие операции, которые предписаны информационной системой, технологией. Защита информации подразумевает операции, позволяющие сделать ее недоступной определенным видам операций.

В связи с тем, что информация не является материальным объектом (вещью), в праве существует две точки зрения на возможность хищения информации (информацию можно похитить и нельзя этого сделать). Здесь под "похищением информации" подразумевается похищение экземпляра информации, т. е. носителя информации вместе с информацией. Если информация размещена на единственном экземпляре и он был похищен, то такое деяние можно рассматривать как хищение. Понятие "утечка информации" подразумевает несанкционированное разглашение информации.

Искажением и подделкой называют операции по сокрытию (устранению), замене или внесению каких-либо элементов информации на синтаксическом, семантическом или прагматическом уровнях.

На синтаксическом уровне подразумеваются операции со знаками (сигналами) информации, при которых не теряется ее смысл. На семантическом уровне — операции с информацией, при которых теряется ее смысл, однако, как известно, в некоторых случаях, адекватный отклик у субъекта при ее

получении не теряется. На прагматическом уровне — операции с информацией, при которых теряется необходимый отклик у субъекта при получении этой информации.

Когда говорят об обороте информации как информационного продукта (товара), то подразумевают, что есть владелец информации, который санкционирует этот оборот. Под "оборотом информации" будем понимать операции по хранению (накоплению, транспортировке во времени), перемещению (транспортировке в пространстве) и смене владельца или статуса информации (транспортировке в некоторой сфере принадлежности с точки зрения гражданских прав). Операции сбора информации и распространения относятся к операциям перемещения информации.

Операция распространения имеет разновидность — предоставление информации, которая отличается от распространения тем, что информация должна предоставляться определенному кругу лиц, и на нее накладывается еще одно ограничение, в частности, непредоставление органами власти определенного вида информации преследуется по закону.

Законодательно запрещено предоставление и распространение информации, которая может унижать честь и достоинство конкретного лица или противоречить понятиям общества о нравственности или отдельным интересам государства.

Сбор информации также регламентируется законом, в частности запрещен незаконный и негласный сбор информации, в том числе сведений, составляющих коммерческую и банковскую тайну. Запрещен сбор информации, непосредственно затрагивающей права и свободы гражданина, кроме той, ознакомление с которой регламентируется законом. Данная информация должна находиться в государственных органах или органах местного самоуправления, собрана законным путем, содержать информацию по конкретному человеку.

Теперь рассмотрим понятия "манипулирование информацией" (дезинформация, сокрытие или искажение), а также "некачественная", "недостоверная" и "ложная" информация.

В законодательных актах широко используются понятия "заведомо ложная информация", "заведомо ложное сообщение", "заведомо ложный донос", "заведомо ложные показания", под которыми понимается дезинформация, информация, не соответствующая действительности, недостоверная. Кроме того, выделяют "предоставление неполной информации", т. е. в этом случае часть информации сокрыта. Существует понятие "дефектной" информации, т. е. имеющей недостатки [9]. Если информацию рассматривать как информационный товар (услугу), предназначенный для потребителей, то тогда в соответствии с [10] информация может иметь недостатки или существенные недостатки, а также быть опасной. Если в качестве получателя информации выступает пользователь, а не потребитель, то тогда на отношения между субъектами, передающими и получающими информацию, действие данного закона не распространяется.

Если какие-либо случайные воздействия на информацию приводят к недостаткам информации, которые делают невозможным или недопустимым понимание или использование информации, то такие недостатки информации считаются существенными, а сама информация является некачественной и дефектной. В этих случаях потребитель информации может предъявить претензии в соответствии с законом РФ "О защите прав потребителей". Если информация распространяется на безвозмездной основе, то пользователь этой информации не может предъявить претензий к распространителю этой информации по качеству информации.

Однако вне зависимости от того, на какой основе распространяется информация, если она фальсифицирована, т. е. в ней сокрыта какая-то ее часть или произведено искажение, или введена какая-либо иная информация, или любая совокупность из этих действий, приводящих к несоответствию сведений, относящихся к элементу действительности, который отражается в этой информации, лица, которых непосредственно затрагивает эта фальсифицированная информация, могут в законном порядке предъявить свои претензии к распространителю этой фальсифицированной информации. К этим лицам, естественно, относятся и лица, ответственные за регулирование общественных отношений в информационной сфере.

Под "распространением заведомо ложной информации" понимается не распространение и иное использование всякой информации, не соответствующей определенным элементам действительности, а только сообщение или несообщение юридически значимой информации. В круг этой информации входит информация, которую лицо, распространяющее информацию, обязано сообщить действительному или потенциальному пользователю или потребителю информации, либо это лицо распространило или использовало эту информацию в корыстных или преступных целях в нарушении закона.

В связи с этим, необходим институт экспертного исследования информации как информационного объекта на предмет его ложности, недостоверности или неполноты.

На сложность расследования неправомерного доступа к компьютерной информации указывается в [11].

Отсюда следует необходимость решения диагностической задачи: удовлетворяет (не удовлетворяет) исследуемый информационный объект установленным требованиям в нормативах, и если не удовлетворяет, то по какой причине, в том числе, создан (искажен) ли информационный объект с умыслом? Для того чтобы ответить на данные вопросы, эксперт должен иметь во-первых нормативы, во-вторых информацию из другого источника об элементе действительности, по поводу которого был создан исследуемый информационный объект.

Сокрытие, замена или внесение каких-либо иных компонент информационного объекта возможно на этапе хранения, перемещения и изменения статуса этого информационного объекта. Любое из вышеуказанных действий (сокрытие, замена, внесение) может привести к ложности, недостоверности, неполноте информации. Сокрытие можно рассматривать как частичное или полное уничтожение (непредоставление) информации. Замену или искажение можно рассматривать как частичное или полное изменение имеющейся информации. Внесение каких-либо иных компонент информации или дезинформацию можно рассматривать как частичное или полное внесение каких-либо дополни-

тельных компонент информации, которые отсутствовали в исходной информации.

Известны два термина: фальсификация и контрафакция. Их можно использовать и в информационной сфере, в частности, под "фальсификацией информационных объектов" (ресурсов, продуктов, товаров, услуг) понимать незаконное, преднамеренное, с корыстной или преступной целью введение в оборот в информационной сфере фальсифицированных информационных объектов, обладающих сокрытыми, замененными или внесенными свойствами, по отношению к элементам действительности, которые они отображают, сопровождающееся причинением материального или морального ущерба собственнику этих информационных объектов, либо лицам, которых непосредственно касается информация из данных информационных объектов. Контрафакция является разновидностью фальсификации и представляет собой намеренное, в коммерческих целях, незаконное введение в коммерческий оборот в информационной сфере фальсифицированных информационных объектов, на которые распространяются действия законов РФ об авторском праве и смежных правах, интеллектуальной собственности, а также международных договоров РФ, при котором был причинен материальный или моральный ущерб автору или собственнику исключительных прав на эти информационные объекты.

В связи с тем, что в публикациях и нормативных документах используются многочисленные синонимы вышеуказанных понятий, назрела необходимость стандартизировать данные термины, нормативно закрепить понятия несанкционированных, противоправных и противозаконных операций с информацией, а также ответственность за эти действия.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности РФ // Российская газета, 28 сентября 2000 г.
2. Нестеров А. В. Некоторые соображения по поводу федерального закона РФ "Об участии в международном информационном обмене" // НТИ. Сер. 1 .— 1999 .— № 3 .— С. 28–31.
3. Нестеров А. В. Некоторые соображения по поводу закона РФ "Об информации, информатизации и защите информации" // НТИ. Сер. 1 .— 1996 .— № 4. — С. 7–11.
4. Нестеров А. В. Информационные особенности развития Деловой среды // НТИ. Сер. 1 .— 1998 .— № 2 .— С. 5–9.
5. ГОСТ Р 50922-96. Защита информации.
6. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации.
7. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая.
8. ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники.
9. Крылов В. В. Расследование преступлений в сфере информации.— М.: Городец, 1998 .— 263 с.
10. Федеральный закон РФ "О защите прав потребителей".
11. Расследование неправомерного доступа к компьютерной информации / Ред. Шурухнов Н. Г.— М.: Щит, 1999.— 253 с.

Материал поступил в редакцию 29.01.2001.