Клименко С. Н.

Регулирование информационных отношений в таможенных органах Российской Федерации

(на примере мер по обеспечению информационной безопасности и защите интеллектуальной собственности)

Клименко Сергей Николаевич

Санкт-Петербургский имени В. Б. Бобкова филиал Российской таможенной академии
Заместитель декана экономического факультета
Преподаватель кафедры административного и таможенного права
Аспирант кафедры конституционного и административного права
Северо-Западного института управления — филиала РАНХиГС (Санкт-Петербург)
sergklim08@mail.ru

РЕФЕРАТ

В статье рассматриваются некоторые аспекты, определяющие роль и место правового регулирования информационных отношений, возникающих в сфере обеспечения информационной безопасности таможенных органов Российской Федерации.

КЛЮЧЕВЫЕ СЛОВА

информационная безопасность, правовое регулирование, таможенные органы, интеллектуальная собственность

Klimenko S. N.

Regulation of Information Relations in CustomsAuthorities of the Russian Federation (on the Example of Measures for EnsuringInformation Security and Protection of Intellectual Property)

Klimenko Sergey Nikolaevich

Saint-Petersburg branch of Russian Customs Academy, named by V. B. Bobkov
Deputy Dean of the Faculty of Economics
Lecture of the Chair Administrative and Customs Law
Graduate student of the Chair of the Constitutional and Administrative Law of North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
sergklim08@mail.ru

ABSTRACT

The article discusses some of the aspects that define the role and place of legal regulation of information relations arising in the sphere of ensuring information security of the customs bodies of the Russian Federation.

KEYWORDS

information security, legal regulation, customs, intellectual property

Основой правового регулирования отношений, возникающих в сфере информации, создаваемой в порядке осуществления творческой деятельности, а также информации, созданной в результате иной интеллектуальной деятельности, является институт интеллектуальной собственности, обеспечивающий реализацию конституционных принципов, определяющих наиболее существенные стороны организации и деятельности субъектов правоотношений в информационной сфере.

Конституция Российской Федерации (ст. 29) закрепляет один из основополагающих демократических принципов правового государства, заключающийся в наделении каждого правом на информацию, правом не только знать, быть информи-

рованным, но и правом распространения этой информации[1]. Это с одной стороны. С другой стороны, помимо закрепления права на информацию Конституция Российской Федерации содержит также нормы, указывающие на то, в каких случаях и при каких обстоятельствах данное право может быть ограничено. Речь в данном случае идет о том, что кроме общедоступных сведений существует и определенный объем информации, касающейся основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства. Получение, распространение и обработка таких сведений подлежат строгому регламентированию законодательством, которое при определенных обстоятельствах устанавливает ограничения в обороте информации между субъектами правоотношений.

Российская Федерация, являясь одним из таких субъектов, вполне объяснимо обладает собственными интересами в информационной сфере. Эти интересы пронизывают не только область соблюдения конституционных прав и свобод граждан на получение, распространение и использование информации, но и область совершенствования безопасности функционирования информационных и телекоммуникационных систем наиболее важных объектов инфраструктуры и объектов повышенной опасности, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности[2].

По сути, информационная безопасность, представляя собой систему общественных отношений, непосредственно связанных с защитой прав и законных интересов личности и общества в отношении информации, в том числе информационных ресурсов государства, является одной из важнейших составляющих национальной безопасности. Понятие системы обеспечения информационной безопасности может быть раскрыто как совокупность органов законодательной, исполнительной и судебной властей, государственных, общественных и иных организаций и объединений, граждан, принимающих участие в обеспечении информационной безопасности в соответствии с законодательством, регламентирующим отношения в данной сфере.

Органы обеспечения информационной безопасности принимают непосредственное участие в противодействии как реальным, так и потенциальным угрозам национальным интересам в информационной сфере, прежде всего в соответствии с их компетенцией, которая, по существу, и является тем фундаментом, на котором строится вся государственная система обеспечения информационной безопасности. Общая структура государственной системы обеспечения информационной безопасности Российской Федерации включает в себя четыре властные подсистемы, образующие ветви власти, различающиеся функциями в области информационной безопасности и соответственно компетенцией: Президент, законодательная, исполнительная и судебная власти.

Отметим, что одну из ведущих позиций в системе национальной безопасности государства занимают представляющие исполнительную власть таможенные органы. Поэтому уделяется пристальное внимание вопросам, решение которых обусловливает выполнение требований, направленных на организацию и обеспечение информационной безопасности в сфере таможенных правоотношений. Так, в частности, Доктрина информационной безопасности[3] декларирует, что таможенная

---

[1] Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. (в действ. ред.) // Российская газета. 2009. № 7.

[2] О Стратегии национальной безопасности Российской Федерации до 2020 года (в действ. ред.) : Указ Президента Российской Федерации от 12 мая 2009 г. № 537 // Собрание законодательства Российской Федерации. 2009. № 20. Ст. 2444.

[3] Доктрина информационной безопасности Российской Федерации. Утв. Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895 (в действ. ред.) // Российская газета. 2000. № 187.

служба кроме возложенных на нее полномочий, направленных на достижение таможенного регулирования, обеспечивает в установленной сфере деятельности исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

С целью реализации мероприятий по обеспечению безопасности информации в таможенных органах создана ведомственная система, представляющая собой совокупность организационной структуры, правового и финансового обеспечения, организационно-технических методов и средств, оперативно-разыскных мер, а также персональной ответственности всех должностных лиц и работников таможенных органов за выполнение требований информационной безопасности. Выстраивание организационной структуры ведомственной системы обеспечения информационной безопасности базируется в первую очередь на разграничении полномочий структурных подразделений Федеральной таможенной службы Российской Федерации (далее — ФТС России) и таможенных органов и включает в себя:

- руководителя Федеральной таможенной службы;
- Совет по информационной безопасности таможенных органов;
- структурные подразделения центрального аппарата ФТС России, принимающие участие в соответствии со своими функциями и полномочиями в обеспечении информационной безопасности таможенных органов, а также иные структурные подразделения центрального аппарата, соблюдающие требования по обеспечению информационной безопасности в служебной деятельности при выполнении возложенных функций и задач;
- Центральное информационно-техническое таможенное управление ФТС России;
- Региональное таможенное управление радиоэлектронной безопасности объектов таможенной инфраструктуры;
- советы по информационной безопасности региональных таможенных управлений;
- постоянно действующие технические комиссии по защите государственной тайны таможен;
- структурные подразделения таможенных органов, принимающие участие в соответствии со своими функциями и полномочиями в обеспечении информационной безопасности таможенных органов;
- иные структурные подразделения таможенных органов, соблюдающие требования по обеспечению информационной безопасности в служебной деятельности при выполнении возложенных на них функций и задач.

Современные вызовы существенным образом изменили политику Федеральной таможенной службы в информационной сфере[1]. Основные усилия ее переориентированы от защиты каждого объекта информатизации таможенных органов к комплексному обеспечению информационной безопасности. Реализация государственной политики в данной сфере возложена на ведомственную систему обеспечения информационной безопасности. К наиболее чувствительным элементам информационной безопасности таможенных органов, исходя из существующих угроз, следует отнести[2]:

- во-первых, информацию, полученную таможенными органами из различных источников и содержащую конфиденциальные сведения различного характера;
- во-вторых, документы и сведения, используемые для статистических целей;

[1] О решении, принятом на заседании коллегии ФТС России, о Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года: Приказ ФТС России от 13 декабря 2010 г. № 2401.

[2] Там же

- в-третьих, технические средства обработки информации;
- в-четвертых, объекты интеллектуальной собственности;
- в-пятых, персональные данные должностных лиц таможенных органов;
- в-шестых, открытые информационные ресурсы таможенных органов, являющиеся, как представляется, одним их наиболее чувствительных элементов;
- наконец, в-седьмых, информационные ресурсы таможенных органов, формирующиеся на базе документов и сведений, представляемых при совершении таможенных операций, а также документов, необходимых для их совершения, и др.[1].

Обеспечивая информационную безопасность указанных объектов, в частности объектов интеллектуальной собственности, создаются необходимые условия для надежного функционирования таможенных органов, эффективность деятельности которых в информационной сфере в значительной степени влияет на эффективность обеспечения экономической безопасности государства.

Пожалуй, главным инструментом в области выполнения задач, возложенных на таможенные органы по обеспечению ведения учета и осуществлению законного контроля за всеми участниками таможенных правоотношений, являются информационные ресурсы. По тематике сведений, сосредоточенных и зафиксированных в документальной информации, ресурс может содержать научную, техническую, экономическую, учебную и иную информацию, в том числе информацию об объектах интеллектуальной собственности.

Формирование и использование ресурсов осуществляется на принципах доступности, достоверности и полноты информации; своевременности предоставления информации; обеспечения информационной безопасности; соблюдения прав и законных интересов третьих лиц; обеспечения конституционных прав лиц в информационной сфере, в том числе защиты персональных данных, информации, создаваемой в результате интеллектуальной деятельности; придания направлению формирования и использования ресурсов статуса самостоятельного вида обеспечения деятельности таможенных органов. Обращает на себя внимание тот факт, что информационные ресурсы таможенных органов, формируемые на базе документов и сведений, представляемых при совершении таможенных операций, а также документов, необходимых для их совершения, имеют ограниченный доступ[2].

Основным условием формирования информационных ресурсов или отдельных элементов является установление соответствующего правового режима. Для определенных видов информации в силу их особого значения устанавливаются специфические правовые режимы. В первую очередь это относится к категории информации, которая не предназначена для широкого распространения (государственная, коммерческая, профессиональная тайна, персональные данные и др.) и в связи с этим подлежит правовой охране от несанкционированного доступа.

Необходимо отметить, что проблема обеспечения безопасности касается не только информации ограниченного распространения, для которой в соответствии с существующими нормами устанавливается особый правовой режим, но и, что немаловажно, информации неограниченного доступа, причем, вероятно, еще более основательно, чем в сфере конфиденциальности. Собственно говоря, конфиденциальность и режим тайн уже сами по себе ограничивают круг пользователей. Открытая же информация может свободно использоваться и распространяться без каких-либо ограничений любыми лицами и, как следствие, подвергаться неправомерному воз-

[1] Таможенный кодекс Таможенного союза : Приложение к договору о Таможенном кодексе Таможенного союза. Принято Решением Межгос. совета ЕврАзЭС на уровне глав государств от 27 ноября 2009 г. № 17 (в действ. ред.) // Таможенный вестник. 2010. № 2. Ст. 44.

[2] Таможенный кодекс Таможенного союза : Приложение к договору о Таможенном кодексе Таможенного союза. Принято Решением Межгос. совета ЕврАзЭС на уровне глав государств от 27 ноября 2009 г. № 17 (в действ. ред.) // Таможенный вестник. 2010. № 2. Ст. 44, 333.

действию — модификации (искажению), уничтожению, присвоению — значительно проще. Ресурсы, которыми обладает сеть Интернет, являются наглядным подтверждением данного факта. Информация, однажды выпущенная в свет, в дальнейшем может распространяться практически беспрепятственно, а создатель (первичный обладатель) такой информации фактически утрачивает возможность воспрепятствовать ее дальнейшей передаче.

К такой информации относят, как правило, сведения об общеизвестных фактах; документы, не носящие конфиденциального характера; информацию, ограничения на доступ к которой были сняты самим владельцем, в результате чего режим конфиденциальности в отношении такой информации был прекращен, а также информацию, представляющую собой разнообразные концепции, идеи, алгоритмы, которые лежат в основе охраняемых авторским правом произведений, а также изобретений или полезных моделей и были правомерно опубликованы в открытых источниках.

Рассмотрим, например, программное обеспечение. Несмотря на то что само программное обеспечение охраняется законодательством как объект интеллектуальной собственности, алгоритмы, заложенные в программу, могут быть отнесены к свободно распространяемой информации. Следует учитывать и то, что открытая информация может быть отнесена к объектам возмездных сделок. В этом случае коммерческий интерес могут представлять, например, информационные массивы, содержащие подборку данных по какой-либо теме.

Таким образом, требования к защите общедоступной информации могут устанавливаться с целью обеспечения защиты информации от неправомерного доступа, модифицирования, блокирования, копирования, предоставления, распространения, уничтожения, также от иных неправомерных деяний и при обеспечении реализации права на доступ[1]. Однако и для информации ограниченного доступа вопросы уяснения, классификации угроз, рисков не остаются простыми и не могут ограничиваться только установлением мер по их усиленной охране.

Немаловажное значение для установления правового режима играет осуществление мероприятий по ограничению доступа к информации. Обладатель ценной информации может предпринимать различные шаги с целью установления мер по охране информации и предотвращению несанкционированного доступа к ней и, как следствие, ограничению ее копирования конкурентами. Одним из таких шагов, к примеру, может являться отнесение такой информации к информации, составляющей коммерческую тайну. Для признания информации таковой, она должна удовлетворять определенным критериям: иметь действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам; к информации у третьих лиц не должно быть свободного доступа на законном основании; в отношении информации ее обладателем должен быть введен режим коммерческой тайны[2]. Необходимо также обратить внимание на то, что действующее законодательство признает информацию, составляющую коммерческую тайну, секретом производства (ноу-хау), т. е. объектом интеллектуальной собственности.

При соблюдении указанных требований обладатель информации приобретает исключительное право на интеллектуальную собственность. Это, в частности, означает наличие у него права требовать от третьих лиц соблюдения установленного режима конфиденциальности и запрещения доступа к информации путем вве-

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ (в действ. ред.) // Российская газета. 2006. № 165.

[2] О коммерческой тайне (в действ. ред.) : Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.

дения превентивных (административно-предупредительных) мер защиты. В случае нарушения этого режима правообладатель вправе использовать гарантированные государством средства защиты.

Однако, как показывает практика, могут присутствовать различные факторы, препятствующие правообладателю защитить свои права в области использования и распространения коммерчески важной информации. К примеру, если информация появляется у третьих лиц правомерно, т. е. без преодоления установленных правообладателем барьеров, или третье лицо получает такую информацию самостоятельно в результате проведенных исследований, то правообладатель будет лишен правомочий воспрепятствовать копированию информации. В другом случае третьи лица получают право использовать информацию свободно, если лицо вводит режим коммерческой тайны в отношении информации, которая в действительности ценностью не обладает либо является доступной из открытых источников. Однако при возникновении спора на третьих лиц будет возложена обязанность представления доказательств того, что информация к коммерческой тайне не относится.

Таким образом, государство, выступая лишь гарантом защиты прав и законных интересов обладателей коммерчески важной информации на ее использование и сохранение в тайне, возлагает на правообладателя всю ответственность за организацию и осуществление мер по защите неприкосновенности этой информации.

В сфере компьютерных технологий к объектам интеллектуальной собственности относятся программы для ЭВМ и базы данных, охраняемые как объекты авторского права, а также различные технические решения, охраняемые в качестве объектов патентного права[1]. В соответствии со ст. 1259 Гражданского кодекса Российской Федерации авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования. Отсюда следует, что охраняемым в качестве объекта интеллектуальной собственности является собственно программа, так называемый «текст» программы, выраженный в какой-либо объективной форме. Сама же идея или концепция такой программы, результат, достигаемый с ее помощью, а также алгоритм его достижения правовой охране не подлежат. В качестве объекта авторского права также подлежат охране базы данных, под которыми Гражданский кодекс Российской Федерации (ст. 1260) понимает представленную в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Таким образом, обладателю информации, лежащей в основе интеллектуальной деятельности, законодательством Российской Федерации, регулирующим отношения в области безопасности информации, в том числе и в таможенной сфере, предоставляются достаточно широкие возможности для защиты этой информации. Для реализации этих возможностей необходимо осуществить правильный выбор существующих форм и методов охраны информации и интеллектуальной собственности в зависимости от обстоятельств, сложившихся в конкретной ситуации.

[1] Гражданский кодекс Российской Федерации. Часть четвертая : Федеральный закон от 18 декабря 2005 г. № 230-ФЗ (в действ. ред.) // Собрание законодательства Российской Федерации. 2006. № 52. Ст. 5496.