УДК 349 Правоведение. 2019. Т. 63, № 1

О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике

А. С. Озерова

Для цитирования: *Озерова А. С.* О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике // Правоведение. 2019. Т. 63, № 1. С. 137–156. https://doi.org/10.21638/spbu25.2019.107

Автор статьи рассматривает информацию как объект правоотношений. В связи с решающим значением роли информации во всех сферах современного общества защита анализируемого социального блага является приоритетной задачей государства. Однако, несмотря на значимость информации, в российском праве отсутствует системное и последовательное законодательное регулирование информационных отношений. Законодательные противоречия, отсутствие единой терминологии и научного подхода не способствуют эффективной правовой защите информации и формированию единообразной судебной практики. На основе системного анализа законодательства и правоприменительной практики разработано авторское понимание информации как объекта правоотношений, а также рассмотрены ее основные признаки. Обосновывается вывод о том, что информация выступает объектом гражданских правоотношений, в связи с чем предлагается вернуть в ст. 128 Гражданского кодекса РФ указание на информацию как объект гражданских прав. Анализируется предмет неправомерного доступа к компьютерной информации (ст. 272 Уголовного кодекса РФ). Предметом преступления, предусмотренного ст. 272 УК РФ, выступает информация, доступ к которой прямо ограничен законом, а также информация, относительно которой наличествует объявленное неопределенному кругу лиц требование обладателя об ограничениях по ее использованию (доступу к ней). Вопрос об отнесении сведений второй категории к охраняемым уголовным законом должен решаться судьей в каждом конкретном деле. Делается вывод о том, что основанием правовой охраны информации должны быть прямое указание закона или установление обладателем общедоступной информации порядка обращения с ней. Общедоступность компьютерной информации означает возможность беспрепятственного ее использования (копирование, распространение), а не блокирования, уничтожения и модификации. Предлагаются критерии для решения судом вопроса о предоставлении правовой защиты сведениям, которые прямо не отнесены законом к категории ограниченного доступа. Анализируются способы неправомерного доступа к компьютерной информации. В целях устранения правовой неопределенности предлагается новое понимание термина «охраняемая законом компьютерная информация».

Ключевые слова: информация, неправомерный доступ к информации, компьютерная информация, основания правовой охраны, уголовно-правовая защита информации, информация ограниченного доступа, конфиденциальная информация.

Информация в современном обществе — уникальный ресурс, влияющий на состояние экономики, технического развития и социальной сферы любого государства. Национальное благосостояние страны и уровень жизни ее граждан определяется в том числе уровнем развития и использования информационных ресурсов.

В связи с решающим значением роли информации во всех сферах современного общества защита этого социального блага — приоритетная задача государства. Однако, несмотря на значимость информации, в российском праве

Озерова Анна Сергеевна — аспирант, Московский государственный университет им. М. В. Ломоносова, Российская Федерация, 119991, Москва, Ленинские горы, 1; annaozerova55@mail.ru

© Санкт-Петербургский государственный университет, 2020

отсутствует системное и последовательное законодательное регулирование информационных отношений.

С 1 января 1995 г. и до принятия Федерального закона от 18.12.2006 № 231-ФЗ «О введении в действие части четвертой Гражданского кодекса РФ»[1] информация была названа в качестве объекта гражданских прав в ст. 128 Гражданского кодекса РФ (далее — ГК РФ). В настоящее время в перечне объектов гражданских прав информация прямо не указана. Представляется, что данный шаг законодателя непоследователен и не вполне согласуется с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации). Так, в ст. 5 Закона прямо закреплено, что информация может являться объектом публичных, гражданских и иных правоотношений, а в подп. 3 п. 3 ст. 6 указывается, что информация может передаваться по договору другому лицу.

Вопрос о возможности отнесения информации к объектам гражданских прав вызывает множество споров среди правоведов[2]. Применяя системный метод толкования и руководствуясь содержанием п. 2 ст. 3, ст. 128 ГК РФ, а также ст. 5 Закона об информации и правовой позицией Конституционного суда РФ (Постановление от 26.10.2017 № 25-П), можно сделать следующий вывод: несмотря на то что информация прямо не названа законодателем в качестве объекта правоотношений в ст. 128 ГК РФ, нельзя утверждать, что она таковым не является.

В качестве объекта гражданских правоотношений информация прямо определена в Законе об информации. В ст. 3 ГК РФ указывается, что гражданское законодательство состоит из ГК РФ и принятых в соответствии с ним иных федеральных законов, которые направлены на регулирование отношений, составляющих предмет гражданского права. Так, нормы Закона об информации (в частности ст. 6, 8, 10) определяют *статус «собственника» информации* (правовое положение участника гражданского оборота), а также регулируют отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации. Соответственно указанный Закон, прямо определяющий информацию в качестве объекта правоотношений, — неотъемлемая часть системы гражданского законодательства.

О взаимосвязи Закона об информации и ГК РФ Конституционный суд РФ указывал в Постановлении от 26.10.2017 № 25-П: «Федеральный законодатель, вводя понятие “обладатель информации”, стремился описать его по аналогии с гражданско-правовыми категориями “собственник”, “титульный владелец”, но с учетом особенностей *информации как нематериального объекта* (здесь и далее в цитатах курсив мой. — *А. О.*)».

К нематериальным благам в соответствии со ст. 150 ГК РФ относятся в том числе честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, имя гражданина и иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона.

Информация как объект гражданских правоотношений также отражена в *судебной практике.* Судом установлено: «Информация о деятельности государ-

---

[1] Здесь и далее, если не указано иное, нормативно-правовые и подзаконные акты, а также судебная практика приводятся по СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2020).

[2] См., напр.: *Кириченко О. В.* Информация как объект гражданских правоотношений // Современное право. 2014. № 9. С. 77–80; *Малинин В. Б.* Правовое регулирование информации // Ленинградский юридический журнал. 2015. № 3. С. 122–126; *Инюшкин А. А.* Информация в системе объектов гражданских прав и ее взаимосвязь с интеллектуальной собственностью на примере баз данных // Информационное право. 2016. № 4. С. 4–7.

ственных органов является объектом публичных отношений. Однако информация о привлеченных к административной ответственности юридических лицах в интересующем заявителя объеме (ИНН/ОГРН, наименование, статья КоАП РФ и др.) не связана с защитой прав самого общества. Поскольку целью получения такой информации является поиск клиентов, потенциально нуждающихся в юридических услугах, и извлечение прибыли; *такая информация обоснованно квалифицирована судом как объект гражданских отношений*»[3]. Данные выводы признаны обоснованными вышестоящими судебными инстанциями[4].

Суды, рассматривая споры о предоставлении специализированной информации (например, «О состоянии окружающей среды, ее загрязнении и информационная продукция»[5]), прибегают к общим положениям гражданского законодательства об исполнении обязательств (ст. 309–310 ГК РФ)[6]. *Специализированная информация*, предоставляемая пользователям (потребителям) на основе договоров возмездного оказания услуг, *выступает предметом указанных договоров*.

С нашей точки зрения, гражданско-правовые отношения, складывающиеся по поводу информации, не должны выходить за сферу действия ст. 1 Закона об информации (перечень регулируемых указанным Законом отношений); по общему правилу положения Закона об информации не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации. Не любой информационный массив должен признаваться объектом гражданских правоотношений; так, сведения, составляющие охраняемую законом тайну, не могут свободно отчуждаться или переходить от одного лица к другому в соответствии со ст. 129 ГК РФ.

Таким образом, определение информации в качестве объекта гражданского права отвечает практическим потребностям и не противоречит ГК РФ. Подход, согласно которому существует необходимость признать информацию в качестве объекта гражданских правоотношений, разделяют многие правоведы[7].

Признание категории «информация» объектом гражданских прав представляет интерес для уголовного права, так как реализация охранительной функции и обеспечение информационной безопасности невозможны без четкого определения социального блага, подлежащего защите в специальном отраслевом законодательстве. Неопределенный на сегодняшний день в гражданском законодательстве правовой статус информации препятствует разрешению вопроса об уголовно-правовой охране сведений, выступающих объектом гражданских правоотношений.

Представляется, что ст. 128 ГК РФ должна быть сформулирована в следующей редакции: «К объектам гражданских прав относятся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе безна-

---

[3] Постановление Тринадцатого арбитражного апелляционного суда от 25.12.2012 по делу № А56-35417/2012.

[4] Постановление Федерального арбитражного суда (далее — ФАС) Северо-Западного округа от 15.05.2013 по делу № А56-35417/2012; Определение Высшего арбитражного суда РФ от 12.09.2013 № ВАС-11893/13 по делу № А56-35417/2012.

[5] Статья 17 Федерального закона от 19.07.1998 № 113-ФЗ «О гидрометеорологической службе».

[6] Постановление Тринадцатого арбитражного апелляционного суда от 10.07.2018 № 13АП-7972/2018 по делу № А56-35101/2016; Постановление Арбитражного суда Восточно-Сибирского округа от 06.04.2015 № Ф02-1074/2015 по делу № А58-3226/2014; Постановление Девятого арбитражного апелляционного суда от 07.06.2018 № 09АП-19499/2018 по делу № А40-244221/17.

[7] См., напр.: *Вайпан В. А.* Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 1. С. 15; *Зверева Е. А.* Информация как объект неимущественных гражданских прав // Врач и информационные технологии. 2004. № 8. С. 60–64; *Кирсанова Е. Е.* Возникновение новых объектов правовой защиты в условиях цифровой экономики // Юрист. 2018. № 11. С. 19–22.

личные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказание услуг; *информация*; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага».

Теперь перейдем непосредственно к понятию информации и определим ее основные признаки как объекта правоотношений.

На сегодня в правовой науке отсутствует единое понимание сущности информации. Согласно ст. 2 Закона об информации, информация — это сведения (сообщения, данные) независимо от формы их представления. Легальная дефиниция не делает различий между сведениями, данными и сообщениями, определяя их как равные по своему правовому режиму виды информации. Соответственно, форма представления информации не влияет на определение ее правового режима. Наличие огромного количества форм выражения информации (носителей), число которых постоянно увеличивается, не позволяет дать их исчерпывающий перечень.

Широкое понимание законодателем информации приводит к невозможности установления на его основе конкретных признаков и свойств рассматриваемой категории, которые помогли бы решить проблемы, стоящие перед правоприменительной практикой. Так, Е. А. Суханов справедливо отмечает: «Абстрактная информация – это не объект гражданского права, это вообще во многих случаях не объект права. Для того чтобы быть объектом правоотношения, информация должна быть объектом субъективного гражданского права его участника»[8].

Анализ судебной практики, правовой литературы и нормативно-правовых актов, предметом которых выступает информация, позволил выявить следующие существенные признаки информации как объекта правоотношений:

— информация обладает следующими характеристиками: *актуальность*[9], *полезность*[10], *новизна*[11], *достоверность*[12]; она не подвержена физическому

---

[8] Перспективы развития гражданского законодательства в России: планы и современные реалии: интервью с Е. А. Сухановым // СПС «КонсультантПлюс». URL: http://www.consultant.ru/law/interview/sukhanov/ (дата обращения: 28.04.2020).

[9] См. ст. 5 Федерального закона от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации» (актуальность информации, содержащейся в реестре поставщиков); ст. 2 Федерального закона от 29.12.2017 № 443-ФЗ «Об организации дорожного движения в Российской Федерации и о внесении изменений в отдельные законодательные акты РФ» (актуальность информации о мероприятиях по организации дорожного движения); ст. 10 Федерального закона от 03.07.2016 № 238-ФЗ «О независимой оценке квалификации» и др.

[10] Постановление Арбитражного суда Московского округа от 17.04.2018 № Ф05-3645/2018 по делу № А40-125308/2017 («полезная информация в рамках оказания услуг»); Постановление ФАС Поволжского округа от 24.12.2012 по делу № А12-21778/2011 («объем полезной информации для идентификации графической информации»); п. 9.1.3 «ГОСТ Р 57189-2016/ISO/TS 9002:2016. Национальный стандарт Российской Федерации. Системы менеджмента качества. Руководство по применению ИСО 9001:2015 (ISO/TS 9002:2016, IDT)» (полезная информация для принятия решений руководством).

[11] Постановление Девятого арбитражного апелляционного суда от 11.02.2015 № 09АП-292/2015 по делу № А40-131004/14 («представленные ЗАО “КомплектСервис” отчеты, не содержат новизны информации»); Постановление Седьмого арбитражного апелляционного суда от 29.07.2015 № 07АП-1044/2014 по делу № А67-1/2014 («субъективная новизна информации, полученной заявителем из неназванных источников, не может являться основанием... для пересмотра судебного акта»); Распоряжение первого заместителя Мэра в Правительстве Москвы от 18.01.2006 № 2-РЗМ («новизна информации, содержащейся в документе»).

[12] Обзор практики рассмотрения судами дел по спорам о защите чести, достоинства и деловой репутации, утв. Президиумом Верховного суда РФ 16.03.2016 (возможность администратора сайта по определению достоверности информации); Определение Верховного суда РФ от 16.01.2018 № 25-КГ17-38 (необходимая и достоверная информация о приобретаемом товаре) и др.

старению, при этом сведения способны потерять актуальность с течением времени; внешнему воздействию могут быть подвержены исключительно материальные носители информации;

— информация как нематериальное благо обладает свойством *неисчерпаемости*[13], что означает возможность одновременного использования определенных сведений множеством лиц без ущерба для них, неоднократное воспроизведение на материальных носителях и изменение форм фиксации без изменения их содержания;

— информация есть *нематериальное благо*, при правомерном пользовании которым не ухудшаются его полезные свойства[14];

— информация обладает *действительной* или *потенциальной ценностью* сведений, содержащихся в ней;

— информация может иметь *стоимостное выражение*; ст. 5 Федерального закона от 29.07.1998 № 135-ФЗ «Об оценочной деятельности в Российской Федерации» определяет информацию в качестве объекта оценки[15]; таким образом, можно говорить о стоимости информации, выражаемой в том числе в доходе, который может быть извлечен при ее использовании и/или ее полезности для решения тех или иных задач;

— информация характеризуется *обособленностью*, т. е. фиксируется в материальной или идеальной форме; В. П. Числин пишет, что «охраняемая законом информация — это документированная информация, содержащая сведения, отнесенные законом к государственной тайне или конфиденциальной информации»[16]; данная точка зрения необоснованно сужает предмет правовой охраны, ведь значимая и неизвестная неопределенному кругу лиц информация не обязательно фиксируется на материальном носителе и имеет определенные реквизиты, носителем информации способен выступать человек; соответственно путем угроз и иных противоправных действий информация может быть получена от ее законного владельца; указанный подход также вытекает из законодательного определения информации (сведения (сообщения, данные) независимо от формы их представления);

— свойством информации, наделенной правовой охраной выступает *наличие специального правового режима*[17]; по нашему мнению, прямое указание закона или установление обладателем информации порядка обращения с ней есть основание правовой охраны информации.

---

[13] *Кузьмин В. П.* Понятие и юридическая сущность информации // Информационное право. 2009. № 2. С. 4–8.

[14] *Салихов И. И.* Информация с ограниченным доступом как объект гражданских правоотношений: дис. … канд. юрид. наук. Казань: Казанский государственный университет им. В. И. Ульянова-Ленина, 2004. С. 21.

[15] Согласно ст. 3 Федерального закона от 29.07.1998 № 135-ФЗ «Об оценочной деятельности в Российской Федерации», под оценочной деятельностью понимается профессиональная деятельность, направленная на установление в отношении объектов оценки рыночной, кадастровой, ликвидационной, инвестиционной или иной предусмотренной федеральными стандартами оценки стоимости.

[16] *Числин В. П.* Уголовно-правовые меры защиты информации от неправомерного доступа: дис. … канд. юрид. наук. М.: Коломенский государственный педагогический институт, 2004. С. 36.

[17] Под правовым режимом понимается порядок регулирования, выраженный в комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создающих особую направленность регулирования (*Алексеев С. С.* Теория права. М.: БЕК, 1995. С. 243).

Статья 5 Закона об информации разделяет информацию на *общедоступную* и *ограниченного доступа* (доступ к которой ограничен федеральными законами). Соответственно отсутствие прямого указания закона об ограничении доступа к тем или иным сведениям означает автоматическое отнесение указанных сведений к категории общедоступных.

Некоторые исследователи говорят о правовой охране сведений, относящихся исключительно ко второй категории (ограниченного доступа). Так, А. М. Доронин указывает, что «охраняемая законом информация — это информация ограниченного доступа, которая имеет не только особенный правовой режим, установленный (закрепленный) соответствующими законами РФ или ее субъектов, но и по своему характеру предназначена для ограниченного круга лиц (пользователей), имеющих право на ознакомление и работу с ней»[18].

По нашему мнению, указанная позиция небесспорна. В случае отсутствия прямого указания закона о наделении сведений статусом «ограниченных в обороте» основанием для правовой охраны может выступать установление обладателем таких сведений порядка обращения с ними (или ограничение доступа к ним).

Сам законодатель выбрал указанный подход, закрепив в п. 3 ст. 6 Закона об информации, что *обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа*.

Согласно ст. 7 Закона об информации к общедоступной информации относятся общеизвестные сведения и *иная информация, доступ к которой не ограничен*. Системное толкование закона позволяет сделать вывод, что по смыслу ст. 7 Закона об информации общедоступность сведений означает их беспрепятственное использование (копирование, распространение), а не блокирование, уничтожение и модификацию.

Соответственно, действия по уничтожению и модификации общедоступной информации будут разновидностью несанкционированного доступа (если обладатель таких сведений установил в их отношении специальный режим обращения с ними, который явствует из обстановки, — например, установление пароля, который препятствует получению доступа для изменения или уничтожения такой информации).

Справедливо следующее высказывание: «Хотя ч. 1 ст. 7 Федерального закона “Об информации” гласит, что доступ к общедоступной информации не ограничен, речь идет о доступе на распространение и трансляцию данной информации. Это подтверждает формулировка ч. 2 ст. 7 Федерального закона “Об информации”, где определяется, что “общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении *распространения* (курсив мой. — *А. О.*) такой информации”»[19].

А. И. Савельев, разделяя указанное мнение, пишет, что идея о невозможности общедоступной информации выступать объектом гражданского оборота высказывалась лишь в доктрине, в гражданском законодательстве такой запрет отсутствует[20].

Полагаем, что лицо, обладающее определенными сведениями, должно предпринимать все разумные меры (правовые, организационные, технические) к тому,

---

[18] *Доронин А. М.* Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М.: Московский университет МВД России, 2003. С. 87.

[19] *Дремлюга Р. И.* Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 56–57.

[20] *Савельев А. И.* Комментарий к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации». М.: Статут, 2015.

чтобы у неограниченного круга лиц отсутствовала беспрепятственная возможность модифицировать или уничтожить такие сведения. В противном случае информацию нельзя рассматривать как объект правовой охраны. Данная обязанность также закреплена в ст. 6 Закона об информации, где указывается, что «обладатель информации обязан принимать меры по защите информации».

По нашему мнению, следующие категории общедоступных сведений могут представлять ценность для их обладателя (в настоящее время законом указанная информация не защищена, т. е. фактически является общедоступной):

— информация о новых решениях и технических знаниях, в том числе не защищаемых законом, полученная благодаря исполнению обязательства по договору подряда; порядок и условия пользования такой информацией определяются соглашением сторон (ст. 727 ГК РФ); указанные сведения не всегда составляют коммерческую тайну, при этом в судебной практике[21] они определяются как конфиденциальные; существует практическая потребность в правовой охране рассматриваемой категории сведений, которые в настоящее время законом не защищены; так, субъекты предпринимательской деятельности, например, указывают, что «под «конфиденциальной информацией понимается любая информация, включая (но не только) информацию, которая в соответствии с законодательством и иными правовыми актами РФ *не может быть отнесена к служебной или коммерческой тайне*, *информацию, которая является общеизвестной* в результате действия (бездействия) раскрывающей стороны, информацию, правомерно полученную от третьих лиц, информацию, независимо разработанную принимающей стороной, но касающуюся раскрывающей стороны и ее деятельности»[22];

— сведения, составляющие сущность идеи, концепции, принципов, методов, процессов, систем, способов, решений технических, организационных или иных задач, открытий, языков программирования, т. е. объектов, которые не защищены авторским правом в силу прямого указания закона (ст. 1259 ГК РФ);

— объединение пользовательского контента, которое имеет ценность для маркетинга; указанный контент представляет собой упорядоченную совокупность данных, безвозмездно и публично размещенных пользователями, в которых в том или иной контексте упоминается предмет маркетинга; в состав пользовательского контента, в частности, могут входить: отзывы, обзоры, отчеты, сравнения, аннотации о предмете маркетинга; компиляция пользовательского и экспертного опыта, а также иная подборка информа-

[21] См., напр., Постановление Девятнадцатого арбитражного апелляционного суда от 29.10.2009 по делу № А48-2382/2009 о признании недействительным договора уступки прав требования между ОАО «ОрелТИСИЗ» и ООО «Росстройизыскания» ввиду нарушения соглашения о конфиденциальности. Суд, ссылаясь на ст. 727 ГК РФ, указал, что уступка требования не допускается в связи с тем, что она противоречит договору субподряда № 2/01-ДР-07 на выполнение проектно-изыскательских работ от 20.02.2007, заключенного между ООО «Смоленсктрансизыскания» и ОАО «ОрелТИСИЗ», в п. 13.1 которого предусматривается, что условия договора, дополнительных соглашений и приложений к нему, конфиденциальны и не подлежат разглашению. Если иное не будет установлено соглашением сторон, то конфиденциальны также все получаемые сторонами друг от друга в процессе исполнения договора сведения, за исключением тех, которые без участия сторон были или будут опубликованы или распространены в иной форме в официальных (служебных) источниках, либо стали/станут известны без участия сторон от третьих лиц.

[22] См., напр.: Постановление Девятнадцатого арбитражного апелляционного суда от 25.02.2009 № 19АП-467/2009 по делу № А48-933/08-1; Постановление Арбитражного суда Московского округа от 25.11.2015 № Ф05-12023/2015 по делу № А40-52978/2014; Апелляционное определение Суда Ямало-Ненецкого автономного округа от 15.01.2015 № 33-3382/2014.

ции, которая претендует на объективность, так как ее источником являются непосредственно пользователи того или иного продукта или эксперты в той или иной области; указанные сведения позволяют анализировать мнения пользователей продукта относительно его свойств, устранять его недостатки и более эффективно продвигать; соответственно, ценность таких сведений для обладателя предмета маркетинга очевидна;

— страницы блогеров, имеющих значительное количество подписчиков, в социальных сетях Интернета; Р. И. Дремлюга отмечает, что информация, размещенная в блогах, не подпадает под определение охраняемых законом сведений: «Все персональные данные, которые размещаются на таких страницах, являются общедоступными в силу п. 2 ч. 2. ст. 10 ФЗ "О персональных данных", так как размещены самим субъектом персональных данных. Неправомерный доступ будет рассматриваться как доступ к неохраняемой законом информации. В то же время такие действия могут привести к существенным негативным последствиям. Упомянутый подход оставляет без уголовно-правовой защиты ключевую фигуру цифровой экономики — лицо, генерирующее информацию»[23].

Указанная классификация представляет практическую значимость, так как охватывает большой круг сведений, которые могут стать объектом информационных правоотношений. Такие сведения выступают объектом гражданского оборота и подлежат защите как гражданско-правовыми[24], так и уголовно-правовыми средствами.

Таким образом, информация как объект правоотношений — охраняемое законом нематериальное благо, обладающее следующими признаками: наличие правовой охраны; обособленность, т. е. фиксация в материальной или идеальной форме (в памяти человека); действительная или потенциальная ценность; актуальность; полезность; новизна; достоверность; неисчерпаемость (возможность неоднократного воспроизведения, одновременного использования множеством лиц без ущерба для нее); возможность стоимостного выражения.

В связи с повышением уровня информатизации в обществе необходимо рассмотреть вопросы уголовно-правовой охраны компьютерной информации. В настоящее время практически все сферы человеческой деятельности охвачены информационными технологиями. Мгновенный поиск информации и обмен ею, развитие научно-технического прогресса, эффективные способы оказания государственных услуг (наличие официальных информационных интернет-ресурсов, которые посвящены деятельности большинства государственных ведомств[25]), — все это преимущества компьютеризации жизни. Однако не стоит забывать о множестве негативных последствий, которые несут в себе современные информационно-коммуникационные технологии. Эффективная защита компьютерной информации (в том числе уголовно-правовыми средствами) сейчас представляет собой одну из наиболее важных задач.

Уголовная ответственность за неправомерный доступ к компьютерной информации установлена ст. 272 Уголовного кодекса РФ от 13.06.1996 № 63-ФЗ (далее — УК РФ). Непосредственный *объект* преступления, предусмотренного ст. 272 УК РФ, — общественные отношения, направленные на охрану всех прав обладателя информации.

---

[23] *Дремлюга Р. И.* Компьютерная информация как предмет преступления… С. 54.

[24] См., напр.: Постановление Арбитражного суда Восточно-Сибирского округа от 06.04.2015 № Ф02-1074/2015 по делу № А58-3226/2014.

[25] Так, сегодня деятельность 21 министерства и 62 ведомств РФ отражена на официальных информационных интернет-ресурсах. URL: https://www.gosuslugi.ru/ (дата обращения: 25.04.2019).

Определение *предмета* преступления, предусмотренного ст. 272 УК РФ, имеет большое практическое значение (например, для разграничения указанного преступления и преступлений против собственности). Некоторые правоведы[26] называют компьютеры в качестве предмета рассматриваемого преступления наряду с компьютерной информацией, компьютерным оборудованием, компьютерной системой и компьютерной сетью. Полагаем, что отнесение компьютера и иных технических устройств к предмету рассматриваемого преступления ошибочно, так как указанный подход не позволяет строго отграничить посягательства на компьютерную информацию и посягательства на собственность.

Представляется, что *завладение чужим компьютером* не образует состава неправомерного доступа к компьютерной информации, если умысел лица был направлен исключительно на завладение материальным носителем, но не самой информацией (например, отсутствовал умысел на копирование компьютерной информации). Указанные деяния должны быть квалифицированы как кража (ст. 158 УК РФ)[27] или умышленные уничтожение и повреждение чужого имущества[28] (ст. 167 УК РФ) в зависимости от умысла виновного. Совокупности со ст. 272 УК РФ эти действия не образуют.

Справедливо утверждение В. С. Карпова о том, что содеянное необходимо квалифицировать по совокупности (ст. 167 и 272 УК РФ), если умысел виновного был направлен на уничтожение компьютерной информации посредством воздействия на компьютер (его повреждения или уничтожения)[29].

Нужно строго разграничивать компьютерную информацию как нематериальное благо и как носитель, на котором указанная информация зафиксирована. Соответственно, предметом рассматриваемого преступления выступает *исключительно компьютерная информация*.

Анализ юридической литературы позволяет сделать вывод, что охраняемая уголовным законом компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ, понимается правоведами:

— как информация, охрана которой прямо предусмотрена законом (нормативистское понимание, формальный подход)[30];

---

[26] См., напр.: *Ахраменка Н. Ф.* Преступления против информационной безопасности (гл. 31 Уголовного кодекса Республики Беларусь 1999 г.): общая характеристика и проблемы квалификации // Противодействие преступности: уголовно-правовые, криминологические и уголовно-исполнительные аспекты: мат-лы III Российского Конгресса уголовного права, состоявшегося 29–30 июня 2008 г. М.: Проспект, 2008. С. 546–547.

[27] См., напр.: Апелляционное определение Свердловского областного суда от 15.02.2018 по делу № 22-1180/2018 (кража планшетного компьютера); Апелляционное определение Амурского областного суда от 29.04.2014 по делу № 22-567/14.

[28] Приговор Приволжского районного суда г. Казани № 1-122/2018 от 11.01.2018 (действия виновного квалифицированы по ч. 1 ст. 167 УК РФ: «Действуя из личной неприязни к К., взял планшетный компьютер “Samsung” и видеорегистратор, бросил их на пол, после чего видеорегистратором нанес по экрану планшетного компьютера три удара, тем самым умышленно повредив планшетный компьютер); Приговор Кировского районного суда по делу № 22-3900/2016 (действия виновного квалифицированы по ч. 1 ст. 167 УК РФ).

[29] *Карпов В. С.* Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид. наук. Красноярск: Сибирский федеральный университет, 2002. С. 146.

[30] См., напр.: *Ястребов Д. А.* Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений // Российский следователь. 2008. № 17. С. 25; *Дворецкий М. Ю.* Корреляции главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Вестник Томского государственного университета. 2012. № 6. С. 266–270.

— как любая информация[31].

Также существует позиция, согласно которой критериями определения компьютерной информации как предмета рассматриваемого преступления выступают:

— причиненный обладателю информации ущерб[32] (в случае установления такового информация подлежит уголовно-правовой охране);

— субъективное значение информации для ее обладателя[33].

Точка зрения, согласно которой под предметом преступления, предусмотренного ст. 272 УК РФ, понимается только та информация, доступ к которой прямо ограничен законом, на наш взгляд, спорна. Сторонники данной позиции ссылаются на Методические рекомендации Генеральной прокуратуры РФ[34], где указано: «По смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т. д.)».

Полагаем, что рассматриваемый подход неоправданно сужает предмет уголовно-правовой охраны, а подзаконный нормативно-правовой акт не может выступать единственным руководством к толкованию уголовного закона. Указанная позиция оставляет без внимания сведения, способные представлять ценность для их обладателя (однако в их отношении отсутствует установленный законом порядок доступа). Думается, данный подход не отвечает потребностям современного общества, все сферы жизни которого связаны с информацией и информационными технологиями.

Противоположный подход, согласно которому уголовно-правовая охрана предоставляется любой компьютерной информации, также небезупречен. Его сторонники утверждают, что «неохраняемой информации в современном информационном поле в условиях постинформационного общества не существует»[35]. По нашему мнению, несанкционированный доступ к любой компьютерной информации не отвечает такому признаку преступного деяния, как «общественная опасность».

Мы разделяем позицию[36], согласно которой предметом преступления, предусмотренного ст. 272 УК РФ, являются:

— информация, доступ к которой прямо ограничен законом;

---

[31] См., напр.: *Айсанов Р. М.* Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: дис. ... канд. юрид. наук. М.: Российская академия правосудия, 2006. С. 59; *Гульбин Ю. Т.* Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10. С. 25; *Волеводз А. Г.* Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. 2002. № 9. С. 34–41.

[32] См., напр.: *Копырюлин А. Н.* Преступления в сфере компьютерной информации6 уголовно-правовой и криминологический аспекты: дис. ... канд. юрид. наук. Тамбов: Тамбовский государственный университет им. Г. Р. Державина, 2007. С. 72.

[33] См., напр.: *Ягудин А. Н.* Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. ... канд. юрид. наук. М.: Казанский юридический институт МВД РФ, 2013. С. 114.

[34] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: http://www.genproc.gov.ru/documents/nauka/execution/document-104550 (дата обращения: 20.04.2020).

[35] *Айсанов Р. М.* Состав неправомерного доступа... С. 58.

[36] *Дремлюга Р. И.* Компьютерная информация как предмет преступления... С. 57.

— информация, относительно которой наличествует явно выраженное и объявленное неопределенному кругу лиц требование обладателя об ограничениях по ее использованию (доступу).

Полагаем, что вопрос об отнесении сведений второй категории к охраняемым уголовным законом должен решаться судьей в каждом конкретном деле. В основу решения суда о предоставлении правовой защиты сведениям, которые прямо не отнесены законом к категории ограниченного доступа, могут быть положены следующие признаки:

— неправомерность доступа, ясная из обстановки (например, когда обладатель информации ограничил доступ к информации, а лицо посредством взлома пароля осуществило несанкционированный доступ к информации);
— установление обладателем информации технических и программных средств защиты информации от несанкционированного доступа;
— действительная или потенциальная ценность рассматриваемой информации для обладателя или заинтересованных лиц (например, взлом аккаунта блогера, имеющего более 1 млн подписчиков, с последующим уничтожением информации может привести к существенному материальному ущербу для его обладателя)[37];
— иные свойства самой информации, а также имеющие значение различные обстоятельства конкретного случая (например, мотив и цель правонарушителя).

Так, суды могут принимать во внимание мотивы и цель виновного (например, корыстную заинтересованность), которыми он руководствовался при совершении несанкционированного доступа к информации. Скажем, в настоящее время многие предприниматели используют социальную сеть «Инстаграм» как платформу для размещения информации о своих услугах и товарах. Большое количество подписчиков в бизнес-аккаунте предпринимателя и длительная история его существования могут свидетельствовать о надежности или качественности того или иного продукта (реклама которого осуществляется в Инстаграме). В борьбе за потребителей недобросовестные конкуренты осуществляют взлом таких страниц. Например, страница врача-ортодонта с более чем 311 тыс. подписчиков была «украдена» конкурентами, и все данные, размещенные на странице, также были удалены[38].

Заметим: судья принимает решение о предоставлении правовой охраны общедоступным сведениям *дискреционно* (в отсутствие императивной нормы, устанавливающей критерии охраноспособности такой информации). Соответственно, предлагаемые выше признаки носят *рекомендательный характер.* Например, корыстный мотив правонарушителя, осуществившего несанкционированный доступ к информации, может быть отражен в мотивировочной части приговора, а также будет учтен на этапе назначения наказания.

Обладатель рассматриваемых сведений (прямо не отнесенных законом к категории охраняемых) должен предпринимать разумные меры к тому, чтобы отсутствовал общедоступный способ их уничтожения или блокирования. Соответственно, комплекс защитных мер, предпринятых обладателем информации, позволит в случае несанкционированного доступа к ней получить правовую охрану.

---

[37] *Дремлюга Р. И.* Компьютерная информация как предмет преступления… С. 54.

[38] URL: https://www.instagram.com/p/BvJUlzcjlrK/?igshid=11tjl6vy5tx7 (дата обращения: 25.04.2019).

Несмотря на то что судебная практика по применению ст. 272 УК РФ не единообразна, подход, согласно которому общедоступная компьютерная информация подлежит уголовно-правовой охране, находит отражение в судебных решениях.

Так, Н., «прекратив свою трудовую деятельность в организации, в которой являлся генеральным директором, и утратив в связи с этим право доступа к учетной записи администратора сайта, принадлежащего организации и используемого в деловых и маркетинговых целях, испытывая неприязненное отношение к руководству, желая опорочить деловую репутацию общества, умышленно уничтожил и модифицировал часть компьютерной информации: изменил изображение слайдера, удалив исходные изображения, но добавив другие изображения, порочащие деловую репутацию общества, удалил контактный телефон и сведения об имеющихся сертификатах, изменил сведения о производстве и качестве сырья, удалил информацию о партнерах, экологической безопасности продукции и т. д.»[39].

Рассматривая вопрос о неправомерном доступе к общедоступной информации, суд указал: «Если владелец информации предпринял меры по ее защите, то информация признается охраняемой по закону в контексте ст. 272 УК РФ, так же, как и информация, которая явно указана законом или другим нормативно-правовым актом»[40].

По мнению Р. И. Дремлюги, «убеждение, что компьютерная информация, для которой обладатель сам устанавливает режим доступа, обладает незначительной ценностью и посягательство на нее не может создавать существенную угрозу охраняемым общественным отношениям или приводить к наступлению общественно опасных последствий... было справедливо несколько десятилетий назад, но сейчас, когда цифровые данные обладают огромной ценностью, ситуация изменилась»[41].

Включение в предмет рассматриваемого преступления информации, доступ к которой ограничен непосредственно ее обладателем (а не законом), согласуется с Законом об информации. В соответствии с п. 3 ст. 6 этого Закона обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

Согласно ст. 16 Закона об информации, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.

Соответственно, указанные выше положения ст. 16 и п. 3 ст. 6 Закона об информации распространяются как на общедоступную информацию, так и на информацию ограниченного доступа. Таким образом, общедоступность компьютерной информации означает возможность беспрепятственного ее использования (копирование, распространение), а не блокирования, уничтожения и модификации. Более того, требования о защите определенных категорий общедоступной информации устанавливаются в нормативно-правовых актах РФ. Так, защиту информации (от уничтожения, модификации и блокирования доступа к ней, а также иных неправомерных действий в отношении нее), *размещенной на официальном сайте образовательной организации* в сети «Интернет» должны обеспечивать

[39] Приговор Октябрьского районного суда г. Архангельска от 14.12.2015 по делу № 1-352/2015.

[40] Определение Курганского областного суда от 25.06.2013 по делу № 22-1475/2013.

[41] *Дремлюга Р. И.* Компьютерная информация как предмет преступления... С. 54.

технологические и программные средства, которые используются для функционирования указанного сайта[42].

В правовой литературе существует точка зрения, согласно которой использование чужих учетно-регистрационных данных не образует состава преступления, предусмотренного ст. 272 УК РФ, так как «информация в этой сети носит открытый характер и она не запрещена к копированию, а уголовный закон запрещает неправомерный доступ только к охраняемой законом информации»[43]. Однако данная позиция противоречит сложившейся судебной практике[44], которая признает указанные действия противоправными.

Так, приговором Октябрьского районного суда г. Рязани[45] действия виновного были квалифицированы по ч. 1 ст. 272 УК РФ. Виновный, используя перехваченные идентификационные данные пользователя (потерпевшей), в обход систем защиты социальной сети, осуществил изменение, копирование и удаление информации на персональной странице потерпевшей в социальной сети «ВКонтакте».

Представляется, что неправомерность действий по использованию чужих паролей и логинов для входа в различных социальные сети *очевидна*. «Учетно-регистрационные данные правомерно могут использоваться только лицом, их получившим на законных основаниях»[46]. Несанкционированный доступ к аккаунту блокирует добросовестному пользователю возможность входа в него[47]. Как уже было указано выше, уголовно-правовой охране подлежит также общедоступная информация, относительно которой наличествует явно выраженное и объявленное неопределенному кругу лиц требование обладателя об ограничениях по ее использованию (доступу). В данном случае регистрационные данные (логин и пароль) выступают технической мерой защиты информации, содержащейся в открытом доступе.

Таким образом, действия по блокированию, уничтожению и модификации общедоступной компьютерной информации (в нарушение установленного обладателем порядка использования указанных сведений) должны квалифицироваться по ст. 272 УК РФ. Особо отметим: действия по копированию таких сведений не могут влечь уголовной ответственности.

По нашему мнению, специфика предмета преступления, предусмотренного ст. 272 УК РФ, в определенной степени повлияла на его объективную сторону. Рассмотрим далее некоторые особенности объективной стороны неправомерного доступа к компьютерной информации.

---

[42] Постановление Правительства РФ от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети “Интернет” и обновления информации об образовательной организации».

[43] *Воробьев В. В.* Преступления в сфере компьютерной информации: дис. … канд. юрид. наук. Н. Новгород: Нижегородская академия МВД РФ, 2000. С. 66.

[44] Приговор Ленинского районного суда г. Барнаула от 11.09.2018 по делу № 1-421/2018; Приговор Череповецкого городского суда от 05.10.2016 по делу № 1-581/2016; Приговор Вологодского городского суда от 17.11.2016 по делу № 1-914/2016; Приговор Промышленного районного суда г. Владикавказа от 15.06.2016 по делу № 1-115/2016.

[45] Приговор Октябрьского районного суда г. Рязани от 25.02.2016 по делу № 1-53/2016.

[46] Приговор Ленинского районного суда г. Тюмени от 17.07.2012 по уголовному делу № 1-619/2012.

[47] Приговор Дзержинского районного суда г. Перми от 06.10.2016 по делу № 1-378/2016 («Когда злоумышленник несанкционированным способом получает доступ на электронный почтовый ящик законного владельца, то в тот период времени, пока злоумышленник находится на почте, доступ законного владельца к данной почте заблокирован, если злоумышленник сменил при этом пароль»).

Объективной стороной рассматриваемого преступления выступает неправомерный доступ к охраняемой законом компьютерной информации. Под доступом к информации в соответствии с п. 6 ст. 2 Закона об информации понимается возможность получения информации и ее использования. Законодательное определение доступа не может быть применимо для целей уголовного права, так как является слишком широким и не отражает значимых для права признаков.

Полагаем, что *правомерный доступ к* компьютерной информации – это возможность использования и/или изменения, уничтожения, блокирования охраняемой законом компьютерной информации, предоставленная обладателем информации (лицом, которое управомочено разрешить доступ к информации в определенном объеме).

Под *неправомерным доступом* необходимо понимать действия по использованию и/или изменению, уничтожению, блокированию охраняемой законом компьютерной информации, если указанные действия были совершены в отсутствие законного основания (без надлежаще полученных прав, вопреки воле обладателя информации, путем нейтрализации средств защиты информации).

Объем доступа, предоставленный обладателем информации, может выражаться, например, в возможности копирования и ознакомления с ней. Тогда совершение иных действий, превышающих указанный объем, определенный обладателем информации, необходимо рассматривать как несанкционированный доступ.

Анализ судебной практики позволяет указать следующие способы получения неправомерного доступа к компьютерной информации: «незаконное приобретение файла, содержащего логины и пароли чужих электронных почтовых ящиков»[48], «получение доступа к учетной записи коллеги, который, не зная о преступной цели, сообщил виновному свои логин и пароль»[49], «незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации»[50].

Можно ли утверждать, что доступ к компьютерной информации был неправомерным, если указанная информация хранилась на компьютере без средств защиты? Например, будут ли влечь уголовную ответственность действия по копированию информации с компьютера, который оставлен без присмотра?

Некоторые правоведы считают, что отсутствие мер защиты информации исключает наступление уголовной ответственности при доступе к такой информации[51]. Другие исследователи полагают, что «отсутствие технических мер защиты информации не означает, что информация исключена из категории охраняемой»[52].

По нашему мнению, указанный вопрос необходимо решать дифференцированно, исходя из специфики предмета преступления, предусмотренного ст. 272 УК РФ.

---

[48] Апелляционное постановление Свердловского областного суда от 18.12.2017 по делу № 22-9487/2017.

[49] Приговор Канавинский районный суд г. Нижний Новгород от 06.06.2018 по делу № 1-283/2018.

[50] Обзор судебной практики по уголовным делам за январь 2016 г. // Информационный бюллетень Белгородского областного суда. 2016. № 2. URL: http://oblsud.blg.sudrf.ru/modules.php?id=4056&name=docum_sud (дата обращения: 28.04.2020).

[51] *Сизов А. В.* Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2009. № 1. С. 32–35; *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток: Дальневосточный государственный университет, 2005. С. 201.

[52] *Дремлюга Р. И.* Компьютерная информация как предмет преступления... С. 55; *Степанов-Егиянц В. Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. С. 31–32.

Если доступ был осуществлен к информации, которая прямо отнесена федеральным законом к категории «ограниченного доступа», то он будет считаться неправомерным вне зависимости от наличия или отсутствия мер защиты. Общественная опасность указанных действий обусловлена отнесением федеральным законом такой информации к категории ограниченного доступа: «В ст. 272 УК РФ законодатель не ставит охрану информации в зависимость от ее технической защищенности»[53].

Авторы, поддерживающие точку зрения, согласно которой информация должна защищаться вне зависимости от наличия мер защиты, проводят аналогию с кражей[54]. Действительно, частная собственность охраняется уголовным законом вне зависимости от того, насколько эффективно ее собственник предпринял меры по ее охране (например, установил замки на дверях квартиры).

Действия по уничтожению, изменению или блокированию общедоступной информации в отсутствие мер защиты таких сведений не повлекут уголовной ответственности. Именно специальный порядок доступа к общедоступной информации, который выражается в совокупности установленных «собственником» мер защиты (в том числе технических), позволяет наделить такие сведения уголовно-правовой охраной.

Что касается последствий неправомерного доступа к охраняемой законом компьютерной информации, то рассматриваемый состав является материальным и предполагает обязательное наступление одного из следующих последствий: *уничтожения*, *блокирования*, *модификации* или *копирования* информации.

Уничтожение охраняемой законом компьютерной информации. Законодатель не определяет в уголовном законе содержание терминов, обозначающих последствия неправомерного доступа к компьютерной информации. Полагаем, что уничтожение компьютерной информации – это частичное или полное удаление информации, независимо от возможности ее восстановления. Ряд ученых утверждает, что «удаление информации виновным, которая впоследствии была восстановлена, следует рассматривать как покушение на уничтожение»[55]. Указанная позиция представляется спорной. Умысел виновного, направленный на уничтожение информации, полностью реализуется в момент ее удаления, – пусть даже кратковременно, но данные становятся недоступными. Соответственно, предоставление виновному «привилегий» неоконченного преступления неоправданно. Полагаем, что наличие у потерпевшего копии уничтоженной информации или последующая техническая возможность ее восстановления не должны влиять на квалификацию содеянного. Справедливо, что даже кратковременное удаление информации может повлечь весьма серьезные последствия, например, в виде дезорганизации работы оборонных, банковских или транспортных систем[56]. Указанный подход соответствует критерию практической достоверности[57].

---

[53] *Степанов-Егиянц В. Г.* Ответственность за преступления... С. 32.

[54] См., напр.: *Дремлюга Р. И.* Компьютерная информация как предмет преступления... С. 55; *Степанов-Егиянц В. Г.* Ответственность за преступления... С. 55–56.

[55] См., напр.: *Быков В. М., Черкасов В. Н.* Новый Закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. № 5. С. 16.

[56] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / отв. ред. А. И. Рарог. М.: Проспект, 2017.

[57] См., напр.: Приговор Советского районного суда г. Казани от 15.05.2018 по делу 1-212/2018 («Уничтожение информации — это приведение информации или ее части в непригодное для использования состояние, независимо от возможности ее восстановления»); Апелляционное постановление Красноярского краевого суда от 30.08.2018 по делу № 22-5298/2018 («Под уничтожением компьютерной информации понимается приведение ее полностью либо в существенной части в не-

Блокирование компьютерной информации. В судебной практике под блокированием компьютерной информации понимается «затруднение доступа пользователя к компьютерной информации без ее уничтожения»[58], «невозможность осуществлять требуемые операции над компьютерной информацией»[59], «выключение из работы функции защиты исполняемого файла программного продукта "Н", отвечающего за передачу информации аппаратному ключу, который ограничивает несанкционированный правообладателем доступ к данным»[60]. В соответствии с п. 3.3.8 ГОСТа Р 53114-2008, «блокирование доступа (к информации): прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей)»[61].

Дискуссионным остается вопрос о том, повлечет ли уголовную ответственность блокирование информации на незначительный промежуток времени. Некоторые исследователи указывают, что блокирование информации, которое не способно нарушить нормальную работу пользователей (на незначительный промежуток времени), не образует состав преступления[62].

Мы не согласны с указанной точкой зрения. Нарушение даже на несколько секунд нормальной работы, предположим, объектов критической информационной инфраструктуры[63] может повлечь за собой необратимые общественно-опасные последствия (например, в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности).

Анализ судебной практики позволяется сделать вывод, что продолжительность блокирования компьютерной информации не влияет на вывод о виновности. Так, действия по блокированию информации на незначительный промежуток времени (65 секунд[64], 6 минут[65], 10 минут[66]) были квалифицированы по ст. 272 УК РФ.

Модификация компьютерной информации – это внесение любых изменений в компьютерную информацию без согласия ее обладателя.

Суды понимают под «модификацией информации» внесение в нее любых изменений, в частности:

пригодное для использования по назначению состояние, независимо от возможности ее восстановления»).

[58] Апелляционное определение Томского областного суда от 12.10.2017 по делу № 22-1652/2017.

[59] Приговор Харабалинского районного суда от 21.11.2016 по делу № 1-178/2016.

[60] Апелляционный приговор Челябинского областного суда от 28.01.2014 по делу № 10-479/2014.

[61] ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст).

[62] *Кочои С., Савельев Д.* Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. 1999. № 1. С. 44–45.

[63] В соответствии со ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», «объекты критической информационной инфраструктуры — это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры».

[64] Приговор Ленинского районного суда г. Тюмени от 17.07.2012 по уголовному делу № 1-619/2012.

[65] Приговор Красногвардейского районного суда от 20.07.2017 по делу № 1-517/2017.

[66] Приговор Трусовского районного суда г. Астрахани от 26.07.2016 по делу № 1-277/2016.

— изменение фотографии в профилях социальных сетей и/или добавление к ним комментариев[67]; изменение пароля к личной странице в социальных сетях или к электронной почте[68];

— изменение объема каких-либо потребительских услуг в личном кабинете потерпевшего[69];

— изменение программных продуктов, которое выразилось в том, что их запуск стал возможным без установления и использования лицензионного ключа[70];

— изменение номера телефона компании, которое повлекло «невозможность потенциальных клиентов воспользоваться услугами организации»[71];

— переадресация абонентского номера потерпевшего на абонентский номер виновного[72];

— изменение информации о доменном имени, в результате которого содержание ресурса перестало быть доступным для пользователей сети Интернет[73].

Копирование компьютерной информации понимается как перенос виновным информации на обособленный материальный носитель[74]. Неправомерно копирование информации, доступ к которой прямо ограничен законом. В отношении общедоступной информации указанное общественно опасное последствие неприменимо. Данный вывод вытекает из предложенного нами определения рассматриваемого предмета преступления.

В правовой литературе отсутствует единство мнений относительно способов копирования компьютерной информации. Так, некоторые исследователи указывают, что «сущность копирования заключается в переносе информации с одного машинного носителя на другой машинный носитель, а также неправомерной записи компьютерной информации в память ЭВМ»[75]. Полагаем, что указанный подход необоснованно сужает сферу применения рассматриваемого преступления.

Анализ правоприменительной практики позволяет сделать вывод, что способами копирования компьютерной информации могут выступать переписывание информации от руки[76], ее распечатывание[77], фотографирование[78].

---

[67] Приговор Череповецкого городского суда от 05.10.2016 по делу № 1-581/2016; Приговор Вологодского городского суда от 17.11.2016 по делу № 1-914/2016.

[68] Приговор Череповецкого городского суда от 04.05.2016 по делу № 1-581/2016; Приговор Ленинского районного суда г. Барнаула от 11.09.2018 по делу № 1-421/2018; Приговор Дзержинского районного суда г. Перми от 06.10.2016 по делу № 1-378/2016; Приговор Красногвардейского районного суда от 20.07.2017 по делу № 1-517/2017; Приговор Городецкого городского суда от 25.07.2018 по делу № 1-133/2018.

[69] Приговор Энгельсского районного суда от 31.08.2016 по делу № 1-516/2016.

[70] Апелляционное определение Томского областного суда от 02.02.2017 по делу № 22-32/2017; Приговор Северского городского суда от 23.06.2016 по делу № 1-190/2016.

[71] Приговор Ленинского районного суда г. Уфы от 30.12.2017 по делу № 1-236/2016.

[72] Приговор Ленинского районного суда г. Тюмени от 07.04. 2016 по делу № 1-366/2016.

[73] Приговор Ново-Савиновского районного суда г. Казани от 18.04. 2016 по делу № 1-160/2016.

[74] См., напр.: Приговор Советского районного суда г. Орска от 17.04.2017 по делу № 1-92/2017; Приговор Ленинского районного суда г. Ижевска от 04.10.2016 по делу № 1-387/2016; Приговор Сызранского городского суда от 12.08.2016 по делу № 1-387/2016.

[75] *Борчева Н. А.* Компьютерные преступления в России: комментарий к Уголовному кодексу Российской Федерации. М.: Прима-Пресс, 2001. С. 8.

[76] Приговор Геленджикского городского суда от 12.01.2016 по делу № 1-36/2016 (виновная «переписала информацию на лист бумаги, являющийся бумажным носителем информации, чем осуществила копирование компьютерной информации»).

[77] Приговор Геленджикского городского суда от 14.02.2017 по делу № 1-48/2017 (виновный «распечатал полученную информацию на листы бумаги, чем осуществил копирование компьютерной информации»).

[78] Приговор Ленинского районного суда г. Краснодара от 11.05. 2017 по делу № 1-282/2017.

Автоматическое создание резервной копии компьютерной информации не должно рассматриваться как копирование, осуществленное виновным, так как умыслом виновного указанное действие не охватывалось. При таких обстоятельствах лицу не может инкриминироваться «копирование информации».

Отсутствие законодательных определений (и даже разъяснений высшими судебными инстанциями) таких терминов, как «охраняемая законом информация», «уничтожение», «блокирование», «модификация», «копирование», является серьезным недостатком[79]. Неопределенность указанных терминов, которые поразному понимаются в судебной практике и правовой науке, нужно устранить. Предлагаем закрепить в примеч. 2 к ст. 272 УК РФ следующее определение термина «охраняемая законом компьютерная информация»: «Под охраняемой законом компьютерной информацией следует понимать информацию, доступ к которой прямо ограничен законом, а также общедоступную информацию, обладателем которой установлен специальный режим доступа к ней, предотвращающий ее уничтожение, блокирование и модификацию».

Статья поступила в редакцию 12 мая 2019 г.;
рекомендована в печать 31 января 2020 г.

On the need to change the approach to the concept of "information" in legislation and judicial practice

Anna S. Ozerova

For citation: Ozerova, Anna S. 2019. On the need to change the approach to the concept of "information" in legislation and judicial practice. Pravovedenie 63 (1): 137–156.
https://doi.org/10.21638/spbu25.2019.107 (In Russian)

The author of the article discusses the meaning of information as an object of legal relations. In connection with the decisive importance of the role of "information" in all spheres of the modern society, the protection of the considered social good is a priority task of the state. However, despite the importance of information, in Russian law there is no systematic and consistent legislative regulation of information relations. Legislative contradictions, the lack of a unified terminology and a scientific approach do not contribute to the effective legal protection of the considered good and the formation of a uniform judicial practice. The author's understanding of the term "information" as an object of legal relations has been developed on the basis of a system analysis of legislation and law enforcement practices, and its main features have been considered. The author substantiates the conclusion that information is the object of civil legal relations. In connection with this, it is proposed to return to Article 128 of the Civil Code of the Russian Federation as an indication of information as an object of civil rights and the subject of unauthorized access to computer information is analyzed (Article 272 of the Criminal Code of the Russian Federation). The subject of the crime under Article 272 of the Criminal Code is information, access to which is directly limited by law, as well as information in relation to which the holder's requirement of restrictions on its use (access) is clearly expressed and declared to an indefinite number of persons. The question of classifying the information of the second category as a protected criminal law must be determined by a judge in each specific case. It is concluded that the basis of the legal protection of information is a direct indication of the law or the establishment by the owner of publicly available information of a procedure for handling it. The general availability of computer information implies the possibility of its unhindered use (copying, distribution), and not obstruction, destruction or modification. Criteria are proposed for a court to rule on the provision of legal protection to information that is not directly classified

[79] См. об этом: *Лопашенко Н. А.* Еще раз об оценочных категориях в законодательных формулировках преступлений в сфере экономической деятельности // Уголовное право. 2002. № 2. С. 43–62.

as restricted by the law and methods of unauthorized access to computer information is analyzed. In order to eliminate legal uncertainty, a new understanding of the term “legally protected computer information” is recommended.

Keywords: information, unauthorized access to information, computer information, grounds for legal protection, criminal law protection of information, confidential information.

References

Aisanov, Ruslan M. 2006. *Composition of unauthorized access to computer information in Russian, international and foreign criminal law*: PhD in law thesis. Moscow, Rossiiskaia akademiia Pravosudiia Publ. (In Russian)

Alekseev, Sergei S. 1994. *Legal theory*. Moscow, BEK Publ. (In Russian)

Akhramenka, Nikita F. 2008. Crimes against information security (Chapter 31 of the Criminal Code of the Republic of Belarus 1999): General characteristics and problems of qualification. *Protivodeistvie prestupnosti: ugolovno-pravovye, kriminologicheskie i ugolovno-ispolnitel'nye aspekty: mat-ly III Rossiiskogo Kongressa ugolovnogo prava, sostoiavshegosia 29–30 iiunia 2008 g*.: 546–547. Moscow, Prospekt Publ. (In Russian)

Borcheva, Natalia A. 2001. *Computer crimes in Russia: Commentary on the Criminal Code of the Russian Federation*. Moscow, Prima-Press Publ. (In Russian)

Bykov, Viktor M., Cherkasov, Valerii N. 2012. New Computer Information Crime Act: Art. 272 of the Criminal Code. *Rossiiskii sud'ia* 5: 14–19. (In Russian)

Rarog, Aleksei I. (ed.) 2017. *Commentary to the Criminal Code of the Russian Federation (itemized)*. Moscow, Prospekt Publ. (In Russian)

Chislin, Vitali P. 2004. *Criminal law measures to protect information from unauthorized*: PhD in law thesis. Moscow, Kolomenskii gosudarstvennyi pedagogicheskii institute. (In Russian)

Doronin, Andrey M. 2003. *Criminal liability for illegal access to computer information*. PhD in law thesis. Moscow, Moskovskii universitet MVD Rossii Publ. (In Russian)

Dremliuga, Roman I. 2018. Computer information as the subject of a crime under Art. 272 of the Criminal Code. *Ugolovnoe pravo* 4: 52–57. (In Russian)

Dvoretskii, Mikhail Iu. 2012. Changes and additions to Chapter 28 of the Criminal Code of the Russian Federation in the context of the optimization of criminal responsibility and the increase of the effectiveness of law enforcement practice. *Vestnik Tomskogo gosudarstvennogo universiteta* 6: 266–270. (In Russian)

Gul'bin, Iurii T. 1997. Computer crimes. *Rossiiskaia iustitsiia* 10: 24–25. (In Russian)

Iagudin, Adel' N. 2013. *Criminal liability for violation of the rules of operation of the means of storage, processing or transfer of computer information and information and telecommunication networks*: PhD in law thesis. Kazan', Kazanskii iuridicheskii institut MVD RF Publ. (In Russian)

Iastrebov, Dmitriy A. 2008. Issues of delimitation of unlawful access to computer information from related offenses. *Rossiiskii sledovatel'* 17: 25–27. (In Russian)

Iniushkin, Andrey A. 2016. Information in the system of objects of civil rights and its relationship with intellectual property on the example of databases. *Informatsionnoe pravo* 4: 4–7. (In Russian)

Karpov, Viktor S. 2002. *Criminal liability for computer crimes*: PhD in law thesis. Krasnoiarsk, Sibirskii federal'nyi universitet Publ. (In Russian)

Kirichenko, Oksana V. 2014. Information as an object of civil legal relation. *Sovremennoe pravo* 9: 77–81. (In Russian)

Kirsanova, Yekaterina E. 2018. The emergence of new objects of legal protection in a digital economy. *Iurist* 11: 19–24. (In Russian)

Kopyriulin, Aleksey N. 2007. *Computer crimes: criminal and criminological aspects*: PhD in law thesis. Tambov, Tambovskii gosudarstvennyi universitet im. G. R. Derzhavina Publ. (In Russian)

Kochoi, Samvel M., Savel'ev Dmitriy. 1999. Responsibility for illegal access to computer information. *Rossiiskaia iustitsiia* 1: 44–45. (In Russian)

Kuz'min, Victor P. 2009. The concept and legal nature of information. *Informatsionnoe pravo* 2: 4–8. (In Russian)

Lopashenko, Natalia A. 2020. Once again about the assessment categories in the legislative formulations of crimes in the sphere of economic activity. *Ugolovnoe pravo* 2: 43–62. (In Russian)

Malinin, Vasiliy B. 2015. Legal regulation of information. *Leningradskii iuridicheskii zhurnal* 3: 120–129. (In Russian)
Savel'ev, Alexander I. 2005. *Commentary to the Federal Law of July 27, 2006 no. 149 "On Information, Information Technologies and Protection of Information".* Moscow, Statut Publ. (In Russian)
Salikhov, Il'sur I. 2004. *Information with limited access as an object of civil legal relations*: PhD in law thesis. Kazan', Kazanskii gosudarstvennyi universitet im. V. I. Ul'ianova-Lenina Publ. (In Russian)
Sizov, Aleksey V. 2009. Unauthorized access to computer information: law enforcement practice. *Informatsionnoe pravo* 2: 32–35. (In Russian)
Stepanov-Egiiants, Vladimir G. 2016. *Responsibility for crimes against computer information on the criminal law of the Russian Federation*. Moscow, Statut Publ. (In Russian)
Tropina, Tatyana L. 2005. *Cybercrime: concept, state, criminal law measures*: PhD in law thesis. Vladivostok, Dal'nevostochnyi gosudarstvennyi universitet Publ. (In Russian)
Vaipan, Victor A. 2018. Legal regulation of the digital economy. *Predprinimatel'skoe pravo. Appendix "Pravo i Biznes"* 1: 12–17. (In Russian)
Volevodz, Alexander G. 2002. Russian legislation on criminal liability for crimes in the field of computer information. *Rossiiskii sud'ia* 9: 34–41. (In Russian)
Vorob'ev, Victor V. 2000. *Computer crimes*: PhD in law thesis. Nizhny Novgorod. Nizhegorodskaia akademiia MVD RF Publ. (In Russian)
Zvereva, Elena A. 2004. Information as an object of non-property civil rights. *Vrach i informatsionnye tekhnologii* 8: 60–64. (In Russian)

Received: May 12, 2019
Accepted: January 31, 2020

Anna S. Ozerova — Postgraduate Student, Moscow State University, 1, Leninskie Gory, Moscow, 119991, Russian Federation; annaozerova55@mail.ru