В.Г. Степанов-Егиянц

ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО УГОЛОВНОМУ ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ

СТАТУТ

Владимир Георгиевич Степанов-Егиянц

Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации

http://www.litres.ru/pages/biblio_book/?art=37675819
Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации:
ISBN 978-5-8354-1279-2

Аннотация

Монография посвящена проблемам обеспечения безопасного обращения компьютерной информации и мерам по противодействию преступлениям в сфере компьютерной информации. Проведено комплексное исследование составов преступлений, предусмотренных гл. 28 УК РФ. На основании подробного анализа научных работ российских специалистов, занимающихся проблематикой преступлений в сфере обращения компьютерной информации, судебно-следственной практики автором сделаны выводы о существовании в данной сфере целого ряда актуальных научных и практических проблем,

сформированы предложения по внесению изменений в некоторые положения действующего законодательства РФ. Монография может быть использована в качестве пособия для преподавателей, аспирантов и студентов юридических вузов, а также теми, кто интересуется преступлениями в сфере компьютерной информации и проблемами борьбы с ними.

Содержание

В.Г. Степанов-Егиянц
Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации

Введение

В связи с интенсивным развитием информационного общества актуальной задачей юридической науки и практики является совершенствование правового регулирования общественных отношений в сфере обеспечения информационной безопасности.

Практически вся современная человеческая деятельность в той или иной степени связана с компьютерами. Информационные технологии вошли в различные сферы жизни (в оборону, экономику, промышленность, транспорт, образо-

вание, культуру, медицину и пр.). Развитая информационная инфраструктура способствует социально-экономическому прогрессу, созданию и распространению научно-технической информации. Объединение компьютеров в сети дает возможность быстрого обмена информацией между пользователями в любом месте земного шара.

В настоящее время в мире насчитывается 3,2 млрд пользователей Интернета (все население Земли составляет 7,2 млрд человек), из них 2 млрд проживают в развивающихся странах. В период с 2000 по 2015 г. удельный вес пользователей сети «Интернет» увеличился почти в семь раз – с 6,5 до 43 % мирового населения[1]. За последние годы Интернет прочно вошел в повседневную и деловую жизнь страны. Россия не отстает и не остается в стороне от глобальных трендов. Российская аудитория Интернета – крупнейшая в Европе, превышает 80 млн пользователей, из них 62 млн человек выходят в онлайн ежедневно[2].

Компьютеризация жизни имеет не только положительные, но и отрицательные стороны. Председатель Правительства РФ Д.А. Медведев точно отметил, что «современные информационно-коммуникационные технологии стали все ча-

---

[1] Данные МСЭ по ИКТ за 2015 г. [Электронный ресурс]. – Режим доступа: http:// www.itu.int/net/pressofifce/press_releases/2015/pdf/17-ru.pdf. Дата обращения: 10.12.2015.

[2] Российская интернет-аудитория является крупнейшей в Европе [Электронный ресурс]. – Режим доступа: http://www.gazeta.ru/tech/news/2015/12/22/n_8043815.shtml. Дата обращения: 10.12.2015.

ще использоваться для военно-политического противоборства. Кроме того, интернет-технологии взяли на вооружение террористы и преступники. Со всеми этими проблемами многие страны сталкиваются уже постоянно. Эти угрозы нельзя игнорировать».

Конституция РФ в ст. 1 провозгласила Россию правовым государством, главной задачей которого является установление законности и правопорядка в обществе, в том числе путем борьбы с преступностью. Уголовное законодательство, обеспечивающее охрану общественных отношений в сфере высоких технологий, и эффективное использование системы уголовно-правовых мер защиты от преступных посягательств являются залогом успешной борьбы с общественно опасными деяниями в сфере компьютерной информации. Ответственность за совершение компьютерных преступлений впервые была введена в отечественное законодательство с принятием нового Уголовного кодекса РФ (далее – УК РФ). В настоящее время гл. 28 УК РФ именуется «Преступления в сфере компьютерной информации» и содержит три состава – ст. 272 (Неправомерный доступ к компьютерной информации), ст. 273 (Создание, использование и распространение вредоносных компьютерных программ), ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

По данным Министерства внутренних дел РФ, в 2006 г.

было зарегистрировано 8889 преступлений в сфере компьютерной информации (7337 – ст. 272 УК РФ, 1549 – ст. 273 УК РФ и 3 – ст. 274 УК РФ); в 2007 г. – 7236; в 2008 г. – 9010; в 2009 г. – 11 636; в 2010 г. – 7398; в 2011 г. – 2698; в 2012 г. – 2820; в 2013 г. – 2563; в 2014 г. – 1739; в 2015 г. – 2382 (1396 – ст. 272 УК РФ, 974 – ст. 273 УК РФ, 12 – ст. 274 УК РФ)[3].

В современный период информационная безопасность общества стала неотъемлемой частью национальной безопасности. В Стратегии национальной безопасности России, утвержденной Указом Президента от 31 декабря 2015 г. № 683 г., в п. 22 отмечается появление новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Одной из угроз военной безопасности РФ является развитие информационных средств ведения войны. Совет Безопасности РФ 5 октября 2015 г. представил проект новой Доктрины информационной безопасности России, в котором указывается, что использование информационного пространства для решения военно-политических задач, а также в террористических и иных целях может нанести серьезный ущерб интересам РФ в информационной сфере.

Разработка мер по борьбе с компьютерной преступностью невозможна без четкой доктрины, определяющей основные

---

[3] Министерство внутренних дел [Электронный ресурс]. – Режим доступа: https:// mvd.ru/folder/101762.html. Дата обращения: 19.10.2015.

направления развития и основные принципы в регулируемой сфере, утвержденной на уровне государства. В России существует Доктрина информационной безопасности от 9 сентября 2000 г. № ПР-1895[4]. Необходимо отметить, что в целом национальная безопасность зависит и от информационной безопасности и с развитием технических средств и информационного общества данная зависимость будет расти. Под информационной безопасностью РФ в Доктрине понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. В Доктрине также выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере. Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны. Вторая составляющая – информационное обеспечение государственной политики РФ. Третья составляющая – развитие современных информационных технологий. Четвертая составляющая – защита информационных ресурсов и телекоммуникационных систем на территории России.

[4] Российская газета. 28.09.2000. № 187.

В 2016 г. планируется принятие новой Доктрины информационной безопасности. Секретарь Совета Безопасности РФ Н.П. Патрушев отмечает, что «наблюдается тенденция смещения военных угроз в информационное пространство, в целях актуализации концептуальных основ обеспечения национальной безопасности по решению Совета Безопасности РФ развернута работа по корректировке основных документов стратегического планирования – Стратегии национальной безопасности РФ до 2020 года и Доктрины информационной безопасности РФ»[5].

Анализ положений проекта Доктрины информационной безопасности позволяет сделать следующие выводы: государство признает рост компьютерной преступности, особенно в кредитно-финансовой сфере; информационное пространство используется в целях разжигания межнациональной и религиозной ненависти; наблюдается тенденция милитаризации информационного пространства и наращивание гонки информационных вооружений, создающих угрозу международному миру, безопасности и стабильности.

Для выработки эффективных мер борьбы с данным видом преступлений необходимо продолжать исследовать теорию и практику применения законодательства о компьютерных преступлениях. Настоящая монография посвящена анали-

---

[5] Из-за новых угроз Россия меняет стратегию национальной безопасности до 2020 г. [Электронный ресурс]. – Режим доступа: https://russian.rt.com/article/89838. Дата обращения: 20.10.2015.

зу общественных отношений, определяющих комплекс теоретических проблем уголовного права, а также обобщению практики применения норм уголовного законодательства, устанавливающего ответственность за преступные посягательства против компьютерной информации.

В ней осуществлен уголовно-правовой анализ составов компьютерных преступлений, предусмотренных ст. 272–274 УК РФ, сформулированы выводы и внесены конкретные предложения по совершенствованию нормативно-правового обеспечения безопасности компьютерной информации.

Глава 1. Уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

§ 1.1. Объект неправомерного доступа к компьютерной информации

Для отграничения неправомерного доступа к компьютерной информации от других преступлений и правонарушений, определения характера и степени общественной опасности деяния, тяжести причиненного или возможного вреда, направленности преступного деяния необходимо установить и определить **объект преступного посягательства**. Установление объекта преступного посягательства служит как бы предварительной программой для выбора той группы смежных составов, среди которых нужно будет уже более тщательно искать необходимую норму[6].

---

[6] *Кудрявцев В.Н.* Объективная сторона преступления. М.: Госюриздат, 1960. С. 93.

По общему правилу **непосредственным объектом** является какое-либо отдельно взятое отношение[7]. Это положение является спорным. Проведенный анализ научных работ в этой области позволяет сделать вывод об отсутствии единого мнения относительно непосредственного объекта преступлений в сфере компьютерной информации. Точное понимание непосредственного объекта преступления необходимо для правильной квалификации преступления, для определения степени общественной опасности.

Ряд ученых определяют непосредственный объект преступления, предусмотренного ст. 272 УК РФ, через «состояние защищенности»: безопасность информационных систем, базирующихся на использовании ЭВМ, системе ЭВМ или их сети[8]; безопасность деятельности всех субъектов, являющихся обладателями информации или операторами информационных систем, по созданию и использованию информации, т.е. по реализации ими своих полномочий в пределах, установленных законом[9]; безопасность использования компьютерной информации, информационных ресурсов

---

[7] Там же.

[8] См.: *Алескеров В.И., Максименко И.А.* Уголовно-правовая и криминалистическая характеристика современных видов преступлений: Лекция. Домодедово: ВИПК МВД России, 2011. С. 10; *Крылов В.В.* Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. 1998. № 3. С. 83.

[9] *Зинина У.В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Дис. … канд. юрид. наук, М., 2007. С. 95.

и систем[10].

Другие исследователи относят к непосредственному объекту неправомерного доступа к компьютерной информации конкретные права и интересы по поводу ее использования: право владельца системы на неприкосновенность информации, содержащейся в системе[11]; конкретные права и интересы, охраняемые уголовным законом, подвергшиеся посягательству в результате совершения общественно опасного деяния[12]; права на информацию ее владельца и третьих лиц[13]; охраняемые законом права и интересы общества, государства, физических и юридических лиц в сфере владения, распоряжения, пользования компьютерной информацией[14]. Представляется не совсем верным определение непосредственного объекта преступления, предусмотренного ст.

---

[10] Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева и А.В. Наумова. М.: Юристь, 1997. С. 346. (Авторы главы – С.В. Бородин и С.В. Полубинская).

[11] *Клепицкий И.А.* Преступления в сфере компьютерной информации // Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. Б.В. Здравомилова. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2000. С. 352.

[12] *Дворецкий М.Ю.* Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. Тамбов: Изд-во ТГУ, 2003, С. 46.

[13] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Отв. ред. В.М. Лебедев. 13-е изд., перераб. и доп. М.: Юрайт, 2013. С. 634, 640, 642.

[14] *Евдокимов К.Н.* Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского региона): Дис. … канд. юрид. наук. Иркутск, 2006. С. 68.

272 УК РФ, через ущерб какому-либо социальному благу и через состояние защищенности информации, поскольку в теории уголовного права преступление направлено на изменение общественных отношений, а не на причинение вреда социальному объекту и не на нарушение какого-либо состояния.

Следует согласиться с теми учеными, которые определяют непосредственный объект неправомерного доступа к компьютерной информации через посягательство на общественные отношения как отношения, обеспечивающие безопасность (неприкосновенность) компьютерной информации[15]; как общественные отношения по соблюдению и обеспечению безопасности законного получения, обработки и использования компьютерной информации, а также нормального функционирования компьютерной техники[16]; как совокупность отношений, возникающих по поводу обеспечения безопасности компьютерной информации и ее носителей[17].

---

[15] См.: *Числин В.П.* Уголовно-правовые меры защиты информации от неправомерного доступа: Дис. … канд. юрид. наук. М., 2004. С. 9; Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2003. С. 15; *Мазуров В.А.* Компьютерные преступления: классификация и способы противодействия: Учеб.-практ. пособие. М.: Палеотип; Логос, 2002. С. 27; *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

[16] *Буз С.А.* Уголовно-правовые средства борьбы с преступлениями в сфере компьютерной информации / С.А. Буз, С.Г. Спирина. Краснодар, 2002. С. 40.

[17] *Малышенко Д.Г.* Уголовная ответственность за неправомерный доступ к

Под **непосредственным объектом** неправомерного доступа к компьютерной информации автор полагает возможным понимать общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

При исследовании объектов непосредственного доступа к компьютерной информации целесообразно вкратце остановиться на таком понятии, как «дополнительный объект неправомерного доступа». Дополнительный объект – это общественные отношения, заслуживающие самостоятельной защиты применительно к целям и задачам издания конкретной нормы, которые охраняются законом лишь попутно, так как они неизбежно ставятся в опасность причинения вреда при посягательстве на основной объект[18].

Дополнительный объект повышает степень общественной опасности исследуемого преступления. Им могут быть отношения в области права собственности, в области авторского права, личные права и свободы граждан, неприкосновенность частной жизни. Как правило, наличие дополнительного объекта при совершении деяния, определяемого как неправомерный доступ к компьютерной информации, влечет за собой квалификацию по совокупности с соответствующими статьями УК РФ. Например, при неправомерном до-

---

компьютерной информации: Дис. … канд. юрид. наук. М., 2002. С. 56.

[18] *Фролов Е.А.* Объект уголовно-правовой охраны и его роль в организации борьбы с посягательствами на социалистическую собственность: Автореф. дис. … д-ра юрид. наук. Свердловск, 1971. С. 25.

ступе, копировании и распространении компьютерной информации о частной жизни лица действия преступника будут квалифицироваться по совокупности ст. 272 и 137 УК РФ.

Большой научный и практический интерес вызывает вопрос определения **предмета неправомерного доступа** к охраняемой законом компьютерной информации. Под предметом преступления в отечественной уголовно-правовой науке обычно понимается элемент нормального правомерного общественного отношения, воздействуя на который, лицо нарушает (пытается нарушить) охраняемое законом общественное отношение[19]. В последнее время в предмет преступления ученые включают не только материальные объекты, но и объекты нематериального мира. Например, С.В. Землюков относит к предмету преступления как материальные, так и нематериальные блага, по поводу которых существуют общественные отношения: жизнь, здоровье, честь, достоинство, права и свободы, имущество и т.п.[20] А.В. Суслопаров считает предметом рассматриваемых составов «данные»[21].

Ряд отечественных исследователей относят к предмету

---

[19] *Никифоров Б.С.* Объект преступления по советскому уголовному праву. М.: Госюриздат, 1960. С. 130.

[20] Российское уголовное право. Общая часть / Под ред. В.С. Комиссарова. СПб.: Питер, 2005. С. 154.

[21] *Суслопаров А.В.* Информационные преступления: Дис. … канд. юрид. наук. Красноярск, 2008. С. 124.

неправомерного доступа к компьютерной информации технические устройства, на которых эта информация хранится. Существует точка зрения, что предметом любого компьютерного преступления следует признать компьютер как информационную систему, носитель информации[22]. Перекликается с ней позиция, в соответствии с которой предметом преступления выступает компьютерная информация, компьютер, компьютерная система или компьютерная сеть[23].

Однако большинство ученых считают такую точку зрения на предмет преступления, предусмотренного ст. 272 УК РФ, ошибочной.

Ю.В. Гаврилин указывает, что «физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не отвечает правовому содержанию общественно опасного действия, присущего преступлению, предусмотренного ст. 272 УК РФ, и, следовательно, не образует основания уголовной ответственности за его совершение»[24]. Представляется, что признание предметом рассматриваемо-

---

[22] Новое уголовное право России. Особенная часть: Учеб. пособие / Г.Н. Борзенков, С.В. Бородин, Б.В. Волженкин, В.С. Комиссаров и др.; под ред. Н.Ф. Кузнецовой. М.: Зерцало, ТЕИС, 1996. С. 273–274.

[23] Информационная безопасность в органах внутренних дел и применение информационных технологий в борьбе с преступностью: Учеб. пособие / А.А. Гайдамакин, А.И. Горев, А.П. Корстов и др. Омск, 2010. С. 85–86.

[24] *Гаврилин Ю.В.* Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / Под ред. Н.Г. Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2001. С. 8.

го преступления технических устройств хранения компьютерной информации приведет к трудностям при разграничении преступлений в сфере компьютерной информации и преступлений против собственности.

Преступления, предметом посягательства которых являются технические средства хранения информации, должны относиться к преступлениям против собственности. Завладение персональным компьютером либо машинным носителем информации как имуществом не может квалифицироваться как доступ к компьютерной информации и влечет ответственность за преступления против собственности[25]. Причем даже если деяние, направленное на завладение компьютером, и повлекло за собой уничтожение хранящейся в нем информации, то квалификация по ст. 272 УК РФ неприменима[26]. Следует согласиться, что при совершении данных действий умысел виновного направлен на общественные отношения по охране собственности, а не против компьютерной информации.

В юридической литературе существует точка зрения, относящая к предмету преступного посягательства, предусмотренного ст. 272 УК РФ, «информационную среду, то есть деятельность субъектов, связанную с созданием, преоб-

[25] *Волеводз А.Г.* Противодействие к компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. С. 66.

[26] *Айсанов Р.М.* Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: Дис. … канд. юрид. наук. М., 2006. С. 71.

разованием и потреблением информации»[27]. Данная позиция отождествляет предмет неправомерного доступа к компьютерной информации с деятельностью субъектов отношений и неоправданно расширяет предмет преступного посягательства.

Признание предметом преступления деятельности участников отношений, являющейся содержанием объекта преступления, не позволяет отграничивать содержание общественных отношений от предметов материального мира[28].

Некоторые ученые, исследующие проблематику предмета анализируемого преступления, относят к предмету неправомерного доступа к компьютерной информации только компьютерную информацию. В.Ю. Максимов считает, что «информация, в том числе и компьютерная, является, без сомнения, общественным благом и в таком случае может быть определена как предмет компьютерного преступления»[29]. А.Е. Ратникова пишет, что «информация как предмет преступления – это сведения, сообщения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированные или не зафиксированные на материальном носителе, воздействуя на которые виновный нарушает общественные отно-

---

[27] *Панфилова Е.И.* Компьютерные преступления / Е.И. Панфилова, А.Н. Попов; Науч. ред. проф. Б.В. Волженкин. СПб.: Изд-во СПб. юрид. ин-та Генеральной прокуратуры РФ, 2003. С. 563–564.

[28] *Винокуров В.В.* Предмет преступления: отличие от смежных понятий // Журнал российского права. 2011. № 12. С. 56–63.

[29] *Максимов В.Ю.* Указ. соч. С. 23.

шения, охраняемые законом»[30].

Внутри группы, относящей к предмету неправомерного доступа к компьютерной информации саму компьютерную информацию, выделяется несколько направлений научной полемики вокруг следующих вопросов:

I. Какая компьютерная информация является предметом преступления, предусмотренного ст. 272 УК РФ: только охраняемая законом либо любая компьютерная информация?

II. Применима ли к компьютерной информации категория собственности?

III. Имеет ли компьютерная информация цену и, если имеет, влияет ли ее цена на привлечение к уголовной ответственности?

Рассмотрим все эти аспекты в отдельности.

I. По вопросу охраны информации законом Р.М. Айсанов полагает, что указание в законе на охраняемый характер информации излишне, а исключение из диспозиции ст. 272 УК РФ категории «охраняемая законом» «не приведет к излишнему расширению его границ, а, напротив, позволит более полно охватить уголовно-правовой охраной информацию, ограниченную законом или собственником в полном досту-

---

[30] *Ратникова А.Е.* Уголовно-правовое обеспечение права на информацию (сравнительно-правовое исследование): Автореф. дис. … канд. юрид. наук. М., 2006. С. 8.

пе»[31]. Автор полагает, что неохраняемой информации в современном информационном поле в условиях постинформационного общества не существует[32]. Перекликается с этой позицией точка зрения Ю. Гульбина, считающего понятие «охраняемая законом компьютерная информация» расплывчатым: неохраняемой информации практически нет, так как если информация не является объектом охраны одного из законодательных актов, то, как правило, она становится объектом охраны другого[33].

А.Г. Волеводз, считая, что «нормы ст. 272 УК РФ направлены на охрану государственных и корпоративных интересов»[34], предлагает ввести в сферу действия ст. 272 УК РФ «всю компьютерную информацию»[35]. А.Н. Копырюлин утверждает, что «уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб собственнику (владельцу, пользователю)[36]. По мнению А.Н. Ягудина, ст. 272 УК РФ защищает любую информацию, имеющую значение для собственни-

---

[31] *Айсанов Р.М.* Указ. соч. С. 59.

[32] Там же. С. 58.

[33] *Гульбин Ю.* Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10. С. 24.

[34] *Волеводз А.Г.* Указ. соч. С. 84.

[35] Там же.

[36] *Копырюлин А.Н.* Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: Дис. … канд. юрид. наук. Тамбов, 2007. С. 72.

ка[37].

Сложно согласиться с теми, кто предлагает исключить из диспозиции ст. 272 УК РФ категорию «охраняемая законом» и относить к предмету преступления любую компьютерную информацию. Обратимся к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[38] (далее – ФЗ «Об информации, информационных технологиях и о защите информации»), разделившему информацию в зависимости от доступа к ней на общедоступную информацию и на информацию, доступ к которой ограничен. Согласно ст. 7 данного Закона «к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен», т.е. основными свойствами общедоступной информации являются общеизвестность и отсутствие ограничений на доступ к ней. Пункт 3 ст. 3 рассматриваемого Закона устанавливает право обладателя информации разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

Автор считает, что в момент, когда обладатель компьютерной информации ограничивает к ней доступ или опреде-

---

[37] *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., 2013. С. 114.

[38] http://base.garant.ru/12148555/#ixzz4AKOcjMQX. Дата обращения: 08.12.2015.

ляет его порядок, она начинает приобретать требуемое качество охраняемой законом в понимании ст. 272 УК РФ. В случае если обладатель компьютерной информации не реализовал свое право на ограничение доступа к информации, то и рассматривать ее как охраняемую законом оснований не имеется.

Данную позицию разделяет В.А. Мазуров, который полагает, что для отнесения информации к категории охраняемой законом достаточно установления собственником (владельцем) порядка обращения с последней[39]. Трудно согласиться с мнением В.П. Числина, что «та информация, которая имеет определенную ценность для собственника, но законодательными актами не определена как конфиденциальная, может быть защищена собственником правовыми средствами в гражданско-правовом порядке путем предъявления иска о возмещении убытков»[40]. Думается, что гражданско-правовые способы защиты прав должны использоваться в совокупности с уголовно-правовыми в случае посягательства против компьютерной информации ограниченного доступа.

Автор согласен с мнением А.М. Доронина, что неправомерный доступ к компьютерной информации общего пользования, т.е. информации, адресованной неограниченному кругу лиц, не образует состава преступления, ответствен-

---

[39] *Мазуров В.А.* Указ. соч. С. 58.

[40] *Числин В.П.* Указ. соч. С. 31–32.

ность за совершение которого предусмотрена ст. 272 УК РФ[41]. Полагаем, что само существование такого разделения информации говорит об отсутствии уголовно-правовой защиты общедоступной информации от неправомерного доступа и о необходимости сохранения в диспозиции ст. 272 УК РФ категории «охраняемая законом». Государство берет под свою охрану совокупность общественных отношений по правомерному и безопасному использованию не любой компьютерной информации, а только той, которая находится под защитой закона[42].

Автор поддерживает мнение большинства правоведов, считающих, что предметом преступления, указанного в ст. 272 УК РФ, является не любая информация, находящаяся в компьютерной форме, а только охраняемая законом[43]. Данная информация является предметом неправомерного доступа: это документированная информация, содержащая сведения, отнесенные законом к государственной тайне или

---

[41] См.: *Доронин А.М.* Указ. соч. С. 96; *Шарков А.Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: Дис. … канд. юрид. наук. Ставрополь, 2004. С. 63.

[42] *Доронин А.М.* Указ. соч. С. 87.

[43] См.: *Дворецкий М.Ю.* Изменения и дополнения главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Материалы Междунар. науч.-практич. конф. Тамбов: Изд. дом ТГУ им. Г.Р. Державина, 2013. С. 77; *Кочои С., Савельев Д.* Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. 1999. № 1; *Шарков А.Е.* Указ. соч. С. 28.

конфиденциальной информации[44]; это информация ограниченного доступа, которая не только имеет специальный правовой статус, установленный соответствующими законами РФ или субъектов Федерации, но и по своему характеру предназначена для ограниченного круга лиц (пользователей), имеющих право на ознакомление и работу с ней[45]. Охраняемой законом, по смыслу УК РФ, будет являться такая компьютерная информация, доступ к которой ограничен в соответствии с законом[46]. Доступом к информации, как установлено в ч. 6 п. 1 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации», является возможность получения информации и ее использования. В правовой науке не существует общепринятого классификатора отнесения информации к категории ограниченного доступа.

О.А. Гордов к признакам информации ограниченного доступа относит ценность скрываемых сведений; отсутствие свободного доступа к сведениям на законных основаниях; наличие превентивных мер, принимаемых обладателем сведений для охраны их от доступа третьих лиц[47]. К информации ограниченного доступа можно отнести следующие виды

---

[44] *Числин В.П.* Указ. соч. С. 36.

[45] *Доронин А.М.* Указ. соч. С. 87.

[46] *Кочои С., Савельев Д.* Указ. соч.

[47] *Городов О.А.* Основы информационного права России: Учеб. пособие. СПб.: Юрид. центр Пресс, 2003.

информации:

а) государственную тайну. Порядок отнесения сведений к государственной тайне, их засекречивания и рассекречивания регулируется Федеральным законом от 21 июля 1993 г. № 5485-I «О государственной тайне»[48]. Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (ст. 2);

б) банковскую тайну. В соответствии с Федеральным законом от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности»[49] кредитные организации и их сотрудники обязаны гарантировать тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Это положение Закона также распространяется на операции с электронными денежными средствами, которые зачастую являются мишенью для компьютерных преступников;

в) персональные данные. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[50] персональными данными является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных

---

[48] СЗ РФ. 1997. № 41. Ст. 4673.

[49] ВСНД РСФСР. 1990. № 27. Ст. 357.

[50] СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

данных). Право граждан на сохранность персональных данных в тайне может быть ограничено лишь в необходимых случаях и только федеральным законом;

г) информацию, носящую конфиденциальный характер. Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»[51] утвержден перечень сведений конфиденциального характера. Эти сведения могут быть распределены по следующим группам:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. В соответствии со ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются; органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Так, например, в соответствии со ст. 12 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»[52] сведения,

[51] СЗ РФ. 1997. № 10. Ст. 1127.

[52] СЗ РФ. 1997. № 47. Ст. 5340.

ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат. В соответствии с данным Законом также должна обеспечиваться тайна усыновления: работники органов записи актов гражданского состояния не вправе без согласия усыновителей сообщать какие-либо сведения об усыновлении и выдавать документы, из содержания которых видно, что усыновители не являются родителями усыновленного ребенка.

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» [53] и другими нормативными правовыми актами Российской Федерации. Однако действующий УПК РФ уже не содержит понятие «тайна следствия». В нем используются: «данные предварительного расследования» и «тайна совещания судей».

В соответствии с указанным Законом государственная защита потерпевших, свидетелей и иных участников уголовного судопроизводства – это осуществление предусмотренных настоящим Федеральным законом мер безопасности,

[53] СЗ РФ. 2004. № 34. Ст. 3534.

направленных на защиту их жизни, здоровья и (или) имущества, а также мер социальной поддержки указанных лиц в связи с их участием в уголовном судопроизводстве уполномоченными на то государственными органами. По решению органа, осуществляющего меры безопасности, может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные регистрационные знаки используемых им или принадлежащих ему транспортных средств.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации (далее – ГК РФ) и федеральными законами (служебная тайна). В настоящее время статья, определяющая служебную тайну, исключена из ГК РФ.

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами. В частности, к ним относятся:

– врачебная тайна – информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, его диагнозе и иные сведения, полученные при его обследовании и лечении (п. 1 ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в

Российской Федерации»)[54];

– нотариальная тайна – в соответствии со ст. 16 Основ законодательства о нотариате от 11 февраля 1993 г. № 4462-I[55] нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности;

– адвокатская тайна – любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю[56];

– тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений – одна из разновидностей права на неприкосновенность частной жизни, которая гарантируется Конституцией РФ и может быть ограничена только федеральным законом. В соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи»[57] (далее – ФЗ «О связи») операторы связи обязаны обеспечить соблюдение тайны связи. Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только

---

[54] Российская газета. 23.11.2011. № 263.

[55] Российская газета. 13.03.1993. № 467.

[56] См. ст. 8 Федерального закона от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (СЗ РФ. 2002. № 23. Ст. 2102).

[57] http://www.consultant.ru/popular/communication/. Дата обращения: 11.12.2015.

отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна). В соответствии с Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[58] коммерческой тайной является режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доход, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Права на результаты интеллектуальной деятельности и средства индивидуализации охраняются в соответствии с требованиями части четвертой ГК РФ[59].

Таким образом, все перечисленные виды информации, охраняемой законом, могут быть предметом преступления, предусмотренного ст. 272 УК РФ. На основе анализа действующих федеральных законов исследователями был сделан вывод, что в настоящий момент существует более 30 видов тайн, которые выступают в качестве прямых ограниче-

---

[58] СЗ РФ. 2004. № 32. Ст. 3283.

[59] http://base.garant.ru/10164072/. Дата обращения: 11.12.2015.

ний при реализации информационных прав и свобод. А в совокупности с подзаконными нормативно-правовыми актами количество видов тайн будет составлять уже более 40[60].

Проведенное исследование судебной практики по делам о привлечении к ответственности по ст. 272 УК РФ после вступления в силу ФЗ «Об информации, информационных технологиях и о защите информации» позволило сделать вывод, что суды при вынесении приговоров зачастую дают неправильное определение охраняемой законом компьютерной информации, применяя утративший силу Федеральный закон «Об информации, информатизации и защите информации».

Так, Долгопрудненский городской суд Московской области в приговоре от 6 декабря 2011 г. по уголовному делу № 1-175/11 установил, что П., имея в своем пользовании установленный по месту его проживания персональный компьютер, являясь пользователем услуги ООО «ОК» – «МД» на основании заключенного им абонентского договора с ООО «ОК» о предоставлении услуг доступа в компьютерную сеть «Интернет», имея умысел на неправомерный доступ к конфиденциальной информации о логинах и паролях абонентов услуги «МД», предоставляемой ООО «ОК», в нарушение ст. 21 Федерального закона «Об информации, информатизации и защите информации» в неустановленное время, обнару-

---

[60] *Лопатин В.Н.* Правовая охрана и защита права на тайну. (Начало) // Юридический мир. 1999. № 5–6. С. 42.

жив на неустановленном сайте компьютерной сети «Интернет» данные о логине и пароле абонента услуги «МД» Х., скопировал их в память на жесткий диск своего компьютера. После чего П., находясь по указанному адресу, осознавая возможность незаконного использования данных о логине и пароле абонента услуги «МД» Х., предвидя при этом наступление последствий в виде блокирования работы ЭВМ законного пользователя – Х., связанной с выходом в компьютерную сеть «Интернет», и желая наступления этих последствий, без разрешения Х., реализуя свой преступный умысел, направленный на неправомерный доступ к компьютерной информации, в определенный период времени без оплаты осуществлял неправомерный доступ к компьютерной информации, связанный с выходом в компьютерную сеть «Интернет» под учетными данными указанного абонента, что повлекло блокирование доступа к компьютерной информации для Х., создав условия, исключающие пользование информацией, находившейся в сети «Интернет» ее законным пользователем[61].

Как следует из приведенного приговора, суд в обоснование своих выводов применил нормы Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации», который в момент рассмотрения дела уже более пяти лет не действовал.

---

[61] База данных решений судов общей юрисдикции [Электронный ресурс]. – Режим доступа: http://www.gcourts.ru/case/6576093. Дата обращения: 17.09.2015.

II. Перейдем к анализу следующего дискуссионного вопроса в уголовно-правовой науке о возможности применения к информации категории собственности. В науке существует точка зрения, согласно которой «категория собственности может быть применима только к материальным носителям нематериальных объектов, в частности информации»[62], «право собственности относится не к информации, а к ее материальным носителям»[63]. Данную позицию сторонники этой точки зрения аргументируют отсутствием на законодательном уровне понятия «собственник информации» и использованием категории «обладатель информации». Мы считаем такой взгляд ошибочным, поскольку в диспозиции ст. 272 УК РФ предусмотрена ответственность именно за неправомерный доступ к компьютерной информации, а не к средствам хранения компьютерной информации.

Напомним, что понятия «собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения» и «владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения», использовавшиеся в Федеральном законе «Об инфор-

---

[62] См.: *Бачило Н.А.* О концепции правового обеспечения информатизации России / Н.А. Бачило, Г.В. Белов, В.А. Копылов и др. // Труды Института законодательства и сравнительного правоведения при ВС РФ. 1992. № 52. С. 4–17; *Копылов В.А.* Информационное право: Учебник. 2-е изд., перераб. и доп. М.: Юристь, 2002. С. 26–135.

[63] *Гаврилов О.А.* Информатизация правовой системы России. Теоретические и практические проблемы: Учеб. пособие. М.: Юридическая книга, 1998. С. 44.

мации, информатизации и защите информации», были заменены единым понятием «обладатель информации» (ч. 5 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации»[64]).

Действующее законодательство под обладателем информации понимает лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. С нашей точки зрения, из формулировки статьи следует, что категория «обладатель информации» объединяет в себе категорию «собственник информации» и категорию «владелец информации». Так, лицо, создавшее определенные данные, является собственником информации и может ограничить доступ к ней. При получении на основании закона или договора информации от собственника лицо считается владельцем информации и обязано обеспечить условия ограничения доступа к ней, определенные собственником.

Представляется, что после введения в действие ФЗ «Об информации, информационных технологиях и о защите информации» для привлечения к уголовной ответственности необходимо определить, был ли нарушен установленный режим доступа к информации. Вопрос о том, кто является субъектом права собственности компьютерной информа-

---

[64] http://base.garant.ru/12148555/#ixzz3IHNT2E7K. Дата обращения: 01.12.2015.

ции, становится в рамках существующего закона менее существенным.

Судебная практика позволяет нам сделать вывод, что суды при квалификации деяний по ч. 1 ст. 272 УК РФ устанавливают, является ли компьютерная информация охраняемой законом, ограничен ли к ней доступ. Так, Ленинский районный суд г. Тюмени в приговоре от 17 июля 2012 г. установил следующее. Гражданин Г., имея преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, достоверно зная, что учетно-регистрационные данные – логин и пароль, необходимые для подключения ЭВМ к интернет-сайту: www.Educon.tsogu.ru, позволяют получить возможность ознакомления с информацией ограниченного доступа (в соответствии со ст. 3, 6, 8, 9, 16 ФЗ «Об информации, информационных технологиях и о защите информации») и правомерно могут использоваться только лицом, их получившим на законных основаниях, осуществил неправомерный доступ к компьютерной информации.

Исследуя судебные приговоры, вынесенные после вступления в силу ФЗ «Об информации, информационных технологиях и о защите информации», мы пришли к выводу, что суды все еще не используют понятие «обладатель» информации, а в приговорах указывают собственника и владельца информации. Кезский районный суд Удмуртской Республики в приговоре от 10 февраля 2011 г. установил, что Л., используя свой персональный компьютер с процессором, сетевым

оборудованием и установленной операционной системой, в комплект которой входит программное обеспечение для доступа в сеть «Интернет» при помощи ADSL-модема с зарегистрированным абонентским номером телефонной линии общего значения, обеспечивающего соединение для сеансов доступа в сеть «Интернет» с учетными данными (логином и соответствующим паролем), принадлежащими Х., в нарушение требований ст. 2, 4, 6, 10, 12, 13, 17 ФЗ «Об информации, информационных технологиях и о защите информации», умышленно, с целью использования чужого логина и пароля для неправомерного доступа к охраняемой законом компьютерной информации, в виде безвозмездного незаконного пользования сетью «Интернет», пренебрегая установленным в Российской Федерации режимом защиты компьютерной информации и стремясь удовлетворить личные интересы, осуществил без согласия **собственника информации** – провайдера и легального пользователя Х. доступ к охраняемой законом компьютерной информации – логина и пароля и использовал эту информацию.

На наш взгляд, положения Закона, регулирующие статус обладателя информации, нуждаются в уточнении и конкретизации. Следует отметить, что законодатель не отказался полностью от применения к информации категории «собственник». В целях реализации норм ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 29 июля 2004 г. № 98-ФЗ

«О коммерческой тайне»[65] утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». В п. 2.5.2 вышеназванного стандарта указано, что под защиту подпадает «информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации»[66].

III. Относительно третьего вопроса, вокруг которого в науке идет полемика, ряд ученых высказывают свою позицию при определении цены информации. Как предмет преступления информация должна помимо формы в виде документа обладать определенной ценностью[67]. В.П. Числин включает в обязательные признаки отнесения компьютерной информации к предмету неправомерного доступа наличие статуса ограниченного доступа и «наличие такого признака информации, как ценность»[68].

В настоящее время не существует единого критерия определения ценности информации. Ее можно определить как максимальную пользу, которую может принести данное ко-

---

[65] СЗ РФ. 2004. № 32. Ст. 3283.

[66] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008.

[67] *Гаврилин Ю.В.* Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / Под ред. Н.Г. Шурухнова. С. 54.

[68] *Числин В.П.* Указ. соч. С. 29.

личество информации, или как те максимальные потери, к которым приведет утрата этого количества информации[69]. Теоретически один и тот же информационный объект может иметь разную ценность для субъектов, поэтому считаем, что такая категория, как «ценность информации», не может влиять на отнесение компьютерной информации к предмету преступления, предусмотренного ст. 272 УК РФ. Полагаем, что ценность информации следует определять ее обладателю.

[69] *Куприянов А.И., Шевцов В.В.* Оптимизация мер по защите с учетом ценности информации // Известия Института инженерной физики. 2012. № 25. С. 2–6.

§ 1.2. Объективная сторона неправомерного доступа к компьютерной информации

Объективная сторона, являясь одной из основных подсистем преступления, состоит из ряда взаимодействующих элементов, которые в своей совокупности образуют процесс внешнего посягательства на объект уголовно-правовой охраны[70]. Определение объективной стороны неправомерного доступа к компьютерной информации содержится в самой дефиниции ст. 272 УК РФ: «неправомерный доступ к охраняемой законом информации». При исследовании объективной стороны преступления, предусмотренного ст. 272 УК РФ, мы будем придерживаться элементного состава объективной стороны, господствующего в теории отечественного уголовного права. Учитывая положения уголовно-правовой доктрины, можно выделить следующие элементы объективной стороны неправомерного доступа к компьютерной информации:

1) общественно опасное деяние в виде неправомерного доступа к охраняемой законом компьютерной информации;

---

[70] *Ляпунов Ю.И.* Общественная опасность деяния как универсальная категория советского уголовного права: Учеб. пособие. М.: Изд-во ВЮЗШ МВД СССР, 1989. С. 79.

2) общественно опасные последствия в виде уничтожения, блокирования, копирования, модификации компьютерной информации;

3) наличие причинной связи между неправомерным доступом к компьютерной информации и наступившими вредными последствиями;

4) способ, место, время, обстановка, орудие и средства совершения преступления.

Первые три элемента объективной стороны являются обязательными, и неустановление хотя бы одного из признаков свидетельствует об отсутствии состава преступления и исключает уголовную ответственность за неправомерный доступ к компьютерной информации.

Способ, место, время, обстановка, орудие и средства преступления считаются факультативными признаками объективной стороны. А.В. Наумов указывает, что «они при любых обстоятельствах делают преступление предметным и обладают качественными характеристиками, влияющими на степень опасности преступления, поскольку выступают факторами, индивидуализирующими конкретное преступное действие (бездействие)»[71].

В отечественной правовой науке не выработан единый подход к содержанию понятия «неправомерный доступ к охраняемой законом компьютерной информации», что при-

---

[71] *Наумов А.В.* Российское уголовное право. Общая часть: Курс лекций. М.: БЕК, 1996. С. 172.

водит к проблемам и ошибкам, допускаемым правоприменителями при квалификации преступлений, предусмотренных ст. 272 УК РФ.

Уголовно-правовой анализ неправомерного доступа к компьютерной информации невозможен без определения понятия **доступ к информации**. Оно выступает в качестве относительно нового предмета исследования для российской науки уголовного права, в которой сформировались различные подходы к его определению.

В словаре русского языка С.И. Ожегова слово «доступ» трактуется как «посещение чего-либо с какой-либо целью» [72]

[72] *Ожегов С.И.* Указ. соч. С. 152.

Конец ознакомительного фрагмента.