С. Г. Еремин, Ю. В. Третьяков

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

В данной статье авторы отмечают, что настоящее время в главу 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» входят: 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». Санкции в рассматриваемых статьях о компьютерных преступлениях альтернативны, кроме двух квалифицированных составов, где в силу тяжести последствий преступления они снижены до относительно определенных.

Под предметом или орудием преступления в сфере дистанционного банковского обслуживания предлагается понимать машинную информацию, компьютер, компьютерную систему, программу, сеть. В случаях когда предметом преступления являются только аппаратно-технические средства электронно-вычислительной техники (например, их хищение, уничтожение), нужно говорить о преступлениях против собственности.

К правовым мерам борьбы с преступлениями в сфере дистанционно-банковского обслуживания следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, направленных на защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства и системы судопроизводства. Сюда же следует включить вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных стандартов. В целом четко законодательная позиция, прописанная методика раскрытия и расследования данной категории преступлений будут способствовать повышению эффективности деятельности оперативных сотрудников, следователей и экспертов в борьбе с преступностью в сфере компьютерных технологий.

Ключевые слова: уголовное законодательство, нормы уголовного права, машинная информация, компьютер, компьютерная система, компьютерная программа, компьютерная сеть, компьютерные преступления.

S. G. Eremin, Yu. V. Tretyakov

CHARACTERISTICS OF CRIMES OF CRIMINAL LAW IN THE FIELD OF REMOTE BANKING SERVICE

In this article, the authors note that at the present time in the Criminal Code of the Russian Federation the head of "Crime in the field of computer information" contains the following articles of criminally punishable acts: Art. 272. Unlawful access to computer information; Art. 273. Creation, use and distribution of malicious programs for computers; Art. 274. Violation of the rules for the operation of computers, computer systems or their networks. Sanctions in the considered articles on computer crimes are alternative, except for two qualified trains, where, due to the severity of the consequences of the crime, they are reduced to relatively certain.

Under the object or instrument of a crime in the field of remote banking services, it is proposed to consider machine information, computer, computer system, program, network. In cases where the subject of the crime are only hardware and hardware of electronic computers (for example, their theft, destruction), then it will be crimes against property.

The legal measures to combat crimes in the field of remote banking services include the development of norms that establish responsibility for computer crimes, protect the copyright of programmers, improve criminal and civil legislation, as well as the judicial system. This should include issues of public control over the developers of computer systems and the adoption of relevant international standards. In general, a well-developed legislative position, a prescribed method of disclosure and investigation of this category of crimes will help to increase the effectiveness of the activities of operational staff, investigators and experts in combating crime in the field of computer technology.

Key words: criminal legislation; norms of criminal law; computer information; a computer; computer system; computer program; computer network; computer crimes.

К правовым мерам борьбы с преступлениями в сфере дистанционного банковского обслуживания

следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, направленных на защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также системы судопроизводства. Сюда же следует включить вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных стандартов.

В последние годы появились труды, посвященные проблемам правовой борьбы с компьютерной преступностью, в частности это работы Ю. Батурина, М. Карелиной, В. Вехова, Ю. А. Куриленко, Б. П. Смагоринского, Э. А. Ли, Е. В. Бурцева, А. Ф. Родина, С. Я. Казанцева, О. Э. Згадзай, И. С. Дубровина, Н. Х. Сафиуллина.

Законодательство Российской Федерации встало на путь борьбы с компьютерной преступностью [1]. В связи с этим представляется важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с компьютерными преступлениями [2].

В Уголовном кодексе Российской Федерации (далее — УК РФ) криминализирован ряд деяний, совершаемых в сфере компьютерной информации, чему посвящена глава 28 «Преступления в сфере компьютерной информации» [3].

В уголовном законодательстве *под компьютерными преступлениями* рекомендовано понимать закрепленные уголовным законом общественно опасные деяния, в которых машинная информация выступает объектом преступного посягательства. Предметом или орудием преступления в сфере дистанционного банковского обслуживания (ДБО) надлежит считать машинную информацию, компьютер, компьютерную систему, программу, сеть. В случаях когда предметом преступления являются только аппаратно-технические средства электронно-вычислительной техники (например, их хищение, уничтожение), нужно говорить о преступлениях против собственности.

Встречаются случаи, когда электронно-вычислительной технике причиняется вред с помощью непосредственного воздействия на нее путем различных информационных команд. Это возможно, если преступникам удастся ввести движущиеся части компьютера (жесткий диск, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора либо зациклить работу компьютера, чтобы при использовании минимального количества его участков произошли их нагревание и выход из соответствующего рабочего состояния.

В указанных выше ситуациях квалификацию преступлений следует проводить по совокупности статей УК РФ (глав о преступлениях против собственности и компьютерных преступлениях), так как страдают два объекта уголовно-правовой охраны, равно как и при использовании в качестве орудия совершения преступления не информационной, а аппаратно-технической части (например, нанесение телесных повреждений принтером и т. п.).

Глава 28 УК РФ «Преступления в сфере компьютерной информации» призвана обеспечить охрану информационной безопасности, включая аппаратно технические средства — материальные носители информационных ресурсов. Неправомерное использование информации может быть различным (нарушение неприкосновенности интеллектуальной собственности, нормальной финансово-хозяйственной деятельности организаций, разглашение сведений о частной жизни граждан, имущественный ущерб в виде убытков и неполученных доходов, потеря репутации фирмы), поэтому законодатель вполне оправданно сосредоточил компьютерные преступления в разделе IX УК РФ «Преступления против общественной безопасности и общественного порядка».

С уголовно-правовой точки зрения общим объектом компьютерных преступлений будет выступать совокупность всех общественных отношений, охраняемых уголовным законом. Родовым объектом — общественная безопасность и общественный порядок, видовым — совокупность общественных отношений по правомерному и безопасному использованию информации, а непосредственным — диспозиции конкретных статей УК РФ. Следует учитывать, что обычно непосредственный объект основного состава компьютерного преступления сформулирован альтернативно, в квалифицированных же составах преступления их количество увеличивается.

В результате анализа соответствующих статей УК РФ возникает вопрос: является ли компьютерная информация лишь предметом преступлений или она может быть их средством, если электронно-вычислительная техника используется для совершения других посягательств на иной объект? Авторы УК РФ изложили составы главы 28 таким образом, что информация в каждом случае является лишь предметом совершения компьютерного преступления. Вместе с тем при ее использовании как средства совершения другого преступления отношения по ее охране нарушаются, поскольку такая информация сама будет выступать предметом общественно опасного деяния. Из отдельных нормативных правовых актов следует, что нельзя противоправно воспользоваться компьютерной информацией, хранящейся в элетронно-вычислительной машине, не взломав

ее защиту, не выполнив неправомерные действия, закрепленные в ст. 20 Федерального закона «Об информации, информатизации и защите информации»: утечки, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования и других форм незаконного вмешательства в информационные ресурсы и системы [4].

В случае когда не будут затронуты сведения, хранящиеся на конкретном компьютере и используемые его законным владельцем, может быть причинен вред другим машинам, с которыми он связана сетью. В итоге при совершении хищения денежных средств с помощью электронно-вычислительной техники, уголовная ответственность должна наступать по правилам идеальной совокупности преступлений. Многие составы главы 28 УК РФ относятся к преступлениям небольшой и средней тяжести, только один из них — к тяжким преступлениям. Объективная сторона названных составов в основном формулируется как материальные преступления, поскольку они представляют общественно опасные деяния и последствия, здесь видна причинная связь между этими признаками.

Уничтожение, блокирование, модификация и копирование компьютерной информации не исключают совершения самостоятельных действий, поэтому представляется правильным рассматривать основанием уголовной ответственности за неправомерный доступ к ней случаи, когда доступ сопряжен с ее уничтожением, блокированием и другими действиями, придающими значение причины и необходимых условий.

Исходя из ч. 2 ст. 9 УК РФ время совершения и окончания деяния каждого из рассматриваемых видов преступлений взаимообусловлены и совпадают независимо от времени наступления последствий. При этом общественно опасные деяния будут выражаться в действиях и редко в бездействии (иногда такой признак объективной стороны, как способ совершения преступления, является обязательным для основного и квалифицированного состава преступления). В остальных случаях способ, обстановка (место, время), орудия и средства совершения преступления могут рассматриваться как смягчающие либо отягчающие обстоятельства.

Что касается признаков субъективной стороны анализируемых составов преступлений, то здесь очевиден только один — вина (точнее, с учетом ч. 2 ст. 24 УК РФ для всех таких преступлений ее наличие обусловлено формой умысла, кроме двух квалифицированных составов, предусматривающих умысел по отношению к преступному действию и неосторожность к общественно опасным последствиям). Отметим, что наличие факультативных признаков субъективной стороны, равно как и объективной, не играют роли для квалификации преступлений данного вида.

Мотивом совершения преступных действий по делам данной категории являются корысть, хулиганские побуждения, месть, сокрытие другого преступления и т. д. При квалификации преступления иногда затруднительно отграничить причинение невиновного вреда и вреда по неосторожности, поскольку очевидным является повышенная сложность и скрытность всех процессов в компьютерных сетях. Субъект нескольких составов преступлений — специальный, а в других — любой гражданин.

Согласно ст. 20 УК РФ уголовная ответственность за совершение преступлений в сфере обеспечения компьютерной безопасности наступает с 16 лет. В статьях 28 главы УК РФ диспозиции являются описательными (бланкетными либо отсылочными), для правильного их применения надлежит изучить ст. 35 УК РФ и нормативные правовые акты, закрепляющие охрану компьютерной информации, правила эксплуатации компьютерной техники. Санкции в рассматриваемых статьях о компьютерных преступлениях альтернативны, кроме двух квалифицированных составов, где в силу тяжести последствий преступления они снижены до относительно определенных.

В настоящее время в УК РФ глава «Преступления в сфере компьютерной информации» содержит: 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».

1. Куриленко Ю. А. Использование компьютерных технологий в деятельности сотрудника ОВД // Судебная экспертиза. 2008. № 2. С. 117—119; Ли Э. А. Совершенствование использования компьютерных технологий в расследовании преступлений: автореф. дис. … канд. юрид. наук. Бишкек: Кыргызско-российский славянский университет, 2011; Использование компьютерных технологий в деятельности следователя / под ред. проф. Б. П. Смагоринского. Волгоград: ВА МВД России, 2003; Бурцева Е. В. Информационные технологии в юриспруденции: учеб. пособие. Тамбов: Изд-во ТГТУ, 2012; Информационные технологии в юриспруденции / под ред. С. Я. Казанцева. М.: Академия, 2011.

2. Конституция Российской Федерации от 12 декабря 1993 г. Доступ из справ.-правовой системы «КонсультантПлюс»; Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 декабря 2001 г. № 174-ФЗ Доступ из справ.-правовой системы «КонсультантПлюс»; Вопросы Министерства внутренних дел Российской Федерации: указ Президента Российской Федерации от 1 марта 2011 г. № 248. Доступ из справ.-правовой системы «КонсультантПлюс»;

3. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс»;

4. О безопасности: закон Российской Федерации от 5 марта 1992 г. № 2446-1. Доступ из информ.-правового портала «Гарант»; О правовой охране программ для электронных вычислительных машин и баз данных: закон Российской Федерации от 23 сентября 1992 г. № 3523-1. Доступ из информ.-правового портала «Гарант»; О государственной тайне: закон Российской Федерации от 21 июля 1993 г. № 5485-1. Доступ из информ.-правового портала «Гарант»; О персональных данных: закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из информ.-правового портала «Гарант»; Об информации, информационных технологиях и о защите информации: закон Российской Федерации от 27 июля 2007 г. №149-ФЗ. Доступ из информ.-правового портала «Гарант».

1. Kurilenko Yu. A. Use of computer technologies in the activity of an ATS officer // Forensic examination. 2008. № 2. P. 117—119; Lee E. A. Improving the use of computer technology in the investigation of crimes: the author's abstract. dis. ... cand. jurid. sciences. Bishkek: Kyrgyz-Russian Slavonic University, 2011; The use of computer technology in the activities of the investigator / Ed. prof. B. P. Smagorinsky. Volgograd: Ministry of Internal Affairs of Russia, 2003; Burtseva E. V. Information technologies in jurisprudence: Textbook. allowance. Tambov: Publishing House of TSTU, 2012; Information technology in jurisprudence / ed. S. Ya. Kazantsev. Moscow: Academy, 2011.

2. The Constitution of the Russian Federation of December 12, 1993. Access from the legal system "Consultant Plus"; The Code of Criminal Procedure of the Russian Federation: Feder. Law of December 18, 2001 No. 174-FZ Access from the "Consultant Plus" legal system; Issues of the Ministry of Internal Affairs of the Russian Federation: Decree of the President of the Russian Federation No. 248 of March 1, 2011. Access from the consultant-legal system "ConsultantPlus";

3. The Criminal Code of the Russian Federation of June 13 1996 No. 63-FZ. Access from the legal system "ConsultantPlus";

4. On security: the law of the Russian Federation of March 5, 1992 No. 2446-1. Access from the information-legal portal "Garant"; On the legal protection of programs for electronic computing machines and databases: the law of the Russian Federation of September 23, 1992 No. 3523-1. Access from the information-legal portal "Garant"; "On State Secrets": the law of the Russian Federation of July 21, 1993 No. 5485-1. The electronic resource of the Garant system; On personal data: the law of the Russian Federation of July 27, 2006 No. 152-FZ. Access from the information-legal portal "Garant"; On Information, Information Technologies and Information Protection: the Law of the Russian Federation of July 27, 2007 No. 149-FZ. Access from the information-legal portal "Garant".