УДК/UDC 343.3/.7

Преступления в сфере компьютерной информации: юридический анализ, проблемы квалификации

Безруков Андрей Вадимович
старший преподаватель кафедры «Уголовное право»
Пензенский государственный университет
г. Пенза, Россия
SPIN-код: 1471-0092

Безрукова Олеся Владимировна
кандидат юридических наук, доцент кафедры «Уголовное право»
Пензенский государственный университет
г. Пенза, Россия
e-mail: olesia_8013-10@mail.ru
SPIN-код: 9738-9830

Аннотация

Статья посвящена некоторым проблемам, возникающим при квалификации преступлений в сфере компьютерной информации. Проанализированы составы: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ). Рассмотрены некоторые положительные изменения российского законодательства; приведен ряд примеров трудностей, возникающих при квалификации преступлений в сфере компьютерной информации; сформулированы предложения по совершенствованию действующего российского уголовного законодательства в области информационной безопасности.

Ключевые слова: преступления в сфере компьютерной информации; проблемы квалификации; неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной ин-

формации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру РФ.

Crimes in the Field of Computer Information: Legal Analysis, Problems of Qualification

Bezrukov Andrey Vadimovich
senior lecturer of the Department of Criminal Law
Penza State University
Penza, Russia
SPIN-код: 1471-0092

Bezrukova Olesya Vladimirovna
Candidate of Law, assistant Professor of the Department of Criminal Law
Penza State University
Penza, Russia
e-mail: olesia_8013-10@mail.ru
SPIN-код: 9738-9830

Abstract

The article is devoted to some problems that arise in the qualification of crimes in the field of computer information. Analyzed compositions: illegal access to computer information (article 272 of the criminal code), the creation, use and distribution of malicious computer programs (article 273 of the criminal code), violation of rules of exploitation of means of storage, processing or transmission of computer information and information-telecommunication networks (article 274 of the criminal code), undue influence on the critical information infrastructure of the Russian Federation (article 274.1 of the criminal code). Some positive changes in Russian legislation are considered; a number of examples of difficulties encountered in the qualification of crimes in the field of computer information are given; proposals are formulated to improve the current Russian criminal legislation in the field of information security.

Key words: crimes in the field of computer information, problems of qualification, illegal access to computer information, creation, use and distribution of malicious computer programs, violation of the rules for the operation of storage, processing or transmission of computer information and information and telecommunications networks, illegal impact on the critical information infrastructure of the Russian Federation.

Преступления в сфере компьютерной информации устанавливаются гл. 28 УК РФ (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»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру РФ»). По данным Министерства внутренних дел Российской Федерации, в период за январь — декабрь 2019 года количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 68,5% по сравнению с 2018 годом, составив 294,4 тыс. [1] Из приведенной статистики видно, что уровень преступности в данном направлении значительно увеличился, и подобная тенденция наблюдается на протяжении последних нескольких лет.

Стоит отметить, что преступления в сфере компьютерной информации отличаются высокой латентностью. То есть их реальное количество гораздо больше зафиксированного в статистических данных. Главным фактором здесь выступает нежелание самих потерпевших обращаться к правоохранительным органам и стремление к использованию альтернативных способов восстановления своих прав (восстановление аккаунта через администратора).

Практика применения уголовно-правовых норм показывает, что квалификация преступлений, совершаемых в сфере компьютерной информации, представляет определенные трудности.

Так, уголовная ответственность по ст. 272 УК РФ наступает в случае неправомерного доступа к компьютерной информации. Преступление считается оконченным с момента ее уничтожения, блокирования (ограничения доступа к информации), модификации (изменения), копирования (на внешний носитель или иной компьютер). При этом под компьютерной информацией понимаются сведения (сообщения, данные), представляемые в форме электрических сигналов, независимо от средств

их хранения, обработки и передачи [2]. Для данного преступления характерна умышленная форма вины по отношению к совершаемым действиям и неосторожная форма — по отношению к последствиям, поскольку принято считать, что лицо не может заранее предвидеть, какой ущерб последует за деянием, соответственно, желать его наступления также не может. При квалификации по ст. 272 УК РФ проблемным видится отсутствие общепринятого толкования термина «охраняемая законом информация». Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры РФ, указывают, что неправомерные манипуляции с открытой (общедоступной информацией) не подпадают под действие ст. 272 УК РФ [3]. Однако существует обширная судебная практика по делам, связанным с неправомерным доступом к общедоступной информации в сети Интернет. В таких случаях суды ссылаются на то обстоятельство, что виновное лицо осуществило неправомерные действия в отношении общедоступной информации, охраняемой Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4]. Согласно ст. 16 данного законодательного акта 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.

Таким образом, ст. 272 УК РФ может применяться не только в отношении информации особого статуса и секретности, но обеспечивать должную уголовно-правовую охрану общедоступной информации.

Ст. 273 УК РФ устанавливает ответственность за создание, использование и распространение вредоносных компьютерных программ. То есть уголовно наказуемо создание (т. е. написание хотя бы одной копии

программы, информации), распространение (т. е. передача программы или носителя иным лицам), использование (т. е. внедрение программы в компьютер или компьютерную сеть независимо от того, повлекло ли это какие-либо последствия). Учитывая, что практически каждый из нас сталкивался с использованием против него вредоносных программ, то данная норма является одной из наиболее распространенных в группе преступлений в сфере компьютерной информации. Так, в 2017 году атаки на информационную инфраструктуру ряда государств, в том числе России, вирусов-шифровальщиков WannaCry и Petya нанесли огромный ущерб. В общей сложности только от WannaCry пострадало более 500 тыс. компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям, в более чем 150 странах мира [5].

Принципиально важно для квалификации деяний по ст. 273 УК РФ то, что в правовой науке так и не сложилось единообразного понимания вредоносной программы, что вызывает затруднения при ответе на вопрос, а является ли вообще та или иная программа вредоносной. Отчасти содержание понятия вредоносной программы содержится в иных актах, например в ГОСТе Р 50922-2006 «Защита информации. Основные термины и определения» [6]. Согласно п. 2.6.5 ГОСТа Р 50922-2006, вредоносная программа — это программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. В свою очередь, многие исследователями подчеркивают, что основным отличием вредоносных программ от другого программного обеспечения, которое также может производить копирование, уничтожение, модификацию информации, определяется тем, что все действия производятся без уведомления пользователя, скрытно от него, а сам пользователь зачастую и не подозревает о наличии такой программы на его устройстве.

Однако подобное толкование несовершенно, поскольку вирусы-шпионы, основной целью которых является не копирование или модификация, а сбор данных о пользователях устройств, фактически не подпа-

дают под данное определение. Поэтому более логичным представляется понимать под вредоносной программой код или его часть, специально созданные для выполнения или способствующие выполнению несанкционированных действий в информационной системе, которые могут привести к причинению вреда. Кроме того, проблемными видятся квалификация «использования контрафактного программного обеспечения», «использования лицензионных программ злоумышленниками», а также непосредственное «распространение информации о вирусе или его размещение в общедоступных сетях без непосредственного прямого использования».

Установление уголовной ответственности по ст. 274 УК РФ за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям имеет целью предупреждение невыполнения пользователями своих обязанностей, влияющих на сохранность компьютерной информации. Субъективная сторона предусматривает как умышленную, так и неосторожную форму вины, а специальным субъектом является лицо, обязанное соблюдать соответствующие правила.

Диспозиция ст. 274 УК РФ является бланкетной и отсылает непосредственно к конкретным положениям, закрепляющим правила эксплуатации оборудования, обработки и передачи информации и др. При этом данные правила должны устанавливаться правомочным лицом, так как общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети Интернет, не существует [7]. В отличие от ряда иных специальных правил, сосредоточенных в конкретных нормативных актах, правила эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не консолидированы и содержатся во множестве источников, в связи с чем отсутствует четкий их перечень.

К действиям по смыслу ст. 274 УК РФ можно, например, отнести:

— нарушение запрета на подключение служебного оборудования к сети Интернет;
— предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации;
— несанкционированное разглашение логина или пароля пользователя;
— отключение средств противовирусной защиты и др.

Преступное бездействие может проявляться в несоблюдении или прямом игнорировании соблюдения установленных правил, обеспечивающих должную работу средств хранения, обработки или передачи охраняемой компьютерной информации. При этом уголовный закон исключает уголовную ответственность, если обозначенные ст. 274 УК РФ деяния не повлекли за собой крупного ущерба (ч. 1), тяжких последствий или угрозы их наступлении (ч. 2).

Введение ст. 274.1 УК РФ «Неправомерное воздействие на объекты критической информационной инфраструктуры РФ» обусловлено частотой хакерских атак на государственные ведомственные ресурсы. Так, только за период с 2019 г. по март 2020 г. были совершены крупные атаки на сайт Сбербанка, результатом которых стало опубликование персональных данных нескольких миллионов пользователей [8–9].

Данная норма является специальной по отношению к ст. ст. 272, 273 и 274 УК РФ. Кроме того, она является бланкетной и отсылает к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [10].

Предметом преступления является компьютерная информация, программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. В свою очередь, если лицу по независящим от него обстоятельствам не удалось причинить вред, то содеянное следует квалифицировать как покушение на преступление по ч. 3 ст. 30, ч. 1 ст. 274 УК РФ.

На данный момент рост преступлений в сфере компьютерной информации наблюдается не только по данным составам, но и в рамках иных разделов УК РФ при совершении деяний с использованием информационно-телекоммуникационных технологий (мошенничество, организация азартных игр, пропаганда террористической деятельности и др.) [11]. Такая ситуация обусловила необходимость дальнейшего развития и внесения поправок в уголовный закон по расширению перечня составов преступлений, совершаемых в электронной среде. В этом направлении в уголовной науке сформировалась точка зрения о необходимости:

1. Введения такого способа совершения преступления, как «с применением компьютерных средств», «с применением информационных технологий» или др.
2. Введения отдельного раздела в Уголовном кодексе РФ, который был бы полностью сконцентрирован на компьютерных преступлениях. Однако, во-первых, в данном случае нарушается системность уголовного законодательства, а во-вторых, вопрос об определенности перечня компьютерных преступлений по-прежнему остается нерешенным [12, с. 316].

Что касается первого пункта, меры в данном направлении уже частично принимаются законодателем. Так, была введена статья «Мошенничество в сфере компьютерной информации», что значительно упростило квалификацию деяний в правоприменительной практике, так как ранее подобные действия приходилось квалифицировать по совокупности преступлений по статьям «Мошенничество» и «Неправомерный доступ к компьютерной информации». При этом судебная практика подтверждает, что и в настоящее время есть потребность в подобной квалификации. Примером выступает приговор Автозаводского районного суда г. Тольятти Самарской области от 5 июля 2019 г. по делу № 1-227/2019 [13].

Согласно материалам уголовного дела, Зволь П. В. путем мошенничества в сфере компьютерной информации похитил денежные средства, принадлежащие ПАО «МегаФон», в размере 500 699 рублей 97 копе-

ек. Преступление совершено при следующих обстоятельствах: «. . . Зволь П. В. устроился в компанию „МегаФон“. В его должностные обязанности входило: продажа SIM-карт, обслуживание, подключение услуг. В компании Мегафон он проходил обучение по пользованию программным обеспечением СБМС. . . С лицевых счетов друзей он перекидывал SIM-карты на лицевые счета абонентов с денежными средствами, чтобы вернуть денежные средства, уплаченные абонентом в счет будущих услуг, проводил возврат авансового платежа в качестве банковского перевода, затем просил их пойти в банк и обналичить денежные средства. Виновным себя признал только по ст. 159.6 УК РФ, а по ст. 272 УК РФ вину не признал, поскольку ст. 159.6 УК РФ охватывает умысел на совершение ст. 272 УК РФ, так как без доступа к СБМС он не мог провести указанные действия. Его умысел был направлен не на завладение информацией, а на извлечение денежных средств».

Суд в приговоре разъяснил: «. . . мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. ст. 272, 273 или 274.1 УК РФ. Занимая указанную должность, Зволь П. В. произвел неправомерный доступ к информационно-биллинговой системе ПАО „МегаФон“, к которой имел допуск, в том числе и в отсутствие абонентов ПАО „МегаФон“ и без их ведома и согласия, произвел модификацию компьютерной информации путем изменения сведений о состоянии лицевых счетов абонентов». Действия подсудимого суд посчитал правильным квалифицировать по ч. 1 ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем модификации компьютерной информации, и по ч. 3 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло модификацию компьютерной информации, совершенное лицом с использованием своего служебного положения.

Таким образом, с учетом стремительного развития количества и видов преступлений, совершаемых с применением информационно-коммуникационных технологий в сети Интернет, в уголовном законе все еще остается множество пробелов в данной сфере.

Список литературы

1. Состояние преступности в России за январь — декабрь 2019 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://media.mvd.ru/files/application/1748898 (дата обращения: 05.12.2019).

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 № 63-ФЗ (ред. от 02.12.2019) // Справочно-правовая система «Консультант Плюс».

3. Русскевич Е. А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. № 10 (94). С. 46–50.

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 03.04.2020) // Справочно-правовая система «Консультант Плюс».

5. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. М.: ИНФРА-М, 2019. 227 с.

6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // Кодекс. URL: http://docs.cntd.ru/document/1200058320 (дата обращения: 05.12.2019).

7. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (дата обращения: 05.12.2019).

8. Персональные данные 60 млн клиентов Сбербанка утекли в сеть // Хабр. URL: https://habr.com/ru/news/t/469903/ (дата обращения: 05.12.2019).

9. Сбербанк зафиксировал рост числа DDoS-атак на свои системы // Известия. URL: https://iz.ru/999095/2020-04-13/sberbank-zafiksiroval-rost-chisla-ddos-atak-na-svoi-sistemy (дата обращения: 05.12.2019).

10. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 года № 187-ФЗ // Российская газета. 2017. № 167.

11. Краткая характеристика состояния преступности в Российской Федерации за январь — апрель 2020 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://xn–b1aew.xn–p1ai/reports/item/20176492/.

12. Чуриков Н. А. Преступления в сфере компьютерной информации: проблемы квалификации и совершенствования уголовного законодательства в данной сфере / Н. А. Чуриков, С. С. Медведев // Образование и наука в современных реалиях: материалы Междунар. науч.–практ. конф. (Чебоксары, 4 июня 2017 г.). В 2 т. Т. 2 / редкол.: О. Н. Широков [и др.]. Чебоксары: ЦНС «Интерактив плюс», 2017. С. 312–317.

13. Приговор Автозаводского районного суда г. Тольятти Самарской области от 5 июля 2019 г. по делу № 1-227/2019 // Автозаводский районный суд г. Тольятти. URL: https://avtozavodsky–sam.sudrf.ru/modules.php?name=sud_delo&name_op=case&_id=148510205&_uid=1fce1d3c-8472-42cd-b7f7-04aa36bff989&_deloId=1540006&_caseType=0&_new=0&srv_num=1 (дата обращения: 05.12.2019).

References

1. The State of Crime in Russia for January—December 2019 // The official website of the Ministry of Internal Affairs of the Russian Federation. URL: https://media.mvd.ru/files/application/1748898 (access date: December 5, 2019).

2. The Criminal Code of the Russian Federation: Federal Law of June 13, 1996 No. 63-FZ (as amended on December 2, 2019) // Consultant Plus.

3. Russkevich, Ye. A. Illegal Access to Computer Information: Theory and Judicial Practice // Sudya. 2018. No. 10 (94). Pp. 46–50.

4. On Information, Information Technology and Information Protection: Federal Law of July 27, 2006 No. 149-FZ (as amended on April 3, 2020) // Consultant Plus.

5. Russkevich, Ye. A. Criminal Law and "Digital Crime": Problems and Solutions. Moscow: INFRA-M, 2019. 227 p.

6. GOST R 50922-2006. Data Protection. Basic Terms and Definitions // Codex. URL: http://docs.cntd.ru/document/1200058320 (access date: December 5, 2019).

7. Methodological Recommendations for Prosecutorial Supervision of the Implementation of Laws in the Investigation of Crimes in the Field of Computer Information // GARANT.RU. URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (access date: December 5, 2019).

8. Personal Data of 60 Million Sberbank Customers Leaked Online // Habr. URL: https://habr.com/ru/news/t/469903/ (access date: December 5, 2019).

9. Sberbank Recorded an Increase in the Number of DDoS Attacks on Its Systems // Izvestiya. URL: https://iz.ru/999095/2020-04-13/sberbank-zafiksiroval-rost-chisla-ddos-atak-na-svoi-sistemy (access date: December 5, 2019).

10. On the Security of Critical Information Infrastructure of the Russian Federation: Federal Law of July 26, 2017 No. 187-FZ // Rossiyskaya gazeta. 2017. No. 167.

11. A Brief Description of the State of Crime in the Russian Federation for January—April 2020 // The official website of the Ministry of Internal Affairs of the Russian Federation. URL: https://xn–b1aew.xn–p1ai/reports/item/20176492/.

12. Churikov, N. A. Crimes in the Field of Computer Information: Problems of Qualification and Improvement of Criminal Legislation in This Field / N. A. Churikov, S. S. Medvedev // Education and Science in Modern Realities. In 2 vol. Vol. 2 / O. N. Shirokov [et al.] (eds.). Cheboksary: Interactive Plus, 2017. Pp. 312–317.

14. The Sentence of the Avtozavodsky District Court of Tolyatti of July 5, 2019, Case No. 1-227/2019 // Avtozavodskiy District Court of Tolyatti. URL: https://avtozavodsky–sam.sudrf.ru/modules.php?name=sud_delo&name_op=case&_id=148510205&_uid=1fce1d3c-8472-42cd-b7f7-04aa36bff989&_deloId=1540006&_caseType=0&_new=0&srv_num=1 (access date: December 5, 2019).