УДК/UDC 343.34

Неправомерный доступ к компьютерной информации: теория и практика применения уголовного закона

Яшков Сергей Александрович
кандидат юридических наук, доцент, доцент кафедры уголовного права, криминологии и уголовного процесса
Екатеринбургский филиал Московской академии Следственного комитета Российской Федерации
г. Екатеринбург, Россия
e-mail:jasa79@rambler.ru

Аннотация

Статья посвящена исследованию проблем квалификации компьютерной преступности. Автором анализируется статистика совершения компьютерных преступлений в Российской Федерации, особое внимание обращается на наиболее распространенное из них неправомерный доступ к компьютерной информации. Приводятся примеры из судебной практики. Кроме того, автором предпринимается попытка дать уголовно-правовую характеристику объективной стороны состава преступления, предусмотренного ст. 272 Уголовного кодекса Российской Федерации, и поставить вопрос о сложностях квалификации действий виновного, осуществившего неправомерный доступ к охраняемой законом компьютерной информации, не повлекшего уничтожения, блокирования, модификации либо копирования компьютерной информации.

Ключевые слова: компьютерные преступления, блокирование, модификация, копирование, компьютерная информация, неправомерный доступ.

Illegal Access to Computer Information: Theory and Practice of Criminal Law Application

Yashkov Sergey Aleksandrovich
Candidate of Law, assistant professor, assistant professor of the Department of Criminal Law, Criminology and Criminal Procedure
Yekaterinburg branch of the Moscow Academy of the Investigative Committee of the Russian Federation
Yekaterinburg, Russia
e-mail:jasa79@rambler.ru

Abstract

The article is devoted to the study of the problems of qualification of computer crime. The author analyzes the statistics of computer crimes in the Russian Federation, paying special attention to the most common of them - illegal access to computer information. Examples from judicial practice are given. In addition, the author attempts to give a criminal-legal description of the objective side of the offense under Art. 272 of the Criminal Code of the Russian Federation, and raise the issue of the difficulties of qualifying the actions of the guilty person who has carried out illegal access to computer information protected by law, which did not lead to the destruction, blocking, modification or copying of computer information

Key words: computer crimes, blocking, modification, copying, computer information, illegal access.

В настоящее время в связи с бурным развитием техники и технологий, особенно компьютерных, большое значение в жизнедеятельности человека играет информация и информатизация. В то же время на фоне протекания процессов всеобщей глобальной цифровизации отчетливо прослеживается тенденция формирования криминальных угроз принципиально нового плана, затрагивающих сферу компьютерной информации и информационно-телекоммуникационных технологий [1]. С каждым годом увеличивается количество компьютерных преступлений [2].

Действующий Уголовный кодекс Российской Федерации (далее по тексту — УК РФ) [3] предусматривает четыре состава преступления в сфере компьютерной информации, за совершение которых наступает ответственность. К ним относятся: 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) и неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

В целях настоящего исследования наиболее интересным из представленных является состав преступления, предусмотренный ст. 272 УК РФ. Согласно статистическим данным, опубликованным на официальном сайте Министерства внутренних дел Российской Федерации [4], за январь–декабрь 2019 г. в России было зарегистрировано 2883 преступления в сфере компьютерной информации, а на долю преступлений, предусмотренных ст. 272 УК РФ, пришлось 2420 преступлений.

Если посмотреть статистику за январь–декабрь 2020 г., то всего было зарегистрировано 4498 преступлений в сфере компьютерной информации, из которых 4105 связаны с неправомерным доступом к компьютерной информации [4].

Статистика за январь–октябрь 2021 г. показывает, что за этот период в России было зарегистрировано 5564 преступления в сфере компьютерной информации, из которых 5207 были зарегистрированы по признакам ст. 272 УК РФ [4].

Анализ представленных статистических данных свидетельствует о том, что среди всех компьютерных преступлений чаще всего совершаются преступления, связанные с неправомерным доступом к компьютерной информации.

В связи с этим хотелось бы обратиться к проблемным вопросам квалификации данного состава преступления, особенно учитывая, что «анализ существующей следственной практики показывает, что неправомерный доступ к компьютерной информации, с одной стороны, является одним из самых распространенных компьютерных преступлений, а с другой стороны, достаточно сложным в расследовании, т. к. у следо-

вателя возникают определенные трудности при квалификации деяния» [4].

Так, по объективной стороне состав данного преступления сформулирован как материальный. Это означает, что уголовно наказуемыми действия субъекта будут только в том случае, если наступят последствия, указанные в законе, — уничтожение, блокирование, модификация либо копирование компьютерной информации.

Рассмотрим несколько примеров из судебной практики.

Так, приговором суда гражданка М. была признана виновной в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ. Гражданка М., будучи сотрудницей профессионального образовательного учреждения, не желая продолжать трудовую деятельность с новым руководством, решила удалить новостные сообщения о деятельности организации с официального сайта учреждения. С этой целью, используя собственный ноутбук, она осуществила выход в информационно-телекоммуникационную сеть «Интернет», открыла страницу сайта учреждения, а потом путем незаконного ввода аутентификационной информации, а именно пароля и логина, которые у нее имелись в связи с ранее занимаемой должностью, обеспечила себе доступ к сайту в режиме администратора. После чего гражданка М. осуществила уничтожение с сайта новостной ленты путем ее удаления [5].

В другом примере гражданка В., работая в салоне сотовой связи, используя биллинговую программу, осуществила неправомерный доступ к аккаунту социальной сети, принадлежащему другому лицу, после чего изменила от него пароль, а впоследствии удалила данный аккаунт. Она также была осуждена по ч. 1 ст. 272 УК РФ. В приговоре было отражено, что своими действиями гражданка В. совершила неправомерный доступ к охраняемой законом компьютерной информации, что повлекло модификацию и блокирование компьютерной информации [6].

Еще в одном случае приговором суда гражданин Б. осужден за неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации. Так, у граж-

данина Б., работавшем в отделе безопасности ИК УФСИН России по Республике Мордовия, возник умысел осуществить неправомерный доступ к базам данных УФСИН России по Республике Мордовия с целью их дальнейшего копирования в скрытую папку служебного компьютера для личного просмотра, что им и было осуществлено с помощью выхода в информационно-телекоммуникационную сеть «Интернет» и использования компьютерной программы для сканирования сети «IPScan» [7].

Приведенные примеры судебной практики показывают то, что трудностей с привлечением к уголовной ответственности по ст. 272 УК РФ в Российской Федерации не имеется при условии, если неправомерный доступ к компьютерной информации приводит к уничтожению, блокированию, модификации либо копированию компьютерной информации.

Вместе с тем возникает вопрос, какую уголовно-правовую оценку дать действиям лица, если неправомерный доступ к компьютерной информации им был осуществлен, однако последствий, указанных в законе, не наступило?

Например, судебной практике известен такой случай. Гражданин В., используя компьютер, подобрав пароль доступа к почтовому ящику организации, получил возможность ознакомиться с находящимися в нем входящими и исходящими сообщениями. После этого с целью дальнейшего ознакомления с перепиской, осуществляемой по данному почтовому ящику, гражданин В. создал фильтр для пересылки копий входящих и исходящих электронных писем с данного почтового ящика на другой почтовый ящик. Кроме того, получив возможность администрирования указанного электронного почтового ящика, он впоследствии удалил с него несколько писем, а также поменял ранее привязанный к нему законным владельцем абонентский номер к другому абонентскому номеру.

Как видно, в результате действий гражданина В. наступил целый комплекс последствий, указанный в ч. 1 ст. 272 УК РФ. Здесь имеется и копирование компьютерной информации, и ее уничтожение, и модификация.

За содеянное гражданин В. был осужден [8]. Однако возникает вопрос — как квалифицировать его действия, если бы он остановился на стадии незаконного доступа к почтовому ящику и только лишь ознакомился с его содержимым, например входящими или исходящими сообщениями?

Анализируя объективную сторону состава преступления, а именно действие, выраженное в «неправомерном доступе к охраняемой законом компьютерной информации», можно представить, что доступ следует рассматривать и как процедуру (сами действия), и как состояние (последствие действий, связанных с неправомерным доступом).

Совершенно очевидно, что в случае совершения «процедурных» действий, направленных на неправомерный доступ к информации, могут быть последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации.

Но если же в процессе этих действий не последовали указанные последствия, можно ли говорить о составе преступления?

Так, в приведенном выше случае субъект преступления подобрал пароль к почтовому ящику. Представляется, что нет смысла утверждать, что здесь имели место такие последствия, как уничтожение и блокирование компьютерной информации. Про модификацию тоже вряд ли приходится говорить, поскольку к почтовому ящику с помощью какого-либо программного обеспечения был подобран «родной» пароль, и вход в него осуществлен именно с его использованием.

Вопрос же о последствиях копирования в данном случае более сложен и неоднозначен.

Процесс копирования компьютерной информации можно представить как копирование файла с одной стороны и копирование информации — с другой.

Копирование файла — это создание его копии, содержащей информацию. Копирование имеет место, например, при переносе файлов на оптический, жесткий диски или на любой другой носитель.

Отсюда следует, что под копированием с данной точки зрения можно понимать лишь действия по созданию копии файла на каком-либо носителе. Таким образом, «ознакомление» с информацией с экрана, допустим, монитора нельзя рассматривать как копирование файла.

Копирование информации представляет собой создание копии какой-либо информации. Любая копия информации предполагает стопроцентную идентичность оригиналу. Следовательно, считывание информации с экрана монитора также не может признаваться копированием информации, поскольку в большинстве случаев мозг человека не сможет запомнить и потом воспроизвести все то, что было на экране монитора.

Так, например, если на экране монитора открыта программа с какой-либо базой данных, в которой большое количество ячеек, имеющих собственное название, а в этих ячейках зафиксировано множество наименований продукции и ее стоимость, то запомнить даже одну страничку этой базы для среднестатистического человека будет невозможным.

Таким образом, исходя из понятия компьютерной информации, данном в примечании к ст. 272 УК РФ, согласно которому под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, можно сделать вывод, что копирование компьютерной информации следует понимать в узком смысле этого слова, т. е. копирование файла, содержащего информацию.

Отсюда следует, что в настоящее время по российскому уголовному законодательству является проблематичной квалификация неправомерных действий, связанных с доступом к компьютерной информации с целью ее ознакомления.

Представляется, что нельзя признать данные действия также и покушением по следующим причинам.

Как было указано выше, состав преступления, предусмотренный ст. 272 УК РФ, является материальным, и для его окончания требуется наступление последствий.

В случае отсутствия таковых согласно уголовному закону преступление может квалифицироваться как неоконченное, т. е. в данном конкретном случае как покушение. Например, лицо осуществило неправомерный доступ к компьютерной информации, считало ее с экрана монитора, а последствия, указанные в законе, не наступили (учитывая, что ознакомление с информацией не является копированием). Поскольку последствий не наступило, следовательно, деяние виновного необходимо считать неоконченным.

С подобной квалификацией трудно согласиться, т. к. неправомерный доступ, если рассматривать его и как процесс (сами действия), и как состояние (последствие действий, направленных на незаконное проникновение в компьютерную систему), представляет собой непосредственные действия по незаконному доступу к информации, вне зависимости о того, наступили предусмотренные законом последствия или нет.

Так, если они в процессе доступа имели место, то состав окончен. Если же нет, но с информацией лицо ознакомилось, нельзя сказать, что оно не осуществляло тех действий, которые именуются «неправомерным доступом» до того момента, как стало возможным считать информацию с экрана монитора. Таким образом, такие действия следует признавать оконченными.

Думается, что анализируемые действия в настоящее время скорее следует квалифицировать согласно действующему УК РФ не по нормам гл. 28 «Преступления в сфере компьютерной информации», а по нормам гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» или гл. 22 «Преступления в сфере экономической деятельности», предусматривающим ответственность за нарушение неприкосновенности частной жизни, тайны переписки, почтовых и иных сообщений (ст. 137–138), незаконное получение сведений, составляющих коммерческую, налоговую, банковскую тайны (ст. 183).

Список литературы:

1. Давыдов В. О., Малахвей Е. Д. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 2. С. 94–100.

2. Дроздова Е. К., Суранов М. С. Криминалистическая характеристика неправомерного доступа к компьютерной информации // Организационное, процессуальное и криминалистическое обеспечение уголовного производства: материалы VI Международной научной конференции студентов и магистрантов. 2017. С. 33–34.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_-10699/ (дата обращения: 18.11.2021).

4. Официальный сайт МВД Российской Федерации. URL: https://мвд.рф (дата обращения: 18.11.2021).

5. Евдокимов К. Н. Актуальные вопросы квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: сборник материалов межвузовской научно-практической конференции. Гл. ред. П. А. Капустюк. Отв. ред. Р. А. Забавко. 2017. С. 119–125.

6. Приговор Октябрьского районного суда г. Саранска Республики Мордовия от 09.09.2019г. (по делу № 1-226/2019) // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru (дата обращения: 18.11.2021).

7. Приговор Бугурусланского районного суда Оренбургской области от 18.07.2019 (по делу № (1)-149/2019) // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru (дата обращения: 18.11.2021).

8. Приговор Зубово-Полянского районного суда Республики Мордовия от 11.09.2019 (по делу № 1-123/2019) // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru (дата обращения: 18.11.2021).

9. Приговор Кировского районного суда г. Перми Пермского края от 10.10.2019 (по делу № 1-355/2019) // ГАС РФ «Правосудие». URL: https://bsr.sudrf.ru (дата обращения: 18.11.2021).

References:

1. Davydov V. O., Malakhvey E. D. On some aspects of the forensic characteristics of crimes associated with illegal access to computer information // Bulletin of the Tula State University. Economic and legal sciences. 2019. No. 2. Pp. 94–100.

2. Drozdova E. K., Suranov M. S. Forensic characteristics of illegal access to computer information // Organizational, procedural and forensic support of criminal proceedings: materials of the VI International scientific conference of students and undergraduates. 2017. Pp. 33–34.

3. The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ // Consultant Plus. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (access date: November 18, 2021).

4. Official website of the Ministry of Internal Affairs of the Russian Federation. URL: https: //mv.d.rf (access date: November 18, 2021).

5. Evdokimov K. N. Topical issues of qualification of illegal access to computer information at the stage of initiation of a criminal case // Criminal law of the Russian Federation: problems of law enforcement and prospects for improvement: collection of materials of the interuniversity scientific-practical conference. Ch. ed. P. A. Kapustyuk. Resp. ed. R. A. It's funny. 2017. Pp. 119–125.

6. The verdict of the Oktyabrsky District Court of the city of Saransk of the Republic of Mordovia dated 09.09.2019. (in case No. 1-226 / 2019) // GAS RF "Justice". URL: https://bsr.sudrf.ru (access date: November 18, 2021).

7. The verdict of the Buguruslansky District Court of the Orenburg Region dated 18.07.2019. (in case No. (1) -149/2019) // GAS RF "Justice". URL: https://bsr.sudrf.ru (access date: November 18, 2021).

8. The verdict of the Zubovo-Polyansky District Court of the Republic of Mordovia dated 11.09.2019. (in case No. 1-123 / 2019) // GAS RF "Justice". URL: https://bsr.sudrf.ru (access date: November 18, 2021).

9. 8. The verdict of the Kirovsky District Court of the city of Perm, Perm Territory dated 10.10.2019. (in case No. 1-355 / 2019) // GAS RF "Justice". URL: https://bsr.sudrf.ru (access date: November 18, 2021).