ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2018.12(4).590-600

ПРОБЛЕМНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 273 УК РФ, НА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА

К. Н. Евдокимов[1], Н. Н. Таскаев[2]
[1] Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Иркутск, Российская Федерация
[2] Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
20 апреля 2017 г.

Дата принятия в печать
15 августа 2018 г.

Дата онлайн-размещения
14 сентября 2018 г.

Ключевые слова
Следователь; стадия возбуждения уголовного дела; преступления в сфере компьютерной информации; вредоносные компьютерные программы

Аннотация. В настоящее время серьезную угрозу для общественных отношений во всех наиболее значимых сферах жизни российского общества (наука, образование, экономика, финансовая сфера, оборона, общественная безопасность и т. д.) представляет компьютерная преступность, которая постоянно эволюционирует и трансформируется, приобретая в Российской Федерации транснациональный, организованный, экономический и политический характер. При этом вред, причиняемый российскому обществу преступлениями в сфере компьютерной информации, носит колоссальный экономический характер, исчисляемый сотнями миллиардов рублей, и, к сожалению, с каждым годом только возрастает. Одним из самых сложных является расследование преступлений в сфере компьютерной информации, связанных с созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ). При этом использование вредоносных компьютерных программ часто выступает как способ совершения других преступных деяний и достижения иных преступных целей, непосредственно не связанных с причинением вреда охраняемой законом компьютерной информации. В связи с отсутствием разъяснений Верховным Судом Российской Федерации судебной практики по уголовным делам о преступлениях в сфере компьютерной информации следователями на стадии возбуждения уголовного дела, а также на других стадиях предварительного следствия допускаются многочисленные ошибки в юридической оценке совершенных преступных деяний. Между тем юридическая квалификация преступлений в сфере компьютерной информации на стадии возбуждения уголовного дела имеет фундаментальное значение для разрешения наиболее значимых правовых и процессуальных вопросов при расследовании данной категории преступлений, а также для дальнейшего судебного рассмотрения и вынесения справедливого обвинительного приговора по уголовному делу. В статье проводится анализ российской судебно-следственной практики по уголовным делам о создании, использовании и распространении вредоносных компьютерных программ, а также по смежным составам преступления. Авторы дают рекомендации по наиболее полной правовой квалификации преступлений, предусмотренных ст. 273 УК РФ, вносят предложения по совершенствованию следственной практики на стадии возбуждения уголовного дела.

PROBLEMS OF QUALIFYING CRIMES UNDER ARTICLE 273 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION AT THE STAGE OF INITIATING CRIMINAL PROCEEDINGS

Konstantin N. Evdokimov[1], Nikolai N. Taskaev[2]
[1] Irkutsk Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Irkutsk, the Russian Federation
[2] Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2017 April 20

Accepted
2018 August 15

Available online
2018 September 14

Abstract. At present public relations in all most vital spheres of the life of Russian society (science, education, economy, finance, defense, public safety, etc.) are seriously threatened by cybercrimes, which are constantly evolving and changing acquiring a transnational, organized, economic and political identity in the Russian Federation. The economic damage inflicted on the Russian society by cybercrimes is tremendous and could be counted in hundreds of billions of rubles and, sadly, is it growing from year to year. Especially difficult is the investigation of cybercrimes connected with the creation,

Keywords
Investigator; the initiation stage of a criminal case; cybercrimes; harmful software

use and dissemination of harmful software (Art. 273 of the CC of the RF). The use of harmful software is often a method of committing other crimes and reaching other criminal goals not immediately connected with damaging computer information protected by law. There are no clarifications of the Supreme Court of the Russian Federation regarding the court practice on criminal cases of cybercrimes, and the investigators make numerous mistakes in the legal assessment of criminal actions at the stage of initiating criminal proceedings as well as at other stages of preliminary investigation. Meanwhile, the legal qualification of cybercrimes at the stage of initiating criminal proceedings has a fundamental importance for resolving most vital legal and procedural problems in the investigation of such crimes as well as for the court hearing and passing a fair guilty verdict on a case. The authors analyze Russian court and investigation practice on criminal cases involving the creation, use and dissemination of harmful software as well as related offences. They offer recommendations on the most complete legal definition of crimes under Art. 273 of the CC of the RF and present their suggestions on improving court practice at the stage of initiating criminal proceedings.

Квалификация преступления на стадии возбуждения уголовного дела определяет виды и объем юридических прав и обязанностей участников уголовного процесса по данному делу: следователя, прокурора, судьи, потерпевшего, свидетеля, эксперта, специалиста, подозреваемого, обвиняемого, подсудимого и др. (например, право подсудимого на рассмотрение его уголовного дела судом в особом порядке).

От правильной квалификации преступного деяния зависит выбор формы расследования; подследственность уголовного дела; определение меры пресечения в отношении подозреваемого (обвиняемого); подсудность уголовного дела; вид и мера уголовного наказания, которая может быть применена к виновному; возможность применения к обвиняемому, подсудимому, осужденному акта амнистии или помилования; возможность условного осуждения и условно-досрочного освобождения осужденного, применения к нему более мягкого наказания или отсрочки исполнения наказания, установленного обвинительным приговором суда [1–3].

Одним из преступлений, при квалификации которого на стадии возбуждения уголовного дела у органов предварительного следствия могут возникнуть ошибки [1–5] или сложности в юридической оценке совершенного деяния, является деяние, предусмотренное ст. 273 УК РФ, — создание, использование и распространение вредоносных компьютерных программ.

Так, по данным МВД России, в период с 2010 по 2017 г. было приостановлено расследование в связи с неустановлением (либо нерозыском) лица, совершившего преступление, по следующему количеству уголовных дел: в 2010 г. приостановлено 58 уголовных дел, в 2011 г. — 75, в 2012 г. — 108, в 2013 г. — 106, в 2014 г. — 119, в 2015 г. — 193, в 2016 г. — 329, в 2017 г. — 410[1]. При этом из зарегистрированных по ст. 273 УК РФ в 2010 г. 1 010 уголовных дел в суд направлено 914, в 2011 г. из возбужденных 693 уголовных дел в суд направлено 558, в 2012 г. соответственно 889 уголовных дел и направлено в суд 664, в 2013 г. из зарегистрированных 764 уголовных дел в суд направлено с обвинительным заключением 575 уголовных дел, в 2014 г. из зарегистрированных 585 уголовных дел в суд направлено 344, в 2015 г. из 974 уголовных дел в суд направлено 369, в 2016 г. из 751 уголовного дела в суд направлено 299, в 2017 г. из 802 возбужденных уголовных дел в суд с обвинительным заключением направлено только 281[2].

Таким образом, уголовно-правовая статистика показывает, что в настоящее время сложилась тревожная тенденция, указывающая на то, что количество раскрытых и направленных в суд уголовных дел о совершении преступлений, предусмотренных ст. 273 УК РФ, ежегодно сокращается. В 2017 г. этот показатель составил всего около 35 % от числа зарегистрированных уголовных дел, остальные преступления остались нераскрытыми, в то время как в 2010 г. количество раскрытых преступлений и направленных в суд уголовных дел превысило 90 % от числа зарегистрированных органами внутренних дел. Сложившаяся негативная тенденция говорит о серьезных проблемах в расследовании преступлений рассматриваемого вида, в том числе, по мнению авторов [6–10], об ошибках следователей при квалификации преступного деяния на стадии возбуждения уголовного дела.

Мы солидарны с теми учеными [11–20], которые полагают, что деяние, предусмотренное

[1] Преступления в сфере компьютерной информации // Единый отчет о преступности: сводный отчет по России. Ф. 491, кн. 1. URL: http://mvd.ru.

[2] Там же.

ст. 273 УК РФ, относится к одному из наиболее общественно опасных и сложных в расследовании преступлений в сфере компьютерной информации. Это обусловлено высокой степенью его латентности (многие компьютерные вирусы самоуничтожаются) и технической сложностью выявления правоохранительными органами. Вместе с тем указанный вид преступления носит массовый и широкомасштабный характер, поскольку антивирусными программами ежегодно в мире детектируются миллиарды атак компьютерных вирусов через сеть Интернет и создание миллионов новых вредоносных компьютерных программ, причиняющих огромный вред российскому обществу и государству. Так, только в 2015 г. ущерб российской экономике от действий киберпреступников составил около 203 млрд р., или 0,25 % ВВП страны. При этом президент России Владимир Путин сообщил о 24 млн кибератак на сайты и информационные системы органов власти России[3].

По данным международной исследовательской компании Allianz Global Corporate & Specialty, в 2016 г. общий ущерб от интернет-преступности для мировой экономики (включая прямые потери, недополученную прибыль и расходы на восстановление систем) превысил 575 млрд дол. Это около 1 % мирового ВВП. В 2017 г. ущерб мировой экономики от участившихся кибератак, по расчетам Сбербанка, перевалил за 1 трлн дол., а через три года — вырастет до 2 трлн дол. (для сравнения: мировой оборот наркоторговли в настоящее время оценивается примерно в 500 млрд дол. в год) [21].

Возвращаясь к квалификации создания, использования и распространения вредоносных компьютерных программ следователем на стадии возбуждения уголовного дела, необходимо отметить, что состав данного преступления является формальным и для привлечения виновного к ответственности не требуется наступления общественно опасных последствий.

Уголовная ответственность наступает за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Как самостоятельное преступление указанное деяние в судебно-следственной практике встречается достаточно редко и в большинстве эпизодов совершается в совокупности с другими преступлениями как способ достижения различных преступных целей.

Одним из преступлений, которое квалифицируется следователями по ст. 273 УК РФ, является DDoS-атака (от англ. Distributed Denial of Service — распределенная атака типа «отказ в обслуживании»). DDoS-атака представляет собой информационное воздействие на официальные сайты, веб-страницы, интернет-ресурсы органов государственной власти, банков, коммерческих организаций, электронных СМИ и т. д. с целью их блокирования либо затруднения доступа пользователей к компьютерной информации. Данное деяние совершается с использованием вредоносной программы, которая создает поток непрерывных электронных запросов с большого количества компьютеров на хорошо защищенный сервер, который не успевает их обработать, что и приводит к его дальнейшему блокированию.

Так, 13 ноября 2015 г. старшим следователем СЧ по РОПД СУ УМВД России по Курганской области А. было возбуждено уголовное дело в отношении гр-на Б. за совершение преступления, предусмотренного ч. 1 ст. 273 УК РФ. В ходе расследования было установлено, что 25 января 2013 г. гр-н Б., находясь дома по адресу: Курганская область, Шадринский район, село Красномыльское, дом № **, со своего персонального компьютера, используя вредоносное программное обеспечение G-bot 1.9.5 d, осуществил DDoS-атаку на сайт http://www.shadrinsk-med.ru, заблокировав работу и доступ пользователей на сайт ГБПОУ «Шадринский медицинский колледж». Никаких требований администрации медицинского колледжа гр-н Б. не выдвигал, так как решил только проверить работу вредоносного программного обеспечения G-bot 1.9.5 d, приобретенного у неустановленного лица в сети Интернет.

Постановлением старшего следователя СЧ по РОПД СУ УМВД России по Курганской области А. от 10 марта 2016 г. уголовное дело № 26-1030-15 по обвинению Б. в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, в соответствии с ч. 1 ст. 75 УК РФ, ст. 212 и 213 УПК РФ прекращено в связи с деятельным раскаянием[4].

[3] Ущерб от киберпреступности в 2015 году превысил 200 млрд рублей. URL: http://www.vedomosti.ru/technology/articles/2016/04/13/637546-uscherb-ot-kiberprestupnosti.

[4] Уголовное дело № 26-1030-15. Архив Следственной части по РОПД СУ УМВД России по Курганской области за 2016 г.

В другом случае следователь СО по Кировскому району города Иркутска Е. возбудил уголовное дело № 347224 в отношении несовершеннолетнего П. за совершение преступления, предусмотренного ч. 1 ст. 273 УК РФ. Следователем было установлено, что 7 декабря 2014 г. около 15 часов несовершеннолетний П., заранее приобретя в сети Интернет вредоносную компьютерную программу для блокирования компьютерной информации, находясь у себя дома по адресу: Хабаровский край, Верхнебуреинский район, поселок Новый Ургал, дом №**, кв. № **, со своего домашнего компьютера, подключенного к сети Интернет, осуществил DDoS-атаку на сайт www.gt-time.ru, заблокировав в период с 15 до 16 часов веб-страницу и электронную почту интернет-магазина «Золотое время», занимающегося продажей часов и ювелирных изделий, расположенного по адресу: город Иркутск, улица Б. Хмельницкого, дом 1.

После чего несовершеннолетний П. через свой ложный аккаунт «Артем Бурнашев» в социальной сети «ВКонтакте» вышел на страницу «ВКонтакте» консультанта магазина «Золотое время» в городе Иркутске гр-на М. и потребовал перечислить ему на электронный кошелек в платежной системе «ВебМани» №**** денежные средства в сумме 2 тыс. р., а также купить у него за 13 тыс. р. компьютерную программу-скрипт для защиты от DDoS-атак.

Руководство магазина согласилось на требования П., пообещав перечислить ему деньги в январе 2015 г., после чего несовершеннолетний П. прекратил DDoS-атаку. Впоследствии П. был задержан сотрудниками полиции. Своими незаконными действиями П. причинил интернет-магазину «Золотое время» в городе Иркутске материальный ущерб в сумме 30 тыс. р.

Постановлением следователя СО ОМВД России по Верхнебуреинскому району Хабаровского края Г. от 14 октября 2015 г. уголовное дело № 347224 по обвинению несовершеннолетнего П. в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, на основании п. 3 ч. 1 ст. 27 УПК РФ, подп. 7 п. 1 и подп. 1 п. 6 постановления Государственной Думы Федерального Собрания Российской Федерации «Об объявлении амнистии в связи с 70-летием Победы в Великой Отечественной войне 1941–1945 годов» от 24 апреля 2015 г. № 6567-6 ГД прекращено вследствие акта амнистии[5].

[5] Уголовное дело № 347224. Архив Следственного отдела ОМВД России по Верхнебуреинскому району Хабаровского края за 2015 г.

Как видно из приведенных примеров следственной практики, действия виновных в обоих случаях были квалифицированы следователями по ч. 1 ст. 273 УК РФ.

Между тем в уголовном деле по обвинению П. следователем был установлен корыстный мотив незаконных действий несовершеннолетнего П., что не нашло своего отражения в квалификации деяния ни в постановлении о возбуждении уголовного дела, ни в постановлении о прекращении уголовного дела. По нашему мнению, в данном эпизоде преступные действия П. должны были быть квалифицированы следователем по ч. 2 ст. 273 УК РФ как использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности.

Кроме того, совершение несовершеннолетним П. DDoS-атаки на сайт www.gt-time.ru, повлекшей блокирование веб-страницы и электронной почты интернет-магазина «Золотое время», сопровождалось требованием о передаче ему денежных средств под угрозой продолжения блокирования сайта магазина «Золотое время». Таким образом, использование П. вредоносной программы для проведения DDoS-атаки следует рассматривать в совокупности с вымогательством денежных средств у владельцев указанного интернет-магазина.

С учетом вышесказанного полагаем правильным квалифицировать преступные действия П. дополнительно по ч. 1 ст. 163 УК РФ как вымогательство, т. е. требование передачи чужого имущества под угрозой уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего.

Анализируя типичные ошибки следователей при квалификации преступлений в сфере компьютерной информации на стадии возбуждения уголовного дела, следует отметить, что деяния, предусмотренные ст. 273 УК РФ, в подавляющем большинстве случаев совершаются в совокупности с другими преступлениями. Например, наиболее часто встречаемым в российской судебно-следственной практике преступным деянием, совершенным с использованием вредоносных компьютерных программ, являет-

ся установка на компьютерные устройства контрафактного (нелицензионного) программного обеспечения, что нарушает авторские и смежные права законных правообладателей.

Так, следователем СО по Кузьминскому району города Москвы Б. было возбуждено уголовное дело в отношении гр-на И. за совершение преступлений, предусмотренных ч. 2 ст. 146, ч. 2 ст. 273 УК РФ. В результате расследования было установлено, что гр-н И., имея умысел, направленный на незаконное приобретение, хранение контрафактных экземпляров программ для электронно-вычислительных машин, а также на их использование путем сбыта, разместил в сети Интернет на сайте «Авито.ру» объявление об установке им программ для ЭВМ. Далее И. скопировал из сети Интернет на принадлежащий ему ноутбук марки HP контрафактный экземпляр программы для ЭВМ Project Expert 7 Professional, авторские права на которую принадлежат ООО «3 А Финанс», т. е. приобрел контрафактный экземпляр программы для ЭВМ Project Expert 7 Professional в целях сбыта.

В дальнейшем гр-н И., реализуя свой преступный умысел, направленный на незаконное использование путем сбыта объектов авторских прав, принадлежащих ООО «3 А Финанс», вопреки воле правообладателя программы для ЭВМ, действуя из корыстных побуждений, будучи осведомленным о том, что стоимость лицензионного образца устанавливаемой им программы для ЭВМ Project Expert 7 Professional составляет 102 025 р. 00 к., в нарушение ч. 1 ст. 44 Конституции РФ, абзаца 3 ч. 1 ст. 1229, ч. 1 ст. 1270 ГК РФ, находясь в помещении, расположенном по адресу: ****, сбыл путем установки на жесткий диск ноутбука марки ASUS заведомо контрафактный экземпляр программы для ЭВМ Project Expert 7 Professional.

В процессе установки контрафактного экземпляра программы для ЭВМ Project Expert 7 Professional гр-н И. использовал вредоносную программу «2 Взломать (запусти меня).bat» (эмулятор), предназначенную для модификации, копирования компьютерной информации и нейтрализации средств ее защиты, при помощи которой нейтрализовал средства защиты программы для ЭВМ Project Expert 7 Professional, что привело к возможности использования данной программы без лицензионного ключа.

Завершив установку и настройку вышеуказанного нелицензионного экземпляра программы для ЭВМ и убедившись в его работоспособности, И. получил от заказчика денежные средства в сумме 3 тыс. р., после чего был задержан сотрудниками ОЭБ и ПК УВД по ЮВАО ГУ МВД России по городу Москве при проведении оперативно-розыскного мероприятия «проверочная закупка».

Приговором Кузьминского районного суда города Москвы от 18 декабря 2013 г. квалификация преступлений по ч. 2 ст. 146, ч. 2 ст. 273 УК РФ признана правильной и гр-н И. был осужден к наказанию в виде лишения свободы сроком на один год условно с испытательным сроком в течение одного года со штрафом в размере 25 тыс. р.[6]

Между тем, по мнению авторов, квалификация следователем преступных деяний гр-на И. по ч. 2 ст. 146 УК РФ — как совершение нарушения авторских прав, т. е. незаконное использование объектов авторского права, а равно приобретение, хранение контрафактных экземпляров произведений в целях сбыта, совершенные в крупном размере; по ч. 2 ст. 273 УК РФ — как совершение использования компьютерных программ, заведомо предназначенных для модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности является недостаточной и требует дополнительной квалификации по ч. 2 ст. 272 УК РФ — неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло модификацию и копирование компьютерной информации, совершенное из корыстной заинтересованности.

Свою позицию обосновываем следующими аргументами. Контрафактная компьютерная программа представляет собой не что иное, как лицензионную программу (либо ее копию), у которой система защиты компьютерной информации удалена или нейтрализована вредоносной программой, используемой преступником. Поскольку преступнику нужно осуществить инсталляцию (установку) контрафактных программных продуктов со своего носителя информации на компьютерное устройство заказчика, то с этой целью он проводит манипуляции с компьютерной информацией (копирует программное обеспечение на компьютер заказчика, вводит ложные коды для системы защиты программы для запуска на компьютере заказчика, проводит модификацию информации, указывая неограниченный срок действия программного продукта,

[6] Уголовное дело № 1-968/13. Архив Кузьминского районного суда города Москвы за 2013 г.

и др.) лицензионной программы с нейтрализованной защитой. Тем самым без согласия законного правообладателя преступник осуществляет неправомерный доступ к компьютерной информации лицензионной программы с блокированной системой защиты для модификации и копирования компьютерной информации из корыстной заинтересованности.

Таким образом, использование вредоносных компьютерных программ необходимо преступнику для нейтрализации средств защиты лицензионной программы и возможности беспрепятственной работы с ней, а при дальнейшей установке взломанной лицензионной программы на любое компьютерное устройство уже происходит неправомерный доступ к компьютерной информации, влекущий ее модификацию (введение новых паролей, кодов доступа, ключей идентификатора и т. д.) и копирование (перенос функционала программы, программных файлов, контента и т. д.) без согласия законного владельца или правообладателя.

В поддержку своей позиции приведем следующий пример из судебно-следственной практики. Следователем СО ОВД Октябрьского района города Кирова А. было возбуждено уголовное дело в отношении гр-на П. за совершение преступлений, предусмотренных ч. 2 ст. 146, ч. 2 ст. 272, ч. 2 ст. 273 УК РФ. В результате расследования было установлено, что гр-н П., обладая навыками работы на персональном компьютере по установке и настройке программного обеспечения, руководствуясь корыстным мотивом, имея умысел на использование контрафактных экземпляров компьютерных произведений, разместил в сети Интернет на сайте irr.ru объявление рекламного характера с предложением осуществить на платной основе установку нелицензионных программ на компьютеры.

28 марта 2014 г. в период с 6 до 10 часов гр-н П., действуя с целью сбыта контрафактных экземпляров компьютерных программных продуктов, из корыстных побуждений, в целях личного обогащения, инсталлировал на предоставленный гр-кой Р. в ходе оперативно-розыскного мероприятия «проверочная закупка» персональный компьютер дистрибутивы контрафактных программных продуктов: «Microsoft Windows 7 Домашняя расширенная Rus», «Microsoft Office Профессиональный 2007 Rus», Autodesk AutoCAD 2014 Rus, Autodesk 3ds Max 2010 Rus, CorelDRAW Graphics Suite X6 Rus, законными правообладателями которых на территории РФ являются корпорации Microsoft, Autodesk Inc. и Corel. Тем самым незаконно с целью сбыта осуществил перевозку и сбыт указанных контрафактных экземпляров компьютерных произведений и, осознавая, что их использование путем инсталляции повлечет причинение ущерба их правообладателям в размере стоимости лицензионного программного обеспечения, вопреки воле последних в нарушение ч. 1 ст. 44 Конституции РФ и ч. 4 ГК РФ незаконно использовал вышеуказанные объекты авторского права.

Кроме того, имея умысел на неправомерный доступ к охраняемой законом компьютерной информации, во время инсталляции на предоставленный ему заказчиком Р. персональный компьютер вышеуказанных программных продуктов с целью нейтрализации средств защиты информации данных программ и для дальнейшего незаконного их использования гр-н П. поочередно осуществил запуск процесса активации данных программных продуктов с появлением соответствующего окна запроса кода активации.

В момент процесса активации программных продуктов гр-н П. в продолжение своего преступного умысла осуществил запуск вредоносных компьютерных программ, с помощью которых перехватил механизм генерации активационного кода программ, модифицировав память персональной ЭВМ (функция MemPatch), содержащую исполняемые коды программного продукта, что привело к блокированию исходных функций проверки корректности кодов активации данных программных продуктов и незаконной выдаче кода активации программного продукта, являющегося средством защиты от несанкционированного доступа. Действуя далее, П. ввел незаконно полученные им коды активации в соответствующее окно запроса программ, т. е. умышленно осуществил нейтрализацию средств защиты данной компьютерной информации программных продуктов от несанкционированного доступа, что позволило запускать установленный им контрафактный программный продукт без установленного правообладателем кода активации.

По завершении установки контрафактного программного обеспечения, П. получил вознаграждение от Р. в размере 1 500 р. и был задержан сотрудниками полиции.

Приговором Октябрьского районного суда города Кирова от 23 июля 2014 г. квалификация преступлений, совершенных П., признана правильной, а сам гр-н П. был осужден к наказанию

в виде одного года шести месяцев ограничения свободы[7].

Другим типичным преступлением, совершенным с использованием вредоносных компьютерных программ, при квалификации которого на стадии возбуждения уголовного дела следователями допускаются ошибки, является хищение денежных средств из банкоматов. Так, следователем ОВД Верх-Исетского района города Екатеринбурга Свердловской области К. было возбуждено уголовное дело в отношении граждан Республики Молдова Р., В., К. за совершение преступлений, предусмотренных ч. 2 ст. 273, ч. 3 ст. 272, ч. 3 ст. 183, ч. 1 ст. 274, пп. «а», «б» ч. 4 ст. 158, п. «а» ч. 4 ст. 158, ч. 1 ст. 30, пп. «а», «б» ч. 4 ст. 158 УК РФ.

В результате расследования было установлено, что Р., В., К. и иные неустановленные лица вступили в преступный сговор из корыстных побуждений, создав организованную преступную группу. В течение июня — июля 2014 г. в составе организованной группы приняли активное участие в совершении регулярных тяжких преступлений против собственности в виде тайного хищения наличных денежных средств в крупных и особо крупных размерах из банкоматов марки NCR, принадлежащих коммерческим банкам, расположенным в городах Санкт-Петербурге, Домодедове (Московская область), Бор (Нижегородская область), Нижнем Новгороде, Перми, Екатеринбурге, путем предварительного незаконного сбора сведений о коммерческой тайне банков, посредством неправомерного и скрытного доступа к компьютерной информации с использованием вредоносной компьютерной программы Backdoor.Win32.Tyupkin.d, влекущей нарушение правил эксплуатации банкоматов, похитили денежные средства на общую сумму 17 319 000 р. и завершили приготовление к тайному хищению денежных средств из двух банкоматов на сумму 7 929 300 р.

Приговором Верх-Исетского районного суда города Екатеринбурга Свердловской области от 11 декабря 2015 г. квалификация преступлений, совершенных гражданами Республики Молдова Р., В. и К., признана правильной и за совершение 11 преступлений, предусмотренных ч. 2 ст. 273 УК РФ, 9 преступлений, предусмотренных ч. 3 ст. 272 УК РФ, 9 преступлений, предусмотренных ч. 3 ст. 183 УК РФ, 6 преступлений, предусмотренных ч. 1 ст. 274 УК РФ, 6 преступлений, предусмотренных пп. «а», «б» ч. 4 ст. 158 УК РФ, 3 преступлений, предусмотренных п. «а» ч. 4 ст. 158 УК РФ, 2 преступлений, предусмотренных ч. 1 ст. 30, пп. «а», «б» ч. 4 ст. 158 УК РФ, указанные лица были осуждены к наказанию в виде лишения свободы сроком на пять лет шесть месяцев с отбыванием наказания в исправительной колонии общего режима[8].

Вместе с тем Федеральным законом от 29 ноября 2012 г. № 207-ФЗ в Уголовный кодекс Российской Федерации была введена ст. 159.6, предусматривающая наказание за мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. В постановлении Пленума Верховного Суда Российской Федерации «О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» от 5 апреля 2012 г. № 6, а именно в пояснительной записке к вышеуказанному проекту Федерального закона говорится, что «предлагается также выделить в самостоятельный состав преступления мошенничество в сфере компьютерной информации (статья 159.6 УК РФ законопроекта), когда хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты имущества (имущественных прав) и осуществляется путем ввода, удаления, модификации или блокирования компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество».

[7] Уголовное дело № 1-235/2014. Архив Октябрьского районного суда города Кирова за 2014 г.

[8] Уголовное дело № 1-584/2015. Архив Верх-Исетского районного суда города Екатеринбурга Свердловской области за 2015 г.

Таким образом, по мнению авторов и с учетом позиции Верховного Суда Российской Федерации, хищение денежных средств из банкоматов с помощью вредоносных программ следует квалифицировать не по ст. 158 УК РФ («Кража»), а по соответствующей части ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»).

В подтверждение авторской позиции приведем приговор Кировградского городского суда Свердловской области от 5 августа 2016 г., которым за совершение преступлений, предусмотренных ч. 2 ст. 273, ч. 2 ст. 272, ч. 1 ст. 274, ч. 2 ст. 159.6 УК РФ были осуждены гр-н Ш. — к наказанию в виде двух лет шести месяцев лишения свободы с отбыванием в колонии-поселении и гр-н Т. — к наказанию в виде двух лет исправительных работ с удержанием ежемесячно в доход государства 15 % заработка с отбыванием в местах, определяемых органом местного самоуправления.

Судом было установлено, что Ш. и Т., вступив в преступный сговор из корыстных побуждений, в течение 2014–2015 гг. приняли активное участие в совершении регулярных преступлений против собственности в виде хищения чужого имущества путем ввода, блокирования, модификации компьютерной информации, совершенных группой лиц по предварительному сговору, со счетов коммерческих банков, расположенных в городах Кызыле, Абакане, Казани, Екатеринбурге, путем предварительного незаконного сбора сведений о коммерческой тайне банков, посредством неправомерного и скрытного доступа к компьютерной информации с использованием вредоносной компьютерной программы, предназначенной для удаленного эмулирования функции купюроприемника банкомата, без фактического внесения денежных средств и перевода денежных средств на банковские карты, влекущей нарушение правил эксплуатации банкоматов, похитили денежные средства на общую сумму 2 658 273 р.

Действия Ш. и Т. были квалифицированы судом по ч. 2 ст. 272 УК РФ — неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло блокирование, модификацию компьютерной информации, совершенное из корыстной заинтересованности; по ч. 1 ст. 274 УК РФ — нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации и оконечного оборудования, повлекшее блокирование, модификацию компьютерной информации, причинившее крупный ущерб; по ч. 2 ст. 159.6 УК РФ (в редакции ФЗ от 29 ноября 2012 г. № 207) — мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества путем ввода, блокирования, модификации компьютерной информации, совершенное группой лиц по предварительному сговору; по ч. 2 ст. 273 УК РФ — использование и распространение вредоносных компьютерных программ, заведомо предназначенных для несанкционированного блокирования, модификации, копирования компьютерной информации, совершенные группой лиц по предварительному сговору из корыстной заинтересованности[9].

Авторская позиция также подтверждается постановлением Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48, которое в п. 20 указывает, что «по смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) — ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. 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 статье 272, 273 или 274.1 УК РФ»[10].

[9] Приговор Кировградского городского суда Свердловской области от 5 августа 2016 года по уголовному делу № 1-105/2016. URL: https://rospravosudie.com/court-kirovgradskij-gorodskoj-sud-sverdlovskaya-oblast-s/act-533504266.

[10] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48 // Российская газета. 2017. 11 дек.

ISSN 2500-4255

Вместе с тем авторы считают юридическую оценку рассматриваемого компьютерного преступления по ч. 2 ст. 273, ч. 2 ст. 272, ч. 1 ст. 274, ч. 2 ст. 159.6 УК РФ недостаточной и требующей дополнительной квалификации по соответствующей части ст. 183 УК РФ («Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»), поскольку, по нашему мнению, компьютерная информация, содержащаяся в банкоматах, должна оцениваться следователем как сведения, составляющие коммерческую и банковскую тайну.

Свою позицию обосновываем тем, что в соответствии с ч. 2 ст. 3 Федерального закона «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ информация, составляющая коммерческую тайну, — это сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу их неизвестности третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Кроме того, в соответствии с ч. 1 ст. 3 Федерального закона «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ коммерческая тайна — режим конфиденциальности информации, позволяющей ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Так, в соответствии с п. 5 Приложения № 1 к «Положению о коммерческой и банковской тайне ОАО «Банк Москвы», утвержденному приказом от 17 февраля 2009 г. № 242, коммерческой тайной являются сведения о ежедневных остатках денежных средств в хранилищах банка, к чему относятся и сведения о лимите денежных средств банкомата и разграничении этих денежных средств в кассетах банкомата по номиналу и количеству купюр на текущий момент[11].

Также в соответствии с п. 5 Перечня сведений конфиденциального характера, утвержденного указом Президента Российской Федерации от 6 марта 1997 г. № 188, коммерческая тайна является конфиденциальной.

В соответствии с ч. 4 ст. 4 Федерального закона «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации.

Таким образом, подобная информация о финансовом состоянии банкомата имеет действительную коммерческую ценность в силу неизвестности ее третьим лицам, вследствие чего на законном основании никто не имеет свободного доступа к сведениям о количестве наличных денежных средств, размещенных в банкомате. Поэтому авторы считают, что компьютерная информация, содержащаяся в банкоматах, должна оцениваться следователем как сведения, составляющие коммерческую и банковскую тайну.

Резюмируя вышесказанное, полагаем, что при уголовно-правовой оценке преступных деяний, совершенных с созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ), окончательная квалификация деяний на стадии возбуждения уголовного дела должна осуществляться следователем:

– при совершении DDoS-атак на сайты организаций, сопряженных с требованием денежных средств у владельцев за снятие блокирования компьютерной информации, — по соответствующим частям ст. 273, 163 УК РФ;

– в случае установки контрафактных экземпляров компьютерных программ на любые стационарные или мобильные компьютерные устройства — по соответствующим частям ст. 146, 272, 273 УК РФ;

– при совершении хищений денежных средств из банкоматов с использованием компьютерных вирусов для получения контроля над программным обеспечением банкоматного устройства, отключением связи между банкоматом и банком, а также неконтролируемой выдачей денежных купюр — по ст. 159.6, 183, 273, 274 УК РФ.

[11] Банк Москвы. URL: http://www.bm.ru.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов — М. : Право и Закон, 1996. — 182 с.

2. Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук : 12.00.08 / Р. Р. Гайфутдинов. — Казань, 2017. — 243 с.

3. Евдокимов К. Н. Сравнительно-правовой анализ законодательства России и зарубежных стран, регламентирующего уголовную ответственность за совершение компьютерных преступлений / К. Н. Евдокимов // Юридический мир. — 2017. — № 3. — С. 45–49.

4. Евдокимов К. Н. Особенности уголовно-правовой квалификации преступлений, предусмотренных статьями 159.6, 272 УКРФ, на стадии возбуждения уголовного дела / К. Н. Евдокимов // Библиотека уголовного права и криминологии. — 2017. — № 2 (20). — С. 161–173.

5. Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : автореф. дис. ... канд. юрид. наук / А. Н. Копырюлин. — Тамбов, 2007. — 242 с.

6. Степанов-Егиянц В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. … д-ра юрид. наук : 12.00.08 / В. Г. Степанов-Егиянц. — М., 2016. — 389 с.

7. Buchan R. Cyber War and International Law / R. Buchan, N. Tsagourias // Journal of Conflict & Security Law. — 2012. — Vol. 17 (2). — P. 183–186.

8. Colin B. The Future of Cyberterrorism / B. Colin // Crime and Justice International. — 1997. — March. — P. 15–18.

9. Barker K. Cyber Criminals on Trial, by Russell G Smith, Peter Grabosky and Gregor Urbas / K. Barker // International Journal of Law and Information Technology. — 2012. — Vol. 20. — P. 242–245.

10. Herzog F. Straftatenim Internet, Computerkriminalität und die Cybercrime Convention / F. Herzog // Política criminal. — 2009. — Vol. 4, № 8. — P. 407–427.

11. Kabay M. Studies and Surveys of Computer Crime / M. Kabay. — Northfield, 2001. — 30 p.

12. Lipinsky D. A. Social danger of offence in the scientific and legislative definitions in Russia and other countries / D. A. Lipinsky, A. A. Musatkina // Journal of Advanced Research in Law and Economics. — 2018. — Vol. 8, № 5. — P. 1549–1555.

13. Lipinsky D. A. The characteristic of social danger of offence in scientific and legislative definitions in the member countries of the commonwealth of independent states and European countries / D. A. Lipinsky, A. A. Musatkina // Mediterranean Journal of Social Sciences. — 2015. — Vol. 6, № 3. — P. 613–616.

14. O'Connell M. Cyber Security without Cyber War / M. O'Connell // Journal of Conflict & Security Law. — 2012. — Vol. 17, iss. 2. — P. 187–209.

15. Broadhurst R. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime / R. Broadhurst, P. Grabosky, M. Alazab, S. Chon // International Journal of Cyber Criminology. — 2014. — Vol. 8, iss. 1. — P. 1–20.

16. Ryder N. E-Crime / N. Ryder, A. S. Reid // Information & Communications Technology Law. — 2012. — Vol. 21. — P. 203–206.

17. Shinder D. L. Scene of the Cybercrime. Computer Forensics Handbook / Debra L. Shinder. — Rockland : Syngress, 2003. — 752 p.

18. Verton D. Black Ice: The Invisible Threat of Cyberterrorism / D. Verton. — New York, 2004. — 304 p.

19. Weisser B. Cyber Crime — The information Society and Related Crimes. Section 2. Special Part. National Report on Germany [Electronic resource] / B. Weisser // Electronic Review of the International Association of Penal Law. Preparatory Colloquium Section 2. Moscow, 24–27 April 2013. Criminal Law. Special Part. — Mode of access: http://www.penal.org/sites/default/files/files/RM-8.pdf.

20. Yar M. The Novelty of «Cybercrime» An Assessment in Light of Routine Activity Theory / M. Yar // European Journal of Criminology. — 2005. — Vol. 2 (4). P. 407–427.

21. Грамматчиков А. Идет кибервойна народная [Электронный ресурс] / А. Грамматчиков, О. Вандышева // Эксперт. — 2017. — 30 янв. — Режим доступа: http://expert.ru/expert/2017/05/idet-kibervojna-narodnaya.

REFERENCES

1. Vekhov V. B. *Komp'yuternye prestupleniya: sposoby sovershenia i raskrytiya* [Computer Crimes: Ways of Committing and Resolving]. Moscow, Pravo i Zakon Publ., 1996. 182 p.

2. Gaifutdinov R. R. *Ponyatie i kvalifikatsiya prestuplenii protiv bezopasnosti komp'yuternoi informatsii. Kand. Diss.* [The concept and definition of crimes against digital information. Cand. Diss.]. Kazan, 2017. 243 p.

3. Evdokimov K. N. Comparative legal analysis of the legislation of Russia and other countries regulating criminal liability for cybercrimes. *Yuridicheskii mir = Juridical World*, 2017, no. 3, pp. 45–49. (In Russian).

4. Evdokimov K. N. Specific features of criminal law qualification of crimes under Art. 159.6, 272 of the CC of the RF at the stage of initiating criminal proceedings. *Biblioteka ugolovnogo prava i kriminologii = Library of Criminal Law and Criminology*, 2017, no. 2 (20), pp. 161–173. (In Russian).

5. Kopyryulin A. N. *Prestupleniya v sfere komp'yuternoi informatsii: ugolovno-pravovoi i kriminologicheskii aspekty. Avtoref. Kand. Diss.* [Crimes in the sphere of digital information: criminal law and criminological aspects. *Cand. Diss. Thesis*]. Tambov, 2007. 242 p.

6. Stepanov-Egiyants V. G. *Metodologicheskoe i zakonodatel'noe obespechenie bezopasnosti komp'yuternoi informatsii v Rossiiskoi Federatsii (ugolovno-pravovoi aspekt). Dokt. Diss.* [Methodological and legislative support of digital security in the Russian Federation (a criminal law aspect). Doct. Diss.]. Moscow, 2016. 389 p.

7. Buchan R., Tsagourias N. Cyber War and International Law. *Journal of Conflict & Security Law*, 2012, vol. 17 (2), pp. 183–186.

8. Colin B. The Future of Cyberterrorism. *Crime and Justice International*, 1997, March, pp. 15–18.

9. Barker K. Cyber Criminals on Trial, by Russell G Smith, Peter Grabosky and Gregor Urbas. *International Journal of Law and Information Technology*, 2012, vol. 20, pp. 242–245.

10. Herzog F. Straftatenim Internet, Computerkriminalität und die Cybercrime Convention. *Política Criminal*, 2009, vol. 4, no. 8, pp. 407–427.

11. Kabay M. *Studies and Surveys of Computer Crime*. Northfield, 2001. 30 p.

12. Lipinsky D. A. Social danger of offence in the scientific and legislative definitions in Russia and other countries. *Journal of Advanced Research in Law and Economics*, 2018, vol. 8, no. 5, pp. 1549–1555.

13. Lipinsky D. A., Musatkina A. A. The characteristic of social danger of offence in scientific and legislative definitions in the member countries of the Commonwealth of Independent States and European countries. *Mediterranean Journal of Social Sciences*, 2015, vol. 6, no. 3, pp. 613–616.

14. O'Connell M. Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 2012, vol. 17, iss. 2, pp. 187–209.

15. Broadhurst R., Grabosky P., Alazab M., Chon S. Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 2014, vol. 8, iss.1, pp. 1–20.

16. Ryder N., Reid A. S. E-Crime. *Information & Communications Technology Law*, 2012, vol. 21, pp. 203–206.

17. Shinder D. L. *Scene of the Cybercrime. Computer Forensics Handbook*. Rockland, Syngress, 2003. 752 p.

18. Verton D. *Black Ice: The Invisible Threat of Cyberterrorism*. New York, 2004. 304 p.

19. Weisser B. Cyber Crime — The information Society and Related Crimes. Section 2. Special Part. National Report on Germany. *Electronic Review of the International Association of Penal Law. Preparatory Colloquium Section 2. Moscow, 24–27 april 2013. Criminal Law. Special Part*. Available at: http://www.penal.org/sites/default/files/files/RM-8.pdf.

20. Yar M. The Novelty of «Cybercrime» An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2005, vol. 2 (4), pp. 407–427.

21. Grammatchikov A., Vandysheva O. There is a patriotic cyberwar on. *Ekspert = Expert, January 30,* 2017. Available at: http://expert.ru/expert/2017/05/idet-kibervojna-narodnaya. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Евдокимов Константин Николаевич — доцент кафедры государственно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: kons-evdokimov@yandex.ru.

Таскаев Николай Николаевич — доцент кафедры государственно-правовых дисциплин Института государства и права Байкальского государственного университета, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: TaskaevNN@bgu.ru.

ДЛЯ ЦИТИРОВАНИЯ

Евдокимов К. Н. Проблемные вопросы квалификации преступлений, предусмотренных статьей 273 УК РФ, на стадии возбуждения уголовного дела / К. Н. Евдокимов, Н. Н. Таскаев // Всероссийский криминологический журнал. — 2018. — Т. 12, № 4. — С. 590–600. — DOI: 10.17150/2500-4255.2018.12(4).590-600.

INFORMATION ABOUT THE AUTHORS

Evdokimov, Konstantin N. — Ass. Professor, Chair of State and Law Disciplines, Irkutsk Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: kons-evdokimov@yandex.ru.

Taskaev, Nikolai N. — Ass. Professor, Chair of State and Law Disciplines, Institute of State and Law, Baikal State University, Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: TaskaevNN@bgu.ru.

FOR CITATION

Evdokimov K. N., Taskaev N. N. Problems of qualifying crimes under Article 273 of the Criminal Code of the Russian Federation at the stage of initiating criminal proceedings. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 4, pp. 590–600. DOI: 10.17150/2500-4255.2018.12(4).590-600.