УДК 343.98:343.72

А. Ю. ШАПОШНИКОВ,
кандидат юридических наук
Самарский государственный университет, г. Самара, Россия

КРИМИНАЛИСТИЧЕСКИЙ И УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВИРУСОВ[1]

Цель: рассмотреть и проанализировать механизм совершения мошеннических действий с использованием компьютерных вирусов; требующих перечисления денежных средств; определить квалификацию преступлений данного вида; разработать рекомендации по организации расследования данного вида мошенничеств.

Методы: диалектический подход к познанию социальных явлений, который определил выбор конкретных методов исследования: компаративного, герменевтического, дискурсивного, формально-юридического, системного.

Результаты: В результате проведенных исследований определен механизм преступного поведения и его основные стадии, рассмотрен вопрос определения размера материального ущерба, в том числе на этапе возбуждения уголовного дела, предложены отдельные рекомендации по организации раскрытия и расследования преступлений данного вида.

Научная новизна: в статье впервые анализируются криминалистические и уголовно-правовые аспекты практики расследования мошенничеств, совершаемых с использованием компьютерных вирусов, требующих перечисления денежных средств, а также спорные вопросы квалификации преступлений данного вида.

Практическая значимость: основные положения и выводы статьи могут быть использованы в научной, педагогической и практической деятельности при рассмотрении вопросов раскрытия, расследования и предупреждения компьютерных преступлений.

Ключевые слова: мошенничество; вредоносные компьютерные программы; компьютерные вирусы; Trojan; компьютерные преступления; преступное намерение; хищение денежных средств; электронные платежные системы; пострадавший от мошеннических действий.

Введение

Постоянное развитие и совершенствование компьютерной техники приводит к ее повсеместному распространению, повышению уровня ее доступности для различных слоев населения, а развитие технологий связи обеспечивает возможность подключения к сети Интернет практически в любом месте. Но, как и у большинства достижений научно-технического прогресса, у компьютерной техники есть оборотная сторона – она активно используется злоумышленниками для совершения преступлений.

Одним из наиболее распространенных видов криминального использования компьютерной техники является создание и распространение вредоносных программ. С момента написания первого вируса в ноябре 1983 г. появилось множество компьютерных вирусов и иных угроз [1, 2].

Результаты исследования

Компьютерные вирусы используются злоумышленниками для различных целей: от простого повреждения операционной системы отдельного компьютера, копирования учетных записей пользователя и паролей до создания сети зомбированных компьютеров для DOS-атак и хищения средств с использованием электронных платежных систем. В данной статье мы рассмотрим криминалистический и правовой анализ небольшой группы вредоносных программ, требующих перевода денежных средств на номер сотового телефона или электронный кошелек. Специалисты отмечают, что идея требования денег с использованием вирусов появилась именно в России [3]. Опубликованная криминальная статистика[2], к сожалению, не содержит достаточной информации для оценки реального масштаба ущерба, причиняемого вирусами данного вида, кроме того, огромное количество пострадавших просто не обращаются в правоохранительные органы, что обеспечивает высокий уровень латентности подоб-

[1] Статья выполнена при финансовой поддержке РГНФ и Правительства Самарской области в рамках научного проекта № 13-13-63001 «Совершенствование правового механизма комплексной охраны собственности от правонарушений, совершаемых путем злоупотребления доверием, использования служебного положения и обмана».

[2] URL: http://crimestat.ru/ (дата обращения: 10.11.2014)

ных правонарушений. Основу рассматриваемой группы вирусов составляют различные вариации «троянцев» (вирусы типа Trojan). В основе данной вредоносной программы лежит принцип «троянского коня». Программа, как правило, скрывается внутри или под видом вложения в электронное письмо, рабочую программу, баннер и другие файлы либо просто загружается с инфицированного сайта. Попав на компьютер, вирус активируется и блокирует нормальную работу операционной системы в целом или отдельных программ, шифрует файлы. Например, вирус **Trojan.Encoder.6** при активации начинал шифровать хранящиеся на жестких дисках файлы документов. Другие виды подобных вирусов активируются при запуске компьютера и не позволяют пользователю загрузить операционную систему. Объединяет все подобные вирусы схожее требование – для разблокирования компьютера или расшифровки файлов пользователю предлагают перевести деньги, как правило, в сумме от 300 до 1 500 рублей на указанный номер электронного кошелька или пополнить счет сотового телефона. В некоторых случаях пользователю предлагают отправить СМС-сообщение на короткий номер, что в итоге приводит к списанию средств со счета абонента. Требование выводится на экран в виде текста, причем, что интересно в России требование написано на русском языке и требуется перевод денежной суммы в рублях, в Украине – в гривнах и т. д. Изучение доступных скриншотов подобных вирусов позволяет отметить ряд интересных особенностей. Прежде всего, привлекает внимание общий подход к содержанию сообщений. Текст требования составлен так, что пользователь прямо обвиняется в совершении преступлений, например в просмотре, хранении и распространении детской порнографии, либо использовании нелицензионного программного обеспечения. Сообщается, что в виду выявленных преступлений компьютер заблокирован. Пользователю предлагают оплатить штраф или приобрести лицензию, далее приводится инструкция, каким образом и какую сумму пострадавший должен перевести на счет мошенников. В некоторых случаях сообщения содержат эмблемы и логотипы Министерства внутренних дел России или Следственного комитета РФ, составлены от имени данных правоохранительных структур. Встречается вирус, который содержит обвинения и требования от имени лаборатории Касперского. В сообщении, как правило, присутствует угроза, например, «в случае если в течение 12 часов штраф не будет уплачен, все данные на вашем персональном компьютере будут безвозвратно удалены, а дело передано в суд для разбирательства по ч. 1 ст. 242 УК РФ», или «по вашему адресу будет направлена следственно-оперативная группа, для вашего задержания и проведения следственных мероприятий» и т. д. В некоторых случаях в сообщении приводится IP-адрес компьютера, с утверждением, что это адрес компьютера пользователя и что именно с этого IP-адреса рассылается детская порнография. Фактически приведенный в сообщении IP- адрес не имеет никакого отношения к реальному IP-адресу пострадавшего пользователя. Практически все вирусы данного вида содержат строку для введения кода разблокировки. Варианты сообщения данного кода зависят от способа оплаты: если выбраны СМС-сообщения, то код якобы будет прислан на номер сотового; если e-mail, то код якобы пришлют в отвесном письме. Чаще встречается следующее: «в случае оплаты суммы, равной штрафу или превышающей ее, на фискальном чеке терминала будет напечатан код разблокировки», однако на фискальном чеке никакой код отпечатан быть не может, и потерпевший его не найдет. Как показывает анализ сообщений и запросов, связанных с подобными вредоносными программами, подавляющее большинство пользователей пытаются справиться с ними самостоятельно, без обращения в правоохранительные органы [4]. Причем значительное количество обращений содержат сведения о том, что потерпевший уже перечислил требуемую злоумышленником сумму, но так и не получил обещанного кода разблокировки.

Причины, по которым потерпевшие не обращаются в правоохранительные органы, по нашему мнению, кроются в содержании сообщения и сумме «выкупа», требуемой мошенниками.

Подавляющее большинство пострадавших «ловит» вирус при обращении к сайтам, содержащим порнографические материалы, или при скачивании бесплатных файлов с инфицированных торрентов. В нашем обществе просмотр порнографических материалов не одобряется, поэтому потерпевший стремится скрыть подобную неблагоприятную информацию о себе и, следовательно, не обращается в правоохранительные органы. Тоже самое

относится к скачиванию «пиратских» файлов, – опасаясь реальной или мнимой ответственности, пользователь предпочтет не обращаться к представителям закона. Кроме того, требуемая преступниками сумма является относительно небольшой. Если запрошенная сумма менее 1 000 рублей (подавляющее большинство вредоносных программ за разблокировку компьютера требует порядка 800 рублей), то в соответствии с законодательством РФ, этот вид мошенничества подпадает под определение «мелкого хищения». Теряя подобную незначительную сумму, граждане не обращаются в правоохранительные органы, предпочитая решать проблему самостоятельно. Кроме того, большая часть населения России скептически относятся к способности правоохранительных органов найти виновных и привлечь их к ответственности. При проведении данного исследования нам не удалось найти ни одного уголовного дела, возбужденного по фактам требования перевода денег за разблокирование компьютера, пораженного вирусом. Пик активности «троянов» данного вида приходился на 2006–2011 гг. В настоящее время основные антивирусные программы распознают их и блокируют.

Фактически, авторами подобных вирусов была реализована эффективная система мошеннических действий. По имеющимся данным[3], подобные вирусы и схемы мошеннических действий используются и в настоящее время. Нельзя исключать возможности появления новых вирусов, использующих схожий принцип мошенничества, поэтому мы проанализируем некоторые криминалистические и правовые аспекты проблемы установления и привлечения к ответственности виновных.

Одной из основных причин, по которой мошенничество с использованием троянов не вызвало пристального внимания правоохранительных органов, по нашему мнению, является сложность квалификации подобных преступлений.

Прежде всего, следует обратить внимание на сложность самого способа совершения преступления: оно состоит из нескольких этапов, каждый из которых может образовывать отдельное преступление, а все вместе – систему криминального промысла. Так, первоначально должен быть создан компьютерный вирус (правовой термин – вредоносная программа), что само по себе образует состав преступления, предусмотренного ст. 273 УК РФ. Поскольку троян блокирует доступ к операционной системе, не позволяя пользователю получить доступ к компьютерной информации, он полностью отвечает правовым критериям вредоносной программы. Кроме того, рассматриваемые нами виды вирусов требуют перевода денег, следовательно, создатели и распространители действуют из «корыстной заинтересованности», т. е. их действия должны быть квалифицированы по ч. 2 ст. 273 УК РФ. На втором этапе вирус активируется и требует у пострадавшего перевести денежные средства для получения кода разблокирования системы. Подобное требование часто сопровождается угрозой уничтожения информации либо привлечения к уголовной ответственности. Возникает вопрос, каким образом можно квалифицировать данные действия (как мошенничество или как вымогательство), особенно при наличии угроз и временного таймера. Полагаем, что основу выдвигаемых злоумышленниками требований составляют обман и введение в заблуждение, поскольку именно на этом построена основная схема преступления. Потерпевший перечисляет денежные средства не из-за угроз, а поскольку не обладает достаточными знаниями для нейтрализации вируса и его последствий и полагает, что ему действительно пришлют код для разблокирования системы. Поскольку угрозы в сообщении не конкретизированы, непосредственный контакт между преступником и потерпевшим отсутствует. По нашему мнению, потерпевший в данной ситуации располагает определенной свободой выбора, которая отсутствует при вымогательстве. Следовательно, его действия обусловлены не угрозами, а именно обманом и введением в заблуждение, и он, по сути, добровольно отправляется к терминалу и перечисляет деньги. Полагаем, что действия преступников в данном случае должны быть квалифицированы по ч. 1 ст. 159.6 УК РФ. Вместе с тем серьезной проблемой остается вопрос размера причиненного ущерба. Для признания рассматриваемых действий преступлением требуется, чтобы стоимость похищенного превышала 1 000 рублей, когда как подавляющее большинство вирусов-мошенников требует перевода меньшей суммы, как правило, 600–900 рублей. Полагаем, что в данном случае необходимо отталкиваться

[3] URL: http://crimestat.ru/ (дата обращения: 10.11.2014)

от направленности умысла. При создании и распространении подобного вируса преступники рассчитывают получить денежные средства от неопределенного круга лиц, личностные характеристики которых для них не имеют значения. Значение имеет только общая сумма, полученная в итоге от всех пострадавших. Полагаем, что все мошеннические действия на самом деле образуют одно продолжаемое преступление, охваченное единым умыслом, но направленным изначально на неопределенный круг потерпевших. Таким образом, по нашему мнению, действия виновных образуют состав мошенничества только после того, как общая сумма полученных денежных средств превысит 1 000 рублей, т. е. фактически после того, как второй потерпевший перечислит требуемую сумму.

Выводы

Раскрытие и расследование подобных преступлений требует определенной криминалистической методики, учитывающей специфику не только компьютерных преступлений, но и мошенничества. Для построения системы доказательств необходимо установить:

1) факт создания компьютерного вируса, личность его автора;

2) факт распространения вируса, способ распространения, способы и схемы сокрытия «трояна», механизм активации, основные действия, совершаемые вирусом;

3) факт выдвижения требований о перечислении денежных средств, содержание текстового сообщения, размер требуемой суммы;

4) наличие в сообщении ложной или вводящей в заблуждение информации;

5) факт передачи (пересылки) денежных средств злоумышленнику;

6) факт получения им денежных средств или распоряжение ими по своему усмотрению, в том числе путем создания схемы, при которой они направляются иному лицу.

Необходимость установления и доказывания указанных фактов требуют использования специальных знаний в области программирования, проведения исследований вирусов и способов их распространения. Кроме того, необходимо получение информации от финансовых учреждений или операторов сотовой связи о личности держателей номеров, карт и счетов, о движении денежных средств, расчетах и т. д. Расследование представляет собой сложный комплекс следственных действий и оперативно-розыскных мероприятий. По нашему мнению, сотрудники правоохранительных органов во многом скептически относятся к проблеме организации противодействия «троянам-мошенникам», поскольку полагают, что причиняемый ими ущерб малозначителен. Однако, мы считаем, что подобные компьютерные вирусы представляют серьезную угрозу для всех пользователей, а общий размер ущерба можно установить на основе примерных расчетов. Так, вирус Trojan.RpcTonzil за несколько часов заразил компьютеры более чем 50 тысяч пользователей социальной сети «ВКонтакте» [5]. Предположим, что гипотетический «троян» столь же эффективно распространился через социальную сеть и требует перечислить злоумышленникам 1 000 рублей за разблокирование операционной системы. Даже если злоумышленникам пришлет деньги только 0,1 % пострадавших, то криминальный доход составит 5 млн рублей.

Полагаем, что данный вид мошенничеств, совершаемых с использованием компьютерных вирусов, требует серьезного исследования с целью формирования единого подхода к квалификации и разработки эффективной частной криминалистической методики расследования и предупреждения преступлений данного вида.

Список источников

1. Москапленко Е. Вирус блокирует Windows, требует отправить SMS для разблокировки системы. «Trojan. Winlock.3300». Методы! URL: http://evgmoskalenko.com/virusy/virus-blokiruet-windows.html (дата обращения: 10.11.2014)

2. Что такое троянская программа? URL: http://www.kaspersky.ru/internet-security-center/threats/trojans (дата обращения: 10.11.2014)

3. В Интернете появилась новая и более опасная модификация троянской программы Trojan.Encoder.6. Портал для вебмастера. URL: http://wb0.ru/forum/index.php?showtopic=426 (дата обращения: 10.11.2014)

4. Онлайн – Dr.Web. Как разблокировать Windows от вируса вымогателя? URL: http://serfock.ru/soft/add-soft/online-unlock-windows (дата обращения: 10.11.2014)

5. Юрина Т. Около 50 тысяч пользователей сетью «ВКонтакте» получили вирус. URL: http://36on.ru/news/people/30787-okolo-50-tysyach-polzovateley-setyu-vkontakte-poluchili-viru (дата обращения: 10.11.2014)

В редакцию материал поступил 15.09.14

Информация об авторе

Шапошников Андрей Юрьевич, к кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики, доцент кафедры безопасности информационных систем, Самарский государственный университет

Адрес: 443011, г. Самара, ул. Ак. Павлова, 1, тел.: (846) 278-09-76

E-mail: shaposhnikofff@mail.ru

Как цитировать статью: Шапошников А.Ю. Криминалистический и уголовно-правовой анализ мошенничеств, совершаемых с использованием компьютерных вирусов // Актуальные проблемы экономики и права. 2014. № 4 (32). С. 302–306.

A. YU. SHAPOSHNIKOV,

PhD (Law)

Samara State University, Samara, Russia

CRIMINALISTIC AND CRIMINAL-LEGAL ANALYSIS OF FRAUD COMMITTED WITH COMPUTER VIRUSES[1]

Objective: to examine and analyze the mechanism of committing fraud using computer viruses, requiring transfer of funds; to determine the qualifications of such crimes; to develop recommendations on the organization of investigation of this type of fraud.

Methods: the dialectic approach to the cognition of social phenomena determined the choice of specific research methods; comparative, hermeneutic, discursive, formal-legal, systemic.

Results: As a result of studies, the mechanism of criminal behavior and its main stages were identified; the issue is viewed of determining the size of the material damage, including at the stage of criminal prosecution; specific recommendations are offered for the organization of the disclosure and investigation of crimes of this type.

Scientific novelty: In the article for the first time the criminalistic and criminal-legal aspects of investigation practice are analyzed for the fraud committed using computer viruses, requiring transfer of funds, as well as controversial issues of qualification of crimes of this type.

Practical value: The main provisions and conclusions of the article can be used in scientific, educational and practical activities when viewing the issues of disclosure, investigation and prevention of computer crimes.

Key words: fraud; malicious computer programs; computer viruses; Trojan; computer crimes; criminal intent; theft of funds; electronic payment systems; victim of the fraud.

References

1. Moskaplenko, E. *Virus blokiruet Windows, trebuet otpravit' SMS dlya razblokirovki sistemy. «Trojan. Winlock. 3300». Metody!* (The virus blocks Windows, and demands to send SMS for unblocking the system. «Trojan. Winlock. 3300». Methods!), available at: http://evgmoskalenko.com/virusy/virus-blokiruet-windows.html (accessed: 10.11.2014)

2. *Chto takoe troyanskaya programma?* (What is Trojan software?), available at: http://www.kaspersky.ru/internet-security-center/threats/trojans (accessed: 10.11.2014)

3. *V Internete poyavilas' novaya i bolee opasnaya modifikatsiya troyanskoi programmy Trojan. Encoder. 6. Portal dlya vebmastera* (In the Internet a new and more dangerous modification of the Trojan program Trojan. Encoder. 6 appeared. Portal for webmaster), available at: http://wb0.ru/forum/index.php?showtopic=426 (accessed: 10.11.2014)

4. *Onlain – Dr. Web. Kak razblokirovat' Windows ot virusa vymogatelya?* (Online – Dr. Web. How to unblock Windows from a virus of a racketeer?), available at: http://serfock.ru/soft/add-soft/online-unlock-windows (accessed: 10.11.2014)

5. Yurina, T. *Okolo 50 tysyach pol'zovatelei set'yu «VKontakte» poluchili virus* (About 50 thousand user of "VKontakte" network got a virus), available at: http://36on.ru/news/people/30787-okolo-50-tysyach-polzovateley-setyu-vkontakte-poluchili-viru (accessed: 10.11.2014)

Received 15.09.14

Information about the author

Shaposhnikov Andrey Yuryevich, PhD (Law), Associate Professor of the Chair of Criminal Procedure and Criminalistics, Associate Professor of the Chair of Information Systems Safety, Samara State University

Address: 1 Academician Pavlov Str., 443011, Samara, tel.: (846) 278-09-76

E-mail: shaposhnikofff@mail.ru

How to cite the article: Shaposhnikov A.Yu. Criminalistic and criminal-legal analysis of fraud committed with computer viruses. *Aktual'niye problemy ekonomiki i prava*, 2014, no. 4 (32), pp. 293–297.

[1] The article is written with the financial support of RSSF and Samara region government within the frameworks of scientific project no.13-13-63001 «Improving the legal mechanism of the complex protection of property against crimes committed with violation of trust, abuse of official position, or fraud».