УДК 34

Судебная практика по уголовным делам, связанным с хищениями, совершаемыми с использованием вредоносного программного обеспечения

Виноградов Евгений Александрович

Соискатель,
факультет подготовки научно-педагогических
и научных кадров по кафедре оперативно-разыскной
деятельности и специальной техники,
Московский университет МВД России им. В.Я. Кикотя,
117437, Российская Федерация, Москва, ул. Академика Волгина, 12;
e-mail: 40mvd@bk.ru

Аннотация

Преступники, совершающие хищения денежных средств, посредством использования вредоносных программ, привлекаются к уголовной ответственности как по ст. 159.6 УК РФ, так и по совокупности преступлений, в том числе тех, которые предусмотрены ст. 272, 273, 210, 183, 174.1 УК РФ. Сложность квалификации заключается в том, что как у оперативных и следственных работников, так и у судебных органов не выработан единый подход к установлению объективных признаков таких деяний. Необходимо закрепление на уровне Верховного Суда Российской Федерации основных формулировок и алгоритма действий при их использовании в процессе квалификации анализируемых преступлений.

Для цитирования в научных исследованиях

Виноградов Е.А. Судебная практика по уголовным делам, связанным с хищениями, совершаемыми с использованием вредоносного программного обеспечения // Вопросы российского и международного права. 2025. Том 15. № 7А. С. 104-111.

Ключевые слова

Судебная практика, квалификация, хищения с использованием вредоносных программ, неправомерный доступ к компьютерной информации, незаконное получение сведений, составляющих банковскую тайну, организованная преступность, легализация денежных средств, полученных преступным путем, судебный штраф, способы выявления и раскрытия преступлений и преступников, многоэпизодные преступления.

Введение

Использование вредоносного программного обеспечения при совершении корыстных преступлений против собственности позволяет злоумышленникам не только получать сверхвысокий нелегальный доход, но и оставаться в большинстве случаев невыявленными и, соответственно, не привлеченными к уголовной ответственности. По тем же преступлениям, которые все же удалось выявить и даже довести до судебного разбирательства, складывается достаточно неоднородная практика как в силу того, что существуют многочисленные законодательные неопределенности, связанные, например, с формулировками понятий «программное обеспечение», «компьютерная информация», «вредоносность информационно-телекоммуникационных средств» и т.д., так и в силу того, что сотрудники оперативных и следственных органов не всегда обладают необходимыми для квалификации таких преступлений компетенциями. Более того, практический опыт показывает, что суды, как правило, тоже имеют недостаточный уровень знаний в сфере оборота компьютерной информации.

Основное содержание

В рамках данного исследования было рассмотрено свыше 50 приговоров судов различных субъектов Российской Федерации, а также определений и постановлений судов апелляционной инстанции, решений и определений Верховного Суда Российской Федерации. Анализ показал, что суды исходят из разного понимания как способов совершения хищения с использованием вредоносного программного обеспечения, отнесения вредоносного программного обеспечения к орудиям или средствам совершения преступления, необходимости дополнительной квалификации таких противоправных деяний по тем нормам, которые предусматривают ответственность за неправомерное получение и разглашение сведений, составляющих коммерческую или банковскую тайну, а также за легализацию денежных средств, полученных преступным путем, так и оценки тех доказательств, которые имеются по таким делам, учета особенностей отдельных оперативно-розыскных и следственных мероприятий и действий и т.д.

Кроме того, согласно изученным материалам судебной практики по отдельным делам выносились постановления о прекращении производства по делу как в связи с назначением судебного штрафа, так и в связи с истечением сроков давности, а также в связи с примирением сторон. Причем при схожих обстоятельствах одни суды усматривали возможность назначения такой меры уголовно-правового характера, как судебный штраф. Например, Бабушкинский районный суд г. Москвы, установив, что условия, при которых может быть назначена иная мера уголовного воздействия в виде судебного штрафа в отношении И. и К., чьи противоправные действия были квалифицированы по ч. 2 ст. 273 УК РФ, соблюдены, постановил прекратить уголовное преследование с назначением судебного штрафа в размере 20000 руб. для каждого подсудимого [Приговор Бабушкинский районный суд г. Москвы от 14.12.2021]. Другие суды исходили из того, что прекращать уголовное преследование при таких условиях недопустимо.

Особую озабоченность вызывает неоднородный подход судов к тем уголовным делам, по которым к ответственности привлекались лица, допустившие совершение не одного хищения, а многократных хищений с использованием вредоносных программ. В большей степени такая неоднородность просматривается даже не в квалификации преступных деяний, хотя в одних случаях имеется дополнительная квалификация как преступной деятельности преступного

сообщества (по ст. 210 УК РФ), а в других – только группа лиц по предварительному сговору, а в наказании, которое в большинстве случаев связано с лишением свободы, но в некоторых случаях лишь с условным его назначением, что, конечно, не может не сказываться негативно на росте преступности анализируемого вида.

Затронутые выше проблемные вопросы заслуживают более глубокого анализа и изучения. Но в данной работе хотелось бы подробнее остановиться на таком аспекте квалификации хищений денежных средств, совершенных посредством использования вредоносного программного обеспечения, как огромный разброс в мнениях судей по поводу достаточности квалификации таких преступлений только по ст. 159.6 УК РФ как корыстных преступлений против собственности или, наоборот, необходимости в дополнительной квалификации как преступлений в сфере оборота компьютерной или банковской информации.

Необходимо отметить, что согласно содержанию разъяснений Пленума Верховного Суда РФ деяния, связанные с хищениями денежных средств, совершаемых с помощью вредоносных программ, должны квалифицироваться по совокупности ст. 159.6 УК РФ и ст. 272, 273 или 274.1 УК РФ [Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»]. Однако чрезмерно обобщенные формулировки, которые использует ВС РФ, не позволяют однозначно установить, что является ли вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей всегда неправомерным или такое вмешательство может быть и правомерным. Именно в данном вопросе, на наш взгляд, кроется та неопределенность, которая не позволяет судам использовать единый подход.

Так, согласно изученным материалам в некоторых случаях суды исходили из того, что для квалификации хищения денежных средств с помощью вредоносных программ достаточно применить только ст. 159.6 УК РФ. Например, Центральный районный суд г. Тюмени квалифицировал деяние, совершенное группой лиц по предварительному сговору, а именно К., Х., Ш. и неустановленным лицом, которое заключалось в том, что указанные лица совместно подыскивали банковские карты, производили заражение мобильного устройства с помощью вредоносного программного обеспечения, получали доступ к мобильному банковскому приложению, с помощью которого совершали переводы денежных средств потерпевших на я в распоряжении преступников, по ч.2 ст. 159.6 УК РФ [Приговор Центрального районного суда г. Тюмени от 03.09.2018].

При этом в приговоре суда содержатся сведения о том, что указанные лица использовали неустановленное вредоносное программное обеспечение, которое предварительно было приобретено неустановленным лицом, на счет которого иные участники преступной группы перечисляли денежные средства потерпевших (всего двадцать два человека). Суд счел, что признака «совершение преступления организованной группой» в данном случае не усматривается, так как подсудимых связывали дружеские отношения, а какого-либо распределения ролей, структурированности и иерархии преступная группировка не имела.

В качестве еще одного примера можно привести приговор Куйбышевского районного суда г. Новокузнецка Кемеровской области, согласно которому по ч.4 ст. 159.6 УК РФ были привлечены к ответственности И. и П., которые также при участи неустановленного лица совершали хищения денежных средств со счетов юридических лиц, оказывающих

туристические услуги, посредством использования неустановленного вредоносного программного обеспечения [Приговор Куйбышевского районного суда г. Новокузнецка Кемеровской области от 29.09.2020]. Суд в приговоре указал, что неустановленное лицо совершило рассылку электронного письма, содержащего вредоносные для компьютерных систем элементы, с помощью которых был получен удаленный доступ к интерфейсам кассиров, в чьи обязанности входило оформление проездных билетов. Подсудимые прии скивали лиц, готовых предоставить паспортные данные, оформляли проездные документы, которые впоследствии возвращали, а денежные средства распределяли согласно установленным ролям. По данному уголовному делу группа лиц была признана организованной группой.

Обращает на себя внимание тот факт, что в отдельных приговорах суд также квалифицирует содеянное дополнительно по ст. 210 УК РФ как участие в преступном сообществе, созданного для хищения денежных средств (например, приговор Басманного районного суда г. Москвы в отношении Н., который был признан виновным в преступлениях, предусмотренных ч.4 ст. 159.6 УК РФ, а также в преступлении, предусмотренном ч.2 ст. 210 УК РФ) [Приговор Басманого районного суда от 11.10.2022].

В других случаях схожие по существу деяния квалифицировались по совокупности ст. 159.6 УК РФ и по ст. 272 УК РФ или по ст.273 УК РФ. То есть уполномоченные лица признавали, что в случае хищения денежных средств посредством использования вредоносных программ необходимо учитывать не только корыстный характер такого преступления, путь даже корысть и обращена на цифровые данные в том или ином виде, но и их направленность на неправомерный доступ к таким данным, а также тот факт, что такой доступ преступники получают за счет вредоносного программного обеспечения (либо его создания и использования, либо создания, использования и распространения).

Так, Московский районный суд города Чебоксары Чувашской Республики признал З. виновным в совершении преступлений по ч.2 ст. 273 УК РФ и ч.4 ст. 159.6 УК РФ [Приговор Московского районного суда г. Чебоксары Чувашской Республики по делу № 1- 180/2018]. В решении данного суда, действительно, указывается, что было совершено не просто хищение денежных средств путем воздействия на цифровые данные, но и способ воздействия – приобретение и распространение вредоносных программ. Помимо этого в способе совершения данного преступления выделяются и такие элементы, как использование программных продуктов, не обладающих качеством вредоносности, а именно программа для массовой рассылки сообщений клиентам оператора сотовой сети, а также дополнительного оборудования, а именно – аренда сервера. Данное дело было рассмотрено в особом порядке, подсудимый был признан виновным, но наказание в виде лишения свободы было признано условным.

Отдельные суды усматривают необходимость квалификации содеянного по совокупности преступлений, предусмотренных ст. 159.6 УК РФ и ст. 174.1 УК РФ. Так, Дорогомиловский районный суд признал И. виновным по ч. 2 ст.273, п. «б» ч.4 ст.174.1, ч.4 ст.159.6 УК РФ [Приговор Дорогомиловского районного суда г. Москвы от 10.04.2024]. Преступное деяние, по мнению суда, выразилось не только в том, что И. совершил хищения цифровой валюты с электронных кошельков пользователей интернет ресурса «www.blockchain.com» путем ввода незаконно полученных, посредствам фишингового сайта «www.blochchian.ru» и вредоносного программного обеспечения «BrowserAutomationStudio», аутентификационных данных пользователей, но и в том, что он использовал такие программы для несанкционированного копирования компьютерной информации, а также осуществил легализацию иного имущества, приобретенного лицом в результате совершения им преступления, путем покупки

недвижимости (жилого дома и земельного участка), которую оформил на своего отца, неосведомленного о преступном умысле И.

По приговору Первомайского районного суда г. Краснодара подсудимые были признаны виновными уже по совокупности ч. 3 ст. 272 УК РФ и ч. 4 ст. 159.6 УК РФ [Приговор Первомайского районного суда г. Краснодара по делу № 1-50/2018]. Преступными были признаны деяния З., Б., а также неустановленного лица, которые заранее объединились в устойчивую преступную группу для совершения в её составе с корыстной заинтересованностью неправомерного доступа к охраняемой законом информации. Преступники с помощью вредоносных программ получали неправомерный доступ к охраняемой законом компьютерной информации, приобретали сим-карты операторов сотовой связи и банковские карты с подключенной услугой доступа к системе ДБО, оформленные на лиц, которые их не использовали и не были осведомлены об их использовании в преступной деятельности, с помощью которых производили хищение и обналичивание чужих денежных средств.

Еще более сложной и многозадачной увидели преступную деятельность, связную с хищением денежных средств посредством использования вредоносных программ, суды, которые квалифицировали такие деяния уже по совокупности ст. 159.6 УК РФ, ст. 272 УК РФ и ст. 273 УК РФ. Так, Октябрьский районный суд города Архангельска квалифицировал содеянное Л. и Ф. по совокупности ч.2 ст.273, ч.3 ст.272, ч.4 ст.159.6 УК РФ [Приговор Октябрьского районного суда г. Архангельска по делу № 1-7/2017]. Подсудимые приобрели вредоносную программу, которая позволяла без ведома владельцев мобильных телефонов отправлять от их имени SMS-сообщения с командами о запросе баланса денежных средств, находящихся на счетах банковских карт граждан, и о переводе денежных средств с данных счетов на счета третьих лиц без уведомления о произведенных операциях, используя свойства вредоносной программы, осуществляли неправомерный доступ к охраняемой законом, компьютерной информации граждан, переводили денежные средства с их счетов на иные банковские счета и распоряжались похищенными у потерпевших деньгами по своему усмотрению.

Помимо этого отдельные суды усматривают необходимость в дополнительной квалификации по ст. 183 УК РФ за незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну. Так, приговором Центрального районного суда г. Читы Забайкальского края Л., который посчитал, что получение информации о банковском счете потерпевшего, которая охраняется Федеральным законом Российской Федерации «О банках и банковской деятельности» от 02 декабря 1990 года № 395-1, а именно о реквизитах и о состоянии банковского счета банковской карты № ПАО «Сбербанк России», представляет собой объективную строну преступления, уголовная ответственность за которое наступает по ч.3 ст. 183 УК РФ.

По всем рассмотренным делам способом, с помощью которого удалось выявить преступление, было обращение потерпевших с заявлением о привлечении к уголовной ответственности неустановленных лиц, совершивших хищение денежных средств (цифровых объектов) посредством неправомерного доступа к компьютерной информации. Однако в отношении способов выявления самих преступников единой схемы не усматривается. Так, по одним противоправным деяниям лица, совершившие хищения, были выявлены посредством осуществления таких оперативно-розыскных мероприятий как наведение справок и прослушивание телефонных переговоров, по другим – использовались такие следственные действия, как осмотр места происшествия с изъятием записей видеокамер, установленных в

отделениях банков, получение информации о соединениях между абонентами и (или) абонентскими устройствами путем направления запросов в организации, предоставляющие услуги сотовой связи.

В процессе расследования уполномоченные лица получали доказательства посредством обыска жилища, для осуществления которого привлекались специалисты для обследования персональных компьютеров подозреваемых и программного обеспечения, установленного на таковые, осмотра предметов, а именно оптических дисков, в хранилищах которых содержится переписка преступников с иными пользователями. Особое место отводится заключениям экспертов как в отношении исправности технических средств, изъятых у преступников, так и в отношении содержания накопителей на жестких магнитных дисках, а также в отношении сущности программного обеспечения, которое использовалось преступниками для неправомерного доступа к компьютерной и иной информации.

Заключение

Таким образом, приходим к выводу, что неоднородность оперативной, следственной и судебной практики по преступлениям, связанным с хищениями денежных средств, совершаемых с использованием вредоносного программного обеспечения, выступает фактором, снижающим эффективность уголовно-правового воздействия на преступников. Оперативные и следственные органы при выявлении, раскрытии и расследовании преступлений данной категории не всегда оценивают в должной мере весь спектр возможных доказательств, а также не всегда используют те оперативные мероприятия и следственные действия, которые будут наиболее информативными. Суды, в свою очередь, рассматривая уголовные дела по преступлениям со схожими объективными и субъективными признаками, приходят к выводам, которые зачастую кардинально отличаются как по квалификации, так и по избранию меры наказания. Поэтому, считаем, что необходимо не просто выработать единый алгоритм выявления и раскрытия таких противоправных деяний, но и единый подход к их квалификации, что актуализирует необходимость разработки на уровне Верховного Суда такого документа, который бы не фрагментарно разъяснял отдельные особенности только мошенничества в сфере компьютерной информации или только преступлений, связанных с неправомерным доступом к компьютерной информации или оборотом вредоносных программ, а их совокупности.

Библиография

1. Приговор Бабушкинский районный суд г. Москвы от 14.12.2021 // [Электронный ресурс] Режим доступа: URL: https://mos-gorsud.ru/rs/babushkinskij (дата обращения: 30.03.2025).
2. Приговор Центрального районного суда г. Тюмени от 03.09.2018 // [Электронный ресурс] Режим доступа: URL: https://centralny--tum.sudrf.ru (дата обращения: 30.03.2025).
3. Приговор Куйбышевского районного суда г. Новокузнецка Кемеровской области от 29.09.2020 // [Электронный ресурс] Режим доступа: URL: https://kuybyshevsky.kmr.sudrf.ru (дата обращения: 30.03.2025).
4. Приговор Басманого районного суда от 11.10.2022 // [Электронный ресурс] Режим доступа: URL: https://mos-gorsud.ru/rs/basmannyj (дата обращения: 30.03.2025).
5. Приговор Московского районного суда г. Чебоксары Чувашской Республики по делу № 1- 180/2018 // [Электронный ресурс] Режим доступа: URL: https://moskovsky.chv.sudrf.ru (дата обращения: 30.03.2025).
6. Приговор Дорогомиловского районного суда г. Москвы от 10.04.2024 // [Электронный ресурс] Режим доступа: URL: https://mos-gorsud.ru/rs/dorogomilovskij (дата обращения: 30.03.2025).
7. Приговор Первомайского районного суда г. Краснодара по делу № 1-50/2018// [Электронный ресурс] Режим доступа: URL: https://pervomaisky.krd.sudrf.ru (дата обращения: 30.03.2025).
8. Приговор Октябрьского районного суда г. Архангельска по делу № 1-7/2017 // [Электронный ресурс] Режим

доступа: URL: https://oktsud.arh.sudrf.ru (дата обращения: 30.03.2025).

Judicial Practice in Criminal Cases Related to Thefts Committed Using Malicious Software

Evgenii A. Vinogradov

Applicant for a Degree,
Faculty of Training Scientific-Pedagogical and Scientific Personnel,
Department of Operational-Search Activity and Special Equipment,
Moscow University of the Ministry of Internal
Affairs of Russia named after V.Ya. Kikot,
117437, 12 Akademika Volgina str., Moscow, Russian Federation;
e-mail: 40mvd@bk.ru

Abstract

Criminals committing theft of funds through the use of malicious software are prosecuted under both Article 159.6 of the Criminal Code of the Russian Federation and a combination of crimes, including those provided for in Articles 272, 273, 210, 183, and 174.1 of the Criminal Code of the Russian Federation. The complexity of qualification lies in the fact that neither operational and investigative officers nor judicial authorities have developed a unified approach to establishing the objective features of such acts. It is necessary to consolidate, at the level of the Supreme Court of the Russian Federation, the main formulations and algorithms for their use in the process of qualifying the analyzed crimes.

For citation

Vinogradov E.A. (2025) Sudebnaya praktika po ugolovnym delam, svyazannym s khishcheniyami, sovershaemymi s ispol'zovaniyem vredonoskogo programmnogo obespecheniya [Judicial Practice in Criminal Cases Related to Thefts Committed Using Malicious Software]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (7A), pp. 104-111.

Keywords

Judicial practice, qualification, theft using malicious software, unlawful access to computer information, illegal obtaining of information constituting bank secrecy, organized crime, money laundering, judicial fine, methods of detecting and solving crimes and criminals, multi-episode crimes.

References

1. Verdict of the Babushkinsky District Court of Moscow dated 12/14/2021 // [Electronic resource] Access mode: URL: https://mos-gorsud.ru/rs/babushkinskij (date of appeal: 30.03.2025).
2. Verdict of the Central District Court of Tyumen dated 03.09.2018 // [Electronic resource] Access mode: URL: https://centralny--tum.sudrf.ru (date of request: 30.03.2025).
3. The verdict of the Kuibyshevsky District Court of Novokuznetsk, Kemerovo region, dated 09/29/2020 // [Electronic resource] Available at: URL: https://kuybyshevsky.kmr.sudrf.ru (date of request: 30.03.2025).

4. The verdict of the Basmany district Court of 11.10.2022 // [Electronic resource] Access mode: URL: https://mos-gorsud.ru/rs/basmannyj (date of appeal: 30.03.2025).
5. Verdict of the Moscow District Court of Cheboksary, Chuvash Republic in case no. 1- 180/2018 // [Electronic resource] Access mode: URL: https://moskovsky.chv.sudrf.ru (date of request: 30.03.20256
. The verdict of the Dorogomilovsky District Court of Moscow dated 04/10/2024 // [Electronic resource] Access mode: URL: https://mos-gorsud.ru/rs/dorogomilovskij (date of request: 30.03.2025).
7. The verdict of the Pervomaisky District Court of Krasnodar in case no. 1-50/2018// [Electronic resource] Access mode: URL: https://pervomaisky.krd.sudrf.ru (date of appeal: 30.03.2025).
8. Verdict of the Oktyabrsky District Court of Arkhangelsk in case no. 1-7/2017 // [Electronic resource] Access mode: URL: https://oktsud.arh.sudrf.ru (date of request: 30.03.2025).