Федеральное государственное казенное образовательное учреждение высшего образования «Уральский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра уголовного процесса

Е. Л. Федосеева
С. А. Воропаев
Р. Н. Кузнецов

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИЧИНЕНИЕМ ИМУЩЕСТВЕННОГО УЩЕРБА ПРАВООБЛАДАТЕЛЯМ И ПОТРЕБИТЕЛЯМ ЦИФРОВОГО КОНТЕНТА

Учебно-методическое пособие

Екатеринбург
2020

ББК 67.410.212.2
Ф328

Федосеева Е. Л.

Ф328 ***Особенности квалификации и расследования преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента:*** *учебно-методическое пособие* / Е. Л. Федосеева, С. А. Воропаев, Р. Н. Кузнецов. – Екатеринбург: Уральский юридический институт МВД России, 2020. – 50 с.

ISBN 978-5-88437-693-9

Рецензенты: **К. В. Вишневецкий,** начальник кафедры уголовного права и криминологии Краснодарского университета МВД России, доктор юридических наук, профессор;
В. Н. Борков, начальник кафедры уголовного права Омской академии МВД России, доктор юридических наук, доцент

В учебно-методическом пособии раскрывается правовая природа цифрового контента, игрового аккаунта и его дополнительного функционала; рассматриваются особенности квалификации и методика расследования преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента. Пособие будет способствовать формированию профессиональных компетенций, в числе которых способность юридически правильно квалифицировать факты, события и обстоятельства; способность осуществлять расследование экономических преступлений и др. Направлено на реализацию приоритетного профиля подготовки «Деятельность подразделений дознания».

Предназначено для профессорско-преподавательского состава, курсантов и слушателей образовательных организаций МВД России, обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность, по программам повышения квалификации и переподготовки, сотрудников подразделений дознания и предварительного следствия территориальных органов внутренних дел Российской Федерации.

Обсуждено на заседании кафедры уголовного процесса УрЮИ МВД России (протокол № 23 от 13 ноября 2019 г.).

Рекомендовано для использования в образовательном процессе методическим советом УрЮИ МВД России (протокол № 5 от 12 декабря 2019 г.).

ISBN 978-5-88437-693-9 ББК 67.410.212.2

Введение

Одной из наиболее динамично развивающихся сфер общественных отношений является оборот объектов виртуальной реальности, а именно онлайн-игр. Размеры данного оборота уже давно превысили многомиллиардные суммы по всему миру. Россия не находится в стороне от данного процесса. Организаторы онлайн-игр активно продвигают на рынке свой товар, предлагая потенциальным участникам не только участие в играх, как на безвозмездной, так и на возмездной основе, но и приобретение как самих игровых аккаунтов, так и дополнительных ресурсов к ним. Стоимость этих виртуальных аккаунтов может исчисляться тысячами абсолютно реальных денежных единиц различных стран. Вследствие этого наблюдается и рост противоправных посягательств на данные игровые аккаунты с корыстным мотивом, в том числе для их дальнейшей перепродажи.

По этой причине для органов внутренних дел должны быть подготовлены необходимые теоретические разработки по выявлению, пресечению и расследованию случаев данных противоправных действий, имеющие прикладной характер.

Объектом данного исследования являются правовые отношения, складывающиеся в процессе расследования преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента.

В учебно-методическом пособии раскрывается правовая природа онлайн-игр как объектов различного правового регулирования, особенности квалификации, предмета доказывания и производства проверочных и отдельных следственных действий по преступлениям, связанным с причинением ущерба правообладателям и потребителям цифрового контента в сети «Интернет».

Пособие может применяться в практической деятельности подразделений органов внутренних дел при расследовании компьютерных преступлений, а также в образовательном процессе обучающихся образовательных организаций МВД России по специальности 40.05.01 Правовое обеспечение национальной безопасности при изучении учебных дисциплин «Расследование преступлений в сфере компьютерной информации», «Методы и способы получения доказательственной информации с электронных носителей».

Использование пособия в учебном процессе будет способствовать формированию у обучающихся профессиональных компетенций, необходимых в конкретных практических ситуациях, возникающих в ходе расследования уголовных дел, связанных с деятельностью по возбуждению уголовных дел, производству следственных и процессуальных действий по преступлениям указанной категории, таких как:

– способность принимать решения и совершать юридические действия в точном соответствии с законодательством Российской Федерации (ПК-3);

– способность разрабатывать и правильно оформлять юридические и служебные документы (ПК-5);

– способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения (ПК-9);

– способность реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в инте-

ресах предупреждения, пресечения, раскрытия и расследования преступлений (ПК-11);

– способность правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации (ПК-13);

– способность производить предварительное расследование (в форме предварительного следствия) по уголовным делам о преступлениях, подследственных органам внутренних дел.

Применение изложенных в пособии методических рекомендаций в практической деятельности позволит активизировать и повысить эффективность расследования уголовных дел по преступлениям в сфере компьютерной информации, не допускать ошибок со стороны должностных лиц, осуществляющих расследование.

Глава 1. Правовая природа онлайн-игр и доменных имен как объектов гражданских прав

Технический прогресс приводит к усложнению технологий, многократному увеличению объема технических знаний, доступных человечеству, постоянному появлению новых научных, технических достижений. Одним из достижений человечества является виртуальная реальность, в частности, реализуемая посредством разработки многопользовательских ролевых онлайн-игр. Разработчики онлайн-игр моделируют виртуальные пространства, в рамках которых проходит игровой процесс, создаются игровые аккаунты, которые бесплатно или на возмездной основе передаются участвующим игрокам, сами организаторы онлайн-игр активно продают дополнительные ресурсы для игровых аккаунтов. Игроки, в свою очередь, активно торгуют своими игровыми персонажами и их ресурсами. По данным аналитического агентства Newzoo (Newzoo's 2017 GlobalGamesMarketReport), на 2017 г. объем мировых продаж онлайн-игр составил рекордные 109 млрд долларов, а на 2020 год прогнозируются мировые продажи уже на 128,5 млрд долларов[1].

При этом возникает вопрос о правовой природе виртуальных ценностей, являются ли они объектами правового регулирования, и если являются, то к какому отраслевому правовому регулированию относятся, какие правовые последствия будут иметь место в случае противоправных посягательств на данные объекты виртуальной реальности. Невзирая на виртуальный характер рассматриваемых объектов в имущественном обороте, они уже очень давно оцениваются в реальных денежных средствах, один из наиболее впечатляющих примеров – это продажа в 2012 г. виртуальной недвижимости в игре EntropiaUniverse на 2,5 млн долларов.

Органы внутренних дел должны оперативно и адекватно современным условиям реагировать на новые явления в общественной жизни с тем, чтобы в случае совершения нарушения прав и законных интересов граждан и организаций, незамедлительно пресекать совершенные правонарушения, выявлять виновных в их совершении лиц.

[1] См.: Серьезные забавы: почему видеоигры становятся популярнее кино. URL: https://www.forbes.ru/tehnologii/357631-sereznye-zabavy-pochemu-videoigry-stanovyatsya-populyarnee-kino (дата обращения: 3 сентября 2019 г.).

Правонарушений же, связанных с объектами виртуальной реальности, достаточно много, и их количество, без всякого сомнения, будет только возрастать. На сегодняшний день фиксируется большое количество случаев противоправного завладения игровыми аккаунтами с целью их дальнейшей перепродажи целиком или по частям.

Так, несколько лет назад в один из отделов полиции города Воронежа в три часа ночи поступило сообщение о совершении преступления – у заявителя угнали танк ИС 2. Речь шла, конечно же, о танке в онлайн-игре «WorldofTanks», который посредством взлома игрового аккаунта был похищен у игрока. Аналогичный случай хищения танка в онлайн-игре имел место в соседней Беларуси[1].

Мировая практика при этом многогранна и разнообразна. Так в 2005 г. QuiChengwei, пользователь онлайн-игры LegendsofMir III, передал во временное пользование своему знакомому меч, который тот не возвратил, а продал на аукционе eBay за сумму, эквивалентную 820 евро. Полиция отказалась вмешиваться в данный спор. Отчаявшись найти помощь у правоохранительных органов, QuiChengwei просто убил своего знакомого[2].

Более того, как ни странно, но онлайн-игры активно используются участниками организованных преступных сообществ, в том числе террористической направленности, как защищенный канал связи, поскольку участники данных онлайн-игр имеют возможность общения между собой в рамках самой игры (ведение чата). И если при обычных условиях ведение разговора о том, чтобы подвезти боеприпасы, взрывчатку, о планировании убийства, военного наступления, взрыва и чего-то иного подобного будет противоестественно и вызовет очевидные подозрения, то подобные разговоры в рамках чата игроков онлайн-игр «звучат» вполне естественно и органично.

В целом, сфера применения онлайн-игр должна быть подвержена тщательному правовому анализу с тем, чтобы органы внутренних дел имели четкое, адекватное требованиям современных реалий теоретическое обоснование своих правоприменительных действий при реагировании на правонарушения при преступных посягательствах на объекты виртуальной реальности.

Приступая к правовому анализу правовой природы онлайн-игр и ее элементов, прежде всего следует определиться, а что представляет собой непосредственно сама онлайн-игра? Ее конституирующие признаки выделил профессор права университета Вайкато Вэйн Рамблс[3]. Онлайн-игра, по его мнению, характеризуется:

– общим пространством: мир игры позволяет множеству игроков одновременно находиться и взаимодействовать в нем друг с другом;

– графическим интерфейсом: пользователи взаимодействуют друг с другом в искусственном 3D-окружении;

---

[1] См.: *Лисаченко А. В.* Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. 2014. № 2. URL: https://base.garant.ru/57564882/ (дата обращения: 3 сентября 2019 г.).

[2] См.: *Li C.* Death sentence for on-line gamer // China Daily. 2005. URL: http://www.chinadaily.com.cn/english/doc/2005-06/08/content_449494.htm (дата обращения: 11 сентября 2019 г.).

[3] См.: Senior Lecturer, TePiringa – Faculty of Law, University of Waikato. URL: https://docplayer.net/12372264-Curriculum-vitae-wayne-andrew-rumbles-i-t-law-specialist-senior-lecturer-te-piringa-faculty-of-law-university-of-waikato.html (дата обращения: 15 сентября 2019 г.).

– непосредственностью: пользователи взаимодействуют друг с другом в реальном времени;

– интерактивностью: мир реагирует на действия игроков в нем – игроки имеют возможность влиять на мир;

– сохранностью мира: мир продолжает существование вне зависимости от нахождения в нем конкретного пользователя;

– социализацией сообществом: игровой мир позволяет и стимулирует социальные взаимодействия внутри себя.

Таким образом, онлайн-игра – это общий для многих пользователей виртуальный мир, выраженный графическим интерфейсом, способный на протяжении долгого времени сохраняться неизменным, служа местом социализации для пользователей[1].

Гражданский кодекс Российской Федерации в ст. 128 к объектам гражданских прав относит: вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе, имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказания услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага.

Следует отметить, что цифровые права в ст. 128 ГК РФ появились буквально с 1 октября 2019 г., именно с этого дня законодательные новеллы в гражданском законодательстве вступили в юридическую силу. Ранее в юридической литературе шли многочисленные дискуссии о правовой природе объектов виртуальной собственности, как с отрицанием их правовой природы, так и с признанием права на их существование в правовом поле.

Более того, и арбитражная судебная практика также неоднозначно подходила к спорам по поводу объектов виртуальной реальности. Суды отказывались рассматривать по существу требования истца, связанные с невозможностью использовать виртуальные предметы, приобретенные за реальные деньги в онлайн-играх Lineage 2 и AION, на основании положений главы 58 ГК РФ о невозможности судебной защиты требований из организации игр и пари по общему правилу[2].

Доминирующей была позиция, согласно которой объекты виртуальной реальности относились к категории «иное имущество», что наиболее детально обосновывал А. И. Савельев[3]. Видится, что данная позиция обоснованна и не утрачивает актуальности и сегодня. Основным объектом гражданского права является имущество, которое условно разделяется на вещи, имущественные права и имущественные обязанности. Вещи – это данные природой или созданные человеком ценности материального мира, выступающие объектом гражданского законода-

---

[1] См.: *Петров В. Е.* Защита прав потребителей онлайн-игр // Экономика и право. XXI век. 2016. № 4. URL: https://base.garant.ru (дата обращения: 17 сентября 2019 г.).

[2] См.: *Архипов В. В., Килинкарова Е. В., Мелащенко Н. В.* Проблемы правового регулирования оборота товаров в сети Интернет: от дистанционной торговли до виртуальной собственности // Закон. 2014. № 6. URL: http://www.consultant.ru (дата обращения: 19 сентября 2019 г.).

[3] См.: *Савельев А. И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=76915#012446862479931575 (дата обращения: 19 ноября 2019 г.).

тельства. Вещи отвечают двум основным признакам: первый – способность удовлетворять потребности человека; второй – их овеществленный характер. Следовательно, онлайн-игры, не отвечающие данным признакам, к вещам не относятся.

Имущественные обязанности – это прежде всего обязательства, обязанность выполнения каких-либо действий, будь то передача имущества, денег, выполнение работ или оказание услуг. Имущественные права, в свою очередь, представляют собой права требования выполнения в свою пользу передачи тех же имущественных благ, выполнения работ или оказания услуг. Объектами имущественных прав могут являться результаты работ, услуг, интеллектуальной деятельности, программное обеспечение.

Следовательно, онлайн-игры до появления в гражданском законодательстве правовой нормативно определенной категории «цифровые права» относились к имущественным правам, зачастую называемым «иным имуществом». Впрочем, появление категории «цифровые права» не влияет на данное сложившееся правило, поскольку цифровые права появились совсем недавно, и на настоящий момент еще нет практики применения данной правовой категории.

Правовая природа цифровых прав регламентирована ст. 141.1 ГК РФ, вступившей в силу 1 октября 2019 г., в которой законодатель выделяет следующие признаки цифровых прав:

– цифровые права должны быть названы в таком качестве в федеральном законе;

– осуществление таких прав, распоряжение или ограничение распоряжения ими возможны только в информационной системе;

– по общему правилу обладателем цифрового права считается лицо, которое может им распоряжаться;

– переход цифрового права по сделке не требует согласия должника;

– прямо допускается оборотоспособность цифровых прав (к ним будут применимы общие положения о купле-продаже).

Таким образом, цифровые права должны быть названы в федеральном законе; на текущий момент имеется лишь один такой пример, это так называемый закон о краудфандинге, а именно Федеральный закон от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты РФ», в ст. 8 которого регламентировано использование утилитарных цифровых прав. Данный закон вступил в силу лишь 1 января 2020 г. Но нет сомнений, что со временем будет разработан Федеральный закон, которым онлайн-игры приобретут свой законный статус объектов цифровых прав.

Помимо гражданско-правовых отношений онлайн-игры являются также и объектами налоговых правоотношений, поскольку организаторы многопользовательских ролевых онлайн-игр ведут активную торговлю как самими игровыми аккаунтами, так и ресурсами к ним. Налоговые органы применяют к данным ресурсам специальный термин «дополнительный игровой функционал». Так, если в отношении неактивированных данных и команд компьютерной онлайн-игры лицензиар по договору передает права лицензиату (физическому лицу) на использование программы для ЭВМ, а лицензиат перечисляет лицензиару за указанное

право соответствующее вознаграждение, то применение освобождения от НДС при указанной передаче прав на основании подп. 26 п. 2 ст. 149 Налогового кодекса РФ правомерно[1]. Следует при этом отметить разнообразие арбитражной практики по налогообложению участников договорных отношений по продаже онлайн-игр. Так, по одному из рассматриваемых дел налогоплательщик – юридическое лицо оспаривал доначисление ему налога, полагая, что заключает с гражданами лицензионные договоры. Суд, установив, что компания является разработчиком и администратором онлайн-игры, сделал вывод, что между сторонами заключен смешанный договор, включающий в себя элементы лицензионного договора и договора возмездного оказания услуг по организации игрового процесса. Поскольку услуги облагаются НДС, налог доначислен правильно[2].

Функционирование онлайн-игр невозможно без должного уровня правового регулирования использования доменных имен, под которыми в самом широком смысле понимается непосредственно адрес сайта, место его размещения в сети «Интернет». Законодательно, доменное имя – это обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной там.

Зачастую название онлайн-игры является составляющим элементом доменного имени, по сути, его электронным адресом. При этом не следует умалять экономической составляющей ценности доменного имени. В случае его широкой известности, лаконичности, броскости доменное имя может иметь ценность как отдельный объект гражданских прав. Так, например, несколько лет назад доменное имя business.com было продано в США за 340 млн долларов. В России в последнее время особенную популярность приобрели доменные имена RU, РФ, а также ДЕТИ. По аналогии с онлайн-играми сложился оборот доменных имен. В целом, в контексте настоящего исследования доменные имена в большей степени производны от онлайн-игр.

Таким образом, можно сделать вывод о том, что онлайн-игры и доменные имена являются полноценными отдельными объектами правового регулирования; в рамках регулятивных отношений являются объектами гражданского и налогового права. В рамках гражданского законодательства относятся к имущественным правам, порой законодательно называемым «иное имущество»; а в рамках налогового законодательства получили наименование «дополнительный игровой функционал».

На основании изложенного можно заключить, что онлайн-игры при охранительном регулировании могут являться объектами преступных посягательств, влекущих меры оперативного реагирования органами внутренних дел в рамках оперативно-разыскной деятельности, предварительного расследования совершенного преступления и являющихся в дальнейшем основанием для искового производства в рамках гражданского процесса при взыскании причиненного имущественного вреда обладателю прав на онлайн-игры.

---

[1] Письмо ФНС России от 23 января 2017 г. № СД-4-3/988@. URL: http://www.consultant.ru (дата обращения: 19 сентября 2019 г.).

[2] Постановление АС Московского округа от 18 июня 2015 г. № Ф05-7093/2015 по делу № А40-91072/14. URL: http://www.consultant.ru (дата обращения: 21 сентября 2019 г.).

Глава 2. Особенности квалификации преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента

2.1. Социально-правовая обусловленность криминализации причинения имущественного ущерба правообладателям и потребителям цифрового контента

Одновременное взаимодействие множества пользователей и правообладателей цифрового контента, обеспеченное доступностью и повсеместностью компьютерных технологий и сети «Интернет», породило большое количество вопросов цивилистического, уголовно-правового и уголовно-процессуального характера при необходимости обеспечения нормального развития общественных отношений в указанной сфере.

Наиболее популярным и распространенным видом такого виртуального взаимодействия во многих странах мира, в том числе и Российской Федерации, являются массовые многопользовательские ролевые онлайн-игры.

От обычной компьютерной игры массовые многопользовательские ролевые онлайн-игры отличаются тем, что они не прекращаются с выключением компьютера отдельного пользователя, при этом изменения внутри игры, в том числе по отношению к «выключенному» игроку, продолжают происходить постоянно.

Следует отметить, что существует разновидность указанных игр, в которых изменения происходят не только в виртуальном пространстве по правилам разработчика, но и в реальном мире на основе общественных отношений, перетекающих из цифровой оболочки в окружающую действительность. Речь идет о так называемых симуляторах реальной жизни, в рамках которых игроки могут вводить конвертируемые денежные средства, приобретая виртуальные ценности, осуществлять определенную виртуальную деятельность, увеличивая ценность виртуальных объектов, и снова выводить в реальный мир конвертируемые денежные средства, обменивая их на указанные виртуальные объекты.

Пользователь, заключив соглашение с правообладателем, получает полномочия по управлению поведением виртуального персонажа, взаимодействуя с миллионами других виртуальных фигур. При этом в ходе такого взаимодействия могут осуществляться деяния, причиняющие реальный материальный ущерб, а также ущерб в виде упущенной выгоды, как правообладателям, так и пользователям таких игр.

Возможность причинения ущерба вытекает, с одной стороны, из реальных затрат, которые осуществил правообладатель при разработке либо приобретении программного продукта, обеспечивающего работу указанного сервиса, а также из права извлекать доход от предоставления данного электронного ресурса в пользование, с другой стороны, из затрат игроков на приобретение для своего персонажа навыков и умений, на получение «виртуальных ценных предметов», «виртуальной валюты» за реальную конвертируемую валюту. Суммы затрат со стороны игроков при этом достигают нескольких десятков миллионов рублей, не говоря уже о размерах расходов правообладателей обозначенного цифрового контен-

та[1]. На сайтах экономической статистики Интернета есть информация о прогнозе экспертов в области мировой экономики о том, что выручка в сегменте онлайн-игр в 2019 г. составит 12 692 млн долларов США[2]. Уже сейчас в онлайн-игры вовлечены более 500 млн игроков, при этом прослеживается тенденция стабильного роста этого количества[3]. Следует отметить, что ежегодный прирост численности игроков онлайн-игр выражается миллионами пользователей.

Существенный оборот денежных средств внутри цифрового игрового онлайн-пространства, рост количества игроков и правообладателей онлайн-игр, без всяких сомнений, требует защиты этого «нового сектора экономики» от общественно опасных посягательств, в том числе и уголовно-правовыми средствами.

Статистика МВД России по количеству преступлений, совершенных с использованием компьютерных или телекоммуникационных технологий, фиксирует следующие цифры: в 2017 г. было зарегистрировано 90 587 таких преступлений, из них раскрыто 20 424, что составляет примерно 22,5 % от всех зарегистрированных преступлений данного вида за указанный период; в 2018 г. было зарегистрировано 174 674 таких преступлений, из них раскрыто 43 362, что составляет примерно 25 % от всех зарегистрированных преступлений данного вида за указанный период; с января по июль 2019 г. (за 7 месяцев) было зарегистрировано 140 184 таких преступлений, из них раскрыто 33 894, что составляет примерно 24 % от всех зарегистрированных преступлений данного вида за указанный период[4].

Отмечая в период с 2017 по 2019 гг. динамику существенного роста зарегистрированных преступлений, совершенных с использованием компьютерных или телекоммуникационных технологий (ежегодно указанная цифра увеличивалась в 2 раза), следует отметить, что в 2016 г. и ранее данный вид преступлений еще отсутствовал в официальных статистических отчетах МВД России. Это свидетельствует об очень активном развитии анализируемого негативного социального явления. Кроме того, по высокой активности роста исследуемых преступлений и относительно невысокой раскрываемости (около четверти от всех зарегистрированных преступлений данного вида) можно сделать вывод о проблемах как законодательного, так и правоприменительного порядка, возникающих при защите нарушенных прав и интересов в указанной сфере.

Необходимость выявления и систематизации проблем квалификации и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий подтверждается особым значением, которое придает Министерство внутренних дел Российской Федерации этому вопросу. В рамках решений коллегии МВД России Следственному департаменту МВД России совместно с заинтересованными подразделениями системы МВД России поручено проведение анализа следственно-судебной практики расследования уголовных дел о преступлениях, совершенных с использованием информационно-

[1] См.: 10 самых дорогих игровых предметов. URL: https://gmbox.ru/materials/35758-10-samih-dorogih-igrovih-predmetov (дата обращения: 5 сентября 2019 г.).
[2] См.: Statista. Onlain Games. URL: https://www.statista.com/outlook/212/100/online-games/worldwide (дата обращения: 6 сентября 2019 г.).
[3] См.: Тренды онлайн-игр. URL: https://plarium.com/ru/blog/trendy-onlayn-igr-2017/ (дата обращения: 6 сентября 2019 г.).
[4] См.: Сайт официальной статистики МВД России. URL: https://xn--b1aew.xn--p1ai/reports/1/ (дата обращения: 6 сентября 2019 г.).

телекоммуникационных технологий, в целях выявления проблемных вопросов в указанном направлении и подготовки предложений по совершенствованию правоприменения и законодательного регулирования указанной сферы[1].

Анализ законодательной основы противодействия преступлениям, совершенным с использованием компьютерных или телекоммуникационных технологий, в целом, а также посягательствам, причиняющим имущественный ущерб правообладателям и потребителям цифрового контента в массовых многопользовательских ролевых онлайн-играх, в частности, выявил достаточно обширную нормативно-правовую базу.

В рамках Доктрины информационной безопасности Российской Федерации, утвержденной указом Президента Российской Федерации от 5 декабря 2016 г. № 646, в качестве одной из «основных информационных угроз» для нашего государства отмечены «возрастающие масштабы компьютерной преступности, прежде всего, в кредитно-финансовой сфере, а также увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий»[2]. Несколько ранее был принят другой стратегический документ – «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утвержденный Президентом Российской Федерации 24 июля 2013 г. № Пр-1753[3].

Кроме стратегических документов, а также Гражданского кодекса Российской Федерации, Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации, к законодательной основе противодействия исследуемому виду посягательства можно отнести следующие нормативные правовые акты: Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»; Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»; указ Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и раз-

[1] Приказ МВД России от 25 ноября 2019 г. № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км». URL: https://мвд.рф/Fotoarhiv/Meroprijatija_s_uchastiem_rukovodstva.

[2] Доктрина информационной безопасности Российской Федерации. URL: https://rg.ru/2016/ 12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 9 сентября 2019 г.).

[3] Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/ information/ document114/ (дата обращения: 10 сентября 2019 г.).

мещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет»); указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Несмотря на широкий спектр нормативных документов, к сожалению, следует констатировать необходимость продолжения масштабной работы по правовой регламентации защиты общественных отношений в сфере компьютерных или телекоммуникационных технологий.

В настоящее время нельзя однозначно сделать вывод о том, что нормы гражданского права каким-либо образом регламентируют виртуальное имущество. Вместе с тем существуют позиции отдельных цивилистов, которые считают возможным на современном этапе развития виртуального имущества применять при возникновении гражданских споров по нему расширительное толкование норм главы 60 ГК РФ «Обязательства вследствие неосновательного обогащения», рассматривая при этом в качестве указанных объектов «иное имущество», регламентированное положениями ст. 128 ГК РФ[1].

Данный подход не поддерживается судебной практикой. При вынесении решений суды часто квалифицируют нарушения отношений по поводу виртуального имущества, применяя ст. 1062 ГК РФ[2]. В частности, ч. 1 ст. 1062 ГК РФ указывает, что «требования граждан и юридических лиц, связанные с организацией игр и пари или с участием в них, не подлежат судебной защите, за исключением требований лиц, принявших участие в играх или пари под влиянием обмана, насилия, угрозы или злонамеренного соглашения их представителя с организатором игр или пари, а также требований, указанных в п. 5 ст. 1063 ГК РФ».

Уголовное законодательство в вопросе определения правового статуса виртуального имущества, безусловно, зависит от правовой регламентации данного явления гражданским правом. В этой связи суды при наличии признаков преступлений в сфере компьютерной информации, сопряженных с воздействием на виртуальное имущество, несмотря на наличие причиненного ущерба правообладателю или потребителю цифрового контента, рассматривают его лишь в рамках главы 28 УК РФ. Однако в этой сфере возникает много вопросов, имеющих уголовно-правовое значение. Например, может ли виртуальное имущество выступать предметом взятки, использоваться как признак преступления при легализации? Возникают вопросы о соотношении общественной опасности преступления в сфере компьютерной информации, причинившего имущественный ущерб, и преступлений против собственности с использованием цифровых технологий, а также об отдельных аспектах соучастия, моменте окончания преступления и пр.

Уголовно-процессуальное законодательство, находясь в тесной связи с уголовно-правовым, в вопросе определения статуса виртуального имущества, в ча-

[1] См.: Гражданское право в комментариях. Правовая природа виртуальных объектов, приобретаемых за реальные деньги // Вестник гражданского права. 2014. № 1. Т. 14. С. 148.

[2] См.: Решение Савеловского районного суда города Москвы от 9 июля 2018 г. по делу № 02-3433/2018. URL: http://forwardlegal.ru/posts/igry-prava-kak-zashchitit-virtualnoe-imushchestvo/; Решение Лефортовского районного суда города Москвы от 25 ноября 2011 г. по делу № 2-3379/2011. URL: http://forwardlegal.ru/posts/igry-prava-kak-zashchitit-virtualnoe-imushchestvo/ (дата обращения: 11 сентября 2019 г.).

стности, не может дать четкой регламентации о подследственности по месту преступления, причинившего ущерб правообладателю или потребителю цифрового контента.

Стремительно растущая значимость общественных отношений, связанных с оборотом виртуального имущества, гигантские обороты реальных конвертируемых денежных средств в анализируемой сфере позволяют с уверенностью говорить о том, что криминализация причинения имущественного ущерба правообладателям и потребителям цифрового контента является социально обусловленной. Вместе с тем широкий спектр проблем при защите указанных общественных отношений, рост преступлений, связанных с компьютерными или телекоммуникационными технологиями, трудности при их раскрытии свидетельствуют о необходимости совершенствования уголовно-правовых средств противодействия на законодательном, правоприменительном и доктринальном уровнях.

2.2. Особенности уголовно-правовой оценки преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента

Преступления, связанные с причинением имущественного ущерба правообладателям и потребителям цифрового контента, являются одним из видов преступлений в сфере информационно-телекоммуникационных технологий. В литературе по объектам преступлений также выделяют такие виды, как посягательства на информационную безопасность в широком смысле; преступления, причиняющие вред авторским правам в сфере программного обеспечения; а также общественно опасные деяния, причиняющие вред различным объектам уголовно-правовой охраны с помощью программно-технических средств и информационно-телекоммуникационных сетей[1].

Анализ выводов ученых, исследовавших вопросы правового статуса виртуальных ценностей, позволяет сделать вывод о следующем содержании цифрового контента в контексте многопользовательских онлайн-игр.

Цифровой контент в указанном смысле включает такие элементы:

– непосредственно саму многопользовательскую онлайн-игру;

– игровой аккаунт; игрового персонажа; игровую валюту;

– игровое имущество; игровые привилегии.

Во-первых, «ущерб» правообладателям цифрового контента в виде онлайн-игры может наступить в результате признания такой игры азартной. То есть обусловлен деятельностью государственных органов по обеспечению законности, в том числе и уголовно-правовыми средствами.

Понятие азартной игры формулируется в ст. 4 Федерального закона от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации». В частности, под азартной игрой закон устанавливает «основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным организатором азартной игры».

[1] См.: *Русскевич Е. А.* Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 76–77.

За незаконную организацию и проведение азартных игр предусмотрена административная (ст. 14.1.1.КоАП РФ) и уголовная ответственность (ст. 171.2 УК РФ). Однако изучив содержание диспозиций указанных составов, а также судебную практику, мы пришли к выводу о том, что использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», в рамках указанных составов предполагает не только отсутствие специального разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне либо лицензии на осуществление деятельности по организации и проведению азартных игр в букмекерских конторах и тотализаторах вне игорной зоны, но и использование игрового оборудования. Проведенный анализ 60 обвинительных приговоров по ст. 171.2 УК РФ с наличием признака «использование информационно-телекоммуникационных сетей, в том числе сети "Интернет"» показал, что ответственность в данном случае несут лица, которые, разместив персональные компьютеры, как правило, со специализированным программным обеспечением и доступом к сети «Интернет» в отдельном помещении, расположенном за пределами игорной зоны, извлекали доход от ставок, которые принимались от лиц, привлекаемых к игре в указанном помещении. По сути, рулетки, игровые автоматы и прочее оборудование в таких случаях было заменено на компьютеры, имеющие доступ к сайтам, на которых размещены азартные игры, либо компьютеры, оснащенные программным обеспечением, создающим виртуальную имитацию указанного оборудования, объединенные локальной сетью[1].

Однако в рамках диспозиции ч. 1 ст. 171.2 УК РФ «использование информационно-телекоммуникационных сетей, в том числе сети «Интернет» выступает в качестве альтернативного признака «использованию игрового оборудования вне игорной зоны». Этот вывод вытекает из грамматического толкования нормы. Законодатель установил разделительный союз «либо» между указанными признаками в диспозиции анализируемой нормы. К сожалению, разъяснений Верховного Суда Российской Федерации на счет возможности применения ст. 171.2 УК РФ при использовании информационно-телекоммуникационных сетей, в том числе сети «Интернет» без использования игрового оборудования вне игорной зоны нет. В связи с этим практика складывается, исходя из процессуальной необходимости полноты и достоверности собранных доказательств, которые более очевидны при наличии конкретного места преступления и специального оборудования.

Вместе с тем доступ к сайтам, где проводятся азартные онлайн-игры, может быть ограничен государственными органами при наличии нарушения требований Федерального закона от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации», а также Федерального закона от 11 ноября 2003 г. № 138-ФЗ «О лотереях».

[1] Приговор Приволжского районного суда города Казани Республики Татарстан по ч. 2 ст. 171.2 УК РФ № 1-292/2017. URL: http://www.sud-praktika.ru/precedent/544807.html (дата обращения: 11 сентября 2019 г.); Приговор Куйбышевского районного суда города Омска по ч. 1 ст. 171.2 УК РФ № 1-402/2017. URL: http://www.sud-praktika.ru/precedent/ 467243.html (дата обращения: 11 сентября 2019 г.); Приговор Дзержинского районного суда города Оренбурга по ч. 1 ст. 171.2 УК РФ № 1-334/2017. URL: http://www.sud-praktika.ru/precedent/422336.html (дата обращения: 8 сентября 2019 г.).

На официальном сайте Федеральной налоговой службы размещена характеристика азартных онлайн-игр, незаконно использующих цифровой контент. По информации ФНС России, «азартные игры и лотереи на указанных сайтах организуются и проводятся следующим образом:

– принимаются ставки на матчи киберспорта (аналогично ставкам в букмекерских конторах), розыгрыш осуществляется с использованием генератора случайных чисел, где выигрышем служит игровой инвентарь (например, оружие для онлайн игры counter-strike);

– баланс (игровой счет) пополняется с помощью популярных платежных систем;

– выигрыш выплачивается через начисление на личный счет игровых монет (виртуальная валюта сайта, которую можно конвертировать в денежные средства) и «скинов» (игровой инвентарь);

– выигрыш в виде игрового инвентаря автоматически поступает в личный кабинет (аккаунт) самой распространенной игровой платформы Steam (служит платформой для хранения и обмена игрового инвентаря);

– некоторые сайты позволяют игрокам обменять выигрыш (игровой инвентарь) на реальные деньги»[1].

В связи с нарушением законодательства, сайты, использующие цифровой контент в качестве азартной онлайн-игры, периодически ограничиваются в доступе.

Во-вторых, ущерб правообладателям цифрового контента в виде онлайн-игры может наступить в результате противоправных действий со стороны потребителей цифрового контента, которые в сети «Интернет» обозначаются такими терминами, как «читерство» и «ботоводство».

«Бот – это программа, в заданном пользователем или автоматическом режиме выполняющая ряд действий с помощью интерфейсов, обычно используемых людьми»[2]. Такая программа, имитируя партнеров сетевой игры, помогает в обход лицензионного соглашения с ее правообладателем, получать дополнительные привилегии, которые по лицензионному соглашению могут быть приобретены при условии либо больших объемов трудозатрат от игрока, либо его дополнительных материальных вложений.

Читерство, согласно описанию словаря синонимов, – это «жульничество, мошенничество, мухлеж»[3]. В сетевых онлайн-играх это явление выражается в получении преимущества в обход лицензионного соглашения с правообладателем цифрового контента посредством использования внешних программных средств и нестандартного аппаратного обеспечения.

Ответственность за причинение ущерба правообладателю цифрового контента такими способами может наступать за неправомерный доступ к компьютерной информации, за создание, использование и распространение вредоносных компьютерных программ, а также за нарушение авторских и смежных прав.

---

[1] За два месяца благодаря ФНС России ограничен доступ к шести сайтам, где проводят азартные игры с помощью игровых платформ. URL: https://www.nalog.ru/rn77/news/ activities_fts/6961054/ (дата обращения: 7 сентября 2019 г.).

[2] Энциклопедия интернет-маркетинга. URL: https://www.seonews.ru/glossary/bot/ (дата обращения: 5 сентября 2019 г.).

[3] См.: Словарь синонимов. URL: https://dic.academic.ru/dic.nsf/dic_synonims/ (дата обращения: 5 сентября 2019 г.).

В качестве иллюстрации такого преступного посягательства на цифровой контент можно привести следующий пример из судебной практики. Так, приговором Хорошевского районного суда города Москвы № 1-260/2014 от 17 июня 2014 г. по делу № 1-260/2014 гражданин Петров был осужден по ч. 2 ст. 272 УК РФ, ч. 2 ст. 146 УК РФ за деяние, выразившееся в неправомерном доступе к охраняемой законом компьютерной информации – онлайн-игре, в которой он разместил программу-бот, после чего незаконно создал ряд виртуальных ценностей внутри игры и реализовал их другим пользователям за реальные ликвидные денежные средства[1].

Если собственность правообладателя на онлайн-игру и ее правовая природа как вида цифрового контента не вызывает существенных споров, то относительно игрового аккаунта, игрового персонажа, игровой валюты, игрового имущества и игровых привилегий не все так однозначно.

Аккаунт, как и игрового персонажа, запрещено отчуждать большинством правил пользовательских соглашений. Однако даже платные премиальные или привилегированные аккаунты либо персонажи высокого уровня развития не представляют ценности без самих игровых привилегий перед другими игроками или виртуальных ценностей, размещенных внутри аккаунта. В связи с этим игровая валюта, игровое имущество и игровые привилегии – это как раз та часть цифрового контента онлайн-игр, которая является целью общественно вредного, а иногда общественно опасного посягательства. Вместе с тем, к сожалению, следует констатировать тот факт, что механизм уголовно-правового регулирования в настоящее время либо совсем не определяет противоправности таких деяний, либо, криминализировав отдельные способы завладения таким цифровым контентом, по своим средствам противодействия явно не соответствует характеру и степени общественной опасности посягательства.

Так, например, на наш взгляд, очевидно, что общественно опасные деяния, выраженные в предъявлении незаконного требования о передаче имущества под угрозой уничтожения, блокирования или хищения анализируемого цифрового контента, либо такие деяния, когда под воздействием угрозы потерпевшего вынуждают совершить или отказаться от совершения сделки, не обладают противоправностью, несмотря на определенное внешнее сходство с вымогательством (ст. 163 УК РФ) или принуждением к совершению сделки или к отказу от ее совершения (ст. 179 УК РФ). Обусловлено это отсутствием в рамках отмеченных составов преступлений способа, связанного с угрозой подобного характера в отношении цифрового контента, который в судебной практике не признается имуществом, а Гражданский кодекс РФ не уточняет его статуса.

Общественно опасными, на наш взгляд, но, к сожалению, непротивоправными в настоящий момент будут действия по легализации имущества и денежных средств, добытых преступным путем, через придание правомерного вида владения ими путем совершения сделок с «непризнанным» виртуальным имуществом.

В судебной практике, как мы уже отмечали, цифровой контент достаточно часто признается как часть игрового процесса, и суды не разрешают споры по

[1] Приговор Хорошевского районного суда города Москвы от 17 июня 2014 г. по делу № 1-260/2014. URL: https://sudact.ru/regular/doc/HFQ9r1760Arn (дата обращения: 6 сентября 2019 г.).

нему, но есть примеры из судебной практики, в рамках которых суд, рассмотрев гражданское дело, признавал виртуальное имущество в качестве услуги имущественного характера.

Речь идет об апелляционном определении Ленинского районного суда города Кемерово № 11-59/2013 от 26 апреля 2013 г. по делу № 11-59/2013[1] в рамках апелляционной жалобы на решение мирового судьи по гражданскому спору гражданина Мацукова Д. П. с ООО «Мэйл.РуГеймз», которую апелляционная инстанция удовлетворила. Изначально мировой суд отказал в удовлетворении исковых требований гражданина о взыскании с ответчика в пользу истца денег за блокировку его учетной записи, в связи с чем, Мацуков, по его мнению, не смог воспользоваться оплаченной услугой. Апелляционная судебная инстанция пришла к выводу о том, что решение мирового судьи необходимо отменить, так как рассматриваемая онлайн-игра не является азартной игрой или пари, в связи с этим положения гл. 58 ГК РФ, в том числе и ст. 1062 ГК РФ, по мнению суда, в данном случае применению не подлежат. Более того, удовлетворив иск Мацукова Д. П., суд признал, что приобретенные им виртуальные ценности в рамках онлайн-игры за дополнительные ликвидные деньги следует рассматривать как услугу имущественного характера.

Рассматривая случаи применения норм о цифровом контенте как услуге имущественного характера, можно сделать вывод, что данный виртуальный предмет в рамках уголовно-правовых отношений может выступать предметом взятки или коммерческого подкупа.

Рассматривая квалификацию хищения цифрового контента, причиняющего ущерб его пользователям, представляется целесообразным основываться на зарубежном опыте защиты законных интересов лиц в виртуальном пространстве и отечественном подходе к общественной опасности как к признаку преступления, связанному с возможностью причинения вреда охраняемым уголовным законом общественным отношениям или угрозой причинения такого вреда.

Говоря о зарубежном опыте в данном контексте, имеют в виду правовую концепцию так называемого «волшебного круга». Суть ее состоит в том, что если хищение предусмотрено правилами многопользовательской игры с использованием ресурсов, доступных в рамках пользовательского соглашения, то такое деяние при его квалификации не обладает общественной опасностью, то есть с точки зрения норм уголовного законодательства является малозначительным и не влечет никаких правовых последствий. Если же хищение цифрового контента связано с нарушением установленных пользовательским соглашением правил (взлом программного кода, незаконное завладение и использование чужих персональных данных и прочее), то такое деяние в зависимости от размера ущерба представляет общественную опасность и должно влечь уголовно-правовые последствия.

К сожалению, несмотря на то, что законодатель регламентировал правовую природу цифровых прав в ст. 141.1 ГК РФ, вступившей в силу 1 октября 2019 г., цифровой контент в рамках многопользовательских онлайн-игр до сих пор нельзя отнести к данной категории, так как цифровые права по смыслу ст. 141.1 ГК РФ

[1] Апелляционное определение Ленинского районного суда города Кемерово Кемеровской области от 26 апреля 2013 г. по делу № 11-59/2013. URL: https://sudact.ru/regular/doc/ uQ81NVpYhP1v/ (дата обращения: 7 сентября 2019 г.).

должны быть названы в таком качестве в отдельном федеральном законе, которого пока не существует.

В этой связи судебная практика при причинении ущерба правообладателям или пользователям цифрового контента не применяет нормы уголовного законодательства о защите отношений собственности. При хищении цифрового контента суды при наличии признаков составов преступлений вменяют ст. 272, 273, 274 УК РФ, которые направлены на защиту общественных отношений в сфере компьютерной информации[1]. Безусловно, исходя из предметного содержания умысла лиц, совершающих анализируемые посягательства, такое положение в корне неверно, так как основной непосредственный объект преступления определяется именно направленностью преступного умысла. Более того, незаконное изъятие и (или) обращение цифрового контента может происходить и без причинения вреда информационной безопасности, при воздействии на самого обвиняемого насилием или угрозой, при использовании его персональных данных, полученных без воздействия на программное обеспечение, при присвоении или растрате вверенного цифрового контента и пр.

Однако в связи с отсутствием на сегодняшний день правовой регламентации цифрового контента, которая бы позволяла без всяких сомнений отношения по поводу него отнести к отношениям собственности, применение норм уголовного законодательства, охраняющих компьютерную информацию, является наиболее обоснованным правоприменительным решением, позволяющим реализовывать задачи уголовного законодательства, указанные в ч. 1 ст. 2 УК РФ, без нарушения принципа законности, не допускающего применение уголовного закона по аналогии.

Цифровой контент многопользовательских онлайн-игр является разновидностью охраняемой законом компьютерной информации, следовательно, общие подходы при квалификации преступлений в сфере компьютерной информации при наличии их признаков будут распространяться и на преступления, связанные с воздействием на указанный цифровой контент.

Основным непосредственным объектом преступлений, предусмотренных ст. 272, 273 и 274 УК РФ, выступает безопасность компьютерной информации. При этом следует отметить, что с введением в УК РФ ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» в рамках главы 28 УК РФ расширился объект уголовно-правовой охраны. В качестве основного непосредственного объекта ст. 274.1 УК РФ выступает безопасность критической информационной инфраструктуры Российской Федерации.

Предметом ст. 272 и 273 УК РФ выступает компьютерная информация, определение которой сформулировано в примечании к ст. 272 УК РФ. При этом для ст. 273 УК РФ это компьютерная информация, которая достаточно часто бывает в форме вредоносной компьютерной программы, основное ее назначение должно быть связано с несанкционированным уничтожением, блокированием, модификацией, копированием компьютерной информации или нейтрализацией средств защиты компьютерной информации.

[1] См. Приложение 1.

Предметом ст. 274 УК РФ помимо компьютерной информации являются информационно-телекоммуникационные сети и оконечное оборудование.

Понятие информационно-телекоммуникационной сети Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ определяет следующим образом: «информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники».

Понятие оконечного оборудования регламентируется Федеральным законом «О связи» от 7 июля 2003 г. № 126-ФЗ, под ним закон предлагает понимать «технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей».

Предметом ст. 274.1 УК РФ выступает критическая информационная инфраструктура Российской Федерации. Понятие указанного предмета раскрывается в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ следующим образом: «критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». В том же законе указано, что «объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры».

Объективная сторона преступления, предусмотренного ч. 1 ст. 272 УК РФ характеризуется деянием в виде неправомерного доступа к охраняемой законом компьютерной информации, альтернативными последствиями в виде уничтожения, блокирования, модификации либо копирования информации, а также причинной связью между деянием и последствиями.

Неправомерным доступом будут являться действия лица, связанные с незаконным установлением контроля над охраняемой законом компьютерной информацией, в отношении которой были приняты меры защиты, ограничивающие перечень лиц, имеющих право ее использования. Следует отметить, что сам факт ознакомления с информацией без возможности ее уничтожения, блокирования, модификации или копирования не может рассматриваться в качестве доступа к ней.

Уничтожение информации – это результат воздействия на нее, выраженный в приведении ее в состояние, при котором она не может быть восстановлена или использована по назначению.

Блокирование информации – это результат воздействия на нее, выраженный в отсутствии возможности ее получения или использования по назначению при условии сохранности.

Модификация информации – это результат воздействия на нее, выраженный во внесении в нее изменений.

Копирование информации – это результат воздействия на нее, выраженный в получении хотя бы еще одного экземпляра и более информации той же формы и содержания. Следует отметить, что распечатка информации на принтере, ее ска-

нирование с экрана компьютера по смыслу ст. 272 УК не является признаком анализируемого преступления[1].

Объективная сторона преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется деянием в виде совершения хотя бы одного из перечисленных действий: 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.

Создание – это действия, результатом которых стало получение компьютерной программы или иной компьютерной информации, готовой к использованию в таком виде по указанному в диспозиции ст. 273 УК РФ назначению.

Распространение – это действия по предоставлению доступа к указанному в ст. 273 УК РФ предмету другому лицу на возмездной или безвозмездной основе.

Использование – это действие по целенаправленному извлечению свойств компьютерной программы или иной компьютерной информации, предназначенной для несанкционированного воздействия на компьютерную информацию, указанного в ст. 273 УК РФ.

Объективная сторона преступления, предусмотренного ст. 274 УК РФ, состоит из деяния в виде нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям; альтернативных последствий в виде уничтожения, блокирования, модификации либо копирования информации, а также крупного ущерба; причинной связью между деянием и последствиями.

Нарушение указанных правил может выражаться как в форме действия, так и бездействия. Важно установить, какое конкретное правило было нарушено. В связи с этим требуется применение специальных норм, определяющих требования к поведению лиц, в чьи полномочия входит эксплуатация средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также обеспечение доступа к информационно-телекоммуникационным сетям.

Статья 274.1 УК РФ отличается от иных статей, входящих в главу 28 УК РФ, тем, что в ч. 1, 2 и 3 данной статьи включены самостоятельные составы преступлений, объективная сторона которых содержит признаки, аналогичные ст. 272, 273 и 274 УК РФ.

Субъект в ч. 1, 2 ст. 272, ч. 1 ст. 273, ч. 1, 2 ст. 274.1 УК РФ общий – это физическое вменяемое лицо, достигшее 16 лет.

Субъект ст. 274, а также ч. 3 ст. 274.1 УК РФ специальный – это физическое вменяемое лицо, достигшее 16 лет, на котором лежит обязанность соблюдения указанных в данных нормах правил.

Субъект ч. 3, 4 ст. 272, ч. 2, 3 ст. 273, ч. 4, 5 ст. 274.1 УК РФ может быть как общим, так и специальным.

---

[1] См.: *Попов А. Н.* Преступления в сфере компьютерной информации: учеб. пособие. СПб.: С-Пб. юрид. ин-т (филиал) Университета прокуратуры РФ, 2018. С. 52.

Субъективная сторона ст. 273 и ч. 1 ст. 274.1 УК РФ характеризуется только умышленной формой вины. Субъективная сторона остальных преступлений, запрещенных нормами главы 28 УК РФ, может характеризоваться как умышленной, так и неосторожной формой вины.

Квалифицирующие признаки, которые содержатся в главе 28 УК РФ, выражаются в крупном ущербе, совершении деяния из корыстной заинтересованности, группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения. Кроме того, в качестве отягчающих признаков устанавливаются тяжкие последствия или угроза наступления таких тяжких последствий.

Крупный ущерб установлен в примечании к ст. 272 УК РФ и составляет сумму, превышающую один миллион рублей. Следует отметить, что данная сумма складывается не только из прямого ущерба, но и из упущенной выгоды.

Оценочный признак, характеризующийся как тяжкие последствия, определяется в каждом конкретном случае судом. Это может быть особо крупный материальный ущерб, большое количество потерпевших, вынужденное прекращение деятельности юридического лица, гибель человека или причинение ему тяжкого вреда здоровью, аварии, катастрофы и прочее.

Так, например, приговором Коминтерновского районного суда города Воронежа № 1-302/2017 от 3 мая 2017 г. Стуков С. А. был осужден по ч. 3 ст. 273 УК РФ за создание, использование и распространение вредоносных компьютерных программ, повлекших тяжкие последствия. В качестве таковых были установлены особо крупный размер ущерба, обусловленный массовым использованием в сети автозаправочных комплексов ОАО «Воронежнефтепродукт» вредоносного программного обеспечения, предназначенного для недолива топлива клиентам и его бесконтрольной реализации. Сумма ущерба составила не менее 150 млн рублей[1].

Проведя анализ общей характеристики объективных и субъективных признаков преступлений, составляющих главу 28 УК РФ, перейдем к соотношению составов преступлений в сфере компьютерной информации между собой, а также с иными составами преступлений.

При создании вредоносной компьютерной программы и ее дальнейшем использовании для получения доступа к охраняемой законом компьютерной информации, в том числе цифрового контента многопользовательских онлайн-игр, при наступлении последствий, предусмотренных ст. 272 УК РФ, следует вменять совокупности ст. 272 УК РФ и ст. 273 УК РФ, поскольку признаки их объективной стороны носят самостоятельный характер.

Неправомерный доступ к компьютерной информации, которая содержалась в личных сообщениях потерпевших, при условии уничтожения, блокирования, модификации или копирования этой информации, должен квалифицироваться не только по ст. 272 УК РФ, но и по ст. 138 УК РФ, которая направлена на защиту конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

[1] Приговор Коминтерновского районного суда города Воронежа от 3 мая 2017 г. № 1-302/2017 URL: http://www.sud-praktika.ru/precedent/421591.html (дата обращения: 2 сентября 2019 г.).

Аналогично должен решаться вопрос при неправомерном доступе к государственной, коммерческой, налоговой или банковской тайне с помощью программных средств. При наличии признаков данное деяние должно квалифицироваться по совокупности ст. 272 и 275 либо 276 УК РФ, а также ст. 272 и 183 УК РФ.

Ранее мы уже рассматривали пример с посягательством на цифровой контент многопользовательской ролевой игры, в рамках которого нарушалось авторское право посредством модификации авторского программного продукта против воли автора. В таких случаях деяние следует квалифицировать по совокупности преступлений, предусмотренных ст. 272 и, соответственно, 146 УК РФ.

В постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении или растрате» разъяснено, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ[1]. При этом следует отметить, во-первых, что для вменения совокупности ст. 159.6 УК РФ со ст. 272 УК РФ требуется не только наличие неправомерного доступа, но и наступивших в результате этого деяния последствий, указанных в ст. 272 УК РФ. Во-вторых, следует обратить внимание на некое противоречие, которое состоит в том, что в одном случае по отношению к использованию поддельного другим лицом официального документа высшая судебная инстанция разъясняет, что это является способом мошенничества, который не требует дополнительной квалификации по ст. 327 УК РФ и полностью охватывается мошенничеством. В другом случае в этом же постановлении суд отмечает необходимость вменения совокупности ст. 273 УК РФ и 159.6 УК РФ при использовании вредоносной компьютерной программы в рамках специального вида мошенничества.

Разъяснения суда об отсутствии признаков ст. 159.6 УК РФ при введении персональных данных, логинов, паролей, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Данное деяние, по мнению высшей судебной инстанции, должно квалифицироваться как кража. В этой связи использование вредоносной программы, обеспечившей доступ к персональным данным, позволившее их скопировать, а впоследствии использовать при введении для авторизации и хищения денежных средств, следует квалифицировать по совокупности ст. 158, 272 и 273 УК РФ.

Проведя соотношение преступлений в сфере компьютерной информации между собой и с иными составами преступлений, проанализируем существующие особенности уголовно-правовой оценки места совершаемого преступления. Место преступления в уголовно-правовом аспекте влияет на квалификацию преступления. Так, например, азартные игры запрещены вне игорной зоны. В связи с этим может возникнуть вопрос уголовно-правового значения, влияющий на оценку признаков преступления, предусмотренного ст. 171.2 УК РФ: как квалифицировать деяние, если игровой процесс организован вне игорной зоны, а сервер, на котором распо-

[1] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». URL: https://www.garant.ru/products/ipo/prime/doc/71723288/.

ложена игра, находится в рамках игровой зоны, или же наоборот? Вопрос о месте преступления имеет и очень важное уголовно-процессуальное значение, связанное с определением территориального расположения органа, который будет осуществлять проведение предварительного расследования.

Следует отметить, что место в уголовно-правовом значении и место в уголовно-процессуальном значении могут не совпадать. В этом нет ничего удивительного, так как иные признаки состава преступления также могут иметь процессуальное значение, отличающееся от уголовно-правового. Так, например, «потерпевшим» в уголовно-правовом смысле по п. «в» ч. 2 ст. 105 УК РФ «Убийство малолетнего» будет сам потерпевший – лицо, которое для виновного заведомо не достигло 14 лет. Вместе с тем «потерпевшим» в процессуальном значении в данном случае будет выступать законный представитель убитого.

Место в уголовно-правовом значении напрямую не определено нормами уголовного законодательства. Однако многие ученые предлагают определять этот признак состава преступления через «время совершения преступления», которое определено в ч. 2 ст. 9 УК РФ, где указывается, что под ним понимается «время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий». При этом нельзя отождествлять «время совершения преступления» и «время окончания преступления». В свою очередь «время окончания преступления» можно условно поделить на «юридический» и «фактический» моменты. Какого же уголовно-правовое значение такого разграничения времени преступления?

«Время совершения преступления» является началом исчисления сроков давности по преступлению; возраст субъекта определяется на момент совершения деяния, а не наступившего последствия, даже если это последствие является обязательным признаком; возраст потерпевшего определяется на момент совершения преступления и пр. Другими словами «время совершения преступления» – это момент, который определяет оценку объективных и субъективных признаков состава преступления.

«Юридический момент окончания преступления» – это момент, влияющий на оценку этапа развития преступного посягательства. В зависимости от конструкции состава преступления этот момент может быть связан с совершением деяния (ст. 273 УК РФ) или же наступления последствий (ст. 272 УК РФ). Существуют особенности оценки момента окончания преступления в единичных сложных составах, таких как продолжаемое и длящееся преступление.

«Фактический момент окончания преступления» влияет на определение условий правомерности необходимой обороны, крайней необходимости, на особенности квалификации при фактических ошибках и пр.

Возвращаясь к вопросу о месте совершения преступления в сфере компьютерной информации в уголовно-правовом значении, следует отметить, что это место, где выполняется деяние, независимо от места наступления общественно опасных последствий, а также размещения орудий и средств преступления. В этой связи ответим на поставленный ранее вопрос об игорной зоне. Если организация и (или) проведение азартных игр с использованием сети «Интернет» осуществляется вне игорной зоны, а сервер, на котором находится игра, – внутри нее, то местом совершения преступления (территория за пределами игорной зо-

ны) будет место действий, направленных на организацию и (или) проведение азартных игр с использованием сети «Интернет». Таким образом, местом преступления в таком случае может быть даже исправительная колония. Следует отметить, что в уголовно-правовом значении при соучастии местом совершения преступления будет место совершения деяния исполнителем. Если речь идет о соисполнительстве, то местом будет та территория, где осуществлена большая часть общественно опасного деяния.

Уголовно-процессуальное значение места совершения преступления, в отличие от уголовно-правового, будет состоять в том, что в качестве места будет рассматриваться территория, на которой преступление окончено. В уголовном процессе есть исключения из данного правила, которые связаны с обеспечением эффективного судопроизводства. В этом смысле предварительное расследование может проводиться по месту нахождения обвиняемого или большинства свидетелей.

Подводя итог исследованию вопросов квалификации преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента, сделаем вывод о том, что развитие общественных отношений, связанных с оборотом виртуального имущества, породившее большое количество неразрешенных вопросов правоприменения, носящих межотраслевой характер, свидетельствует о необходимости комплексного совершенствования правовых средств защиты указанных общественных отношений.

Глава 3. Особенности расследования преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента

3.1. Особенности предмета доказывания и производства проверочных действий по преступлениям, связанным с причинением имущественного ущерба правообладателям и потребителям цифрового контента

Значительная часть противоправных действий в сети «Интернет» направлена на хищение «виртуального имущества», хранящегося на игровых аккаунтах пользователей. Появление имущества, которое можно облачить в реальные денежные средства, вызывает интерес у преступников, поскольку такие ценности возможно похитить. Данное имущество предоставляется различными способами правообладателем (владельцем, создателем) онлайн-игр потребителю, то есть игроку.

Чаще всего владельцы онлайн-игр получают основной доход следующими способами:

– абонентская плата игроков за использование онлайн-игры;

– продажа лицензированного программного обеспечения (онлайн-игры);

– продажа «виртуального имущества», предметов, недвижимости, иных услуг, предоставляемых игроку правообладателем (собственником программного обеспечения).

Юридически такие правоотношения регулируются пользовательским соглашением, заключаемым между правообладателем и потребителем цифрового контента. После приобретения имущества оно переходит в собственность потребите-

ля цифрового контента (игрока). Аналогия с правом собственности «виртуального имущества» потребителя цифрового контента пока остается условным сравнением, поскольку отношения между пользователями никак не урегулированы ни договором (пользователи между собой договором не связаны), ни законом. Как отмечалось выше, действующее законодательство, в том числе Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», также не содержит определений терминов «виртуальное имущество», «виртуальная собственность».

Проанализировав ряд мнений современных авторов, И. В. Новиков приходит к выводу, что «единообразного мнения по поводу квалификации правовой природы виртуальной собственности на сегодняшний момент не существует»[1].

Изучив работы данного автора и соглашаясь с его мнением, приведем описание исследуемого термина, данное на страницах онлайн-словарей сети «Интернет». «Виртуальная собственность – информационный объект, права на который принадлежат одному или нескольким владельцам. Установление права владения и распоряжения виртуальной собственностью возможно двумя путями: при создании информационного объекта (авторское право или интеллектуальная собственность); при передаче (в письменном виде, с заключением соответствующего договора или при согласии пользователя с пользовательским соглашением) права владения и распоряжения на весь информационный объект или его часть, от создателя (автора) покупателю (пользователю). Также возможен вариант передачи такого права способом предоставления сертификата на владение информационным объектом или его частью»[2].

Между тем законодательные изменения в этой области имеются. В частности с 1 октября 2019 г. в главе 6 ГК РФ вводится новая норма (ст. 141), определяющая понятие «цифровые права», которая, как мы надеемся, позволит регулировать гражданско-правовые, а в дальнейшем и уголовно-правовые отношения в области информационных систем. Рассматривая порядок производства проверочных действий по преступлениям, связанным с хищением виртуального имущества игроков в онлайн-играх, мы не беремся соотносить понятие «цифровые права» с виртуальным имуществом и давать правовую оценку этим терминам.

Следует различать характер действий злоумышленника в отношении виртуального имущества. Например, если в процессе онлайн-игры у «персонажа» был похищен его меч или любое другое приобретенное за реальные денежные средства имущество, а ограбление было запланировано сценарием (правилами) игры, то вопрос о хищении здесь не возникает. Однако в случае взлома аккаунта пользователя и хищения его виртуального имущества, это действие, безусловно, можно оценивать в качестве противоправного. При характеристике такого действия в качестве деликта придется, доказывать, что оно причинило вред имуществу потребителя цифрового контента. В данной ситуации имеет место причинение вреда потребителю «виртуального имущества» путем его хищения с помощью доступа к его аккаунту тем или иным способом. Для достижения аналогичного ре-

[1] *Новиков И. В.* Виртуальная собственность: перспективы регулирования // Вопросы российской юстиции. 2019. № 1. URL: http://injust-journal.ru/wp-content/uploads/2019/04/12.00.00 (дата обращения: 1 сентября 2019 г.).

[2] Карта слов и выражений русского языка. URL: https://kartaslov.ru (дата обращения: 1 сентября 2019 г.).

зультата игроку придется снова потратить время, реальные денежные средства. Предметом преступного посягательства будет выступать «виртуальное имущество», которое, по сути, можно перепродать за реальные деньги.

Судебная практика в области разрешения гражданских споров между пользователями онлайн-игр складывается пока не в пользу пострадавшего. Так, Президиум Московского городского Суда РФ, ссылаясь на ст. 1062 ГК РФ, в своем постановлении[1] указал, что «анализ возникших между сторонами правоотношений приведенных выше требований Закона, условий пользовательского соглашения позволяет сделать вывод о том, что наличие либо отсутствие в действиях пользователя нарушения правил игры относится к организации игрового процесса, а поэтому заявленные Путиловым И. А. требования как связанные с участием в игре в силу п. 1 ст. 1062 ГК РФ судебной защите не подлежат». Связано это с тем, что отношения, возникающие в онлайн-играх по поводу виртуального имущества, которое имеет денежную оценку, не охватываются существующей законодательной базой в области игр и пари. Следовательно, отсутствуют и формальные основания для применения к ним положений гл. 58 ГК РФ, что приводит к сложностям при отнесении последствий таких хищений к имущественному ущербу и привлечению к иным видам ответственности (за кражу имущества). Однако с учетом достижений прогресса и разрастания преступной деятельности в информационных сферах такое правовое решение назрело.

Как указывает А. И. Савельев, «право должно быть достаточно эффективным, чтобы пресекать возможные злоупотребления, совершаемые под прикрытием такого игрового процесса, особенно когда речь идет об объектах, пусть и виртуальных, но обладающих реальной рыночной ценностью, а также об отношениях, которые составляют часть реальной жизни реальных людей»[2].

Общепринятое толкование норм уголовного права предметом имущественных преступлений определяет вещь, предмет материального мира, которому нанесен вред вследствие противоправных деяний со стороны преступника. Однако положения гл. 28 УК РФ предусматривают ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации. Следовательно, в правоприменительной практике в качестве предмета преступного посягательства рассматривается что-то нематериальное, такое как компьютерная программа или компьютерная информация.

Если для хищения виртуального имущества используются вредоносные программы или неправомерный доступ к игровому серверу (к примеру, кража пароля от игрового персонажа), то в современных реалиях отсутствия уголовно-правовой регламентации противоправных отношений с виртуальным имуществом такое деяние подпадает только под признаки состава преступления, предусмотренного ст. 272 УК РФ. Если аккаунт был взломан (неправомерный доступ был осуществлен) с помощью вируса, то есть с использованием вредоносных

[1] Постановление Президиума Московского городского суда РФ. URL: http://of-law.ru/grazhdanskij-protsess/postanovleniya-suda-po-grazhdanskim-delam/ (дата обращения: 1 сентября 2019 г.).

[2] *Савельев А. И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. URL: http://of-law.ru/stati/pravovaya-priroda-virtualnykh-ob-ektov-priobretaemykh-za-realnye-dengi-v-mnogopolzovatelskikh-igrakh.html (дата обращения: 20 ноября 2019 г.).

компьютерных программ, то в том числе такие действия квалифицируются по ст. 273 УК РФ. На практике рассматриваемым преступным действиям дается правовая оценка по совокупности преступлений. Так, действия, связанные с хищением виртуального имущества, квалифицируются в Следственной части ГСУ ГУ МВД России по Свердловской области в том числе по п. «г» ч. 3 ст. 158 УК РФ. В некоторых случаях, если преступные действия связаны с хищением чужого имущества или приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, – по ст. 159.6 УК РФ.

Неправомерный доступ к компьютерной информации – это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации[1].

В рамках рассматриваемых нами противоправных действий неправомерный доступ (по-простому взлом цифрового аккаунта), по сути, является способом совершения нового вида хищений – кражи «виртуального имущества» потребителя цифрового контента. Под данным имуществом имеется ввиду объект, законные права на который принадлежат одному или нескольким владельцам.

Можно выделить два способа совершения противоправных действий, встречающихся в сфере взлома игровых аккаунтов путем неправомерного доступа к компьютерной информации.

1. Хищение аккаунтов, на которых не числилось ценное имущество и не были вложены реальные деньги, скажем так, из хулиганских побуждений.

2. Хищение аккаунтов, на балансе которых находились ценные вещи, которые были приобретены путем траты большого количества времени (путем игрового прогресса) или путем вложения на баланс игры реальных денег с целью получения материальной выгоды.

Учитывая особенность следственных ситуаций по хищению «виртуального имущества» пользователей онлайн-игр следует разобраться с предметом доказывания по данным преступлениям.

Предмет доказывания представляет собой совокупность обстоятельств, подлежащих установлению по уголовному делу с целью решения задач уголовного судопроизводства. Любое входящее в предмет доказывания обстоятельство имеет свое собственное уголовно-правовое или уголовно-процессуальное значение. Каждое из них в той или иной степени определяет исход уголовного дела. Так, некоторые элементы предмета доказывания влияют на признание лица виновным в совершении преступления или на его освобождение от уголовного преследования. Другие позволяют правильно квалифицировать содеянное деяние. Третьи обусловливают характер и размер назначаемого уголовного наказания и т. д.

В частности, полагаем возможным выделить следующие обстоятельства, подлежащие установлению по преступлениям, предусмотренным ст. 272 УК РФ, цель которых связана с хищением «виртуального имущества» потребителей цифрового контента в сети «Интернет»: факт доступа к компьютерной информации;

[1] См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генпрокуратурой России. URL: http://www.consultant.ru.

неправомерность доступа к этой информации (нормы закона, охраняющего компьютерную информацию (конкретная статья, часть, пункт); сведения о правообладателе, пользователе этой информации; место неправомерного доступа к компьютерной информации, которое включает местонахождение информации, подвергшейся нападению, и место, откуда осуществлялась компьютерная атака (они могут совпадать или различаться); время неправомерного доступа и вредных последствий от противоправных действий по хищению «виртуального имущества»; орудия преступления, с помощью которых был осуществлен взлом аккаунта. Такими орудиями могут выступать: персональный компьютер, планшеты, смартфоны, носители компьютерной информации, а также программное обеспечение, которые использовались субъектом для неправомерного доступа; способ совершения неправомерного доступа и хищения «виртуального имущества» пользователя цифрового аккаунта; способ воздействия на компьютерную информацию (уничтожение, блокирование, модификация, копирование); вредные последствия неправомерного доступа, их оценка правообладателем и потребителем цифрового контента; характер и размер вреда, причиненного преступлением; субъект неправомерного доступа и хищения «виртуального имущества»; если преступные действия совершены в соучастии, то виновность каждого субъекта преступления, форма вины, мотивы и цели; характеристика обстановки совершения преступления и другие обстоятельства, предусмотренные ст. 73 УПК РФ.

При расследовании создания, использования и распространения вредоносных компьютерных программ устанавливаются обстоятельства доказывающие факты и способы создания, использования вредоносной компьютерной программы либо иной вредоносной компьютерной информации (внесение изменений в существующую программу). Характер воздействия вредоносной программы на компьютерную информацию (уничтожение, блокирование, модификация, копирование, нейтрализация средств защиты компьютерной информации); последствия, причиненные преступлением, их оценка правообладателем компьютерной информации, характер и размер вреда, наступление тяжких последствий; сведения о правообладателе похищенного имущества и потребителе цифрового контента и т. д.

Поводом для возбуждения уголовного дела выступают сообщения граждан (заявление пострадавшего) о взломе аккаунта и краже виртуального имущества. Источниками сообщения в данном случае выступают активные пользователи сети «Интернет», потребители цифрового контента (владельцы аккаунта), геймеры, виртуальное имущество которых похищено. Чаще всего это лица мужского пола в возрасте до 35 лет.

Рассматривая следственную ситуацию, при которой причинен ущерб от хищения «виртуального имущества», следует выделить определенный алгоритм первоначальных проверочных действий[1]:

– необходимо изъять документы, подтверждающие принадлежность аккаунта заявителю. Потребитель цифрового контента (владелец аккаунта) обычно имеет подтверждающие данные о его принадлежности. С учетом изменений в гражданском законодательстве, следует установить, имелись ли у лица цифровые права на пользование аккаунтом, его содержимым в рамках приобретенной онлайн-

[1] См. Приложение 2.

игры. Обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность распоряжаться этим правом (ст. 141.1 ГК РФ);

– выяснить какой вред был причинен заявителю, то есть какое виртуальное имущество было похищено, на какую сумму, истребовать данные, подтверждающие перевод денежных средств на свой аккаунт;

– далее следует получить объяснение с пострадавшего (владельца аккаунта). Он должен дать подробное описание произошедшего и предоставить всю имеющуюся информацию правоохранительным органам (сайт, который предоставляет услуги к игровым ценностям, свой логин, возможно, номер карты и банковские выписки, с которых происходило пополнение интернет-кошелька и т. д.). Данная информация будет необходима для обращения в техническую поддержку или официальное представительство правообладателя цифрового контента;

– далее необходимо направить запрос в компании, предоставляющие услуги сети «Интернет» (оператор связи) и по пользованию онлайн-игрой (владельцу онлайн-игры). В таком запросе необходимо отразить всю известную информацию, для того чтобы получить список IP-адресов, с которых был осуществлен вход в аккаунт потерпевшего. Стоит учитывать, что многие компании хранят истории обмена между пользователями, что так же позволит отследить, куда и кому было передано похищенное имущество и в дальнейшем установить IP-адреса;

– полученные IP-адреса необходимо направить провайдеру, который предоставит информацию об их владельцах (адрес регистрации, ФИО, дата рождения и т. п.); Взаимодействие с оператором связи требуется, чтобы получить информацию о работе пользователя в сети, его трафике;

– необходимо направить поручение органу дознания о производстве оперативно-разыскных мероприятий с целью установления местонахождения заподозренного лица;

– провести осмотр места происшествия. Сложность проведения данного следственного действия вызвана проблемностью определения мест, в которых располагался злоумышленник, если подключался к динамичному IP-адресу.

Необходимо помнить о том, что преступники для осуществления своей незаконной деятельности могут использовать различные методы и способы для затруднения их обнаружения. Например, использование VPN (это технология, которая обеспечивает зашифрованное соединение поверх интернет-соединения), которое значительно затрудняет, а порой и вовсе делает невозможным производство расследования по уголовному делу.

Если место совершения преступления определить на данном этапе не представляется возможным, то целесообразно осмотреть место жительства заявителя, его рабочее место, провести осмотр предметов и документов, в том числе электронных носителей информации, электронных документов, электронных сообщений, сайта или страницы в сети «Интернет». Производство осмотра целесообразно проводить с участием специалиста.

Для принятия решения о возбуждении уголовного дела должностное лицо, осуществляющее проверку сообщения совместно с оперативными службами, должно изучить достаточное количество справочной литературы, знать основные

нормативные акты федерального и ведомственного уровня. Здесь особое значение имеет взаимодействие с узкими специалистами для получения информации технического характера. Оказать помощь следователю в данной ситуации могут любые лица, обладающие необходимыми знаниями и опытом для дачи консультаций по делу. Это квалифицированные сотрудники различных организаций, осуществляющих свою деятельность в сфере информации, информатизации и защиты информации.

Можно выделить несколько подразделений и служб, оказывающих содействие в раскрытии такого рода преступлений:

– Федеральные службы по техническому и экспортному контролю;

– центры защиты информации;

– оперативно-технические подразделения правоохранительных органов;

– подразделения «К» при БСТМ МВД России (Бюро специальных технических мероприятий – подразделение МВД России, одним из направлений деятельности которого является борьба с преступлениями в сфере компьютерных технологий);

– специалисты межрегиональных Центров защиты информации, функционирующих на базе гражданских высших учебных технических заведений;

– научные работники исследовательских институтов и лабораторий, а также учебных заведений.

Решение о возбуждении уголовного дела принимается не только на основании материалов предварительных проверок заявлений потерпевших, организаций и должностных лиц, но и, как указывалось выше, по материалам органов, осуществляющих оперативно-разыскную деятельность при реализации оперативных разработок, результатов оперативно-разыскных мероприятий по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших. Выявлением, предупреждением, пресечением и раскрытием преступлений в сфере компьютерной информации занимается Управление «К» МВД России в пределах своей компетенции.

В соответствии со ст. 11 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» ее результаты могут служить поводом и основанием для возбуждения уголовного дела и использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

В материалах проверки также могут быть и иные документы, предоставляемые по результатам оперативно-разыскных мероприятий (далее – ОРМ), такие как:

– постановление о предоставлении результатов ОРД следователю;

– постановление о рассекречивании этих материалов;

– протоколы ОРМ (оперативного наблюдения, проверочной закупки при распространении носителей с вредоносными компьютерными программами, оперативного эксперимента, снятия информации с технических каналов связи и т. д.);

– стенограммы прослушивания телефонных переговоров и иных сообщений по преступлениям средней тяжести, тяжким и особо тяжким, детализации телефонных соединений абонентов, с обязательным получением судебного решения;

– протоколы об изъятии образцов для сравнительного исследования с участием специалистов;

– протоколы (акты) изъятия компьютерной техники и электронных носителей информации;

– справки об исследовании компьютерной техники и иных видов необходимых первоначальных исследований и другие материалы, в зависимости от каждой конкретной ситуации.

Результаты оперативно-разыскных мероприятий, ревизий, документальных и иных проверок, включая рапорт сотрудника, выявившего преступление, регистрируются в дежурной части и передаются в следственное подразделение с сопроводительным письмом о передаче материалов проверки от имени начальника органа дознания (руководителя оперативного подразделения). Процедура передачи материалов, полученных оперативным путем, предусмотрена инструкцией, утвержденной в соответствии с приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г. «Об утверждении Инструкции о порядке представления результатов оперативно-разыскной деятельности органу дознания, следователю или в суд». Одним из эффективных способов раскрытия преступлений, связанных с хищением виртуального имущества, на наш взгляд, может быть такое оперативно-разыскное мероприятие как «снятие информации с технических каналов связи» и дальнейшее исследование сетевого трафика.

Как указывает Н. Н. Федотов, в российской судебной практике трафик (результаты его экспертизы) почти не использовался в качестве доказательства. Между тем снифинг – перехват и анализ трафика, является основой чуть ли не половины всех методов совершения преступлений.

Анализируя содержимое, а также статистику сетевого трафика, можно определить и доказать совершение пользователем многих действий в Сети, а также получить информацию об устройстве программ, информационных систем и сетей. Сбор и анализ сетевого трафика определенного компьютера может заменить изъятие и экспертизу самого компьютера, поскольку даст такую же информацию, а именно: содержимое электронной почты; свидетельства о просмотре веб-сайтов, размещении информации в Сети, несанкционированном доступе к удаленным узлам, использовании контрафактных программ. И в то же время перехватить трафик бывает проще, чем найти и изъять в исправном состоянии компьютер[1].

Стоит учитывать, что злоумышленник может находиться в другом городе или даже стране, поэтому необходимо международное сотрудничество в рамках запроса или поручения о правовой помощи, которое на стадии возбуждения уголовного дела направляется через Интерпол.

[1] См.: *Федотов Н. Н.* Форензика – компьютерная криминалистика. М.: Onebook.ru, 2012. URL: http://padabum.com/x.php?id=21178 (дата обращения: 2 сентября 2019 г.).

3.2. Особенности производства следственных действий по преступлениям, связанным с причинением имущественного ущерба правообладателям и потребителям цифрового контента

На этапе возбуждения уголовного дела алгоритм расследования и производства следственных действий для различных видов компьютерного пиратства схож. Существует ряд следственных и иных действий, которые служат основой для производства расследования.

Если уголовное дело возбуждено по факту совершения преступления, то первоочередной и самой трудной задачей для следователя будет установление личности преступника, так как все его незаконные действия происходят дистанционно и зачастую анонимно. Для установления личности необходимо собрать определенную доказательную базу (зафиксировать преступный факт, а именно сделать скриншоты, которые следует приобщить к материалам уголовного дела); определить IP-адрес сайта, на котором расположен запрещенный контент. Данную информацию возможно получить путем использования сторонних интернет-сервисов (например utrace) или компьютерных программ, посредствам поручения о производстве ОРМ либо в рамках экспертных исследований.

При помощи различных технических средств и программного обеспечения через запрос провайдеру устанавливается IP-адрес, с которого осуществлялись противоправные действия.

После того как зафиксирован факт преступления и известен IP-адрес, рекомендуется направить запрос интернет-провайдеру о предоставлении следующих данных: ФИО, адрес, паспортные данные, MAC адрес (уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым интерфейсам в компьютерных сетях «Интернет») устройства.

Получение сведений о принадлежности IP-адреса оформляется рапортом оперуполномоченного; сведения из базы данных регистратора приводятся прямо в тексте рапорта.

По установленному IP-адресу следует установить использующий его компьютер и местоположение этого компьютера. Как правило, порядок действий таков:

– (Преступление)
– (IP-адрес)
– (компьютер)
– (человек)

Принадлежность IP-адреса к конкретному компьютеру должна подтверждаться судебной компьютерно-технической экспертизой этого компьютера.

Также необходимо допросить сотрудника оператора связи, через которого происходит доступ в сеть «Интернет», чтобы подтвердить принадлежность IP-адреса конкретному компьютеру.

Получив необходимую информацию, следует решить вопрос о необходимости производства обыска по месту нахождения компьютерной техники либо подозреваемого. Если таким местом является жилое помещение, необходимо возбудить ходатайство перед судом о производства обыска в жилище, о чем вынести мотивированное постановление. Перед производством обыска стоит определить круг

участников следственного действия, в числе которых требуется обязательное участие специалиста и понятых. При производстве обыска необходимо изъять следы пальцев рук с клавиатуры и компьютерной мыши. Далее в протоколе обыска производится опись всей компьютерной техники, периферийных устройств, внешних носителей. Изымается компьютер или ноутбук, внешние носители, которые могут содержать необходимую для расследования информацию (пиратский контент), а также устройство с MAC-адресом (который мы ранее узнали от провайдера), обычно это роутер.

Электронные носители изымаются только с участием специалиста и понятых. Данные требования и порядок изъятия содержатся в ст. 164.1 УПК РФ. Специалист в присутствии понятых может осуществить копирование информации с изымаемых электронных носителей на другие, если об этом ходатайствует владелец электронных носителей. Другие носители информации могут быть предоставлены специалисту владельцем изымаемых носителей или обладателем содержащейся на них информации.

Необходимо произвести осмотр изъятых предметов (в данном случае компьютера, внешних накопительных устройств), в ходе которого описываются интересующие нас файлы (фото, видео, программы и т. п.) поисковая история браузеров. При осмотре содержимого компьютерной техники следует уделять внимание отысканию следов действий пользователя, так называемых лог-файлов. Определить все эти места и указать, к кому именно следует обращаться за соответствующими логами, – это задача для ИТ-специалиста. Даже самый «продвинутый» следователь не в состоянии его заменить. Поэтому привлечение специалиста в таких случаях обязательно.

Чтобы узнать о действиях злоумышленника, получить какие-либо данные о нем при помощи логов, необходимо установить:

- компьютеры и их программы, вовлеченные во взаимодействие;
- события, которые логируются в каждой из вовлеченных программ;
- получить все указанные логи за соответствующие промежутки времени;
- исследовать записи этих логов, сопоставить их друг с другом[1].

Целесообразно осмотреть содержимое электронного почтового ящика подозреваемого. Установить адресатов и содержание интересующей нас переписки. При прохождении сообщения от отправителя к получателю остаются следующие основные следы: копия сообщения на компьютере отправителя; запись в логе каждой MTA (MultiTheftAuto – является модификацией для PC версий игры, с помощью которой игроки могут играть между собой в режиме онлайн); копия сообщения на компьютере получателя с добавленными по пути заголовками.

После изъятия компьютерной техники необходимо собрать доказательства, указывающие, что этой техникой в определенное время пользовался подозреваемый. При установлении и задержании подозреваемого, производится его допрос. При подготовке к допросу необходимо:

– изучить материалы дела, определить очередность проведения допросов;

– предварительно изучить личность допрашиваемого лица;

– получить консультацию специалиста и составить план допроса.

[1] См.: *Федотов Н. Н.* Указ. соч.

Для выбора тактики допроса и определения круга вопросов, следует получить сведения о лице по месту жительства, учебы, работы, досуга.

Расследование данного вида преступлений сопряжено с необходимостью использования специальной терминологии. Такая спецлексика, зачастую не вполне понятна следователю, но абсолютно ясна допрашиваемому. В связи с этим следователю целесообразно проконсультироваться со специалистом, предварительно согласовав с ним формулировки вопросов, подлежащих выяснению, либо пригласить его для участия в следственном действии.

Обычно у специалиста выясняются следующие вопросы: предмет преступного посягательства, ценность компьютерной информации; принцип осуществления неправомерного доступа к компьютерной информации; воздействие, которое было оказано на компьютерную информацию – уничтожение, блокирование, модификация, копирование; последствия неправомерных действий; возможность совершения преступления в одиночку или только в группе; возможные технические способы хищения виртуального имущества пользователей контента и др.

Специалист, ознакомившись с имеющейся у следователя информацией, может дать собственный ответ, конечно же, с определенной долей вероятности. С другой стороны, следователю может потребоваться помощь специалистов в других отраслях знаний, чтобы понять цель преступного воздействия на компьютерную информацию, оценить ее значимость и др. Еще на стадии подготовки допроса следователь должен определить уровень компетентности подозреваемого в области информационных технологий. Эта характеристика будет основополагающей в выборе тактики допроса, в частности, при определении необходимости приглашения к участию в допросе специалиста.

В ходе проведения допросов подозреваемых, обвиняемых по уголовным делам о преступлениях в сфере компьютерной информации и высоких технологий следует выяснить ряд обстоятельств.

Обстоятельства общего характера:

– где и кем (в какой должности) работало допрашиваемое лицо;

– состоит ли на учете у нарколога, психиатра, имеет ли травмы головы;

– какое имеет образование, специальности, дипломы;

– наличие профессиональных навыков и опыта работы с компьютерной техникой и программным обеспечением, уровень владения компьютерной техникой (попросить выразить оценку собственным действиям); уровень его квалификации;

– наличие (отсутствие) на работе правомерного доступа к компьютерной технике и конкретным видам программного обеспечения;

– перечень конкретных операций с компьютерной информацией, которые подозреваемый (обвиняемый) выполняет на своем рабочем месте; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить;

– кто научил его работать с конкретным программным обеспечением;

– закреплены ли за ним по месту работы идентификационные коды и пароли для пользования компьютерной сетью, какова его категория доступа к информации;

– какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети);

– к каким видам программного обеспечения имеет доступ подозреваемый;

– каков источник его происхождения;

– наличие компьютера по месту жительства, круг лиц, им пользующихся;

– какова конфигурация компьютера, имеющегося по месту жительства (по месту работы, изъятого при обыске);

– какое программное обеспечение установлено на компьютере; переустанавливал ли операционную систему и если да, то когда;

– обнаруживались ли программы, источник происхождения которых неизвестен;

– установлены ли на компьютере антивирусные или защитные программы;

– имеется ли наличие правомерного доступа к сети «Интернет» и работы там;

– какие «ники», электронные почтовые ящики, сайты, домашние страницы принадлежат подозреваемому (обвиняемому) в сети «Интернет»;

– кто настраивал удаленный доступ к сети для выхода в Интернет;

– услугами каких провайдеров пользовался для выхода в Интернет;

– наблюдались ли сбои в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время;

– обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения;

– обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети;

– имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника, и какие именно;

– не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации;

– не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения;

– не известны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей;

– ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ.

Обстоятельства, предшествовавшие совершению преступления:

– когда возникло намерение совершить преступление, кто или что повлияло на это решение;

– почему выбрал именно данный объект для преступного посягательства;

– каковы мотивы и цель совершения преступления;

– откуда подозреваемый мог узнать пароль (код) доступа к информации;

– из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ;

– обстоятельства совершения преступления:

– место и время совершения преступления;

– способ проникновения в помещение, где установлена компьютерная техника или способ осуществления неправомерного доступа и компьютерную систему, сеть;

– приемы преодоления информационной защиты: подбор или хищение ключей и паролей; отключение средств защиты; разрушение средств защиты; использование несовершенства защиты;

– от кого получил данные об используемых в потерпевшей организации мерах защиты информации и способах ее преодоления;

– какие средства использованы при совершении преступления: технические, программные, носители информации, комбинированные;

– способ сокрытия неправомерного доступа;

– количество фактов незаконного вторжения в информационные базы данных; создания, использования и распространения вредоносного программного обеспечения; нарушения правил работы с компьютерной техникой, их системы или сети;

– использовалось ли для совершения преступления служебное положение и в чем это конкретно выразилось;

– наличие сговора с другими лицами и данные о них, кто инициатор;

– детали состоявшейся преступной договоренности;

– каково распределение ролей между участниками преступления;

– каковы конкретные действия по подготовке преступления;

– раскаивается ли в содеянном.

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются: выявление элементов состава преступления в переданной ими информации, установление места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем, определение предмета преступного посягательства, размера причиненного ущерба, детальные признаки похищенного, установление иных свидетелей и лиц, причастных к совершению преступления.

В ходе допроса потерпевших можно установить обстоятельства выявления преступления и его последствия, предварительно оценить причиненный ущерб, узнать способы защиты информации, порядок организации охраны объекта, точные данные о предмете преступного посягательства, предварительные данные о личности виновного и ряд других обстоятельств.

Если изъятое устройство (компьютер, ноутбук, смартфон) защищено паролем, а владелец добровольно отказывается его сообщить, то данное устройство направляется на экспертизу, где происходит дешифровка, а также поиск скрытых файлов, если они имеются.

При изъятии компьютерной техники необходимо назначить компьютерную техническую экспертизу, исследовать средства хранения, обработки, защиты или передачи компьютерной информации и информационно-телекоммуникационных сетей, вредоносных компьютерных программ, охраняемой законом компьютерной информации.

Исследование компьютерной информации, технических средств, программного обеспечения проводится с целью получения информации, имеющей значение для уголовного дела в рамках судебной компьютерно-технической экспертизы. Основная масса исследований реализует диагностическую задачу: установить наличие чего-либо, свойства этого объекта, причинную связь между произошедшим событием и свойствами чего-либо.

Примерный перечень вопросов, решаемых в рамках данной экспертизы, следующий:

– относится ли представленное устройство к аппаратным компьютерным средствам;

– к какому типу (марке, модели) относится аппаратное средство, каковы его технические характеристики и параметры;

– какова роль и функциональные возможности данного аппаратного средства;

– какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство;

– каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения от типовых (нормальных) параметров, в т. ч. физические дефекты;

– какие эксплуатационные режимы установлены на данном аппаратном средстве;

– является ли представленное аппаратное средство носителем информации;

– доступен ли для чтения представленный носитель информации;

– каковы характеристики логического размещения данных на носителе информации;

– какие параметры, свойства, характеристики имеют данные, хранящиеся на носителе информации;

– какого вида (явный, скрытый, удаленный, архив) имеется информация на носителе;

– к какому типу относятся выявленные в ходе компьютерной экспертизы данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты и др.) и какими программными средствами они обеспечиваются;

– каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики;

– какие свойства, характеристики имеют выявленные средства защиты компьютерных данных и какие пути ее преодоления возможны;

– какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации;

– каково содержание защищенных данных;

– какие данные находятся на представленном носителе информации;

– какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа и пр.) имеются на носителе информации;

– произвести выборку с представленного объекта полностью всех программных продуктов;

– произвести выборку с представленного объекта полностью всех сведений, содержащих информацию о деятельности ООО «Название»;

– каким образом организован ввод и вывод данных в представленном объекте;

– имеются ли в обнаруженных программных средствах отклонения от нормальных параметров типовых программных продуктов (например, свойства инфицирования, недокументированных функций);

– имеют ли программные средства защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования;

– произвести выборку всей информации базы данных «Предприятия» (в том числе сведения о разработчиках);

– каков общий алгоритм данного программного средства (базы данных);

– какие программные инструментальные средства (языки программирования, компиляторы, стандартные библиотеки) использовались при разработке данного программного средства (базы данных);

– имеются ли на носителе информации тексты (коды) с первоначальным состоянием программы (базы данных);

– подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием? В чем это нашло отражение;

– с какой целью было произведено изменение каких-либо функций в программном средстве;

– использованы ли в алгоритме программы «Название программы» и ее тексте какие-либо специфические (нестандартные) приемы алгоритмизации и программирования;

– каким способом были произведены изменения в программе «Название программы» (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.);

– какова хронология внесения изменений в программном средстве;

– какова хронология использования программного средства (начиная с его инсталляции);

– имеются ли в программном средстве враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы;

– установить, осуществлялась ли выгрузка в базу данных программы, информация из других источников. Если да, то указать все имеющиеся сведения;

– установить MAC и IP-адреса как начальных точек доступа, так и конечных (все имеющиеся сведения);

– установить, организовано ли взаимодействие базы с иными вычислительными ресурсами (например с API);

– установить, содержится ли в представленном объекте программа «Для установления пароля и логина». Если да, то произвести выгрузку программы «Для установления пароля и логина» в полном объеме с указанием места хранения;

– установить наименование программ, даты установки программ, производителей, ключи программ;

– установить, имеется ли в предоставленном объекте история посещения интернет-страниц. Если да, то предоставить в полном объеме за определенный период времени;

– установить, имеется ли в представленном объекте история переписки по электронной почте «адрес электронной почты», если да, то предоставить в полном объеме с указанием MAC и IP-адреса отправителя и получателя (всей имеющейся информации);

– установить принадлежность IP-адреса к конкретному компьютеру;

– установить, имеются ли в представленном объекте персональные данные граждан (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). Если да, то указать место хранения установленных данных, установить, имеется ли способ защиты данной информации.

Целесообразен допрос эксперта с целью разъяснения вопросов, разрешенных в рамках специальных познаний в области компьютерно-технического исследования.

В зависимости от каждой конкретной информации возможно производство и иных следственных действий, если в них возникла необходимость в ходе расследования уголовного дела.

Вопросы для самоконтроля

1. Роль и место онлайн-игр среди объектов гражданских правоотношений.
2. Онлайн-игры как объекты налоговых правоотношений.
3. Утилитарные цифровые права как объекты гражданских правоотношений.
4. В чем состоит социальная обусловленность криминализации причинения имущественного ущерба правообладателям и потребителям цифрового контента?
5. Какие особенности предмета и объекта преступлений, причиняющих ущерб правообладателям и пользователям цифрового контента, вы можете раскрыть?
6. Проведите общую уголовно-правовую характеристику составов преступлений в сфере компьютерной информации в целом. Какими особенностями обладают составы преступлений, связанных с причинением ущерба правообладателям и пользователям цифрового контента?
7. Опишите обстоятельства, подлежащие установлению по преступлениям, предусмотренным главой 28 УК РФ.
8. Каков процессуальный порядок изъятия электронных носителей информации?
9. Перечислите обстоятельства, которые следует выяснять при проведении допросов подозреваемых, обвиняемых по уголовным делам о преступлениях в сфере компьютерной информации.

Заключение

Основной особенностью незаконного обращения в свое пользование цифрового контента в сети «Интернет», которой продиктовано значительное число проблем, связанных с интернет-пиратством, является нематериальный характер нарушения. Действительно, до появления таких способов передачи информации ее распространение всегда было привязано к физическому носителю. В случае же с завладением чужим «виртуальным имуществом» мы имеем дело с принципиально иным способом хищения, а также донесения контента до потребителя – онлайн-доступом, который требует особого подхода, предусматривающего как адаптацию к нему привычных инструментов управления, так и создание новых.

По рассматриваемым преступлениям потерпевшим в большинстве случаев выступает потребитель цифрового контента (игрок), которому причинен имущественный ущерб от хищения «виртуального имущества», чаще всего путем взлома его аккаунта и завладения его содержимым. Правообладатель в данном случае выступает в роли свидетеля, поскольку денежные средства от проданного игроку имущества собственник онлайн-игры не теряет и не обязан в силу пользовательского соглашения возвращать игроку, не отвечая тем самым за действия третьих лиц. Однако существуют примеры, когда потерпевшим от неправомерного взлома и использования программного обеспечения является правообладатель цифрового контента, который в таких ситуациях несет ущерб в виде упущенной выгоды.

На этапе предварительного расследования вред, причиненный хищением «виртуального имущества», оценивается в зависимости от потраченных потребителем цифрового контента денежных средств и, таким образом, приобретает материальный характер, а значит, может являться разновидностью имущественного ущерба.

Аккаунты пользователей онлайн-игр с их содержимым выступают разновидностью охраняемой законом компьютерной информации, следовательно, общие подходы при квалификации преступлений в сфере компьютерной информации при наличии их признаков будут распространяться и на преступления, связанные с воздействием на указанный цифровой контент.

Применение норм уголовного законодательства, охраняющих компьютерную информацию в условиях отсутствия правовой регламентации цифрового контента, которая позволила бы отнести «виртуальное имущество» к частной собственности, представляется в настоящее время наиболее обоснованным правоприменительным решением, способствующим реализации задач уголовного законодательства и являющимся наиболее адекватным способом противодействия киберпреступности.

С учетом технического прогресса и стремительного развития киберпреступности, необходимо не только совершенствовать законодательство, но и повышать уровень подготовки сотрудников правохранительных органов в исследуемой области, а также обеспечивать техническое оснащение подразделений органов внутренних дел. К сожалению, можно констатировать, что в настоящий момент, правоохранительные органы не всегда обладают достаточным инструментарием для расследования преступлений в данной сфере.

Проблема, на решение которой направлено исследование, связана с тем, что в условиях повышения требований к качеству производства предварительного следствия нужны адекватные меры противодействия преступности в сфере компьютерных технологий. Для этого необходимо повышение уровня знаний и навыков должностных лиц в сфере расследования компьютерных преступлений, а также молодого поколения, желающего в будущем связать свою профессиональную деятельность с борьбой с преступностью.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
2. Уголовный кодекс Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
3. Гражданский кодекс Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
4. Уголовно-процессуальный кодекс Российской Федерации (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
5. О средствах массовой информации: закон РФ от 27 декабря 1991 г. № 2124-1 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
6. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
7. О лотереях: Федеральный закон от 11 ноября 2003 г. № 138-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
8. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.garant.ru.
10. О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. № 395-1 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
11. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
12. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента Российской Федерации от 17 марта 2008 г. № 351 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.
13. О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации: Федеральный закон от 29 декабря 2006 г. № 244-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

14. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.garant.ru.

15. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

16. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

17. О некоторых вопросах информационной безопасности Российской Федерации (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет"»: указ Президента Российской Федерации от 22 мая 2015 г. № 260 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

18. О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: указ Президента Российской Федерации от 22 декабря 2017 г. № (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

19. Об организации прокурорского надзора за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях в органах дознания и предварительного следствия: приказ Генерального прокурора Российской Федерации от 5 сентября 2011 г. № 277 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

20. Об организации прокурорского надзора за процессуальной деятельностью органов дознания: приказ Генеральной прокуратуры РФ от 26 января 2017 г. № 33 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

21. Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия: приказ Генерального прокурора Российской Федерации от 28 декабря 2016 г. № 826 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

22. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, Следственного комитета Российской Федерации от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 (действ. ред.) [Электронный ресурс]. – URL: http://www.consultant.ru.

23. Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км: приказ МВД России от 25 ноября 2019 г. № 878 [Электронный ресурс]. – URL: https://мвд.рф/Fotoarhiv/Meroprijatija_s_uchastiem_rukovodstva.

24. *Лисаченко А. В.* Право виртуальных миров: новые объекты гражданских прав [Электронный ресурс] / А. В. Лисаченко // Российский юридический журнал. – 2014. – № 2. – URL: http://www.consultant.ru.

25. *Li C.* Death sentence for on-line gamer [Электронный ресурс] / C. Li // China Daily. – 2005. – URL: http://www.chinadaily.com.cn/english/doc/2005-06/08/ content_449494.htm.

26. *Петров В. Е.* Защита прав потребителей онлайн-игр [Электронный ресурс] / В. Е. Петров // Экономика и право. XXI век. – 2016. – № 4. – URL: http://www.consultant.ru.

27. *Архипов В. В.* Проблемы правового регулирования оборота товаров в сети Интернет: от дистанционной торговли до виртуальной собственности [Электронный ресурс] / В. В. Архипов, Е. В. Килинкарова, Н. В. Мелащенко // Закон. – 2014. – № 6. – URL: http://www.consultant.ru.

28. *Савельев А. И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх / А. И. Савельев // Вестник гражданского права. – 2014. – № 1. – С. 127–150.

29. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

30. Гражданское право в комментариях. Правовая природа виртуальных объектов, приобретаемых за реальные деньги // Вестник гражданского права. – 2014. – № 1. – Т. 14. – С. 148.

31. *Русскевич Е. А.* Уголовное право и информатизация / Е. А. Русскевич // Журнал российского права. – 2017. – № 8. – С. 76–77.

32. *Попов А. Н.* Преступления в сфере компьютерной информации: учеб. пособие / А. Н. Попов. – Санкт-Петербург, 2018.

33. *Новиков И. В.* Виртуальная собственность: перспективы регулирования [Электронный ресурс] / И. В. Новиков // Вопросы российской юстиции. – 2019. – № 1. – URL: http://injust-journal.ru/wp-content/uploads/2019/04/12.00.00.

34. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генпрокуратурой России. – URL: http://www.consultant.ru.

35. *Федотов Н. Н.* Форензика – компьютерная криминалистика [Электронный ресурс] / Н. Н. Федотов. – Москва: Onebook.ru, 2012. – URL: padabum. com/x.php?id=21178.

36. *Ермакова Е. В.* Проблемы защиты прав пользователей, приобретающих виртуальные объекты за реальные деньги в многопользовательских онлайн-играх [Электронный ресурс] / Е. В. Ермакова, Е. С. Поспелова // Эго: экономика. Государство. Общество. – URL: http://ego.uapa.ru/ru/issue/2014/04/17.

Материалы судебной практики и иные источники

37. Постановление Арбитражного суда Московского округа от 18 июня 2015 г. № Ф05-7093/2015 по делу № А40-91072/14 [Электронный ресурс]. – URL: http: // www.consultant.ru.

38. Решение Савеловского районного суда города Москвы от 9 июля 2018 г. по делу № 02-3433/2018 [Электронный ресурс]. – URL: http://forwardlegal.ru/posts/igry-prava-kak-zashchitit-virtualnoe-imushchestvo.

39. Решение Лефортовского районного суда города Москвы от 25 ноября 2011 г. по делу № 2-3379/2011 [Электронный ресурс]. – URL: http://forwardlegal.ru/posts/igry-prava-kak-zashchitit-virtualnoe-imushchestvo.

40. Приговор Приволжского районного суда города Казани Республики Татарстан по ч. 2 ст. 171.2 УК РФ № 1-292/2017 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/544807.html.

41. Приговор Куйбышевского районного суда города Омска по ч. 1 ст. 171.2 УК РФ № 1-402/2017 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/467243.html.

42. Приговор Дзержинского районного суда города Оренбурга по ч. 1 ст. 171.2 УК РФ № 1-334/2017 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/422336.html.

43. Приговор Хорошевского районного суда города Москвы от 17 июня 2014 г. по делу № 1-260/2014 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/HFQ9r1760Arn/?regular-txt=&regular-case.

44. Апелляционное определение Ленинского районного суда города Кемерово Кемеровской области от 26 апреля 2013 г. по делу № 11-59/2013 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/uQ81NVpYhP1v.

45. Приговор Коминтерновского районного суда города Воронежа от 3 мая 2017 г. № 1-302/2017 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/421591.html.

46. Проставление Президиума Московского городского суда РФ от 24 мая 2013 г. № 44г-45/13 [Электронный ресурс]. – URL: https://base.garant.ru/109918233.

47. Серьезные забавы: почему видеоигры становятся популярнее кино [Электронный ресурс]. – URL: https://www.forbes.ru/tehnologii/357631-sereznye-zabavy-pochemu-videoigry-stanovyatsya-populyarnee-kino.

48. Письмо Департамента налоговой и таможенно-тарифной политики Минфина РФ от 20 июля 2012 г. № 03-07-07/69 [Электронный ресурс]. – URL: http://www.consultant.ru.

49. Письмо ФНС России от 23 января 2017 г. № СД-4-3/988@ [Электронный ресурс]. – URL: http://www.consultant.ru.

50. 10 самых дорогих игровых предметов [Электронный ресурс]. – URL: https://gmbox.ru/materials/35758-10-samih-dorogih-igrovih-predmetov.

51. Statista. Onlain Games [Электронный ресурс]. – URL: https://www.statista.com/outlook/212/100/online-games/worldwide.

52. Тренды онлайн-игр [Электронный ресурс]. – URL: https://plarium.com/ru/blog/trendy-onlayn-igr-2017.

53. Сайт официальной статистики МВД России [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/1.

54. Совет Безопасности Российской Федерации [Электронный ресурс]. – URL: http://www.scrf.gov.ru/security/information/document114.

55. За два месяца благодаря ФНС России ограничен доступ к шести сайтам, где проводят азартные игры с помощью игровых платформ [Электронный ресурс] // Сайт ФНС России. – URL: https://www.nalog.ru/rn77/news/ activities_fts/6961054.

56. Энциклопедия интернет-маркетинга [Электронный ресурс]. – URL: https://www.seonews.ru/glossary/bot/ (дата обращения: 5 сентября 2019 г.).

57. Словарь синонимов [Электронный ресурс]. – URL: https://dic.academic.ru/dic.nsf/dic_synonims.

58. Карта слов и выражений русского языка [Электронный ресурс]. – URL: https://kartaslov.ru.

Приложения

Приложение 1

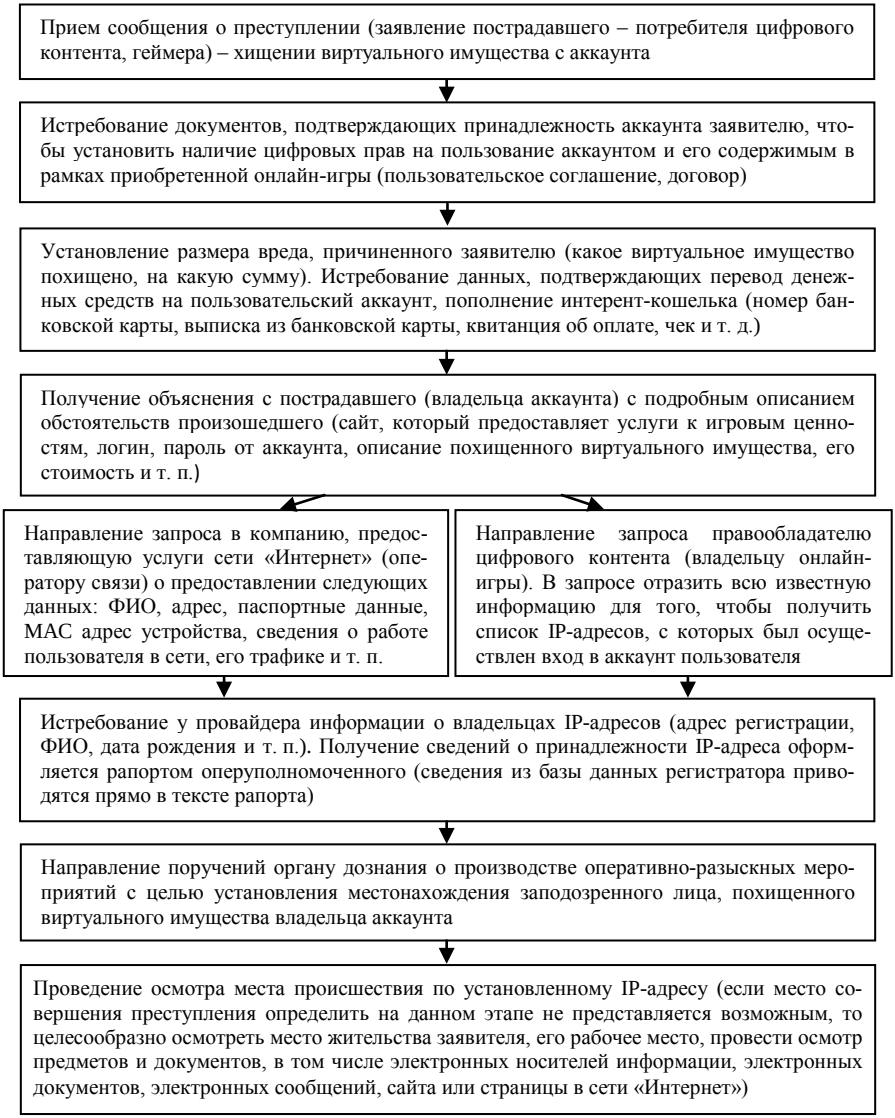
ПАМЯТКА

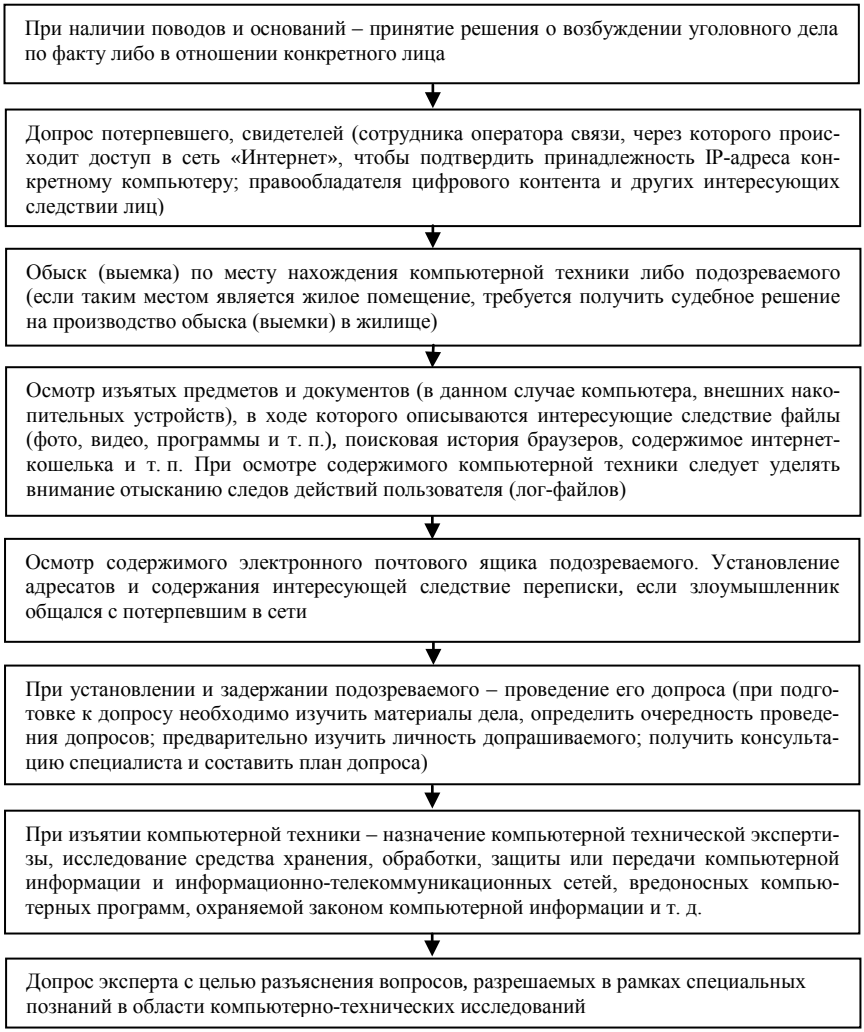
квалификация причинения ущерба правообладателям и потребителям цифрового контента онлайн-игр

Обстоятельства	*Квалификация*
Неправомерный доступ пользователя к программному обеспечению онлайн-игры с размещением в ней программы, позволяющей незаконно безвозмездно создавать «виртуальные ценности», которые по лицензионному соглашению требуют дополнительных материальных вложений со стороны пользователей. Ущерб в виде упущенной выгоды причиняется правообладателю цифрового контента	ст. 272 УК РФ, ст. 146 УК РФ
Неправомерный доступ к аккаунту с изменением персональных данных пользователя посредством использования программного обеспечения, а также неправомерное завладение «виртуальными ценностями» с чужого аккаунта из хулиганских побуждений, если это деяние не причинило ущерба на сумму более одного миллиона рублей («Хищение аккаунта или виртуальных ценностей»)	ч. 1 ст. 272 УК РФ
Неправомерный доступ к аккаунту с изменением персональных данных пользователя посредством использования программного обеспечения, а также неправомерное завладение «виртуальными ценностями» с чужого аккаунта из корыстных побуждений либо если это деяние причинило ущерб на сумму более одного миллиона рублей («Хищение аккаунта или виртуальных ценностей»)	ч. 2 ст. 272 УК РФ

Приложение 2

Примерный алгоритм проверочных и первоначальных следственных действий по преступлениям в сфере причинения имущественного ущерба правообладателям и потребителям цифрового контента (в следственной ситуации о хищении виртуального имущества с аккаунта пользователя сети «Интернет»)




При наличии поводов и оснований – принятие решения о возбуждении уголовного дела по факту либо в отношении конкретного лица
Допрос потерпевшего, свидетелей (сотрудника оператора связи, через которого происходит доступ в сеть «Интернет», чтобы подтвердить принадлежность IP-адреса конкретному компьютеру; правообладателя цифрового контента и других интересующих следствии лиц)
Обыск (выемка) по месту нахождения компьютерной техники либо подозреваемого (если таким местом является жилое помещение, требуется получить судебное решение на производство обыска (выемки) в жилище)
Осмотр изъятых предметов и документов (в данном случае компьютера, внешних накопительных устройств), в ходе которого описываются интересующие следствие файлы (фото, видео, программы и т. п.), поисковая история браузеров, содержимое интернет-кошелька и т. п. При осмотре содержимого компьютерной техники следует уделять внимание отысканию следов действий пользователя (лог-файлов)
Осмотр содержимого электронного почтового ящика подозреваемого. Установление адресатов и содержания интересующей следствие переписки, если злоумышленник общался с потерпевшим в сети
При установлении и задержании подозреваемого – проведение его допроса (при подготовке к допросу необходимо изучить материалы дела, определить очередность проведения допросов; предварительно изучить личность допрашиваемого; получить консультацию специалиста и составить план допроса)
При изъятии компьютерной техники – назначение компьютерной технической экспертизы, исследование средства хранения, обработки, защиты или передачи компьютерной информации и информационно-телекоммуникационных сетей, вредоносных компьютерных программ, охраняемой законом компьютерной информации и т. д.
Допрос эксперта с целью разъяснения вопросов, разрешаемых в рамках специальных познаний в области компьютерно-технических исследований

Содержание

ФЕДОСЕЕВА Елена Леонидовна
ВОРОПАЕВ Сергей Александрович
КУЗНЕЦОВ Роман Николаевич

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИЧИНЕНИЕМ ИМУЩЕСТВЕННОГО УЩЕРБА ПРАВООБЛАДАТЕЛЯМ И ПОТРЕБИТЕЛЯМ ЦИФРОВОГО КОНТЕНТА

Учебно-методическое пособие

Редактура *И. Б. Бебих*
Компьютерная верстка *А. Г. Шабалдиной*

Подписано в печать 02.03.2020. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 2,5. Уч.-изд. л. 3,7
Тираж 50 экз. Заказ № 9

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66