Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2020, 4: 163–166

DOI 10.26163/GIEF.2020.24.65.024
УДК 343.711.9

A.V. Shakhmatov, I.E. Skokov

PROVIDING OPERATIONAL SEARCH SUPPORT IN INVESTIGATING THEFTS OF VIRTUAL PROPERTY IN ONLINE GAMING INDUSTRY ENVIRONMENT

Aleksandr Shakhmatov – Professor, the Department of Internal Affairs Bodies Operational Investigative Activities, St. Petersburg University of the Russian Interior Ministry, Doctor of Law, Professor, Honoured Officer of the Internal Affairs Bodies, St. Petersburg; **e-mail: a-shahmatov@yandex.ru**.
Igor Skokov – Senior Lecturer, the Department of Internal Affairs Bodies Operational Investigative Activities, St. Petersburg University of the Russian Interior Ministry, St. Petersburg; **e-mail: iga-spb74@mail.ru**.

The article discusses prospects of operational search support in solving crimes committed on the Internet in the light of the development of the gaming industry market in Russia. Proposals are made to use the existing information database "Remote fraud" in view of the current trend of the ongoing increase in the number of such crimes.

Keywords: *Virtual property; theft; remote fraud; operational search support; solving Internet crimes.*

А.В. Шахматов, И.Е. Скоков

ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ ПРИ РАССЛЕДОВАНИИ КРАЖ ВИРТУАЛЬНОЙ СОБСТВЕННОСТИ, СВЯЗАННОЙ С ИГРОВОЙ ИНДУСТРИЕЙ В СЕТИ ИНТЕРНЕТ

Александр Владимирович Шахматов – профессор кафедры оперативно-разыскной деятельности в органах внутренних дел, Санкт-Петербургский Университет МВД России, доктор юридических наук, профессор, заслуженный сотрудник ОВД РФ, г. Санкт-Петербург; **e-mail: a-shahmatov@yandex.ru**.
Игорь Евгеньевич Скоков – старший преподаватель кафедры оперативно-разыскной деятельности в органах внутренних дел, Санкт-Петербургский Университет МВД России, г. Санкт-Петербург; **e-mail: iga-spb74@mail.ru**.

В статье рассматриваются перспективы оперативно-розыскного обеспечения при раскрытии преступлений, совершенных в Интернете, в свете развития рынка игровой индустрии на территории России. Вносятся предложения по использованию существующей информационной базы данных федерального уровня (ИБД-Ф) «Дистанционное мошенничество» в рамках существующей тенденции увеличения количества подобных преступлений.

Ключевые слова: *виртуальная собственность; кража; дистанционное мошенничество; оперативно-розыскное сопровождение; раскрытие преступлений в Интернете.*

Современный человек не мыслит себя и свою жизнь без постоянного взаимодействия со всемирной паутиной. Интернет сейчас – это и помощник в хозяйстве, работе, а для кого-то и сама работа напрямую связана со всемирной сетью, также это способ развлечения и досуга. Вполне естественно, что в начале XXI в. вместе с развитием онлайн-игр стала появляться виртуальная собственность. Находясь в современных «онлайновых мирах», игрок, как правило, получает в начале игры ка-

кой-то объект (персонажа), который по мере прохождения игры начинает приобретать определенные навыки или предметы. Все это достигается либо путем значительного проведения времени в игре с выполнением заданий, направленных на улучшение персонажа, либо приобретением виртуальных предметов, позволяющих сразу получить необходимые навыки. И если в первом случае игрок тратит свое время, то во втором – чаще всего это деньги.

Примерная цена мировой игровой индустрии в 2019 г. составила более 148 млрд долл. [10]. В России объем компьютерного игрового рынка в 2019 г. вырос по сравнению с 2018 г. на 15% и составил 129,5 млрд руб. [6]. Согласно всем прогнозам на 2020 г. в силу того, что значительная часть населения страны в течение половины весны и всего лета находилась дома в самоизоляции, данная цифра по итогам года вырастет еще на 10–15%, даже невзирая на определенные финансовые проблемы части населения. Естественно, в рамках данной индустрии появились и элементы рыночных отношений как между производителями контента, так и между игроками. Отдельные элементы этих отношений оцениваются в значительные суммы. Так, в настоящее время рекордсменом по продаже виртуального объекта является покупка виртуальной планеты стоимостью в 6 млн реальных долларов США, в одной из онлайн-игр. Поэтому продажей предмета за несколько тысяч долларов в игровой индустрии никого не удивишь. А там, где появляются большие деньги, там и появляются желающие ими незаконно завладеть. Поэтому, несмотря на все усилия разработчиков игр защитить своих клиентов от краж, количество их вместе с ростом денежного потока неудержимо растет. Объектом кражи являются как виртуальные персонажи, так и отдельные предметы или объекты. Одним из самых дорогих похищенных виртуальных объектов, о каком в настоящее время имеется информация, – это персонаж, на улучшение которого игрок из Китая потратил около 1,4 млн долл.

В настоящее время в среде правоведов ведется дискуссия на тему квалификации ответственности за подобные преступления [4; 5; 7; 9]. Среди самых распространенных предложений – введение уголовной ответственности за кражу виртуальных активов, к которым в проекте закона «О цифровых и финансовых активах», внесенного в Государственную Думу, предлагается отнести не только всевозможные криптовалюты, но и виртуальных персонажей компьютерных игр [1]. Авторы статьи, оставляя за скобками правовую сторону вопроса виртуальной собственности, в настоящее время, тем не менее, исходя из существующей тенденции считают, что в обозримом будущем данная проблема будет решена в том числе и на законодательном уровне, что приведет к изменениям в уголовном законодательстве, а, следовательно, с учетом того, что согласно ст. 2 ФЗ «Об ОРД» одной из задач ОРД является выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших; необходимо говорить о перспективе возникновения еще одного объекта, находящегося в зоне интересов криминалистики и оперативно-розыскной деятельности как науки.

Более того, уже сейчас возникают прецеденты возбуждения уголовного дела по факту кражи виртуального персонажа, расследования его и осуждения злоумышленника. Так, в июне 2014 г. в Московской области был вынесен приговор в отношении гражданина Ш., который, получив доступ к чужим паролям в онлайн-игре, с их помощью присваивал чужие виртуальные предметы, реализовывал их в игровой магазин и затем обналичивал виртуальную валюту. Мировой судья судебного участка № 213 Раменского судебного участка признал 29-летнего местного жителя Дмитрия Ш. виновным в преступлениях, предусмотренных ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации из корыстных побуждений). Было установлено, что Ш., используя хакерское программное обеспечение, получил пароль для входа в одну из платных интернет-игр, а также доступ к сер-

верной части онлайн-игры, в дальнейшем изменив пароли к учетным записям и заблокировав доступ пользователей. Принадлежащие пользователям виртуальные предметы он реализовывал в игровой магазин. Виртуальную (игровую) валюту Ш. конвертировал с использованием систем интернет-платежей в подлинные деньги. В ходе судебного разбирательства гражданин Ш. полностью признал свою вину, раскаялся в содеянном и ходатайствовал о рассмотрении уголовного дела в особом порядке, после чего суд назначил наказание гражданину Ш. в виде 1,2 года ограничения свободы [8]. И это не единственный пример.

В настоящее время инструментом, которым могут воспользоваться сотрудники оперативных подразделений МВД в работе над раскрытием таких преступлений, является проведение оперативно-розыскных мероприятий. На наш взгляд, наиболее целесообразным будет в данном случае проведение таких ОРМ, как «Получение компьютерной информации», «СИТКС», «ПТП», «Наведение справок». Необходимо отметить также и то, что без содействия со стороны создателей онлайн-игр (многие из которых находятся за пределами Российской Федерации) говорить об эффективном противодействии преступлениям данного вида не приходится.

Отдельно обратим внимание на тот факт, что данные преступления могут быть отнесены к категории преступлений с применением так называемых «высоких технологий», и их раскрытие, скорее всего, должно быть возложено не на территориальные подразделения уголовного розыска, а переданы для оперативного сопровождения соответствующим оперативным подразделениям.

В настоящее время согласно указанию министра МВД, в структуре министерства формируются подразделения, специализирующиеся на противодействии преступлениям в сфере IT-технологий.

Заявленная цель создания таких подразделений – повышение результативности предупреждения и пресечения преступлений в IT-сфере, а также совершенствование навыков и обучение наиболее подготовленных сотрудников работе по выявлению, раскрытию и расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий [2].

Для обеспечения информационно-аналитического сопровождения работы данных подразделений в системе МВД создана и работает подсистема ИБД-Ф «Дистанционное мошенничество». Данная база предназначена для сбора, систематизации, обработки и анализа сведений, собираемых в рамках расследования уголовных дел по преступлениям, совершенным дистанционным способом с использованием информационно-телекоммуникационных технологий. В настоящее время в ИБД-Ф помещаются следующие данные:

- данные о номере, зарегистрированном в книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП), номере уголовного дела, фабуле преступления, способе совершения, сумме причиненного ущерба, решении по материалу проверки сообщения о преступлении или уголовному делу, а также сведения о территориальном органе МВД России регионального и районного уровней, в котором зарегистрировано сообщение о происшествии (преступлении) либо расследуется уголовное дело;

- идентификационные данные средств связи, используемые при совершении преступления: международный идентификатор мобильного абонента (IMSI) и международный идентификатор мобильного оборудования (IMEI);

- номера банковских карт и банковских счетов, используемые при совершении преступления;

- установочные данные лиц, зафиксированные в материалах проверки сообщения о происшествиях (преступлениях) или уголовного дела, используемые ими документы, удостоверяющие личность;

- наименование и идентификационный номер налогоплательщика (ИНН) организации, зафиксированные в материалах проверки сообщения о происшествиях

(преступлениях) или уголовного дела;

- данные интернет-ресурсов (адреса сайтов, IP-адреса, адреса электронной почты), используемые при совершении преступлений;

- номера «электронных кошельков», используемые при совершении преступлений [3, с. 89].

Учитывая наличие уже работающей информационной базы, полагаем в качестве расширения ее возможностей внести в раздел модуля ввода информации об интернет-ресурсе сведения о характеристике похищенного имущества в том случае, если были похищены не денежные средства.

Подводя итог, отметим, что рассмотренный в статье вид неправомерного завладения чужим (пусть и виртуальным) имуществом будет представлять в ближайшем будущем проблемы как для общества в целом, так и для правоохранительных органов в частности, и уже сейчас требуется обратить внимание на необходимость специальной подготовки оперативных и следственных кадров, осуществляющих раскрытие и расследование данных преступлений.

ЛИТЕРАТУРА

1. Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Доступ из справочно-правовой системы «КонсультантПлюс».

2. В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий // Министерство внутренних дел РФ: [сайт]. URL: https://мвд.рф/news/item/18809813 (дата обращения: 15.01.2020).

3. *Давыдов В.О., Тишутина И.В.* Об актуальных проблемах криминалистического обеспечения рыскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 81–91.

4. *Карпов А.С.* Проблемы квалификации мошенничества, совершенного с использованием систем дистанционного банковского обслуживания // Отечественная юриспруденция. 2017. № 10. С. 46–47.

5. *Литвинов Н.Д., Федоров А.Н.* Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. 2015. № 12. С. 73–80.

6. Объем российского рынка видеоигр вырос на 14% в 2019 году // B-MAG.ru: [сайт]. URL: https://b-mag.ru/obem-rossijskogo-rynka-videoigr-vyros-na-14-v-2019-godu/ (дата обращения: 10.10.2020).

7. *Петрикова С.В., Лаврушкина А.А.* Особенности состава преступления «Дистанционное мошенничество» // Молодежный научный вестник. 2017. № 11. С. 276–285.

8. Прокуратура Московской области: [сайт]. URL: https://epp.genproc.gov.ru/web/proc_50 (дата обращения: 10.10.2020).

9. *Сердюк П.Л.* Особенности правовой оценки дистанционного мошенничества // Вестник Нижегородской академии МВД России. 2019. № 4. С. 226–228

10. *Batchelor J.* GamesIndustry.biz presents... The Year In Numbers 2019. URL: https://www.gamesindustry.biz/articles/2019-12-17-gamesindustry-biz-presents-the-year-in-numbers-2019 (дата обращения: 01.10.2020).