Научная статья
УДК 343.34
DOI: 10.47475/2311-696X-2024-41-2-109-114

С. 109–114

РОЛЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И СПЕЦИАЛЬНЫХ СЛУЖБ В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ В СФЕРЕ КОМПЬЮТЕРНЫХ ИГР, И ТЕХНИЧЕСКИЕ РЕШЕНИЯ ДЛЯ ИХ ПРЕДОТВРАЩЕНИЯ

Эльвира Юрьевна Латыпова[1], **Руслан Эдуардович Гильманов**[2], **Радик Русланович Бадрутдинов**[3]
[1,2,3] *Казанский инновационный университет имени В. Г. Тимирясова, Казань, Россия*
[1] *elatypova@ieml.ru*
https://orcid.org/0000-0002-7390-4962
[2] *REGilmanov@ieml.ru*
https://orcid.org/0000-0003-2062-5959
[3] *radik-badrutdinov@mail.ru*

Аннотация. Киберпреступления появились в статистике преступности лишь в последние два-три десятилетия, однако это самая активно развивающаяся сфера преступной деятельности. Как активно развивающееся направление преступного поведения, в нем активно появляются всё новые направления, одним из которых являются преступления в сфере компьютерных игр. Данное направление преступной активности появилось сравнительно недавно, что вызывает существенные трудности на практике, так как не всегда ясен повод для возбуждения уголовного дела, возникают сложности с предварительным расследованием и самим доказыванием факта совершения преступления. В статье анализируется содержание деятельности правоохранительных органов и специальных служб в их специфическом приложении к профилактике и расследованию преступлений, связных с компьютерными играми. Рассматривается понятие «хакерства», его деление на виды и исследуется содержание видов такой информационной деятельности. Приводятся способы защиты информации применительно к игровой деятельности. Также предлагаются и обосновываются технические средства для предотвращения преступлений в сфере компьютерных игр, так как именно технические решения для предотвращения преступлений в сфере компьютерных игр играют важнейшую роль реализации деятельности по обеспечению безопасности виртуального игрового пространства, и последующей защиты игроков от различных видов преступной активности, выражающейся в совершении пользователями различных общественно опасных преступлений.

Ключевые слова: преступления, совершаемые в сфере компьютерных игр, компьютерные преступления, информация, защита информации, борьба с цифровыми преступлениями, киберпреступления, хакеры, хакерство

Для цитирования: Латыпова Э. Ю., Гильманов Р. Э., Бадрутдинов Р. Р. Роль правоохранительных органов и специальных служб в борьбе с преступлениями, совершаемыми в сфере компьютерных игр, и технические решения для их предотвращения // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 109–114. DOI: 10.47475/2311-696X-2024-41-2-109-114

Research article

THE ROLE OF LAW ENFORCEMENT AGENCIES AND SPECIAL SERVICES IN COMBATING CRIMES COMMITTED IN THE FIELD OF COMPUTER GAMES, AND TECHNICAL SOLUTIONS FOR THEIR PREVENTION

Elvira Yu. Latypova[1], **Ruslan E. Gilmanov**[2], **Radik R. Badrutdinov**[3]
[1,2,3] *Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia*
[1] *elatypova@ieml.ru*
https://orcid.org/0000-0002-7390-4962
[2] *REGilmanov@ieml.ru*
https://orcid.org/0000-0003-2062-5959
[3] *radik-badrutdinov@mail.ru*

Abstract. Cybercrimes have appeared in crime statistics only in the last two to three decades, but this is the most actively developing area of criminal activity. As an actively developing area of criminal behavior, new directions are actively appearing in it, one of which is crimes in the field of computer games. This area of criminal activity has appeared relatively

© Э. Ю. Латыпова, Р. Э. Гильманов, Р. Р. Бадрутдинов

recently, which causes significant difficulties in practice, since the reason for initiating a criminal case is not always clear, difficulties arise with the preliminary investigation and the very proof of the fact of the commission of a crime. The article analyzes the content of the activities of law enforcement agencies and special services in their specific application to the prevention and investigation of crimes related to computer games. The concept of «hacking» is considered, its division into types and the content of such information activities is investigated. Technical means for the prevention of crimes in the field of computer games are also proposed and justified, since it is technical solutions for the prevention of crimes in the field of computer games that play the most important role in the implementation of activities to ensure the safety of the virtual gaming space, and the subsequent protection of players from various types of criminal activity, expressed in the commission of various socially dangerous crimes by users.

Keywords: crimes committed in the field of computer games; computer crimes; information; information protection; combating digital crimes; cybercrimes; hackers: hacking.

For citation: Latypova EYu, Gilmanov RE, Badrutdinov RR. The role of law enforcement agencies and special services in combating crimes committed in the field of computer games, and technical solutions for their prevention. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(2):109-114. DOI: 10.47475/2311-696X-2024-41-2-109-114 (In Russ.)

Введение

Компьютерные игры уже давно стали одним из самых распространенных видов общедоступных развлечений. Более того, постепенно компьютерные игры меняют свой статус, становясь частью спортивной культуры, подтверждением чего является проведение первых в мире фиджитал-игр, сочетающих в себе элементы фитнеса или физкультуры и цифровых технологий, иначе говоря — функционально-цифровой спорт. Соответственно, как широко распространенное явление, компьютерные игры также могут подпадать под различного рода злоупотребления, что требует вмешательства правоохранительных органов.

Правоохранительные органы и специальные службы, специализирующиеся на борьбе с преступлениями, совершаемыми в сфере компьютерных игр, играют важную роль, что обусловлено их непосредственной работой, а также разработкой способов для того, чтобы раскрытие и привлечение киберпреступников к уголовной ответственности было более эффективным и действительно помогало с решением возникающих проблем [10].

Как уже было отмечено ранее, изучаемая проблема стала новым явлением, которое ещё до конца не рассмотрено с законодательной стороны нашей страны. Действующий Уголовный Кодекс РФ не даёт точной трактовки такому явлению, как «компьютерные преступления», которое, в свою очередь, является более широким по сравнению с преступлениями, совершаемыми в сфере компьютерных игр, понятием. В данном случае можно говорить о том, что такие преступления включены в категорию компьютерных. Преступления в видеоиграх практически аналогичны преступлениям, совершаемым в киберпространстве, таким как кибербуллинг, читерство, фишинг, кража данных, взлом аккаунтов [1, с. 293] и многие другие. Проявлять себя они стали вместе с развитием технологий компьютерных игр, условий игры и также возможностью финансового вложения в них.

Роль правоохранительных органов и специальных служб в борьбе с преступлениями, совершаемыми в сфере компьютерных игр, важна, и имеет ключевое значение для их расследования, привлечения виновных лиц к ответственности, а также в выявлении таких преступлений. Главной целью правоохранительных органов является обеспечение порядка и безопасности в обществе, охрана прав и свобод человека и гражданина. Именно поэтому лица, стоящие на страже закона, ведут активную работу по улучшению раскрываемости киберпреступлений, даже с условием того, что как таковой ответственности за совершения именно этой категории преступлений законодательством не предусмотрено.

Материалы и методы

В подготовке статьи использованы нормативные правовые акты, регламентирующие вопросы уголовно-правового регулирования деятельности, связанной с обережением информационной безопасности, специальная литература по теме исследования. Основой проведенного научного исследования стали общенаучные и частнонаучные методы научного познания, анализ и толкование теоретических и нормативных правовых источников и судебной практики.

Описание исследования

Обеспечение порядка и безопасности в обществе, охрана прав и свобод человека и гражданина являются конституционными правами и свободами, и основополагающими для деятельности правоохранительных органов. Киберпреступления, посягающие на цифровую безопасность [2, с. 83], активно развиваются, в связи с чем требуется постоянное повышение и квалификации сотрудников правоохранительных органов, ведущих активную работу по улучшению раскрываемости киберпреступлений. Госслужащий, который обеспечивает правопорядок в киберпространстве, должен обладать следующими качествами:

— аналитический склад ума;

— способность к распознаванию несанкционированного доступа к охраняемой законом тайне;

— осведомлённость в постоянно изменяющемся характере и способах совершения преступлений в компьютерных играх,

© Э. Ю. Латыпова, Р. Э. Гильманов, Р. Р. Бадрутдинов

— обязательным наличием специальных навыков и знаний в сфере компьютерной информации.

Соответствие данным требованием способно в значительной степени помочь сотруднику правоохранительных органов в осуществлении деятельности по борьбе с киберпреступностью.

В 2020 году МВД впервые заговорило о возможности введения в свои подразделения отряда «киберполиции», который бы специализировался на борьбе с преступлениями, совершаемыми с использованием IT технологий. Такое желание было вызвано резким увеличением количества преступлений, совершаемых на почве виртуальных игр, или непосредственно в них, а также тем, что в настоящее время преступления в сфере компьютерной информации приобретают новый характер и являются довольно острой проблемой [3, с. 293]. Именно поэтому рациональным, по мнению законодателя, является создание отдельной структуры госслужащих правозащитников, сферой деятельности которых будет IT пространство. И хотя на данный момент не создано такого органа, как «киберполиция», в МВД до недавнего времени существовало Управление-К, которое и занималось борьбой с преступлениями в сфере компьютерной информации. В настоящее время функции, возложенные на Управление-К, выполняет Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК)[1]. Так, например, за январь-октябрь 2023 года сотрудники полиции выявили более 560 тыс. преступлений в интернет-пространстве[2], в том числе в видеоиграх. Практически половина вредоносного контента была удалена ими из сети Интернет, и они продолжают работать на благо пользователей киберпространства путём проведения различных расследований, поиска и раскрытия виновных лиц, а также привлечения их к уголовной или иным мерам ответственности.

Известно, что как в сфере компьютерной информации, так и в отношении интересующих нас видеоигр, существует такое понятие, как «хакер». Хакер является человеком, который владеет специальными знаниями в сфере IT-технологий и использует их, как правило, для того чтобы производить взлом систем, кражу конфиденциальной информации [4, с. 39], а также осуществление неправомерного доступа к закрытым источникам. Но, однако же, хакеры делятся:

— на так называемых «чёрных» хакеров, которых характеризуют негативные действия с их стороны. Правоохранители уже давно ведут борьбу с таким явлением, как осуществление хакерских взломов. И обычно под понятием хакера понимается именно правонарушитель;

— «белых хакеров», которые, в отличие от чёрных, производят те или иные действия во благо. Например, для защиты от «чёрных» хакеров и по приведению взломанных систем в порядок. Интересным является также тот факт, что достаточно давно ведётся речь об узаконивании деятельности «белых» хакеров в РФ. Однако же к единому мнению по поводу этого законодатель прийти не может.

Так, например 12 декабря 2023 года первый из пакета законопроектов, направленных на легализацию деятельности «белых» хакеров в России, был внесен в Госдуму, о чём сообщил один из авторов инициативы, член комитета Госдумы по информационной политике, информационным технологиям и связи Антон Немкин[3] [8]. Соответствующие изменения должны быть предложены как для Уголовного кодекса РФ, так и для проекта ФЗ «Об информации, информационных технологиях и защите информации»[4].

Все эти действия, несомненно, являются иллюстрацией того, как правоохранительные органы стараются разработать тактику ведения борьбы с правонарушителями в онлайн пространстве. Применительно к компьютерным играм, например, деятельность так называемых «белых» хакеров может быть обусловлена их помощью в обнаружении пользователей, ведущих нечестную игру [5, с. 295], или же в тех случаях, когда такие игроки предпринимают удачные попытки, связанные с кражей игровых аккаунтов и последующего имущества.

Так, например, на данный момент имеется возможность купить «виртуальное имущество» за реальные деньги и свободно распоряжаться им в ходе игры. Речь в данном случае идёт о больших суммах, например, в сообществе виртуальных трейдеров главным событием 2020-го стала покупка винтовки «Вой» с редким скином и наклейками за 100 000 долларов. Покупателем стал некий коллекционер из Китая, который предпочел остаться анонимным, при том изначально в сделку входило несколько редких предметов, а общая цена была вдвое выше[5]. Произведена данная покупка была в игре StatTrak M4A4 (CS: GO). Схожие сделки относительно отдельных предметов или персонажей в компьютерных играх происходят достаточно часто, но обычно сделка не превышает 10 000 долларов.

Ещё одним громким случаем, который долго обсуждали в сети, стала кража танка в довольно популярной

[1] Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий. URL: https://мвд.рф/mvd/structure1/Upravlenija/убк (дата обращения: 10.03.2024).

[2] В МВД назвали причину роста IT-преступности в России // Известия : [сайт]. URL: https://iz.ru/1615901/2023-12-05/v-mvd-nazvali-prichinu-rosta-it-prestupnosti-v-rossii (дата обращения: 10.03.2024).

[3] В Госдуму внесли проект о легализации «белых» хакеров // ТАСС. URL: https://tass.ru/obschestvo/19519931 (дата обращения: 10.03.2024).

[4] Об информации, информационных технологиях и защите информации : проект федерального закона № 217354-4 // СПС «Гарант». URL: https://base.garant.ru/5274869/ (дата обращения: 10.03.2024).

[5] Малахов М. Миллионы за пиксели: 7 самых дорогих покупок в играх // BroDude.ru. URL: https://brodude.ru/millionyza-pikseli-7-samyh-dorogih-pokupok-v-igrah/ (дата обращения: 10.03.2024).

в настоящее время игре, насчитывающей более 100 тыс. пользователей по всему миру «World of tanks». В феврале 2016 года сотрудники полиции Нижнего Новгорода раскрыли дело о похищении в данной игре танка стоимостью 70 тыс. руб. Делом заинтересовались тогда, когда в полицию обратился 24-х летний мужчина, с заявлением о краже виртуального имущества, а именно танка, который он приобрёл на реальные средства. Правонарушителя, похитившего имущество мужчины, удалось выявить при попытке перепродажи взломанного аккаунта с целью получения прибыли[1]. В итоге мужчину осудили по ч. 2 ст. 272 УК РФ, которая предусматривает уголовную ответственность за неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершённый из корыстных побуждений.

При квалификации данного рода преступлений стоит обращаться к главе 28 УК РФ «Преступления в сфере компьютерной информации». Интерес вызывают именно ст. 272, а также 273, приведём краткую характеристику каждой из них.

Положения статьи 272 УК РФ, направлены на охрану общественной безопасности в сфере компьютерной информации. В примечании номер 1 рассматриваемой статьи говорится о том, что к компьютерной информации относятся сведения и данные, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Преступление может совершаться путём проникновения в компьютерную систему, а также использования специальных технических или программных средств, которые позволяют обойти средства защиты (различные пароли и коды).

Статья 273 УК РФ, в свою очередь, предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ. Выражается это в использовании таких программ, которые способны уничтожить, блокировать, в случае с читерством модифицировать или же копировать компьютерную информацию различного характера.

Сходство данных статей заключается в том, что объектом составов преступления является компьютерная информация. Главное отличие в том, что в ст. 272 речь идёт именно об информации, охраняемой законом, а в ст. 273 УК РФ говорится о непосредственном факте создания, распространения и использования технических средств для повреждения или кражи той или иной информации.

Но не в одной из них не сказано об ответственности, за совершение преступлений в сфере компьютерных игр. Главная проблема при уголовно-правовой квалификации данных преступлений, таким образом, заключается в неточности формулировок, а также в отсутствии понятий, и небольшому количеству практики. В силу чего мы считаем, что рациональным будет продолжить модернизировать уголовную ответственность за компьютерные преступления в рамках самостоятельной главы в Уголовном кодексе, отдельно посвящённую киберпреступлениям, а затем уже и самостоятельный нормативно-правовой акт, посвящённый данной отрасли правоотношений. В связи с постоянным развитием, модернизацией и изменением сферы компьютерных игр в современном обществе, для законодателя, по нашему мнению, это является актуальным.

По мере того, как стала развиваться проблема преступлений, совершаемых в сфере компьютерных игр, правоохранительные органы столкнулись с необходимостью разработки различных технических средств по борьбе с ними. В данном случае технические средства защиты играют важную роль для обеспечения безопасности игрового пространства, а также для превентивных мер, предупреждающих совершение преступных деяний.

Средствами защиты информации является совокупность средств и методов, которые используются для того, чтобы решить различные проблемы, с которыми человек сталкивается при работе с компьютерными устройствами. Например, такие проблемы как: обеспечение безопасности защищаемой информации, предупреждение её утечки и неправомерного завладения информацией, в том числе личного характера, а также обережение моральной и нравственной составляющей действующего законодательства [6, с. 96].

Пожалуй, одним из самых знаменитых и эффективных способов защиты информации является её шифрование, а именно использование различных кодов, шифров и паролей. Так, по мнению В. Ю. Зелепукина, для обеспечения надёжности защиты при помощи паролей, работа системы защиты организуется так, чтобы вероятность выявления секретного пароля и установления соотношения какому-нибудь идентификатору терминала либо файла была как можно меньше. Для этого нужно периодически менять пароль, а количество символов в нём установить довольно большим [7, с. 305]. И это говорит о том, что даже такой надёжный способ защиты информации, как пароль, можно обойти [8, с. 210], поэтому стоит учитывать специфические особенности данного вида защиты.

Если говорить о конкретных средствах защиты информации, то их принято делить на следующие виды:

— технические, которые работают за счёт использования различных механических способов защиты, таких как сигнализации, замки, а также генераторы шума или же различные сканирующие устройства;

— интересующие нас программные, которые работают посредством использования различных программ, по типу идентификации пользователей, шифрованию информации, удалению остаточных файлов. Среди других, указанные средства обеспечения защиты информации имеют преимущество за счёт простоты использования, надёжности, а также своей универсальности и постоянному развитию;

[1] Нижегородская полиция раскрыла кражу «танка» в World of Tanks // РБК. URL: https://www.rbc.ru/technology_and_media/02/03/2016/56d7293d9a79473f782ed597 (дата обращения: 10.03.2024).

© Э. Ю. Латыпова, Р. Э. Гильманов, Р. Р. Бадрутдинов

— смешанные, включающие в себя и аппаратные, и программные средства;

— организационные, или же такие, которые заключаются в подготовке оборудования или помещения для работы.

Перечисленные виды защиты информации направлены на то, чтобы обеспечить безопасность для пользователей компьютерных устройств.

Заключение и вывод

Как уже было отмечено ранее, технические решения для предотвращения преступлений в сфере компьютерных игр играют важнейшую роль в реализации деятельности по обеспечению безопасности виртуального игрового пространства и последующей защите игроков от различных видов преступной активности, выражающейся в совершении пользователями различных общественно опасных деяний, возможно, с применением искусственного интеллекта [9, с. 83]. Таким образом, технические средства для борьбы с преступлениями в сфере компьютерных игр могут быть следующими:

— разработка мониторинга игровых чатов и обменом сообщений между лицами, которая может быть осуществлена посредством разработки систем обеспечения, которым под силу будет производить сканирование сообщений игроков на выявление наличия скрытых угроз, оскорблений или других негативных проявлений. Данный вид технических средств сможет помочь с совершением кибербуллинга;

— создание разнообразных систем отслеживания мошенничества в киберпростанстве, которые смогут обнаруживать подозрительную активность (использование читов, ботов), и за счёт этого контролировать совершение мошенничества в сфере компьютерных игр;

— введение системы поощрения и наказания, а именно, разработка системы, награждающей игроков за честную игру, а в противном случае наказывающая за нарушение установленных правил;

— необходимое сотрудничество с правоохранительными органами, которое сможет развить партнёрские отношения между игровыми компаниями и госслужащими, которые при совместной работе смогут разработать способы защиты в борьбе с киберпреступниками.

Перечисленные технические решения могут стать эффективными способами в предотвращении преступлений, совершаемых в сфере компьютерных игр и обеспечении безопасности пользователей виртуального пространства. Таким образом, технические средства для предотвращения преступлений в сфере компьютерных игр могут быть различными, и заключаются в основном в создании таких программ и систем, которые смогут следить за подозрительной активностью, негативным проявлением, и иными преступными явлениями в сфере киберпространства.

Список источников

1. Гильманов Т. Э., Гордеев М. А. Мошенничество в компьютерных играх путем создания фейкового аккаунта // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова — 2022 : материалы XII Международной научно-практической конференции студентов и аспирантов (Казань, 16 декабря 2022 г.). В 3 т. Т. 3. Казань : Познание, 2023. С. 292–293.

2. Нечаева Е. В., Латыпова Э. Ю., Гильманов Э. М. Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27, № 1. С. 80–86.

3. Гильманов Т. Э., Гордеев М. А. Мошенничество в сфере компьютерных игр: постановка проблемы // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова — 2022 : материалы XII Международной научно-практической конференции студентов и аспирантов (Казань, 16 декабря 2022 г.). В 3 т. Т. 3. Казань : Познание, 2023. С. 293–295.

4. Латыпова Э. Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 35–45.

5. Гильманов Т. Э., Гордеев М. А. Способы использования мошенниками бесплатных скриптов для компьютерных игр // Казанские научные чтения студентов и аспирантов имени В. Г. Тимирясова — 2022 : материалы XII Международной научно-практической конференции студентов и аспирантов (Казань, 16 декабря 2022 г.). В 3 т. Т. 3. Казань : Познание, 2023. С. 295–296.

6. Латыпова Э. Ю., Гильманов Э. М., Абдуллина А. Е., Гильманов Р. Э. Влияние нравственно-моральных норм на содержание уголовно-правовых норм в Уголовном кодексе России // Вестник экономики, права и социологии. 2022. № 1. С. 93–99.

7. Зелепукин В. Ю. Программные средства защиты информации // Теория и практика современной науки. 2017. № 5 (23). С. 304–307.

8. Бегишев И. Р. Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021. Т. 11, № 4. С. 207–220.

9. Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 79–91.

10. Latypova E. Yu., Nechaeva E. V., Gilmanov E. M., Aleksandrova N. V. Infringements on Digital Information: Modern State of the Problem // SHS Web of Conferences. 2019. Vol. 62, Art. 10004. DOI: https://doi.org/10.1051/shsconf/20196210004

© Э. Ю. Латыпова, Р. Э. Гильманов, Р. Р. Бадрутдинов

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

ВКЛАД АВТОРОВ

Латыпова Э. Ю. — идея, определение и формулировка проблемы, научное руководство, формулировка выводов;

Гильманов Р. Э. — подбор научной литературы и судебной практики, исследование преступлений в сфере компьютерных игр;

Бадрутдинов Р. Р. — исследование проблемы преступлений в сфере компьютерных игр и роли правоохранительных органов в их предупреждении.

CONTRIBUTION OF AUTHORS

Latypova E. Yu. — idea, definition and formulation of the problem, scientific guidance, formulation of conclusions;

Gilmanov R. E. — selection of scientific literature and judicial practice, research of crimes in the sphere of computer games;

Badrutdinov R. R. — research of the problem of crimes in the sphere of computer games and the role of law enforcement agencies in their prevention.

Дата поступления статьи / Received: 11.03.2024.
Дата рецензирования статьи / Revised: 19.04.2024.
Дата принятия статьи к публикации / Accept: 25.05.2024.

© Э. Ю. Латыпова, Р. Э. Гильманов, Р. Р. Бадрутдинов