УДК 343.97

# СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

**А. В. Яшин[1], Т. А. Фролова[2]**

[1,2]Пензенский государственный университет, Пенза, Россия

[1]andrej.yashin@yandex.ru
[2]tanafrolova497@gmail.com

***Аннотация.*** Исследуются актуальные проблемы, связанные с предупреждением преступлений, совершаемых в сфере компьютерной информации либо с использованием информационно-телекоммуникационных технологий. Отмечается, что в последние годы население Российской Федерации перешло на мобильные коммуникации, вследствие чего виртуальное пространство стало неотъемлемой частью жизни людей. Вместе с тем в стране ежегодно увеличивается число зарегистрированных киберпреступлений, посягающих на разнообразные общественные отношения. Преступные деяния, осуществляемые злоумышленниками в информационном пространстве, относятся к довольно опасным и непредсказуемым, поскольку причиняют серьезный вред личности, обществу и государству. Делается вывод о том, что киберпреступления представляют угрозу не только для общественной, но и национальной безопасности России. В целях противодействия их совершению предлагаются меры организационного и правового характера, направленные на повышение эффективности деятельности правоохранительных органов в рассматриваемой сфере.

***Ключевые слова***: виртуальное пространство, киберпреступления, компьютерные технологии, персональные данные, правоохранительные органы, киберпространство, цифровизация, киберугрозы

***Для цитирования***: Яшин А. В., Фролова Т. А. Современные проблемы противодействия киберпреступлениям в Российской Федерации // Вестник Пензенского государственного университета. 2023. № 2. С. 58–62.

Вопросы противодействия киберпреступлениям являются довольно актуальными не только в современной России, но и во всем мире. Это связано с тем, что любая информация обладает исключительной важностью и является тем ресурсом, который оказывает огромное влияние на все сферы жизни. Общение посредством сети Интернет занимает значительную часть времени любого члена общества, поскольку уже во всем мире население перешло на мобильные коммуникации и такой способ общения считается самым удобным, оптимальным и быстрым. Тем не менее, помимо многих указанных положительных моментов, существуют довольно серьезные проблемы, связанные с обеспечением информационной безопасности пользователей сети Интернет, а также защитой их персональных данных от несанкционированного доступа и вмешательства со стороны злоумышленников.

К сожалению, за последнее десятилетие в информационном пространстве во много раз увеличилось число лиц, обладающих специальными знаниями и высоким уровнем квалификации [1, с. 97], которые входят в организованные преступные кибергруппы с со-

© Яшин А. В., Фролова Т. А., 2023

временной технической оснащенностью [2, с. 470]. При этом киберпреступники нередко координируются в своей деятельности, используя стратегии прогресса, и достаточно талантливы в сфере кибербизнеса [3, с. 61].

В настоящее время персональные данные каждого гражданина Российской Федерации хранятся в облачных сервисах либо на цифровых носителях. Современными и достаточно удобными местами хранения персональных данных, которые не требуют дополнительной памяти на собственном устройстве, считаются платные серверы. Общеизвестно, что прогресс цифровизации позволяет повысить эффективность использования компьютерных технологий и упростить их эксплуатацию. Однако наряду с этим создаются угрозы проникновения злоумышленников в серверы для хищения личной информации пользователя, вследствие чего правоохранительным органам необходимо повышать эффективность реализации мероприятий по защите жертв киберпреступлений [4, с. 126].

В последние годы многие преступники стали переходить на дистанционный формат в целях реализации своих противоправных действий. Во многом это связано с распространением новой коронавирусной инфекции COVID-19, вследствие чего произошло переструктурирование преступности. В России ежегодно наблюдается снижение уличной преступности, в то же время фиксируется рост зарегистрированных общественно опасных деяний, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступлений), и, согласно официальным статистическим данным, в 2022 г. темп их прироста составил 0,8 % [5]. Это объясняется тем, что молодежь, которая составляет существенную часть населения страны, уходит в социальные сети, тем самым изолируясь от общества.

Киберпреступления совершаются, как правило, при помощи таких основных информационно-технических средств, как:

– мессенджеры (Telegram, Viber, WhatsApp);
– смартфоны;
– интернет-ресурсы (социальные сети, сайты знакомств, форумы);
– средства массовой информации в сети Интернет;
– онлайн-игры;
– навигационная аппаратура;
– беспилотные летательные аппараты [6, с.154].

По оценкам Интерпола преступления, совершаемые в сети Интернет, считаются самыми скоротечными во всем мире. Общественно опасные деяния, осуществляемые виновными в информационном пространстве, относятся к самым непредсказуемым и опасным, поскольку ущерб, причиненный такими видами посягательств, не имеет границ. К сожалению, правоохранительные органы не располагают достоверной информацией о состоянии преступлений в сфере киберпространства в силу их высокого уровня латентности.

На фоне распространения новой коронавирусной инфекции к настоящему времени сложилась определенная классификация киберпреступлений. К ним можно отнести следующие виды:

– публичная пропаганда ложной информации о пандемии COVID-19 и о мерах по противодействию распространения заболеваемости на территории Российской Федерации;

– обман граждан через фишинговые сайты, где происходит сбыт поддельных вакцин, антисептиков, сертификатов о вакцинации; посредством таких сайтов мошенники могут получить и личные персональные данные пользователей [7, с. 88];

– неправомерный доступ к компьютерной информации, в частности, срыв дистанционного учебного занятия;

– несанкционированное проникновение на сайты государственных органов власти, здравоохранения, социальных служб для получения служебной информации в личных целях;

– противоправные деяния на игровых онлайн-платформах;

– кибersталкинг;

– незаконный оборот наркотических средств, психотропных веществ или их аналогов [8, с. 96];

– кибертерроризм;

– мошеннические деяния в банковской сфере и т.д. [9, с. 36].

Следует отметить, что за последние три года чаще всего кибератакам подвергались органы здравоохранения, что неудивительно, поскольку в данный период граждане особо остро нуждались в лекарственных средствах либо способах приобретения вакцины [10, с. 101–102].

В настоящее время во всем мире, в том числе и России, стремительный рост набирает игровая индустрия, которая, во многом благодаря пандемии, подталкивает людей искать новые способы развлечений и общения. Получив такой мощный толчок, игровая отрасль до сих пор остается на подъеме, несмотря на смягчение ограничений. Онлайн-игры считаются достаточно прибыльной платформой, где заработки осуществляются посредством продажи предметов в формате онлайн и осуществления разнообразных подписок. Игровой онлайн-проект постепенно переходит на монетизацию, что становится более привлекательным полем для кибератак [11, с. 175].

Игровые пользователи в целях оптимизации компьютерной системы во время онлайн-игр нередко отключают антивирусные программы, снижая тем самым безопасность самого устройства и своих пользовательских данных. Такая ситуация создает благоприятную почву для преступной деятельности хакеров, приводя онлайн-игроков к следующим видам угроз:

– заражение устройств вредоносными программами, основная опасность которых заключается в способности следить за вводом клавиатуры и изымать с носителей информацию, относящуюся к игровым пользователям и учетным данным [12, с. 29];

– переход на фишинговые сайты, где находятся фальшивые игровые площадки, причем некоторые мошенники используют при этом поддельные URL-адреса, очень схожие с официальными сайтами, что способствует не только причинению вреда пользователю вирусными программами, заложенными на таком сайте, но и хищению у него денежных средств [13, с. 47];

– создание мошенниками специализированных учетных записей, активированных в качестве администраторов сайтов для похищения личных данных пользователей.

В юридической литературе справедливо отмечается, что масштабы и серьезность угроз киберпреступности в последние годы достигли очень высокого уровня, вследствие чего в сфере обеспечения кибербезопасности недостаточно совершенствования только программного обеспечения. Для наиболее эффективной борьбы с киберпреступлениями необходима разработка действенных мер как организационного, так и правового характера [14, с. 102].

В целях противодействия киберпреступлениям предлагается следующее:

– реорганизовать специализированное обучение сотрудников правоохранительных органов, для чего создать программы обучения и переподготовки кадров по таким предметам, как «Основы и методы борьбы с киберпреступностью», «Социальная инженерия», «Правовые основы информационной безопасности»;

– внести изменения и дополнения в ст. 272.1 УК РФ, изменив словосочетание «неправомерный доступ к охраняемой законом компьютерной информации» на «получение путем введения в заблуждение или методом социальной инженерии», поскольку непра-

вомерным доступом является незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации.

В качестве мер, разрабатываемых для предотвращения кибератак, необходимо также минимизировать количество киберпреступлений в сети Интернет путем просвещения населения. Создание эффективной системы оповещения об опасности киберпреступности и мошенничества в сфере компьютерных технологий путем размещения рекламы в школах, средних и высших образовательных организациях, государственных учреждениях, а также транслирования в средствах массовой информации предупредит большую часть населения об опасности, которая может встретиться в сети Интернете.

В качестве мер индивидуальной профилактики киберпреступлений следует проводить разъяснительные беседы с гражданами и обучающимися в учебных заведениях, организовывать и проводить конференции об опасности кибератак и о новых способах, которые помогут обезопасить личные данные пользователей в сети Интернет и на компьютерных носителях. Кроме того, надлежит периодически опубликовывать актуальные новости в интернет-источниках и социальных сетях, чтобы предупредить распространение киберпреступности в игровой и информационной платформах.

Для разработки и усовершенствования методов борьбы с информационными преступлениями необходимо доводить до граждан актуальные статистические сведения о киберпреступности в России, изучить опыт правоохранительных органов в осуществлении информационно-технической защиты населения от мошенников в виртуальном мире и доводить его результаты до населения через средства массовой информации [15, с. 21]. Полезным будет и проведение анализа судебной практики и нормативно-правовой базы, изучение технического обеспечения, рассмотрение сравнительной статистики раскрываемости преступлений в сфере компьютерных технологий. Это позволит разработать новые методы для сокращения кибератак. Следует также перенять и зарубежную практику противодействия киберпреступлениям, поскольку анализ международного опыта способствует выработке наиболее эффективных и современных методов воздействия на киберпреступления. Кроме того, предлагается разработать методические рекомендации, включающие в себя научно-практические советы по устранению пробелов в законодательстве и его совершенствованию, а также разработку новых мер воздействия на мошенников, работающих в дистанционном формате, в целях нейтрализации формирования их преступного поведения [16, с. 85].

На основании изложенного следует сделать вывод, что общественно опасные деяния, совершаемые с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступления), представляют серьезную угрозу национальной безопасности Российской Федерации. Следует полагать, что вышеприведенные предложения смогут снизить уровень киберпреступности и оказать превентивное воздействие на лиц, склонных к осуществлению данных противоправных посягательств.

### *Список литературы*

1. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Сер.: Философские науки. 2021. № 1. С. 95–101.

2. Яковлева М. А. Алгоритм мер эффективной работы правоохранительных органов в сфере предупреждения киберпреступности // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований : материалы междунар. науч.-практ. конф. (г. Санкт-Петербург, 7 декабря 2018 г.). СПб. : С.-Петербург. ун-т МВД России, 2019. С. 469–473.

3. Иванова Ю. А., Сарбаев Г. М. К вопросу о киберпреступности // Цифровые трансформации экономики и права : сб. науч. тез. по материалам Национальной науч.-практ. конф. «Цифровые технологии и управление качеством в технических системах» (г. Москва, 8 декабря 2021 г.). Волгоград : ИП Черняева Ю. И., 2022. С. 58–64.

4. Яшин А. В. Типология жертв преступлений – участников уголовного судопроизводства // Современное право. 2011. № 6. С. 126–128.

5. Статистика и аналитика // Официальный сайт МВД России. URL: https://мвд.рф (дата обращения: 27.02.2023).

6. Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Правовая парадигма. 2020. Т. 19, № 1. С. 151–157.

7. Задера В. В. Проявление киберпреступности на игровых онлайн-платформах: пути законодательного решения // Киберпреступность: риски и угрозы : материалы Всерос. студ. круглого науч.-практ. стола с Междунар. участием (г. Санкт-Петербург, 11 февраля 2021 г.). СПб. : Астерион, 2021. С. 87–90.

8. Чуманов А. С. Проблемы противодействия незаконному обороту наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей // Киберпреступность: риски и угрозы : материалы Всерос. студ. круглого науч.-практ. стола с Междунар. участием (г. Санкт-Петербург, 11 февраля 2021 г.). СПб. : Астерион, 2021. С. 96–99.

9. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10. С. 35–37.

10. Маньков М. А. К вопросу об уголовной ответственности за кибертерроризм // Киберпреступность: риски и угрозы : материалы Всерос. студ. круглого науч.-практ. стола с Междунар. участием (г. Санкт-Петербург, 11 февраля 2021 г.). СПб. : Астерион, 2021. С. 100–105.

11. Мартьянов Н. Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. 2020. № 1. С. 175–177.

12. Маслиенко М. А. Киберпреступность на современном этапе // Проблемы правоохранительной деятельности. 2021. № 2. С. 28–32.

13. Номоконов В. А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45–55.

14. Кобец П. Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт // Научный вестник Омской академии МВД России. 2022. № 2. С. 101–105.

15. Яшин А. В. Постпреступное поведение : автореф. дис. … канд. юрид. наук. Саратов, 2005. 22 с.

16. Яшин А. В. К вопросу о преступном поведении и его механизме // Успехи современного естествознания. 2005. № 1. С. 84–85.

### *Информация об авторах*

***Яшин Андрей Владимирович,*** доктор юридических наук, профессор кафедры «Правоохранительная деятельность», Пензенский государственный университет

***Фролова Татьяна Александровна,*** студентка, Пензенский государственный университет

***Авторы заявляют об отсутствии конфликта интересов.***