АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГОСУДАРСТВА И ПРАВА
2023. Т. 7. № 4
http://journals.tsutmb.ru/current-issues-of-the-state-and-law/

AKTUAL'NYE PROBLEMY GOSUDARSTVA I PRAVA =
= CURRENT ISSUES OF THE STATE AND LAW
2023, vol. 7, no. 4
http://journals.tsutmb.ru/current-issues-of-the-state-and-law-eng/
ISSN 2587-9340 (Print) ISSN 2782-3334 (Online)

НАУЧНАЯ СТАТЬЯ
УДК 343.97
https://doi.org/10.20310/2587-9340-2023-7-4-610-619
Шифр научной специальности 5.1.4

Киберпространство как место совершения преступлений: современные тенденции, особенности, меры предупреждения

© ТРУФАНОВА Александра Юрьевна,
юрист, ООО АФ «Реут», Российская Федерация, Курская область, Медвенский р-он, 307048, с. Верхний Реутец, https://orcid.org/0000-0002-9556-5789, trufanovaalexandra@gmail.com
© СИНЯЕВА Мария Ивановна,
старший преподаватель кафедры уголовного права, ФГБОУ ВО «Юго-Западный государственный университет», Российская Федерация, 305040, г. Курск, ул. 50 лет Октября, 94, https://orcid.org/0000-0003-3477-5448, mari_sinyaeva@mail.ru

Аннотация

Актуальность данной темы обусловлена тем, что развитие технологий, распространенность компьютерной техники и сети Интернет среди населения привели к возникновению глобальной для общества проблемы – киберпреступности. Цель настоящего исследования – провести анализ преступлений, совершенных в информационно-цифровом пространстве в Российской Федерации и определить меры предупреждения для различных сфер данного вида преступлений. На сегодняшний день мы еще не говорим о своевременном повсеместном предотвращения киберпреступности правоохранительными органами, считаем необходимым развивать законодательное регулирование этого направления деятельности и обеспечивать в обязательном порядке необходимую переподготовку правоохранительных органов для повышения знаний в области предупреждения, предотвращения и раскрытия киберпреступлений. Методологию составляют диалектический, структурный, формально-юридический и сравнительно-правовой методы, анализ и синтез. Проанализирована история и причины возникновения преступлений в кибернетическом пространстве, исследованы особенности кибератак и киберпреступлений в различных сферах, а также предложены меры предупреждения для соответствующей преступности. Отмечено, что правовые механизмы ответственности за некоторые виды преступлений отсутствуют в законодательстве из-за постоянно изменяющихся способов совершения преступлений, при которых также возникает сложность их раскрытия у правоохранительных органов. Их решение видится в комплексном применении мер предупреждения, своевременном изменении законодательства и регулярной переподготовки правоохранительных органов.

Ключевые слова

киберпространство, кибернетическое пространство, информационные преступления, киберпреступность, Интернет, компьютеры, компьютерные сети, компьютерные программы

Для цитирования

Труфанова А.Ю., Синяева М.И. Киберпространство как место совершения преступлений: современные тенденции, особенности, меры предупреждения // Актуальные проблемы государства и права. 2023. Т. 7. № 4. С. 610-619. https://doi.org/10.20310/2587-9340-2023-7-4-610-619

ORIGINAL ARTICLE
https://doi.org/10.20310/2587-9340-2023-7-4-610-619

Cyberspace as a crime scene: current trends, features, prevention measures

© Alexandra Yu. TRUFANOVA,
Lawyer, LLC AF "Reut", Verkhny Reutets Vlg. 307048, Medvensky District, Kursk Region, Russian Federation, https://orcid.org/0000-0002-9556-5789, trufanovaalexandra@gmail.com
© Maria I. SINYAEVA,
Senior Lecturer of Criminal Law Department, Southwestern State University, 94 50 Let Oktyabrya St., Kursk, 305040, Russian Federation, https://orcid.org/0000-0003-3477-5448, mari_sinyaeva@mail.ru

Abstract

The relevance of this topic is due to the fact that the development of technology, the prevalence of computer technology and the Internet among the population have led to the emergence of a global problem for society – cybercrime. The purpose of this study is to analyze crimes committed in the information and digital space in the Russian Federation and determine preventive measures for various areas of this type of crime. Today, we are not yet talking about the timely universal prevention of cybercrime by law enforcement agencies; we consider it necessary to develop legislative regulation of this area of activity and to ensure the necessary retraining of law enforcement agencies to increase knowledge in the field of prevention, prevention and detection of cybercrimes. The methodology consists of dialectical, structural, formal legal and comparative legal methods, analysis and synthesis. The history and causes of crimes in the cyberspace are analyzed, the features of cyber attacks and cybercrimes in various fields are studied, and preventive measures for the corresponding crime are proposed. It is noted that the legal mechanisms of responsibility for some types of crimes are absent in the legislation due to the constantly changing methods of committing crimes, which also make it difficult for law enforcement agencies to solve them. Their solution is seen in the comprehensive application of preventive measures, timely changes in legislation and regular retraining of law enforcement agencies.

Keywords

cyberspace, cybernetic space, information crimes, cybercrime, Internet, computers, computer networks, computer programs

For citation

Trufanova, A.Yu., & Sinyaeva, M.I. (2023). Cyberspace as a crime scene: current trends, features, prevention measures. *Aktual'nye problemy gosudarstva i prava = Current Issues of the State and Law*, vol. 7, no. 4, pp. 610-619 (In Russ., abstract in Eng.) https://doi.org/10.20310/2587-9340-2023-7-4-610-619

Введение

Широкое развитие технологий в сфере информационной коммуникации началось в 1990-х гг., когда люди пришли к выводу, что внедрение компьютерных технологий в работу крупных организаций, государственных учреждений, школ, университетов повысит эффективность работоспособности всех сотрудников, а также обеспечит сокращение времени и простоту выполнения различных задач. В начале 1996 г. в связи с тем, что внутренняя политика государства начала стабилизироваться, в государстве начали появляться крупные фирмы, которым было необходимо подключение к IT-технологиям. Образовательный процесс, особенно в высших учебных заведениях, стал переходить к тенденции информационных технологий.

Понимая, как удобен мир технологий в любой сфере жизнедеятельности, люди начали стремиться к получению образования в сфере программирования и IT-технологий. Постепенно в стране начали появляться как специалисты в информационных технологиях, так и новые сами технологии, которые расширяли круг функций и возможностей.

Уже в 1992 г. появился Комитет информатизации при Минкомсвязи Российской Федерации. В 1994 г. президент России Б.Н. Ельцин издал Указ, согласно которому органы государственной власти должны были перейти на полное обеспечение инфор-

мационными технологиями. До 2006 г. активно развивались технологии именно в сфере государственного управления. Но, несмотря на это, гражданское общество также не останавливалось на месте, поэтому начали возникать предпосылки для создания правового регулирования в информационно-цифровом пространстве. В 2006 г. вступил в законную силу Федеральный закон «Об информации, информационных технологиях и о защите информации».

За развитием информационных технологий последовало развитие и распространение уже глобальной сети Интернет. Так, к концу XX века число пользователей достигало всего 70 000 человек, а уже в 2009 г. – 2 300 000. К 2012 г. показатель количества пользователей увеличился почти в 3 раза и достиг численности – 8 700 000[1]. На сегодняшний день число пользователей составляет 5,16 миллиарда человек[2].

Эксперты связывают дальнейшее развитие информационных технологий с использованием нанотехнологий и суперкомпьютеров в XXI веке, для того чтобы выполнять различные процессы с использованием комбинированных вычислений в любом месте мира посредством сети Интернет [1, с. 37].

Развитие кибернетического пространства повлекло за собой возникновение нарушений прав граждан путем утечки информации в информационных системах, незаконного использования персональных данных, хакерских атак и взломов, внедрения вирусных технологий и других приемов, которые существуют наравне с деятельностью пользователей в информационно-правовой сфере.

Преступность в информационно-цифровом пространстве является актуальной сферой преступлений в XXI веке. При этом кибернетическое пространство выступает не только местом совершения преступлений, но и порождает возможности совершения преступлений путем использования информационно-цифровых возможностей, например, использование криптовалюты как средства оплаты заказных преступлений или как средства, на которое покушается преступник.

Наиболее распространенными являются преступления в экономической сфере, в сфере интеллектуальной собственности, в сфере экстремизма и терроризма, в сфере незаконного оборота наркотических средств.

В то же время кибернетическое пространство выступает полем для борьбы с вышеуказанной преступностью, так как в сети Интернет размещаются публикации, направленные на борьбу с преступностью, создаются группы, идеологией которых установлена цель по снижению преступности. После пандемии 2020 г. в России получило распространение дистанционное образование, в нашем случае оно также может выступать средством противодействия киберпреступности, то есть граждане могут проходить курсы по повышению грамотности в сфере антипреступности, а правоохранительные органы проходить дистанционную переподготовку по специализированным темам. Деятельность государства как на федеральном, так и на региональном и муниципальном уровнях связана с информирование граждан о тех или иных способах совершения преступлений в информационно-цифровом пространстве на личных порталах. Таким образом, кибернетическое пространство выступает не только полем совершения преступлений, но и полем для борьбы с такой преступностью.

Но, к сожалению, уровень преступности в кибернетическом пространстве с каждым годом не уменьшается, поэтому для снижения такого уровня требуется внедрение мер противодействия и предупреждения. Только путем данных профилактических мер преступность в информационно-цифровой сфере начнет снижаться.

Результаты исследования

История начала преступности в информационно-цифровом пространстве началась совсем недавно – с конца XX века. Данный промежуток времени определил новый этап развития человечества, который характеризуется оборотом информации в обществе. Информационное общество – это такой тип общества, в котором информация является

[1] Краткий пересказ: IT технологии // Steppe. URL: https://the-steppe.com/kcell-recap?i=it (дата обращения: 29.06.2023).

[2] Статистика Интернета и соцсетей на 2023 год – цифры и тренды в мире и в России // WebCanape. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения: 28.06.2023).

наиважнейшей единицей, наблюдается тенденция распространения и применения информации во всех сферах жизнедеятельности, включая сферу кибернетического пространства. Такое общество не может существовать без информационно-коммуникационных технологий и различных сетей, посредством которых передается вся информация.

С развитием цифровых технологий появилась новая сфера деятельности, в которой происходят все технологические процессы – киберпространство.

Вследствие масштабного распространения технических средств, их доступностью среди населения возникла и продолжает развиваться опасная для общества проблема – киберпреступность. Под киберпреступлением понимают виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные общественно опасные деяния, совершаемые с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера пространству [2, с. 10].

Выделяют несколько этапов преступности в информационно-цифровом пространстве.

Первый этап. В этот период только начинают появляться компьютерные технологии, поэтому как таковой киберпреступности в обществе нет, но начинают появляться предпосылки таких действий.

Интернет как безграничное пространство для передачи информации зарождается в 1960-х гг. Первым киберпреступником стал Дж. Дрейпер. Для тех времен телефонная связь была роскошью, которая была не у всех и очень дорого стоила, поэтому первые информационные преступления были связаны именно с незаконным использованием связи. Так, Дж. Дрейпер решил попробовать частоту звука от свистка, который всегда был подарком в коробке с кукурузными хлопьями. Удивительно, частота свистульки и частота электрического сигнала доступа в телефонную сеть дальней связи совпали. Так, злоумышленник путем звука свистка во время набора номера взламывал телефонную сеть и разговаривал бесплатно[3].

Второй этап. Данный период характеризуется появлением таких опасных для общества личностей – хакеров. Первой хакерской атакой занимались подростки, которые прозвали себя «группа 414». За 9 дней они взломали 60 компьютеров, в числе которых были компьютеры Лос-Аламосской государственной лаборатории, занимающейся исследованием ядерного оружия [3, с. 882].

Резкое поднятие уровня кибератак на компьютерные средства поспособствовало созданию Центра исследования интернет-безопасности CERT, который в настоящее время именуется как Компьютерная группа реагирования на чрезвычайные ситуации.

Третий этап. Этот период характеризуется началом 1990-х гг., когда технологии уже начинают приобретать более изученную совокупность программного обеспечения и всех специфических функций.

В это время совершается первое киберпреступление, субъектами которого оказался русский народ. В 1994 г. весь мир узнал о «деле Владимира Левина», которое получило статус «транснационального сетевого компьютерного преступления» [3, с. 882]. Им были похищены денежные средства из американского банка и переведены на счета тоже русских людей.

Четвертый этап. Данный период имеет свои особенности: деятельность массовых хакерских группировок и кибертерроризм. Временные рамки данного периода не ограничены – с зарождения хакерских группировок (примерно 2000-е гг.) и по настоящее время.

Опасность данного этапа заключается в том, что жертвой таких преступлений выступает чаще всего государство в лице его органов. Так, например, путем DoS атаки было осуществлено приостановление деятельности сайта администрации Курской области[4].

[3] Взлом телефона свистком из коробки хлопьев: история первого хакера // Яндекс Дзен. 2020. 4 июня. URL: https://dzen.ru/media/izzznanka/vzlom-telefona-svistkom-iz-korobki-hlopev-istoriia-pervogo-hakera-5ed8ff9f7275d0171ebef139 (дата обращения: 25.06.2023).

[4] Сайт администрации Курской области снова подвергся хакерской атаке // Курские известия. 2022.

Именно такими преступлениями характеризуется информационная война. В связи с началом специальной военной операции на Украине хакерские атаки увеличиваются. Данный способ незаконного получения информации дает возможность узнать тайную информацию, то есть служит разведкой для совершения опасных для общества деяний.

Таким образом, на сегодняшний день уровень опасности от совершаемых преступлений в информационно-цифровом пространстве достиг высокого развития. Такого рода преступления совершаются ежеминутно в международном пространстве: каждый день гражданам поступают звонки от неизвестных номеров, которые направлены на извлечение персональной информации, каждый день в сети Интернет публикуются материалы, которые призывают к совершению общеопасных действий, каждый день осуществляются кибератаки на важнейшие информационные ресурсы стран и иные общественно опасные деяния. Большинство данных преступлений способствуют причинению вреда отношениям, связанным с собственностью и осуществлением предпринимательской или иной экономической деятельности, но не стоит забывать, что еще существуют террористические преступления, которые также могут причинить вред не определенному человеку, а всему обществу. Тенденции развития информационных технологий опережают трансформацию законодательства, поэтому некоторые преступления сложно определить и приходится использовать аналогию закона или права. Тем не менее российское законодательство в настоящий момент находится не на самом низком уровне развития, поэтому большинство преступлений, совершенные в сфере информационно-цифрового пространства, находят применение в уголовном кодексе.

Для того чтобы снизить уровень преступности в информационно-цифровой сфере, необходимо разработать комплекс мер, который будет оказывать влияние на граждан и работать «регулятором» предупреждения преступности.

Предупреждение преступности может быть эффективным только в случае, если оно базируется на адекватном представлении государства о специфике ее криминогенных детерминант, состоящих из комплекса причин и условий преступности, темпы роста которой превратились в одну из главных угроз национальной безопасности страны [4, с. 216].

Система мер предупреждения преступности в кибернетическом пространстве имеет свои особенности:

1) объектом всегда является конкретный киберперступник или конкретная киберпреступная группа, в отношении которых осуществляется профилактическое воздействие;

2) субъекты представляют собой органы государственной власти, должностных лиц, организации, граждан, которые непосредственно осуществляют меры воздействие на объекты;

3) содержание предупредительной деятельности включает в себя специализированные меры, способы и формы;

4) обеспечение предупредительной деятельности определяется конкретной базой, включающей в себя нормативно-правовые и организационные средства.

Меры предупреждения преступности в информационно-цифровом пространстве являются главным звеном в профилактике преступлений. Именно правовые методы борьбы с преступностью занимают в этой системе главенствующее место. Такие меры исходят не только из разработки новых нормативно-правовых актов и действующего законодательства, но и содержат профилактические меры, направленные на информирование населения каким-либо способом.

К правовым мерам предупреждения преступности, в первую очередь, следует отнести совершенствование законодательства. Необходимо увеличить уголовную ответственность за имеющиеся в уголовном законодательстве составы преступлений, связанные с информационной средой и компьютерными технологиями. Так, у преступников будет возникать сомнение в отношении совершения общественно опасных деяний, так как вероятность применения более длительного наказания или более дорогостоящего штрафа будет отталкивать преступников. Также с

16 июня. URL: https://kursk--izvestia-ru.turbopages.org/kursk-izvestia.ru/s/news/186091/ (дата обращения: 25.06.2023).

развитием коммуникационных цифровых технологий требуется внедрение в законодательство новых составов преступления.

Проведя анализ совершенных преступлений за 2019–2022 гг., можно сделать вывод, что критический рост преступности в информационно-цифровом пространстве наблюдался в 2019 и 2020 гг., так как в 2019 г. совершено более 294000 преступлений, что составило динамику прироста на 70 % по сравнению с 2018 г. Причем 50 % таких преступлений были совершены в сети Интернет[5]. В 2020 г. количество киберпреступности увеличилось на 73,4 %, из которых 91,3 % заняли интернет-преступления[6]. За 12 месяцев 2021 г. преступность, связанная с компьютерными технологиями, увеличилась всего лишь на 1,4 %[7]. В 2022 г. киберпреступность осталась на том же уровне, стабильность таких преступлений характеризует следующим соотношением: каждое четвертое преступление совершено с применением высоких технологий. Несмотря на стабильность киберпреступлений, прогрессивных показателей достигла их раскрываемость – увеличилась на 4,4 %[8].

Деятельность по раскрытию преступлений, которая к 2022 г. смогла привести к минимализации киберпреступности, характеризуется именно внедрением правовых мер. Правоприменительная практика сформировалась, поэтому привлечь к уголовной ответственности преступника стало намного проще, чем было раньше. У преступников появилось опасение быть наказанным, поэтому количество преступлений перестало в огромном масштабе набирать обороты. Но, несмотря на данное снижение роста преступности, к 2023 г. преступность в информационно-цифровом пространстве может увеличиться до 30 %, так как преступления стали обладать низкой раскрываемостью и слабой возможностью определения интернет-преступников[9].

Рассмотрим меры предупреждения кибернетической преступности по основным сферам.

1. Преступления, связанные с виртуальной валютой.

Совершенствование банковской сферы привело к тому, что в мире создали особенную виртуальную валюту – криптовалюту. Цифровая валюта используется пользователями для злоупотребления в различных сферах. Такую валюту принимают на «черных рынках», для покупки наркотических средств, для совершения киберпреступлений и иных действий, которые запрещает законодательство Российской Федерации. В РФ данная валюта не распространяется как повсеместное средство платежа, но регулируется в некоторой степени ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[10].

Для предупреждения и снижения таких преступлений требуется применить следующие меры:

– ввести за незаконные оборот криптовалюты административную и уголовную ответственность в зависимости от количества совершенных преступлений и их тяжести, в том числе включить использование криптовалюты как отягчающую меру для разных видов преступлений;

[5] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 г. // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 18.06.2023).

[6] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 г. // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 18.06.2023).

[7] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2021 г. // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 18.06.2023).

[8] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2022 г. // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 18.06.2023).

[9] По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений // Известия. 2020.13 янв. URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii (дата обращения: 20.06.2023).

[10] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации. 2020. № 31. Ст. 5153.

– ограничить доступ к «черным рынкам» для снижения преступности, используемой средствами криптовалюту;

– обеспечить персональный характер криптовалюты для раскрытия преступлений такого характера.

2. Экономическая преступность в киберпространстве чаще всего проявляется в виде мошенничества или взлома. Зафиксировать преступника крайне сложно, так как в большинстве случаев устанавливается анонимность пользователей.

С переходом банков в формат интернет-банкинга появилась угроза информационной безопасности по отношению не только к персональным данным клиентов, но и к информации служебного пользования [5, с. 47]. Из-за санкционных мер большинство программных обеспечений не подлежат обновлению (например, приложения банков и программы, используемые банковскими сотрудниками), а это, в свою очередь, повышает вероятность кибератак и кражу денежных средств [6, с. 75].

Меры предупреждения данного вида преступности могут быть различны: как правовые, так и социальные:

– требуется обеспечить защиту от мошенничества в онлайн-банках и электронных кошельках. Например, Сбербанк предлагает своим клиентам страхование карты от мошенников[11]. Но почему банк навязывает такую услугу, если основная задача банка – сохранение доверенных денег. Банк изначально отвечает за сохранность денежных средств на счетах клиентов, но при этом предлагает услугу – защиту от мошенников. Полагаем, что все банки в РФ должны обеспечивать сохранность денежных средств от мошенников без дополнительных услуг;

– просвещение граждан в сфере экономической безопасности. Проведение ежемесячных лекций по сохранности денежных средств в школах обеспечит с ранних лет граждан знаниями и защитит их в будущем от преступников;

– совершенствование технических функций цифрового пространства – это поможет снизить преступность в большом количестве, так как технические ограничения для хакеров не дадут им совершить определенные действия.

3. Сфера интеллектуальной собственности занимает особое место среди преступности в сети Интернет, так как предотвратить ее считается почти невозможным. Интеллектуальная собственность включает себя достаточно обширный перечень, поэтому преступления могут быть разного характера.

Предлагаются следующие меры предупреждения:

– усиление контроля со стороны специализированных должностных лиц правоохранительных органов по интеллектуальной собственности в сети Интернет;

– создание единой всемирной базы товарных знаков, так как Интернет является глобальной сферой, поэтому могут быть нарушены права, если под несколькими одинаковыми товарными знаками будет осуществляться какая-либо деятельность;

– создание мини-методички для граждан «Как публиковать информацию в цифровом пространстве, если используешь сведения других лиц»;

– введение водяных знаков, которые располагаются на электронных копиях изображений и фотографий. Данные знаки наносятся с помощью специального программного обеспечения. Водяные знаки включают в себя сведения об авторе и дате изготовления продукта интеллектуального труда [7, с. 120].

4. Терроризм и экстремизм являются глобальной проблемой всей планеты, так как уровень опасности таких деяний самый высокий. Поэтому такие проблемы, как террористические преступления и преступления, включающиеся в себя признаки экстремизма, можно решить только путем международного сотрудничества. Обычно совершение таких преступлений достигается путем использования кибернетического пространства.

Меры предупреждения, прежде всего, должны быть направлены на людей, чтобы избежать опасности от данных преступлений:

– во всех государствах должна быть пропаганда мира на Земле, то есть идеология государств должна быть направлена именно на мирное существование, которое предполагает отсутствие террористических актов, разрушения государственных основ, войн и т. д.;

[11] Защита карт «Сбереги финансы» (Активация Антивируса) // СберСтрахование. URL: https://sberbankins.ru/products/zkantivirus/ (дата обращения: 20.06.2023).

– в дошкольных и школьных учреждениях должна быть предусмотрена культурная и образовательная программа, которая поспособствует пропаганде антитеррора и антиэкстремизма (конкурсы, квесты, интеллектуальные игры);

– в государствах должны быть целевые программы в сфере профилактики экстремизма и терроризма, включающие весь комплекс мер по устранению причин и условий, способствующих распространению этих явлений [8, с. 108];

– правоохранительные органы государств должны быть обеспечены необходимыми средствами для предотвращения терактов и действий экстремистского характера, а также необходимыми технологиями, которые обеспечат полный подконтроль за террористическими группировками;

– необходимо обеспечить суверенное, от зарубежных партнеров, развитие и использование информационного пространства сети Интернет, его инфраструктуры в культурных и образовательных целях по противодействию фактов экстремизма и терроризма [9, с. 104].

5. Незаконный оборот наркотических средств для всех поколений был неудивительным событием в государстве. Такие преступники всегда существовали и будут существовать. В информационно-цифровом пространстве осуществлять преступления такого характера стало еще проще с помощью использования мессенджеров. Особенно популярным среди всех стал Telegram, который обеспечивает защищенность передаваемой информации.

В России с помощью Интернета совершается более 41 % наркопреступлений. Об этом в интервью сообщил А. Некрасов, начальник Главного организационно-аналитического управления Генеральной прокуратуры РФ[12]. М.М. Долгиева, ссылаясь на ГАС «Правосудие», утверждает, что «с 2015 по 2017 г. судами РФ было вынесено 86 приговоров за незаконный сбыт наркотических средств, осуществляемый за криптовалюту, и за последующую ее реализацию» [10, с. 178]. На сегодняшний день криптовалюта распространена еще в большей степени, поэтому покупка наркотических средств с помощью нее продолжается.

Меры предупреждения такой преступности выглядят следующим образом:

– пропаганда здорового образа жизни в обществе. К счастью, в XXI веке здоровый образ жизни становится модой как для детей, так и для взрослых, поэтому количество любителей-спортсменов с каждым годом увеличивается;

– усиленный контроль пограничных органов при перевозке груза из других стран. Путем ужесточенного контроля выявление у перевозчиков наркотических средств на границе обеспечит минимализацию таких веществ в стране, а соответственно сократится рост такой преступности внутри страны;

– усиление государственной поддержки некоммерческих общественных организаций, ставящих своей целью проведение антинаркотических мероприятий и оказание помощи наркозависимым лицам [11, с. 106];

– обучение правоохранительных органов специализированных подразделений в области цифровых преступлений, связанных с наркотическими веществами, а также обеспечение данных органов всеми техническими коммуникациями для более эффективной борьбы с такой преступностью;

– осуществление надзора за банковскими переводами населения для выявления предикатных преступлений, совершенных в сфере незаконного оборота наркотиков [4, с. 220].

Заключение

Преступность в XXI веке набирает популярность именно в сфере информационно-цифрового пространства. Доступность ко всем технологическим возможностям и развитие у граждан знаний в области IT переросло в кибернетическую парадигму. Теперь ни один человек в мире не может признать существование мира без компьютерных технологий. Технические достижения на данном этапе развития общества внедряются во все сферы жизнедеятельности: образование, экономика, политика, производство и т. д.

[12] В Генпрокуратуре заявили, что Интернет все чаще используется для сбыта наркотиков // Новости в России и мире – ТАСС: интернет-сайт. 2021. 24 мая. URL: https://tass.ru/obschestvo/11451751 (дата обращения: 02.06.2023).

Но, к сожалению, изобилие возможностей в кибернетическом пространстве привело к злоупотреблению гражданами. Такое злоупотребление проявляется в самых различных сферах: от продажи и покупки товаров на «черном рынке» до пропаганды и распространения террористических и экстремистских движений. Соответственно, уровень преступности с развитием кибертехнологий начал увеличиваться, так как к общей преступности граждан добавился целый комплекс преступлений особого характера.

Раскрытие преступлений в информационно-цифровой сфере с каждым годом становится сложнее, так как анонимность пользователей в сети Интернет и скрытая их геолокация позволяет исключить прямые факты о совершенном преступлении. Статистические данные показывают, что количество нераскрытых преступлений в сфере IT увеличивается, потому что в обществе возрастает доля профессиональных преступников, которые способны скрыть свои следы.

Для того чтобы снизить уровень преступности, необходимо внедрять меры предупреждения, которые будут выступать способом предотвращения преступности в информационно-цифровом пространстве. В первую очередь, необходимо проводить агитацию среди населения, которая сформирует антипреступную позицию у граждан, а также информировать граждан о способах совершения преступлений в кибернетическом пространстве, чтобы они не стали жертвами преступников.

Во-вторых, требуется постоянная переподготовка правоохранительных органов для повышения уровня знаний о преступности в информационно-цифровом пространстве. Тенденции совершения интернет-преступлений постоянно меняются: раскрыли преступление, совершенное одним способом, – злоумышленник для следующего преступления придумает следующий способ. Именно поэтому правоохранительным органам требуется постоянное повышение знаний в сфере IT.

Подводя итог всему вышесказанному, стоит сделать вывод, что снизить цифровую преступность возможно лишь при применении всех предложенных мер предупреждения в совокупности. Только при антипреступном сознании граждан, их бдительности и эффективной деятельности правоохранительных органов уровень кибернетической преступности будет значительно уменьшен.

Список источников

1. *Хасанова А.Р., Иремадзе Э.О.* История развития современных информационных технологий // Скиф. Вопросы студенческой науки. 2021. № 3 (55). С. 35-40. https://elibrary.ru/znytro
2. *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток, 2005. 235 с. https://elibrary.ru/nnkikf
3. *Зверянская Л.П.* Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Концепт. 2016. № Т15. С. 881-885. https://elibrary.ru/vvehbp
4. *Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С.* Цифровая криминология. М.: Академия управления МВД России, 2021. 244 с. https://elibrary.ru/vckoef
5. *Сверчкова А.Д., Гуляева А.Д.* Анализ динамики экономических преступлений с использованием ИКТ в России // Научные записки молодых исследователей. 2023. Т. 11. № 1. С. 45-55. https://elibrary.ru/yryvuy
6. *Гончар В.В.* Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемым с использованием информационных технологий // Криминалистика в условиях развития информационного общества (59-е Ежегодные криминалистические чтения): сб. ст. Междунар. науч.-практ. конф. М.: Академия управления МВД России, 2018. С. 73-77. https://elibrary.ru/eexhec
7. *Ламбринаки Л.А.* Использование объектов интеллектуальной собственности в сети Интернет // Скиф. Вопросы студенческой науки. 2023. № 1 (77). С. 118-122. https://elibrary.ru/kusbyn
8. *Пинкевич Т.В.* Экстремизм и терроризм: тенденции и проблемы противодействия в СКФО (региональный аспект) // Проблемы теории и практики борьбы с экстремизмом и терроризмом: материалы Всерос. науч.-практ. конф. Москва; Ставрополь: Рос. криминол. ассоц.; Изд-во СКФУ, 2015. С. 105-108.
9. *Тарасов В.Ю.* Предупреждение распространения идей экстремизма и терроризма в сети Интернет // Виктимология. 2023. Т. 10. № 1. С. 101-106. https://doi.org/10.47475/2411-0590-2023-10110, https://elibrary.ru/kobfff

10. *Долгиева М.М.* Криптовалютная наркоторговля в России и за рубежом // Вестник Воронежского института МВД России. 2018. № 4. С. 177-182. https://elibrary.ru/yqxmjv
11. *Бочарова И.В.* Меры предупреждения преступлений в сфере незаконного оборота наркотических средств // Молодой ученый. 2020. № 39 (329). С. 104-106. https://elibrary.ru/eebfiw

References

1. Khasanova A.R., Iremadze E.O. (2021). The history of the development of modern information technologies. *Skif. Voprosy studencheskoi nauki = Sciff. Questions of Students Science*, no. 3 (55), pp. 35-40. (In Russ.) https://elibrary.ru/znytro
2. Tropina T.L. (2005). *Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: dis. ... kand. yurid. nauk* [Cybercrime: Concept, Status, Criminal Legal Measures to Combat It: PhD (Law): diss.]. Vladivostok, 235 p. (In Russ.) https://elibrary.ru/nnkikf
3. Zveryanskaya L.P. (2016). Istoricheskii analiz etapov razvitiya kiberprestupnosti i osobennosti sovremennykh kiberprestuplenii [Historical analysis of the stages of development of cybercrime and features of modern cybercrimes]. *Nauchno-metodicheskii elektronnyi zhurnal «Kontsept» = Scientific and Methodological Electronic Journal "Koncept"*, no. T15, pp. 881-885. (In Russ.) https://elibrary.ru/vvehbp
4. Ishchuk Ya.G., Pinkevich T.V., Smol'yaninov E.S. (2021). *Tsifrovaya kriminologiya* [Digital Criminology]. Moscow, Management Academy of the Ministry of the Interior of Russia Publ., 244 p. (In Russ.) https://elibrary.ru/vckoef
5. Sverchkova A.D., Gulyaeva A.D. (2023). Analysis of the dynamics of economic crimes in IT-sphere in Russia. *Nauchnye zapiski molodykh issledovatelei = Scientific Notes of Young Scientists*, vol. 11, no. 1, pp. 45-55. (In Russ.) https://elibrary.ru/yryvuy
6. Gonchar V.V. (2018). Otde'nye voprosy sovershenstvovaniya podgotovki kadrov, spetsializiruyushchikhsya na rassledovanii prestuplenii, sovershaemym s ispol'zovaniem informatsionnykh tekhnologii [Selected issues of improving the training of personnel specializing in the investigation of crimes committed using information technology]. *Sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Kriminalistika v usloviyakh razvitiya informatsionnogo obshchestva (59-e ezhegodnye kriminalisticheskie chteniya)»* [Proceedings of the International Scientific and Practical Conference "Forensics in the Context of the Development of the Information Society (59th Annual Forensic Readings)"]. Moscow, Management Academy of the Ministry of the Interior of Russia Publ., pp. 73-77. (In Russ.) https://elibrary.ru/eexhec
7. Lambrinaki L.A. (2023). Use of intellectual property objects on the Internet. *Skif. Voprosy studencheskoi nauki = Sciff. Questions of Students Science*, no. 1 (77), pp. 118-122. (In Russ.) https://elibrary.ru/kusbyn
8. Pinkevich T.V. (2015). Ekstremizm i terrorizm: tendentsii i problemy protivodeistviya v SKFO (regional'nyi aspekt) [Extremism and terrorism: trends and problems of counteraction in the North Caucasian Federal District (regional aspect)]. *Vserossiiskaya nauchno-prakticheskaya konferentsiya «Problemy teorii i praktiki bor'by s ekstremizmom i terrorizmom»* [All-Russian Scientific and Practical Conference "Problems of Theory and Practice in the Fight against Extremism and Terrorism"]. Moscow, Stavropol, Russian Criminological Association, North-Caucasus Federal University Publ., pp. 105-108. (In Russ.) https://elibrary.ru/tlbqlv
9. Tarasov V.Yu. (2023). Preventing the spread of ideas of extremism and terrorism on the Internet. *Viktimologiya = Victimology*, vol. 10, no. 1, pp. 101-106. (In Russ.) https://doi.org/10.47475/2411-0590-2023-10110, https://elibrary.ru/kobfff
10. Dolgieva M.M. (2018). Cryptocurrency drug trafficking in Russia and abroad. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh Institute of the Ministry of Interior of Russia*, no. 4, pp. 177-182. (In Russ.) https://elibrary.ru/yqxmjv
11. Bocharova I.V. (2020). Measures to prevent crimes in the sphere of illicit drug trafficking. *Molodoi uchenyi* [Young Scientist], no. 39 (329), pp. 104-106. (In Russ.) https://elibrary.ru/eebfiw

Авторы заявляют об отсутствии конфликта интересов. / Authors declare no conflict of interests.

Поступила в редакцию / Received 12.08.2023
Поступила после рецензирования / Revised 15.11.2023
Принята к публикации / Accepted 17.11.2023