Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

УДК 343.8
doi: 10.35750/2071-8284-2021-3-142-152

Дмитрий Николаевич Жидков
кандидат юридических наук
ORCID: 0000-0003-2135-9234, dmitry_jidkov@mail.ru

Санкт-Петербургский университет МВД России
Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1

О необходимости развития криминалистической общественной профилактики в целях организации противодействия киберпреступности на территории Российской Федерации

Аннотация: В настоящей статье приводится статистический анализ зарегистрированных и раскрытых преступлений, совершённых с использованием компьютерных и телекоммуникационных технологий на территории Российской Федерации. Предлагается определение киберпреступлений. Далее автор выделяет виды преступного поведения, по его мнению, относящиеся к киберпреступности в целом. На основании содержания доклада Генерального секретаря Организации Объединённых Наций «Противодействие использованию информационно-коммуникационных технологий в преступных целях» в статье исследуются основные проблемы, сопровождающие профилактику рассматриваемой категории преступлений, на примере 61 доклада государств-участниц ООН, подготовленных в рамках запросов Генерального секретаря на основании резолюции Генеральной Ассамблеи №73/187 «Краткая информация о национальных и международных трудностях, возникающих при борьбе с использованием ИТТ в преступных целях». В данном исследовании рассматривается текущее положение криминалистической профилактики преступности в России, анализируется современное положение дел, связанное с раскрытием и расследованием киберпреступлений. Вносятся предложения по изменениям в проект федерального закона «О кибердружинах», предлагается развитие централизованной криминалистической общественной профилактики киберпреступлений. Автором на основании ответов на соответствующие запросы в наиболее известные общественные организации, вовлечённые в профилактику киберпреступлений, анализируется деятельность кибердружин на территории Российской Федерации. В резолютивной части статьи автор формирует аргументированные предложения по упорядочению деятельности российских кибердружин в целях повышения эффективности их деятельности.

Ключевые слова: киберпреступность; криминалистическая общественная профилактика; киберпреступления; информационно-телекоммуникационные технологии; средства вычислительной техники; кибершпионаж; кибервымогательство; криптоджекинг; кибертравля

Для цитирования: Жидков Д. Н. О необходимости развития криминалистической общественной профилактики в целях организации противодействия киберпреступности на территории Российской Федерации // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 3 (91). – С. 142–152; doi: 10.35750/2071-8284-2021-3-142-152.

Dmitriy N. Jidkov
Cand. Sci. (Jurid.)
ORCID: 0000-0003-2135-9234, dmitry_jidkov@mail.ru

Saint Petersburg University of the MIA of Russia
1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation

On the need to develop criminalistic public prevention in order to organize counteraction to cybercrime on the territory of the Russian Federation

Abstract: This article provides a statistical analysis of registered and solved crimes committed by using computer and telecommunications technologies on the territory of the Russian Federation, and offers a definition of cybercrime. Further, the author identifies the types of criminal behavior, in his opinion, related to cybercrime in general. Based on the content of the report of the Secretary-General of the United Nations «Countering the use of information and communication technologies for criminal purposes», the article examines the main problems that accompany the prevention of this category of crimes on the example of 61 reports of UN Member States, prepared as part of the requests of the Secretary-General, on the basis of General Assembly resolution No. 73/187 «Summary of national and international difficulties encountered in combating the use of ITT for criminal purposes». This research examines the current state of criminalistic crime prevention in Russia, provides an analysis of the current state associated with the disclosure and investigation of cybercrimes. The article presents proposals for amendments to the draft federal law «On Cyberdrugs», and suggests the development of a centralized forensic public prevention of cybercrime. Based on the responses to the relevant requests to the most well-known public organizations involved in the prevention of cybercrime, the author analyzes the activities of cyberdrugs on the territory of the Russian Federation. In the resolving part of the article, the author forms reasoned proposals for formatting the activities of Russian cyber-soldiers, in order to increase the effectiveness of their activities.

Keywords: cybercrime; criminalistic public prevention; cybercrime; information and telecommunications technologies; computer equipment; cyber espionage; cyber extortion; cryptojacking; cyber bullying

For citation: Jidkov D. N. On the need to develop criminalistic public prevention in order to organize counteraction to cybercrime on the territory of the Russian Federation // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2021. – № 3 (91). – P. 142–152; doi: 10.35750/2071-8284-2021-3-142-152.

Современная преступность представляет угрозу национальной безопасности, оказывает дестабилизирующее воздействие на состояние всех сфер жизнедеятельности государства, общества и личности, существенно тормозит социально-экономические преобразования в России, отражается на уровне жизни населения, порождает недоверие к власти[1]. По нашему мнению, ещё большую опасность для государства и общества представляют открывшиеся перед преступниками современные возможности, связанные с развитием информационно-телекоммуникационных технологий, по совершению как традиционных преступлений, так и преступлений в киберпространстве[2].

Киберпреступлениями являются преступления, совершаемые с использованием информационно-телекоммуникационных технологий[3],

[1] Бабаева Э. У., Волохова О. В., Егоров Н. Н., Жижина М. В., Исютин-Федотков Д. В., Ищенко Е. П., Комиссарова Я. В., Корма В. Д., Кручинина Н. В., Милованова М. М., Паршиков В. И., Уваров В. Н., Харина Э. Н. Криминалистика: учебник для бакалавров и специалистов / отв. ред. д.ю.н., проф. Е. П. Ищенко. – Москва: Проспект, 2020. – С. 353.

[2] Киберпространство – Интернет, WorldWideWeb как совокупность всех доступных ресурсов. Английский термин, введён в употребление писателем-фантастом Уильямом Гибсоном. Толковый словарь русского языка начала XXI века. Актуальная лексика / под ред. Г. Н. Скляревской. – Москва: Эксмо, 2006. – 1136 с. – Библиотека словарей. – С. 453.

[3] Далее по тексту – ИТТ.

средств вычислительной техники[4], интернета, каналов связи, а также сведений о лицах, предметах, фактах, событиях, явлениях, полученных с их помощью.

Современный период развития технологий позволил производителям создать ранее невиданное множество СВТ, что способствовало повсеместному проникновению ИТТ в жизнь людей и, безусловно, спровоцировало стремительный рост количества киберпосягательств, а также позволило преступникам дорабатывать их в целях использования в преступной деятельности.

Согласно ежегодным отчётам ФКУ «ГИАЦ» МВД России «Состояние преступности в России», с января по декабрь 2017–2019 годов зарегистрировано следующее количество преступлений, совершённых с использованием компьютерных и телекоммуникационных технологий: в 2017 году – 90587, в 2018 год – 174674, в 2019 году – 294409, причём с января по сентябрь 2020 года было зарегистрировано 363034 таких преступления. Уровень раскрываемости их в 2017 году составил 24,4 %[5], в 2018 году – 26,6 %[6], в 2019 году – 50,4 %[7], за январь–сентябрь 2020 года – 44,3 %[8]. Эти данные говорят о беспрецедентном росте количества регистрируемых преступлений, совершённых с использованием компьютерных и телекоммуникационных технологий, что свидетельствует о необходимости организации мер противодействия рассматриваемым преступлениям.

Согласно материалам коллегии Министерства внутренних дел Российской Федерации 2019 года[9], сегодня на территории РФ отмечается стабильный рост доли преступлений, совершаемых с использованием ИТТ, постоянно фиксируются факты использования киберпреступниками ранее не изученных способов, методов и специальных аппаратно-программных комплексов[10].

В. А. Колокольцев обратил внимание на то, что наиболее широкое распространение в настоящее время получили преступные деяния с использованием банковских карт, информационно-телекоммуникационной сети интернет, средств мобильной связи и компьютерной техники.

Результаты анализа криминогенной обстановки свидетельствуют, что 79,4 % зарегистрированных преступлений с использованием ИТТ совершенны против собственности, причём подавляющее большинство из них – мошенничества и кражи[11]. На протяжении последних лет отмечается рост количества киберпреступлений против здоровья населения и общественной нравственности. Так, за отмеченный ранее период органами внутренних дел выявлено 18,9 тыс. преступлений, квалифицированных по статье 228[1] УК РФ[12], совершённых с использованием ИТТ[13].

С похожей ситуацией, связанной с резким увеличением киберпреступлений и низким уровнем их раскрытия и расследования, сегодня сталкиваются правоохранительные системы практически всех государств мира. Действующая Конвенция о преступности в сфере компьютерной информации ETS №185 устанавливает виды противоправной деятельности, совершаемой с использованием ИТТ, относящейся к киберпреступлениям, на которые обращают пристальное внимание правоохранительные органы мирового сообщества[14], а именно, преступлений:

– против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств);

– связанных с использованием компьютерных средств (подлог с использованием компью-

[4] Далее по тексту – СВТ.

[5] Состояние преступности в России за январь – декабрь 2017 года. – URL: Главный информационно-аналитический центр (дата обращения 29.01.2020).

[6] Состояние преступности в России за январь – декабрь 2018 года. – URL: Главный информационно-аналитический центр (дата обращения 29.01.2020).

[7] Состояние преступности в России за январь – декабрь 2019 года. – URL: Главный информационно-аналитический центр (дата обращения 29.01.2020).

[8] Состояние преступности в России за январь – сентябрь 2020 года. – URL: Главный информационно-аналитический центр (дата обращения 29.01.2020).

[9] О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий: Решение коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. – № 3 км.

[10] Там же.

[11] Там же

[12] Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества: Статья 228[1] УК РФ // Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 18 февраля 2020 г.).

терных технологий, мошенничество с использованием компьютерных технологий);

– связанных с содержанием данных (детская порнография);

– связанных с нарушением авторских и смежных прав.

Согласно данным, опубликованным на официальном сайте «Лаборатории Касперского», в России наиболее распространёнными являются следующие типы киберпреступлений[15]:

– мошенничества, совершённые с использованием электронной почты и данными аккаунтов;

– хищение либо неправомерное использование личной информации;

– хищение корпоративной, финансовой информации и информации банковских карт;

– кибершпионаж;

– кибервымогательство;

– криптоджекинг (замаскированная от пользователя СВТ деятельность по созданию новых структур для обеспечения функционирования криптовалютных платформ).

При этом разнообразие способов совершения преступлений в рассматриваемой области постоянно расширяется, например, относительно недавно появилась «кибертравля»[16].

Большинство киберпреступлений зачастую совершаются одним или несколькими преступниками, обладающими минимальными специальными знаниями в области информационных и телекоммуникационных технологий, используя их для достижения корыстных целей. Однако при проведённом нами анализе информационных ресурсов, размещённых в сетях DarkNet[17], выявлены электронные площадки «Научно-исследовательские лаборатории», основными задачами которых являются: разработка прикладного программного обеспечения, специальных средств и аппаратно-программных комплексов по заявкам преступников – например, для организации несанкционированного доступа к банковским счетам, для совершения краж и несанкционированного копирования данных о личности и иной информации, кражи финансовых средств.

Российская Федерация также участвует в процессах раскрытия, расследования и предупреждения преступлений рассматриваемой категории. Так, в 2019 году инициатива нашего государства о необходимости разработать Конвенцию о борьбе с использованием информационных технологий в преступных целях получила одобрение в Третьем комитете 74-й сессии Генеральной Ассамблеи ООН[18].

Уже 30 июля 2019 года Генеральный секретарь ООН Антониу Гутерреш выступил с докладом по поданной Россией инициативе. Каждое из 61 государств[19], подготовивших доклады в рамках запросов Генерального секретаря, на основании резолюции Генеральной Ассамблеи №73/187 предоставило краткую информацию о национальных и международных трудностях, возникающих при борьбе с использованием

---

[13] О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий: Решение коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. – № 3 км.

[14] Конвенция о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). – Ст. 2-10. – URL: https://base.garant.ru/4089723/ (дата обращения: 01.03.2020).

[15] Официальный сайт «Лаборатория Касперского». – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 01.03.2020)

[16] Интернет-травля, или кибертравля – намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. Для обозначения явления также используются англицизмы кибермоббинг – это термин, пришедший из английского языка (от англ. Cyber-Mobbing), также интернет-моббинг (Internet-mobbing), кибербуллинг (Cyberbullying), троллинг (trolling – «ловля»), флейм (flame – «пламя»). – URL: https://ru.wikipedia.org/wiki/Интернет-травля (дата обращения: 01.03.2020)

[17] Даркнет (англ. DarkNet, также известен как «Скрытая сеть», «Тёмная сеть», «Теневая сеть», «Тёмный веб») – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная «сеть» не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. – URL: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82 (дата обращения: 01.03.2020)

[18] Работе над конвенцией о борьбе с киберпреступностью дан «зеленый свет» // Официальный сайт ООН. – URL: https://news.un.org/ru/story/2019/11/1367391 (дата обращения: 01.03.2020)

[19] Австралия, Австрия, Аргентина, Армения, Беларусь, Боливия, Ботсавана, Бразилия, Венгрия, Венесуэла, Гана, Германия, Грузия, Израиль, Индия, Иордания, Ирак, Иран, Ирландия, Испания, Италия, Канада, Катар, Китай, Колумбия, Корейская Народно-Демократическая Республика, Коста-Рика, Ливан, Лихтенштейн, Малайзия, Марокко, Монголия, Мьянма, Нидерланды, Никарагуа, Новая Зеландия, Норвегия, Перу, Португалия, Российская Федерация, Румыния, Сальвадор, Саудовская Аравия, Сербия, Сингапур, Сирийская Арабская Республика, Словакия, Словения, Соединенное королевство Великобритания и Северной Ирландии, Соединенные Штаты Америки, Таджикистан, Тайланд, Турция, Филиппины, Франция, Чехия, Швейцария, Шри-Ланка, Эстония, Южная Африка и Япония.

ИТТ в преступных целях[20]. В указанных национальных материалах содержится огромное количество информации, позволяющей определить действительные проблемы как в международной, так и в национальной практике организации противодействия киберпреступности. Также в них содержится и информация, свидетельствующая о низком уровне осведомлённости населения о способах соблюдения информационной безопасности при пользовании ИТТ и СВТ.

Некоторые государства согласно представленным документам открыто заявляют о готовности к разработке в числе прочих и мер профилактики киберпреступлений, совершаемых с использованием ИТТ, а именно:

– Аргентина считает, что одним из ключевых аспектов борьбы с преступностью является профилактика киберпреступности[21], отмечает низкий уровень осведомленности населения и организаций[22];

– многонациональное государство Боливия заявляет, что, поскольку мы имеем дело с явлением, масштабы которого постоянно возрастают, то необходимость профилактики киберпреступности и защиты от неё следует считать обязанностью каждого: государств, компаний, организаций и населения[23]. Также Боливия отмечает и недостаточный уровень осведомлённости и информированности общественности относительно использования информационно-коммуникационных технологий. Отсутствие знаний делает людей более уязвимыми в отношении различных преступлений[24];

– Франция сообщает, что располагает надёжной национальной системой профилактики киберпреступлений, однако нацеленной только на потребности правоохранительных органов, вовлечённых в процессы раскрытия и расследования преступлений рассматриваемой группы[25], поэтому считает необходимым активизацию профилактических мер путём повышения осведомлённости населения о методах, используемых киберпреступниками, действующими в интернете[26];

– Армения делится положительным опытом организации профилактических мероприятий, направленных на снижение киберпреступности, а именно, информирует о систематическом проведении интервьюрований специалистов в области информационной безопасности, организации соответствующих пресс-конференций, создании специализированных телевизионных выпусков с привлечением различных электронных и печатных СМИ к публикациям широкого круга материалов для информирования общественности[27], отмечает необходимость повышения уровня информированности населения о киберпреступности;

– Венгрия в представленных материалах делает акцент на необходимости повышения осведомлённости о мерах кибербезопасности как в государственном, так и в частном секторе[28];

– Монголия заявляет, что основной причиной появления жертв киберпреступности являются неосведомленность общественности об опасности, а также отсутствие соответствующих знаний, новостей и информации о киберпреступлениях;

– Перу озабочено необходимостью охвата пользователей информационно-коммуникационных технологий программой повышения осведомлённости о рисках несоблюдения мер защиты[29];

– интересной является позиция Соединенного королевства Великобритании и Северной Ирландии, что крайне необходимым является поощрение сообщений от граждан о преступлениях рассматриваемой группы[30].

---

[20] Противодействие использованию информационно-коммуникационных технологий в преступных целях: Доклад Генерального секретаря ООН. – 30 июля. – 2019. – С. 4.

[21] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт «e» доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 5.

[22] Там же.

[23] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 47 доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 15.

[24] Там же.

[25] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 102 доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 30.

[26] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт «p» доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 76.

[27] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 20 доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 9.

[28] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 126 доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 36.

[29] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 207 «i» доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 55.

[30] Противодействие использованию информационно-коммуникационных технологий в преступных целях: пункт 393 доклада Генерального секретаря ООН. – 30 июля. – 2019. – С. 98.

Проанализировав содержание доклада Генерального секретаря ООН по резолюции №73/187 Генеральной Ассамблеи[31], можно сделать вывод о том, что сегодня во многих государствах система профилактики киберпреступности крайне несовершенна и неразвита.

Ситуация с киберпреступлениями, сопряжённая с современными тенденциями по использованию ИТТ при совершении различных преступлений, обязывает правоохранительную систему нашего государства активизировать деятельность, направленную на создание и организацию системы криминалистической профилактики киберпреступлений.

Современная российская система криминалистической профилактики, по нашему мнению, должна представлять собой совокупность информационного, методического и технико-криминалистического обеспечения деятельности правоохранительных органов, предназначенной для выявления обстоятельств, методов и способов совершения преступлений различных видов, в том числе и киберпреступлений в целях их раскрытия, расследования и предупреждения.

Правоохранительным органам посильную помощь в раскрытии, расследовании и профилактики киберпреступлений, на наш взгляд, сможет оказать активно развиваемое направление «общественная криминалистическая профилактика», показавшее свою эффективность, например, при проведении эксперимента по поиску похищенного автотранспорта на основе информации о кражах и угонах транспортных средств в Санкт-Петербурге в 2017 году[32].

Общественная криминалистическая профилактика – направление криминалистической профилактики, осуществляемое общественностью на безвозмездной основе при информационном сопровождении органов внутренних дел РФ, включающее в себя практические рекомендации по оказанию общественностью содействия правоохранительным органам в фиксации преступлений и правонарушений и следов их совершения через интернет-сайты, программное обеспечение и другие информационные ресурсы[33].

Во многих государствах сегодня разработано специализированное законодательство, регламентирующее ответственность за совершение киберпреступлений и использование ИТТ при совершении преступлений[34]. Однако наряду с развитием ИТТ преступники и преступные сообщества находят новые пути совершения киберпреступлений быстрее, чем реагирует законодательная власть.

В российском законодательстве нормативного правового акта, охватывающего киберпреступность в целом, на момент подготовки статьи, не существует, как нет пока и акта, регламентирующего профилактику киберпреступности.

На территории Российской Федерации активно развивается общая профилактика преступлений и правонарушений. Так, в нескольких нормативных правовых актах содержатся нормы, в той или иной степени её регламентирующие. Это:

- Конституция Российской Федерации;
- федеральные законы;
- постановления правительства;
- приказы различных министерств и др.

Согласно действующему законодательству, противодействие киберпреступности входит в обязанности полиции, федеральных органов исполнительной власти и некоторых коммерческих организаций, связанных с обеспечением информационной безопасности, однако численность квалифицированного личного состава и сотрудников названных организаций, по нашему мнению, недостаточна для осуществления полноценной криминалистической профилактики киберпреступлений.

В связи с этим считаем, что законодательная инициатива, поданная депутатами Государственной Думы Российской Федерации А. Л. Шхагошевым, Э. А. Валеевым, С. А. Боженовым, А. В. Чернышевым по созданию на территории нашего государства кибердружин[35], является актуальной и могла бы помочь право-

[31] Противодействие использованию информационно-коммуникационных технологий в преступных целях: доклад Генерального секретаря. – 30 июля. – 2019.

[32] Жидков Д. Н. Использование специальных знаний в раскрытии, расследовании и профилактике преступлений, связанных с незаконным завладением транспортным средством: дис. ... кандидата юридических наук : 12.00.12 / Жидков Дмитрий Николаевич. – Санкт-Петербург, 2017. – С. 107–122.

[33] Жидков Д. Н. Там же. – С. 11.

[34] Противодействие использованию информационно-коммуникационных технологий в преступных целях: Доклад Генерального секретаря ООН. – 30 июля. – 2019. – С. 2–103.

[35] В Госдуме подготовили законопроект о кибердружинах 02.11.2018 // Официальный сайт «РИА Новости». – URL: https://ria.ru/20181102/1531986218.html (дата обращения: 01.03.2020).

охранительным органам в раскрытии и расследовании преступлений, связанных с использованием ИТТ и СВТ, а населению – повысить уровень компьютерной грамотности и информационной безопасности.

На протяжении нескольких лет в России формируется направление организации взаимодействия гражданского общества и уполномоченных органов власти в сфере противодействия распространению противоправной информации в киберпространстве в рамках создания кибердружин, однако, несмотря на фактическое распространение деятельности кибердружин, существует ряд трудностей, связанных с непосредственной реализацией данной концепции. Считаем, что прежде всего причиной малой эффективности данного направления является отсутствие:

– единого централизованного руководства, чёткой концепции и стратегии развития;

– определения правового статуса организаций и их участников;

– нормативно урегулированного порядка взаимодействия с правоохранительными органами;

– единой терминологии, задач и функций, методологии и рекомендаций для участников объединений;

– централизованного учёта информации, изученной подобными общественными формированиями;

– анализа уже накопленного эмпирического материала.

На территории Российской Федерации в связи с особенностями законодательства создание кибердружин в основном происходит по следующим направлениям:

1) издаётся соответствующее постановление правительства субъекта РФ, утверждающее типовое положение о деятельности кибердружин на территории субъекта; далее деятельность участников кибердружины регламентируется в соответствии с принятым положением;

2) создаётся некоммерческая общественная организация, утверждается устав организации, в соответствии с которым действуют участники кибердружины;

3) деятельность осуществляется в рамках сообщества граждан, курируемого представителями территориального УМВД России субъекта.

Наиболее известной из существующих кибердружин сегодня является межрегиональное молодежное общественное движение «Кибердружина», созданное на базе общественной организации «Лига безопасного интернета».

Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД России, Комитета Госдумы РФ по вопросам семьи, женщин и детей. Попечительский совет Лиги возглавляет Полномочный представитель Президента Российской Федерации в Центральном федеральном округе Игорь Щеголев. В целях минимизации опасного контента путём самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей[36], данная организация выполняет следующие задачи:

– противодействие распространению опасного интернет-контента доступными способами и средствами;

– объединение профессионального сообщества, участников интернет-рынка для выработки механизмов саморегуляции сообщества во избежание введения цензуры;

– оказание реальной помощи детям и подросткам, которые прямым или косвенным образом стали жертвами распространения опасного интернет-контента;

– помощь государственным структурам в борьбе с созданием и распространением опасного контента: детской порнографии, пропаганды наркомании, насилия, фашизма и экстремизма и т. д.;

– экспертное участие в разработке законодательных инициатив, направленных на ликвидацию опасного интернет-контента[37].

По данным руководителей организации, данное движение объединяет более 20000 волонтеров в России и странах СНГ, имеет представительства в 36 регионах, однако сведений о результативности данной организации нами в ходе исследования получено не было, так как организация отказалась отвечать на запросы о предоставлении информации.

В настоящее время на территории Российской Федерации уже существует несколько региональных кибердружин, действующих в Белгородской и Кемеровской областях. Так, в Кемеровской области по инициативе заместителя председателя Общественного совета при ГУ МВД России по Кемеровской области Д. Е. Осипова была создана региональная общественная организация содействия обеспечению информационной безопасности «Пика»[38], кото-

[36] Официальный сайт «Лига безопасного интернета». – URL: http://ligainternet.ru/liga/about.php (дата обращения: 01.11.2020).

[37] Там же.

[38] Далее по тексту – «КРОО СОИБ «Пика».

рая с 8 июля 2019 года зарегистрирована в органах Минюста РФ. Её главной задачей является оказание помощи правоохранительным органам в обеспечении кибербезопасности. Так, в ходе личного интервьюирования Д. Е. Осипова нами была получена следующая информация: по состоянию на октябрь 2020 года количество участников, действующих в рамках организации, составляет 30 человек; с января по октябрь 2020 года по собранной и представленной ими информации Роскомнадзор РФ заблокировал 292 интернет-ресурса, содержащих запрещённый контент; в 2019 году организацией было исследовано более 20000 ссылок, из которых выявлено 6343 ресурса, содержащих подозрительный контент; Роскомнадзором РФ заблокировано 1117 из них.

Постановлением Правительства Белгородской области от 22 мая 2017 г. №181-пп «Об организации деятельности кибердружин Белгородской области» в целях содействия развитию деятельности кибердружин в Белгородской области, активизации противодействия распространению в сети интернет противоправной информации и информации, способной причинить вред здоровью и развитию личности детей и подростков, а также поддержки комфортной и безопасной среды в сети интернет, в соответствии с Федеральным законом от 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», утверждён регламент деятельности кибердружин Белгородской области[39].

Уполномоченным органом по координации деятельности кибердружин и их взаимодействию с правоохранительными, контрольно-надзорными структурами и иными субъектами профилактики Белгородской области было определено Управление молодёжной политики Белгородской области.

Согласно указанному регламенту, данная кибердружина выполняет следующие задачи:

– реализация эффективных механизмов, форм и методов выявления противоправного контента в интернете;

– информирование населения, в том числе интернет-пользователей, о действиях в случае обнаружения противоправной информации в сети интернет;

– осуществление специальной подготовки, обучение участников кибердружин;

– содействие государственным структурам в борьбе с размещённой в сети интернет информацией, распространение которой в Российской Федерации запрещено;

– участие в разработке законодательных инициатив, направленных на ликвидацию противоправного контента в сети интернет;

– организация информационно-разъяснительной и агитационно-пропагандистской работы по привлечению новых участников кибердружин.

Регламентом также были определены особенности ежедневного мониторинга сети интернет с целью выявления следующей информации о негативных, кризисных и проблемных явлениях в молодежной среде:

– информации, причиняющей вред здоровью, развитию детей и молодёжи, в соответствии с положениями Федерального закона от 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– информации, запрещённой к распространению на основании вступивших в законную силу решений судов о признании информационных материалов экстремистскими;

– информации, включённой в федеральный список экстремистских материалов;

– информации, содержащей признаки призывов к самоубийству, пропаганды наркотиков, детской порнографии, азартных игр;

– публикаций и комментариев проблемного, критического, провокационного характера, просьб о помощи, в том числе психологической;

– информации о чрезвычайных происшествиях, сведений о преступлениях и правонарушениях, в том числе совершённых в отношении представителей молодёжной среды и самими несовершеннолетними.

Возможно, проблемы развития общественной криминалистической профилактики требуют законодательного урегулирования. Нам удалось принять участие в разработке проекта ФЗ «О кибердружинах». Так, автором внесены предложения по изменению некоторых положений представленного на исследование законопроекта, в соответствии с которыми в числе прочих термин «противоправная информация» был утверждён в следующей редакции: «запрещённая к распространению законодательством Российской Федерации информация, за распространение которой предусмотрена уголовная, административная и дисциплинарная ответственность», все предложенные нами изменения были учтены в новой редакции законопроекта.

[39] Об организации деятельности кибердружин Белгородской области: Постановление Правительства Белгородской области от 22 мая 2017 г. № 181-пп.

Президент России В. В. Путин в ходе своих публичных выступлений не раз обозначал эффективность деятельности современных волонтёрских общественных организаций, состоящих из жителей с активной жизненной позицией, желающих бескорыстно помогать государству, обществу, правоохранительным органам в решении огромного числа различных вопросов, отмечал важность и необходимость привлечения граждан к деятельности в различных волонтёрских организациях, а также отмечал результативность их действий[40].

Согласно материалам коллегии Министерства внутренних дел Российской Федерации 2019 года, немалая часть дистанционных мошенничеств совершаются лицами, отбывающими наказание в местах лишения свободы[41]. Схожая ситуация складывается с преступлениями, связанными с кражами и угонами транспортных средств. Так, в ходе проведённого исследования на тему: «Использование специальных знаний в раскрытии и расследовании преступлений, связанных с незаконным завладением транспортными средствами» была выявлена закономерность: большая часть мошеннических телефонных звонков о возврате похищенных транспортных средств осуществлялась с территории одного и того же учреждения ФСИН РФ, предназначенного для отбывания наказания. Данная информация была получена путём использования специализированных социальных групп, развёрнутых в социальной сети «ВКонтакте» (Угонам.Нет, Спуа.РФ), а именно: был организован поиск сведений об абонентских номерах, указанных выше телефонных мошенников, затем информация передавалась в оперативные подразделения ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, разрабатывались рекомендации для потерпевших. Считаем, что в случае централизации подобных действий, к примеру, по выявлению указанным выше способом телефонов и контактных данных телефонных мошенников на территории всего государства, результат был бы более продуктивным.

По состоянию на октябрь 2020 года на территории Белгородской области действуют 22 кибердружины общей численностью свыше 300 человек, осуществляющих мониторинг более 250 сообществ регионального сегмента социальных сетей[42].

Выявленная кибердружинами Белгородской области информация с противоправным контентом поступает в Роскомнадзор РФ, администрациям социальных сетей, в Лигу безопасного интернета. Деятельность указанных общественных организаций и объединений сводится к мониторингу электронных ресурсов, содержащих противоправный контент, и дальнейшей передаче ссылок на него в Роскомнадзор РФ для последующей блокировки.

Практически во всех указанных кибердружинах ведутся специализированные реестры, содержащие следующую информацию: № п/п; Дата выявления; Адрес электронного ресурса; Статус сайта (заблокирован, дубль, недоступен); Комментарий диспетчера.

Считаем положительным опыт работы вышеуказанных общественных объединений и организаций и необходимым включение в работу по анализу сведений, представляемых кибердружинами в Роскомнадзор РФ.

Ввиду изначальных добровольных целей каждой из исследованных кибердружин, действующих на территории РФ, предлагаем использовать единую форму отчёта о выявленных электронных ресурсах, обязательную к направлению в специализированные правоохранительные подразделения для организации соответствующих действий. Далее предлагаем представителям заинтересованных правоохранительных органов, к примеру, университетов, академий и институтов системы образовательных организаций МВД России, централизованно организовать работу по изучению поступившей информации, её предварительной оценке (в соответствии с предложенным перечнем видов противоправного контента) и направлению в соответствующие подразделения, для принятия решений.

В распоряжении правоохранительных органов появится постоянный источник информации о противоправном контенте, размещённом в сети интернет и различных мессенджерах.

При организации централизованной криминалистической общественной профилактики

[40] Официальный сайт «Добровольцы России». – URL: https://добровольцыроссии.рф/news?date_0=2019-01-01&date_1=2020-03-20&type=all&search= (дата обращения: 01.03.2020).

[41] О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий: решение коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. – № 3 км.

[42] Официальный ответ УМВД России по Белгородской области от 16.09.2020 №13/387.

Перечень видов опасного контента:
1. Преступления против личности
1.1. Преступления против жизни и здоровья
1.2. Преступления против свободы, чести и достоинства личности
1.3. Преступления против половой неприкосновенности и половой свободы личности
1.4. Преступления против конституционных прав и свобод человека и гражданина
1.5. Преступления против семьи и несовершеннолетних
2. Преступления в сфере экономики
2.1. Преступления против собственности
2.2. Преступления в сфере экономической деятельности
2.3. Преступления против интересов службы в коммерческих и иных организациях
3. Преступления против общественной безопасности и общественного порядка
3.1. Преступления против общественной безопасности
3.2. Преступления против здоровья населения и общественной нравственности
3.3. Экологические преступления
3.4. Преступления против безопасности движения и эксплуатации транспорта
3.5. Преступления в сфере компьютерной информации
4. Преступления против государственной власти
4.1. Преступления против основ конституционного строя и безопасности государства
4.2. Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления
4.3. Преступления против правосудия
4.4. Преступления против порядка управления
5. Преступления против военной службы
5.1. Преступления против военной службы
6. Преступления против мира и безопасности человечества
6.1. Преступления против мира и безопасности человечества

киберпреступлений, у российских правоохранительных органов может появиться огромное количество информации, связанной не только с совершением киберпреступлений, информации о реализуемых средствах вычислительной техники, специально разработанных для совершения преступлений, но и запрещённые данные, распространяемые посредством использования информационно-телекоммуникационных технологий. Собранный таким способом грамотно систематизированный материал позволит проводить безвозмездное информирование населения об особенностях соблюдения информационной безопасности, а при проработке должной мотивации участников проекта тысячи и миллионы глаз, используя различные поисковые сервисы и просто интернет, смогут в профилактических целях исследовать различные информационные ресурсы, информационные каналы, сайты, мессенджеры и социальные сети, блоги, обращая внимание на запрещённую к свободному распространению информацию.

Информация, полученная на таких ресурсах, по нашему мнению, была бы полезной для сотрудников правоохранительной системы Российской Федерации, а её грамотная обработка и анализ, помимо оперативного значения, способствовали бы созданию различных методических рекомендаций как для правоохранительных органов, так и для населения Российской Федерации.

Список литературы

1. *Осипенко А. Л.* Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право. – 2018. – № 3. – С. 35–37.

2. *Симоненко А. А.* Перспективы развития культуры противодействия преступности // Общество и право. – 2019. – № 3. – С. 11–14.

3. *Грибанов Е. В.* Технологии предупреждения преступлений: проблемы формирования и развития // Государство и право. – 2019. – № 10. – С. 98–101.

4. *Карганов В. В.* Киберпространство и кибербезопасность / Безопасность: информация, техника, управление : Themed collection of papers from International scientific conference. – Санкт-Петербург: ГНИИ «Нацразвитие», 2020. – С. 6–10.

5. *Костарев С. В., Карганов В. В., Липатников В. А.* Технологии защиты информации в условиях кибернетического противоборства : науч. монография / под общ. ред. В. А. Липатникова. – Санкт-Петербург: ВАС, 2020. – 716 с.

6. *Лантух Э. В., Жидков Д. Н.* К вопросу об использовании криминалистической профилактики в раскрытии, расследовании и предотвращении преступлений, связанных с незаконным завладением транспортными средствами // Эксперт-криминалист. – 2016. – № 4. – С. 36–38.

7. *Володин В. М., Рожкова Л. В., Сальникова О. В.* Обеспечение безопасности России и США в информационном и киберпространстве: правовые, политические и экономические аспекты // Право и управление. XXI век. – 2017. – № 4 (45). – С. 64–67.

8. *Бродовский Т. А., Шевченко В. И.* Обзор основных криптовалют, представленных на рынке блокчейн-платформ / В мире компьютерных технологий : сборник статей Всероссийской научно-технической конференции студентов, аспирантов и молодых учёных. Севастополь, 06–10 апреля 2020 года / науч. ред. Е. Н. Мащенко. – Севастополь: Севаст. гос. ун.-т, 2020. – С. 111–116.

9. *Шнейдерова Д. И.* Особенности квалификации криптоджекинга в Республике Беларусь / Борьба с преступностью: теория и практика : тезисы докладов VIII Международной научно-практической конференции. – Могилев: Могилёвский институт МВД Республики Беларусь, 2020. – С. 169–172.

10. *Гребеньков А. А.* Кибервымогательство как информационное преступление / Экономика, управление и право: инновационное решение проблем : сборник статей IX Международной научно-практической конференции. – Пенза: Наука и Просвещение. – С. 152–156.

References

1. *Osipenko A. L.* Ob uchastii organov vnutrennikh del v sisteme obespecheniya kiberbezopasnosti Rossiyskoy Federatsii // Obshchestvo i pravo. – 2018. – № 3. – S. 35–37.

2. *Simonenko A. A.* Perspektivy razvitiya kul'tury protivodeystviya prestupnosti // Obshchestvo i pravo. – 2019. – № 3. – S. 11–14.

3. *Gribanov Ye. V.* Tekhnologii preduprezhdeniya prestupleniy: problemy formirovaniya i razvitiya // Gosudarstvo i pravo. – 2019. – № 10. – S. 98–101.

4. *Karganov V. V.* Kiberprostranstvo i kiberbezopasnost' / Bezopasnost': informatsiya, tekhnika, upravleniye : Themed collection of papers from International scientific conference. – Sankt-Peterburg: GNII «Natsrazvitiye», 2020. – S. 6–10.

5. *Kostarev S. V., Karganov V. V., Lipatnikov V. A.* Tekhnologii zashchity informatsii v usloviyakh kiberneticheskogo protivoborstva : nauch. monografiya / pod obshch. red. V. A. Lipatnikova. – Sankt-Peterburg: VAS, 2020. – 716 s.

6. *Lantukh E. V., Zhidkov D. N.* K voprosu ob ispol'zovanii kriminalisticheskoy profilaktiki v raskrytii, rassledovanii i predotvrashchenii prestupleniy, svyazannykh s nezakonnym zavladeniyem transportnymi sredstvami // Ekspert-kriminalist. – 2016. – № 4. – S. 36–38.

7. *Volodin V. M., Rozhkova L. V., Sal'nikova O. V.* Obespecheniye bezopasnosti Rossii i SSHA v informatsionnom i kiberprostranstve: pravovyye, politicheskiye i ekonomicheskiye aspekty // Pravo i upravleniye. XXI vek. – 2017. – № 4 (45). – S. 64–67.

8. *Brodovskiy T. A., Shevchenko V. I.* Obzor osnovnykh kriptovalyut, predstavlennykh na rynke blokcheyn-platform / V mire komp'yuternykh tekhnologiy : sbornik statey Vserossiyskoy nauchno-tekhnicheskoy konferentsii studentov, aspirantov i molodykh uchonykh. Sevastopol', 06–10 aprelya 2020 goda / nauch. red. Ye. N. Mashchenko. – Sevastopol': Sevast. gos. un.-t, 2020. – S. 111–116.

9. *Shneyderova D. I.* Osobennosti kvalifikatsii kriptodzhekinga v Respublike Belarus' / Bor'ba s prestupnost'yu: teoriya i praktika : tezisy dokladov VÍII Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – Mogilev: Mogilovskiy institut MVD Respubliki Belarus', 2020. – S. 169–172.

10. *Greben'kov A. A.* Kibervymogatel'stvo kak informatsionnoye prestupleniye / Ekonomika, upravleniye i pravo: innovatsionnoye resheniye problem : sbornik statey IX Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – Penza: Nauka i Prosveshcheniye. – S. 152–156.

Статья поступила в редакцию 24.02.2021; одобрена после рецензирования 05.07.2021; принята к публикации 03.09.2021.