Научная статья
УДК 343

КИБЕРПОЛИЦИЯ – СОВРЕМЕННЫЙ ПРАВООХРАНИТЕЛЬНЫЙ ОРГАН В БОРЬБЕ С ИНТЕРНЕТ-ПРЕСТУПНОСТЬЮ

Виталий Александрович Михайлюк
Краснодарский университет МВД России, Краснодар, Россия
viktor_1408@mail.ru

Аннотация. Статья посвящена киберполиции как находящемуся на стадии разработки и формирования правоохранительному органу, призванному противодействовать киберпреступности. В работе анализируются предпосылки создания киберполиции в России, проводится исследование нормативно-правовой базы, зарубежного опыта борьбы с киберпреступностью и существующих в отечественной науке концепций с целью углубленного изучения проблемы киберполиции и восполнения существующих в этой области пробелов. Предполагается, что в условиях развития IT-технологий и масштабной цифровизации, а также пандемии, приведшей к росту как видов, так и числа совершаемых киберпреступлений, необходимо создание киберполиции.

Ключевые слова: правоохранительные органы, киберполиция, интернет, киберпреступность, информация, безопасность.

Для цитирования: Михайлюк В. А. Киберполиция – современный правоохранительный орган в борьбе с интернет-преступностью // Вестник Уфимского юридического института МВД России. 2023. № 1 (99). С. 74–79.

CYBER POLICE IS A MODERN LAW ENFORCEMENT AGENCY IN THE FIGHT AGAINST INTERNET CRIME

Vitaly A. Mikhailyuk
Krasnodar University of the Ministry of Internal Affairs of Russia,
Krasnodar, Russia, viktor_1408@mail.ru

Abstract. TThe article is devoted to the cyber police as a law enforcement agency at the stage of development and formation, designed to counteract cybercrime. The paper analyzes the prerequisites for the creation of a cyber police in Russia, conducts a study of the regulatory framework, foreign experience in combating cybercrime and concepts existing in domestic science in order to in-depth study of the problem of cyber police and fill the gaps existing in this area. It is assumed that in the context of the development of IT technologies and large-scale digitalization, as well as the pandemic that has led to an increase in both the types and number of cybercrimes committed, it is necessary to create a cyber police.

Keywords: law enforcement agencies, cyber police, Internet, cybercrime, information, security.

For citation: Mikhailyuk V. A. Cyber police is a modern law enforcement agency in the fight against internet crime // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No. 1 (99). P. 74–79.

«Киберполиция» (другие названия – интернет-полиция, сетевая полиция) – в ряде стран это общий термин, обозначающий сотрудников правоохранительных органов, секретных служб и других организаций, а также сами эти организации, отвечающие за обеспечение безопасности от интернет-преступлений. Главной целью интернет-полиции является борьба с киберпреступностью, в том числе противодействие многочисленной разновидности противоправных компьютерных мошенничеств, совершаемых в сети Darknet; борьба с противозаконными деяниями, использующими методы соци-

альной инженерии; оргпреступлениями, совершенными посредством мобильных устройств и иных средств доступа к данным в киберпространстве; установление и пресечение фактов распространения и использования «фейковых» материалов в отношении защищаемых законом объектов собственности и права, посягательств на свободу, жизнь и здоровье граждан, общественный порядок и безопасность, государственную целостность и т. д., осуществляемых посредством телекоммуникационных сетей[1].

В своей научной статье А. Л. Осипенко отметил, что противоборство правоохранительных органов с организованной преступностью все в большей степени переводится в киберпространство [1]. Весомым аргументом в пользу необходимости тщательного изучения данной проблематики является тот факт, что сама эта категория в отечественной науке недостаточно проработана, поскольку IT-технологии и, как следствие, киберпреступления и методы борьбы с ними находятся в процессе становления и развития. Существующие пробелы в изучении этой темы оставляют ученым поле для новых исследований.

Проблема киберпреступности и поиска средств борьбы с ней характеризуется высокой степенью актуальности в настоящее время. Пандемия коронавирусной инфекции поставила перед человечеством ряд глобальных вызовов и выявила недостатки во взаимодействии правоохранительных структур разных стран мира.

Пандемия стала катализатором невероятного всплеска уголовных преступлений в Интернете, беспрецедентно жестоких по отношению к информационно не грамотным и наиболее уязвимым людям, в том числе несовершеннолетним[2]. Правоохранительные органы должны быть обеспечены надлежащими инструментами для выявления серьезных трансграничных преступлений.

Вводимые ограничения COVID-19 оказали непосредственное влияние и на Российскую Федерацию. Хотя общий уровень преступности остался прежним, в разы выросло количество совершаемых киберпреступлений. Этой тенденции способствуют и общая цифровизация общества, и влияние изоляции, благоприятствующей человеку черпать в Интернете различные знания, в том числе криминального плана.

Отечественный исследователь А. А. Оганов считает, что «следовало бы организовать не только международную, но и межведомственную кооперацию и на этой основе создать единый стандартный инструментарий для полицейской оперативной работы, который позволил бы осуществлять выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых в теневых информационно-телекоммуникационных сетях» [2].

По данным МВД России преступлений, совершенных с использованием IT-технологий, за 2019 г. зарегистрировано 294 409, что на 68,5 % больше того же периода 2018 г. Тяжкие и особо тяжкие составы – 142 728 деяний (+ 149 %). Отмечается скачок мошенничеств с использованием банковских карт (ст. 159.3 УК РФ). Прирост составил + 280 %, (16 119 преступлений). Удельный вес правонарушений в сфере высоких технологий по итогам 2019 г. равен 14,54 %.

За 2020 г. зарегистрировано 510 396 преступлений. Рост составил + 73,4 %. Из них тяжкие и особо тяжкие составы 267 613 деяний (+ 87,5 %). Наибольший прирост по показателю ст. 228.1 УК РФ (незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов): + 90,7 %, (47 060) преступлений. Удельный вес противоправных деяний в сфере высоких технологий по итогам 2020 г. равен 24,96 %.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 18.05.2022).

[2] Euronews // URL: https://ru.euronews.com/2021/12/08/eu-police-transborder-crime (дата обращения: 18.05.2022).

По итогам 2021 г. отмечается незначительный рост преступности – на 1,4 % (517 722). Наибольший показатель – публичные призывы к осуществлению террористической деятельности. Публичное оправдание терроризма или его пропаганда (ст. 205.2 УК РФ) составили + 35,8 % (315). На фоне снижающегося общего количества зарегистрированных преступлений удельный вес преступности в сфере высоких технологий по итогам 2021 г. увеличился до 25,8 %[1].

В связи с развитием схем социальной инженерии и применением новых мошеннических инструментов, а также на основании характеристики состояния преступности за последние 3 года необходимо отметить, что в данных условиях назрела острая необходимость создания соответствующих IT-эпохе новых правоохранительных органов, способных бороться с современными мировыми вызовами и угрозами в сфере компьютерных технологий.

Так, в конце 2020 г. Министром внутренних дел Российской Федерации В. Колокольцевым было принято решение о создании киберполиции[2]. Глава ведомства отметил, что подразделения будут создаваться по отраслевому принципу. Были озвучены планы по увеличению штата Управления «К» МВД России, которое в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие:

1) преступлений в сфере компьютерной информации;

2) преступлений в сфере противоправных действий в отношении детей и их здоровья, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет);

3) преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации;

4) преступлений, посягающих на авторские права и их незаконное использование[3].

Стоит упомянуть, что Управление «К» представляет собой подразделение МВД России, созданное для противоборства преступлениям в сфере информационных технологий. В поле его деятельности также борьба с незаконным оборотом специальных радиоэлектронных и технических средств.

Представляется, что киберполиция займет место в структуре органов исполнительной власти наряду с полицией, которая, согласно ст. 4 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции», является «Составной частью единой централизованной системы федерального органа исполнительной власти в сфере внутренних дел»[4]. Необходимо отметить, что она будет принципиально новой, хотя и со схожим на первый взгляд функционалом действующих в МВД России подразделений – «Управление «К» и «Специальные технические мероприятия».

Ее основными задачами будут противодействие деятельности преступных организаций в Интернете, онлайн-прием информации о незаконных сетевых действиях, отслеживание и устранение фактов кибермошенничества, мониторинг даркнета, а также борьба с такими общественно опасными явлениями, как «группы смерти», треш-контент, кибербуллинг и т. д. Онлайн-киберполицейские будут мониторить сеть круглосуточно в целях очищения пространства от вредоносного контента, усиления сетевой цензуры, сбора информации

[1] Краткая характеристика состояния преступности в Российской Федерации // URL:https://мвд.рф/reports/item/22678184/, https://мвд.рф/reports/item/28021552/ (дата обращения: 18.05.2022).

[2] В структуре МВД создается киберполиция // URL: https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html (дата обращения: 18.05.2022).

[3] Министерство внутренних дел Российской Федерации // URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 18.05.2022).

[4] О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 21.12.2021) // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 18.05.2022).

о диссидентах и т. д. По нашему мнению, создание такого подразделения имеет на сегодняшний день принципиальное значение и позволит существенно расширить возможности по выявлению, предотвращению и раскрытию сетевых преступлений. Со слов заместителя министра МВД России И. Зубова, этот процесс будет реализован не в самые кратчайшие сроки, так как требует значительных материально-технических ресурсов на переоснащение, а также немалых временных затрат на повышение квалификации сотрудников.

Для сравнения в КНР IT-безопасность реализуется как приоритетное направление. По данным компании Technavio (США), исследующей рынок IT-технологий, Китай вкладывает порядка 3–10 миллиардов долларов ежегодно[1]. Там киберполиция организована в виде интернет-платформы, принимающей обращения граждан, пострадавших от киберпреступлений или ставших свидетелями их совершения. «Тотальная слежка и цензура в Китае – правда. Плохо отзываться о правительстве нельзя. Сообщения в мессенджерах могут в любой момент прочитать. Зарубежные сервисы не работают по умолчанию, ими пользуются через VPN. Серьезные санкции и последствия ждут не пользователей, а создателей VPN-сервисов», – говорится в одном из интервью[2].

Как отмечает В. К. Захарова, идея онлайн-приема и регистрации сообщений граждан КНР реализовывается с 2004 г. В 2016 г. органами общественной безопасности Китая создана госструктура по приему заявлений о нарушениях законности и появлении вредоносной информации, получившая название «cyberpolice» [3].

Создавая киберполицию в России, необходимо учитывать проведенный выше анализ преступности в сфере IT-технологий, которая планомерно растет. Методы преступников совершенствуются, что требует от правоохранителей высоких профессиональных навыков. Так, например сотрудники вынуждены постоянно искать новые методы противодействия развивающимся коммуникационным технологиям, таким как интернет-телефония с использованием шифрования данных Ip-адреса мошенника и возможностью генерирования абсолютно любого номера мобильного или стационарного телефона; бороться с распространением противозаконной террористической деятельностью, реализуемой через социальные сети, мессенджеры, игровые платформы и т. д.; предотвращать распространение фейковой информации, способной вызвать социальный резонанс и привести к нарушениям общественного порядка. Зачастую доступ к серверам, где хранятся необходимые доказательства этой деятельности, находится за пределами территории Российской Федерации и требует механизмов взаимообмена оперативной информацией с соответствующими подразделениями и ведомствами иностранных государств.

Понимание комбинационности всех проблем привело к созданию дополнительной структуры в системе МВД, которая сможет обеспечить определенный успех в данном направлении деятельности.

Как подчеркивают в своей научной статье И. Н. Озеров и К. И. Озеров, киберполиция как отдельный субъект системы Министерства внутренних дел Российской Федерации сможет тщательнее заняться данным вопросом, что позволит эффективно бороться с IT-преступлениями [4].

Необходимо отметить, что киберпреступниками изучаются методики раскрытия преступлений в информационных сетях. Они инвестируют огромные средства в развитие технологий, способствующих развитию преступной деятельности в Интернете, поэтому, создавая новую структуру, необходимо в соответствии с современными требо-

[1] Перспективы и вызовы цифровому будущему // URL: https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html (дата обращения: 18.05.2022).

[2] Жизнь за Великой китайской стеной: как в Китае дела с IT, цензурой и интеграцией в общество // URL: https://habr.com/ru/company/gms/blog/553532/ (дата обращения: 18.05.2022).

ваниями подходить и к профессиональной подготовке сотрудников министерства.

Е. Н. Полунина и А. В. Антонова отмечают, что необходимо создать условия для подготовки компетентных IT-специалистов. Важно разработать особую образовательную программу подготовки квалифицированных сотрудников по борьбе с киберпреступностью, а также подобрать компетентные кадры для обучения будущих киберполицейских [5].

Подведем итог изложенному. Создание киберполиции обусловлено складывающимися на современном этапе правоотношениями и отвечает потребностям информационного общества. В условиях развития IT-технологий и масштабной цифровизации, а также пандемии, приведшей к росту как видов, так и числа совершаемых киберпреступлений, создание и функционирование киберполиции необходимо. Образовательными учреждениями МВД России в настоящее время осуществляется подготовка специалистов в области информационной безопасности, реализуется множество программ повышения квалификации и переподготовки сотрудников по таким направлениям, как оперативно-техническое обеспечение и раскрытие киберпреступлений, информационная безопасность, безопасность информационных технологий и т. д.

С учетом этого для расширения возможностей правоохранительных органов важно уделять особое внимание совершенствованию обучения сотрудников, формированию обозначенных компетенций у каждого выпускника ведомственных образовательных организаций [6].

При этом нельзя забывать и о просвещении граждан в области интернет-безопасности. По нашему мнению, создание киберполиции будет способствовать снижению уровня преступности в информационной среде и создаст общее осознание чувства защиты во всемирном источнике.

СПИСОК ИСТОЧНИКОВ

1. Осипенко А. Л. Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. Краснодарский университет МВД России. 2021. № 1.

2. Оганов А. А. Киберпреступность в отношении несовершеннолетних с использованием информационно-телекоммуникационных сетей: понятия, предложения, определения // Вестник Московского университета МВД России. 2020. № 2.

3. Захарова В. К. Применение современных медиакоммуникационных технологий в деятельности органов общественной безопасности и народной прокуратуры КНР // Академическая мысль. 2018. № 2 (3).

4. Озеров И. Н., Озеров К. И. Новые способы совершения мошеннических действий в сфере IT-технологий в период коронавирусной инфекции // Вестник Белгородского юридического института МВД России. 2021. № 1.

5. Полунина Е. Н., Антонова А. В. Проблемы законодательного регулирования ответственности за «треш-стрим» в Интернете // Закон и право. 2021. № 3.

6. Осипенко А. Л., Луговик В. Ф. // Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений. Краснодарский университет МВД России. Общество и право. 2021. № 2 (76).

REFERENCES

1. Osipenko A. L. Collection of information and police operations to counter organized crime in cyberspace: foreign experience // Society and Law. Krasnodar University of the Ministry of Internal Affairs of Russia. 2021. No. 1. (In Russ.)

2. Oganov A. A. Cybercrime against minors using information and telecommunication networks: concepts, proposals, definitions // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 2. (In Russ.)

3. Zakharova V.K. The use of modern media communication technologies in the activities of public security agencies and the People's Prosecutor's Office of the PRC // Academic Thought. 2018. No. 2 (3). (In Russ.)

4. Ozerov I. N., Ozerov K. I. New ways of committing fraudulent actions in the field of IT technologies during the period of coronavirus infection // Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia. 2021. No. 1. (In Russ.)

5. Polunina E. N., Antonova A. V. Problems of legislative regulation of liability for "trash stream" on the Internet // Law and Law. 2021. No. 3. (In Russ.)

6. Osipenko A. L., Lugovik V. F. // Problems of access of law enforcement agencies to concealed computer information when solving crimes. Krasnodar University of the Ministry of Internal Affairs of Russia. Society and law. 2021. No. 2 (76). (In Russ.)

Информация об авторе:

Михайлюк В. А., кандидат социологических наук.

Information about the author:

Mikhailyuk V. A., Candidate of Sociology.

Статья поступила в редакцию 20.06.2022; одобрена после рецензирования 14.07.2022; принята к публикации 24.03.2023.

The article was submitted 20.06.2022; approved after reviewing 14.07.2022; accepted for publication 24.03.2023.