УДК 343.97

# О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий

***Михайлова И.А.***
Кандидат юридических наук, доцент,
профессор кафедры уголовно-правовых дисциплин
Белгородского юридического института МВД России им. И.Д. Путилина

***Лимарь А.С.***
Кандидат юридических наук,
старший преподаватель кафедры уголовно-правовых дисциплин
Белгородского юридического института МВД России им. И.Д. Путилина

***Гилаев Р.И.***
Оперуполномоченный отделения уголовного розыска отдела полиции
Главного управления МВД России по Красноярскому краю (Красноярск)

*Цифровые технологии, лежащие в основе современных общественных отношений, сменили традиционный формат государственных программ. Телекоммуникационные технологии, с одной стороны, позволяют сократить организационные, временные, финансовые, кадровые и иные издержки, повышают доступность и качество услуг, оказываемых с применением подобных технологий, создают основу для аккумуляции персональных, коммерческих, государственных и иных данных, охраняемых законодательством Российской Федерации. Однако внедрение в различные сферы общественных или публичных отношений новых технологий закономерно порождает развитие преступности в данной области. Как следствие, деятельность правоохранительных органов по противодействию цифровой преступности выступает актуальным направлением современной правоохранительной политики.*

*Целью статьи является исследование мер предупреждения преступлений, совершаемых в сфере информационно-телекоммуникационных технологий. Авторами проведен анализ мероприятий, осуществляемых подразделениями МВД, Следственного комитета, Федеральной службы безопасности Российской Федерации по противодействию таким преступлениям. Определены ресурсы, используемые правоохранительными органами для противодействия киберпреступлениям, выявлены некоторые проблемные вопросы предупреждения и расследования преступлений экстремистской и террористической направленности, мошенничества, совершенных с использованием информационно-телекоммуникационных технологий. По результатам исследования авторами предложены меры по совершенствованию системы противодействия киберпресту-*

*плениям, которые могут быть использованы для дальнейшей научной разработки данной проблематики, а также в практической деятельности правоохранительных органов.*

*Ключевые слова: информационная безопасность, правоохранительные органы, противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий*

Общественно опасные деяния, совершаемые с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступления), представляют серьезную угрозу национальной безопасности Российской Федерации [1, с. 61]. В «Доктрине информационной безопасности Российской Федерации» закреплено, что к числу основных мер обеспечения национальной безопасности в информационной сфере относится, в частности, развитие потенциала правоохранительных органов [2].

Обеспечение информационной безопасности – одно из важнейших направлений деятельности правоохранительных органов. Однако на заседании Коллегии Генпрокуратуры в 2020 г. Генеральный прокурор Российской Федерации И.В. Краснов заявил, что «правоохранительные органы в России практически не могут противостоять киберпреступности, раскрывается лишь 9 % таких преступлений» [3].

Представляется, что одной из основных причин сохранения высокого уровня преступности в сфере IT-технологий является отсутствие в подразделениях МВД России достаточного числа сотрудников, обладающих специальными познаниями в этой сфере.

Методы, способы и средства совершения преступлений с использованием информационных технологий становятся более изощренными [4, с. 55]: используются средства анонимизации и смены фактического IP-адреса, подменные номера телефонов и иные данные для регистрации на интернет-платформах, временные СИМ-карты для мошеннических звонков, а для получения денежных средств от жертвы зачастую используют подставные счета, оформленные на третьих лиц, или вовсе «отмывают» их через виртуальные кошельки. Противодействие таким преступлениям требует высокой квалификации сотрудников, обладающих специальными познаниями в сфере *IT*-технологий.

В «Доктрине информационной безопасности РФ» особое внимание уделяются тому факту, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства [4, с. 55]. Деятельность правоохранительных органов по предупреждению киберпреступлений транснационального характера осложняется тем, что злоумышленник находится за пределами юрисдикции Российской Федерации, а средства шифрования коммуникационной связи выдают соответствующую подменную информацию о фиктивном нахождении преступника.

В целях совершенствования деятельности органов внутренних дел по противодействию указанной группе преступлений в 2022 г. в системе МВД России было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России) [5].

Помимо органов внутренних дел МВД России деятельность по предупреждению и пресечению преступлений в исследуемой сфере осуществляет Следственный комитет Российской Федерации. В структуре СК РФ действует специализированный отдел по расследованию особо тяжких преступлений международного характера, в том числе связанных с хищениями и вымогательством в сети Интернет.

Противодействие преступлениям террористической и экстремистской направленности, совершаемым с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, находится в ведении специализированного Центра информационной безопасности органов ФСБ России, который занимается не только технической защитой компьютерных сетей, но и ведет активную оперативную работу в интернете.

А.А. Кашкаров отмечает, что «предупреждение преступлений экстремистской направленности в информационно-телекоммуникационных сетях, в том числе в сети Интернет, должно иметь комплексный характер. Такого рода деятельность не должна основываться исключительно на блокировке интернет-сайтов и страниц в социальных сетях» [6, с. 353].

Функционирование правоохранительных органов, однако, представлялось бы крайне сложным без содействия иных административных ресурсов, осуществляющих контрольно-надзорные и иные функции в телекоммуникационных сетях. Среди них нельзя не отметить систему ГосСОПКА, Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и ФинЦЕРТ.

Основной кибертехнологией, позволяющей бороться с киберугрозами современности, является функционирующая государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА).

По своей сути, ГосСОПКА – это система сертифицированных отечественных средств и тех-

нологических решений для автоматизированного обнаружения, предупреждения, ликвидации и расшифровки кибератак на объекты критической информационной инфраструктуры (КИИ) Российской Федерации. Кроме того, ГосСОПКА включает в свой состав программные продукты для обмена информацией и криптографической защиты каналов связи. Превентивная защита субъектов критической инфраструктуры осуществляется не только за счёт непосредственного действия указанных технологических средств и ведомственных сил, реагирующих на инциденты, но и также посредством формирования единой системы обмена информацией о кибератаках между участниками ГосСОПКА.

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) обеспечивает координацию деятельности субъектов в рамках государственной системы ГосСОПКА. Аналогичную функцию сбора данных о киберинциденте, их аккумуляции и передачи между правоохранительными службами, но исключительно в финансовой сфере, выполняет ФинЦЕРТ – система информационного обмена между участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере информационной безопасности [7].

По вопросам получения цифровых сведений о злоумышленнике, запрашивают данные о провайдере злоумышленника, осуществляется взаимодействие правоохранительных органов с Роскомнадзором, который предоставляет сведения о месте нахождения и персональных данных лица, на чьё имя зарегистрирован домен в сети Интернет (если преступление совершенно, к примеру, на подменном интерне-портале или ином личном сайте злоумышленника). Роскомнадзор также имеет возможность предпринять меры по блокировке сайтов в сети Интернет по требованию правоохранительных служб в случае, если на них содержится информация, противоречащая законодательству Российской Федерации

В государственной системе Российской Федерации внедрены, тестируются и даже действуют в рамках подведомственности Роскомнадзору и ФСБ РФ такие государственные сервисы, а также автоматизированные информационные системы, базирующиеся на технологиях машинного обучения и искусственного интеллекта, как:

1. «Чистый интернет» (сервис автоматизации поиска запрещенного контента, провокационного материала и зарубежной пропаганды).

2. «Бот-ферма» (генерация биографии фейковым аккаунтам и имитация их активности в соцсетях. Боты будут нужны в первую очередь для сбора информации из закрытых групп для пресечения преступлений экстремистской и террористической направленности).

3. «Вепрь» (автоматизированный поиск материалов о терроризме и экстремизме, о критике властей и несистемной оппозиции, пропаганде ЛГБТ, наркомании, уклонении от армии, поиск суицидального материала, оскорбительные арт-акции, зарубежные призывы к свержениям и т.п.).

4. «Окулус» (на основе нейросетей анализирует фото, видео и тексты на сайтах, в соцсетях и мессенджерах на предмет запрещенной информации).

5. «Кабинет оперативного взаимодействия» (система используется для защищенного общения сотрудников Роскомнадзора с силовыми ведомствами – Генпрокуратурой, ФСБ, СК РФ, ФСО, Росгвардией и МВД. В групповых чатах, например, публикуются отчеты о выявленных агитационных и пропагандистских материалах зарубежного характера, а также о готовящихся иностранных цифровых диверсиях, что позволяет службам своевременно отреагировать для устранения кибер- и физических угроз).

Определив ресурсы, используемые правоохранительными органами для предупреждения преступлений, совершенных с использованием информационно-телекоммуникационных технологий, следует отметить, что современные формы таких преступлений отличаются повышенной экономической опасностью. Онлайн-мошенничество, мошенничество в сети Интернет, интернет-вымогательство и иные преступления такого рода не имеют географических границ, что обуславливает возможность условно совершения преступления в отношении потерпевшего из Московской области лицом, находящимся в ином субъекте РФ. Более того, преступление может вовсе совершаться за пределами Российской Федерации в отношении российских граждан или российскими преступниками в отношении граждан иностранных государств, что осложняет процесс выявления преступления.

Именно поэтому в нынешних условиях борьбы с киберпреступностью к расследованию таких дел должны привлекаться узкоспециализированные следователи, специалисты и эксперты из *IT*-сферы и области технического функционирования компьютерных систем.

Таким образом, сохраняющаяся тенденция роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий (в 2023 г. их зарегистрировано на 29,7 % больше, чем в 2022 г.), свидетельствует о наличии определенных проблем и необходимости совершенствования мер противодействия данным преступлениям.

Следует отметить многообразие форм преступлений в сфере *IT*-технологий: корыстные киберпреступления; идеологические киберпреступления; киберпреступления, ориентированные на дестабилизацию и подрыв государственной или обществен-

ной стабильности; киберпреступления, совершаемые с целью изъятия, изменения, копирования или удаления охраняемых законом сведений; киберпреступления, совершаемые для нарушения нормального функционирования телекоммуникационных сетей и соответствующего аппаратно-программного обеспечения; киберпреступления, посягающие на жизнь и здоровье граждан или ставящие их под угрозу; киберпреступления в сфере информационно-коммуникационных технологий, направленные на нарушение нормального физиологического и психического развития несовершеннолетних, и другие. Согласно статистическим данным, буквально каждый второй гражданин Российской Федерации сталкивался с мошенничеством в онлайн-среде, больше половины граждан страдало от утечки персональных данных в цифровой среде и порядка 82 % физических лиц сталкивалось с попытками преступных посягательств в сфере телекоммуникационных сетей в целом [8], учащаются случаи несанкционированного вмешательства хакеров и иных злоумышленников в критическую информационную инфраструктуру Российской Федерации, что свидетельствует о всесторонности криминальной проблемы.

В то же время, отмечается низкая раскрываемость преступлений в исследуемой сфере общественных отношений. Одна из причин тому – отсутствие надлежащей техники и технологий [9, с. 86], а также профессиональных кадров в сфере информационно-коммуникационных технологий на службе в ОВД, которые могли бы расследовать киберпреступления. Ситуация с расследованием киберпреступления значительно осложняется, если сотрудник ОВД сталкивается с преступным посягательством транснационального характера, когда злоумышленник находится за пределами юрисдикции Российской Федерации, или средства шифрования коммуникационной связи выдают соответствующую подменную информацию о фиктивном нахождении преступника. Немаловажная причина низкой раскрываемости преступлений в исследуемой сфере правоотношений – небольшой размер мошеннических хищений в большинстве случаев (от 10 до 30 тыс. руб.), несоизмеримый с теми временными и техническими затратами, которые потребуются сотрудникам ОВД для расследования преступления. Небольшой размер мошеннических хищений, как сдерживающий механизм, срабатывает и у самого потерпевшего, который, осознавая, как долго будет осуществляться расследование и беря во внимание крайне низкий уровень раскрываемости преступлений такого рода, решает не обращаться в правоохранительные службы для защиты нарушенных прав. Как следствие, большинство дел о телефонном или интернет-мошенничестве прекращаются на стадии предварительного расследования, а споры, которые доходят до суда, обычно заканчиваются отказом в удовлетворении иска.

На основании отмеченных актуальных проблем в деятельности органов внутренних дел представляется возможным сформулировать некоторые предложения по совершенствованию действующей системы противодействия преступлениям, совершаемым в сфере *IT*-технологий:

1. В государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы ГосСОПКА внедрить технологию резервирования каналов связи и обеспечить географическое распределение центров обработки данных, благодаря использованию цифровой технологии облачного хранения. Формирование *IT*-инфраструктуры таким способом позволит обеспечить, с одной стороны, единство субъектов критической информационной инфраструктуры, а с другой – их информационную независимость в случае кибератак. Это также позволит обеспечить сохранность данных о киберинциденте для последующего расследования преступления.

2. Одна из проблем противодействия киберпреступности – отсутствие оперативной информации по совершаемым киберинцидентам, так как органы МВД и СК РФ не подключены к системе ГосСОПКА, ФинЦЕРТ и НКЦКИ. Как следствие, указанные правоохранительные ведомства не получают информацию о совершённом киберпреступлении в сфере телекоммуникационных технологий и не могут предпринять меры по проверке данных и расследованию преступления. Предлагается интегрировать ОВД и СК РФ в систему ГосСОПКА, ФинЦЕРТ и НКЦКИ для более эффективного межведомственного взаимодействия по борьбе с преступлениями в сфере телекоммуникации.

3. В силу отсутствия специальной профессиональной подготовки значительная часть сотрудников ОВД не готова к расследованию преступлений в сфере телекоммуникационных технологий. Объясняется это тем, что действующая образовательная система не ориентирована на подготовку будущих сотрудников ОВД и СК РФ, готовых расследовать узконаправленные компьютерные и иные киберпреступления. Обычно такая подготовка в рамках образовательной программы не является профильной и ей уделяется незначительное время, а сама теоретическая основа подготовки не отвечает реалиям криминогенной обстановки. Современная кадровая политика в ОВД и СК РФ должна быть ориентирована на профессиональную подготовку будущих специалистов вне специализированных отделов по борьбе с киберпреступностью, однако готовых расследовать наиболее типичные формы мошенничества в сети Интернет.

4. Еще одна проблема – слабое техническое и технологическое оснащение непрофильных органов

МВД и СК РФ в рамках борьбы с преступностью в сфере телекоммуникационных технологий. Решение технологического «голода», в частности, и в структуре МВД и СК РФ видится в государственно-частном партнёрстве, где современные компьютерные и информационные технологии для изобличения всех сведений о киберинциденте могут быть разработаны или взяты с учётом служебных модификаций у частных российских компаний, предоставляющих услуги и реализующих продукты телекоммуникационной безопасности. Как следствие, частные цифровые разработки отечественного производства могут быть интегрированы в деятельность правоохранительных органов, что позволит повысить уровень технологической и технической возможности государственных ведомств в борьбе с преступлениями в сфере телекоммуникационных технологий.

5. Значительная часть преступных киберпосягательств имеет транснациональный характер, поэтому в целях совершенствования системы противодействия таким преступлениям важное значение имеют дипломатические инициативы Российской Федерации по обеспечению международного содействия (информационного, ведомственного, юрисдикционного, технического и технологического, кадрового, методического, научного) с международными структурами стран БРИКС и ШОС, открытых к взаимодействию.

*Литература:*


1. Яшин А.В., Фролова Т.А. Современные проблемы противодействия киберпреступлениям в Российской Федерации // Вестник Пензенского государственного университета. – 2023. – № 2. – С. 58–62.
2. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 2016. – № 50. – Ст. 7074.
3. Генпрокурор РФ заявил о бессилии правоохранительных органов перед киберпреступниками. – URL: https://www.interfax.ru/russia/699548.
4. Антонян Е.А., Бархатова Е.В. Противодействие киберпреступности // Евразийский Союз Ученых (ЕСУ). – 2019. – № 7(64). – С. 54–57.
5. Приказ МВД России от 29.12.2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС КонсультантПлюс.
6. Кашкаров А.А. О некоторых особенностях предупреждения распространения информации экстремистской и иной деструктивной направленности в информационно-телекоммуникационных сетях, в том числе сети «Интернет» // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2019. – Т. 5, № 3. – С. 352–357.
7. ФинЦЕРТ: структурное подразделение Банка России. URL: https://www.cbr.ru/information_security/fincert/.
8. 82% россиян сталкивались с попытками мошенничества. – URL: https://nafi.ru/analytics/82-rossiyan-stalkivalis-s-popytkami-moshennichestva/ (дата обращения: 18.04.2024).
9. Акапьев В.Л., Дрога А.А., Савотченко С.Е. Профилактика преступленийв сфере информационных технологий // Алтайский юридический вестник. – 2022. – № 4(40). – С. 84–89.


## On the Activities of Law Enforcement Agencies to Counteract Crimes Committed in the Field of Information and Telecommunication Technologies


***Mikhailova I.A., Limar A.S.***
***Belgorod Law Institute of Ministry of the Internal of the Russian Federation named after I.D. Putilin***
***Gilaev R.I.***
***The Main Directorate of the Ministry of Internal Affairs of Russia for the Krasnoyarsk Territory***



*Digital technologies underlying modern social relations have replaced the traditional format of state programmes. Telecommunication technologies, on the one hand, make it possible to reduce organisational, time, financial, personnel and other costs, increase the availability and quality of services provided using such technologies, create a basis for the accumulation of personal, commercial, state and other data protected by the legislation of the Russian Federation. However, the introduction of new technologies*

*into various spheres of social or public relations naturally gives rise to the development of crime in this area. As a consequence, the activities of law enforcement agencies to counteract digital crime is a relevant area of modern law enforcement policy.*

*The purpose of this article is to study measures to prevent crimes committed in the sphere of information and telecommunication technologies. The authors have analysed the measures taken by the units of the Ministry of Internal Affairs, the Investigative Committee, and the Federal Security Service of the Russian Federation to counter such crimes. The resources used by law enforcement agencies to counteract cybercrimes are identified, some problematic issues of prevention and investigation of extremist and terrorist crimes, fraud committed with the use of information and telecommunication technologies are revealed. Based on the results of the study, the authors proposed measures to improve the system of countering cybercrime, which can be used for further scientific development of this issue, as well as in the practical activities of law enforcement agencies.*

*Key words: information security, law enforcement agencies, countering crimes committed using information and telecommunication technologies*