Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2023. – Т. 9 (75). № 4. – С. 283 – 286.

УДК 343.985:004

ВЛИЯНИЕ ФАКТОРА ЦИФРОВИЗАЦИИ НА ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Ховавко С. М.
Крымский филиал Краснодарского университета МВД России

В статье рассматриваются тенденции современных процессов цифровизации, а также их влияние на оперативно-розыскную деятельность органов внутренних дел. Приводятся статистические данные о структуре и динамике совершения киберпреступлений. Проводится ретроспективный анализ уголовного законодательства в части усиления ответственности за совершение преступлений с использование сети Интернет. Дается характеристика особенностей совершения киберпреступлений, а также описываются новые и перспективные методики проведения отдельных оперативно-розыскных мероприятий в условиях цифровизации. Делаются выводы об основных направлениях повышения эффективности противодействия киберпреступности в условиях цифровизации.

Ключевые слова: цифровизация, киберпреступления, сеть Интернет, оперативно-розыскная деятельность, оперативно-розыскные мероприятия.

Цифровизация — одно из приоритетных направлений развития России на ближайшие годы. К 2024 г. все государственные информационные системы будут переведены на единую цифровую платформу. Цифровизация – это процесс превращения аналоговых данных и рабочих процессов в цифровой формат. В настоящее время интернет и цифровые технологии активно внедряются во все сферы социально-экономической деятельности и повседневный быт. Вместе с тем, глобальная цифровизация и развитие информационных технологий привело к увеличению количества киберпреступлений. В соответствие с официальной статистикой правоохранительных органов почти две трети из них было совершено с использованием сети Интернет и более трети с применением мобильной связи. Мошенничества составили 43%, а кражи 31%. В 2022 г. количественные показатели противоправных деяний в сфере информационно-телекоммуникационных технологий увеличились на 28,7%, при этом их удельный вес в общих количественных показателях преступности возрос до 32,9%, а по тяжким и особо тяжким до 56,4%. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9%, в том числе совершенных с использованием сети Интернет 28,8%, расчетных (пластиковых) карт – 35,7% [1; 2]. В 2021 и 2022 гг. общий суммарный ущерб от киберпреступлений в России превысил 300 млрд. руб. Эксперты признают причиной роста киберпреступности низкую цифровую грамотность граждан. Кроме того, Сеть используется злоумышленниками для распространения незаконного контента, в первую очередь это касается экстремистской идеологии и порноматериалов.

Расширение масштабов цифровизации и лавинообразный рост интернет-контента обусловило законодательные инициативы в части усиления уголовно-правовой защиты граждан и организаций. В 2018 г. ужесточена ответственность за совершение краж денежных средств с банковского счета, которые караются лишением свободы на срок до 6 лет (п. «г» ч. 3 ст. 158 УК РФ). Ранее законодателем введен специальный состав мошенничества, совершенного с использованием электронных средств платежа (статья 159.3 УК РФ), к которым в соответствии с ФЗ «О национальной

платежной системе» относятся средства и (или) способы, позволяющие составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, иных технических устройств. При этом неправомерный оборот данных средств платежа (незаконное их изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт) относится к тяжким преступлениям и влечет наказание до 6 лет лишения свободы (ч. 1 ст. 187 УК РФ). В отдельный состав преступления выделено мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), связанное с хищением чужого имущества путем получения доступа к компьютерной системе и совершения определенных действий (ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства). Повышенная уголовная ответственность также установлена за совершение с использованием сети Интернет таких преступлений, как доведение до самоубийства (ст. 110 УК РФ), вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни (ст. 151.2 УК РФ), сбыт наркотических средств, психотропных веществ или их аналогов (ст. 228.1 УК РФ), незаконные изготовление и оборот порнографических материалов (ст. 242 УК РФ), призывы к осуществлению террористической и экстремистской деятельности (ст. 205.2 и 280 УК РФ), и ряда других преступлений.

В настоящее время законодатель также планирует ужесточить санкции статей УК РФ, предусматривающих ответственность за незаконное использование информационно-коммуникационных технологий, путем дополнения перечня наказаний конфискацией имущества. К таким преступлениям отнесены: неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения обработки или передачи компьютерной информации, неправомерное воздействие на критическую информационную инфраструктуру. Перевод ряда преступлений, совершенных с использованием сети Интернет, в категорию тяжких дает полномочия для оперативных подразделений проводить в целях выявления и документирования этих преступлений оперативно-розыскные мероприятия судебного санкционирования [3], тем более, что такие оперативно-розыскные мероприятия, как «получение компьютерной информации», «снятие информации с технических каналов связи», «прослушивание телефонных переговоров» являются неотъемлемой частью методики документирования рассматриваемых преступлений. Появление в 2016 г. такого оперативно-розыскного мероприятия, как «получение компьютерной информации» было обусловлено именно фактором цифровизации [4]. Методика таких оперативно-розыскных мероприятий, как «снятие информации с технических каналов связи» и «получение компьютерной информации», постоянно совершенствуется с учетом современного состояния и перспектив развития технологий.

Цифровизация дает возможности оперативным подразделениям разрабатывать и внедрять в оперативную работу новые методики проведения отдельных оперативно-розыскных мероприятий, например, проведение оперативно-розыскного мероприятия «отождествления личности» стало возможным в сети Интернет, как непосредственно свидетелями или потерпевшими, так и с применением цифровых технологий распознавания лица или голоса; также стало возможным проведение в сети Ин-

тернет или с использованием средств мобильной связи оперативно-розыскного мероприятия «опрос» в залегендированной форме, в том числе с использованием технологии изменения голоса. Перевод данных в цифровой формат позволяет интегрировать различные базы данных и получать к ним удаленный доступ, что существенно облегчает и ускоряет проведение такого оперативно-розыскного мероприятия, как «наведение справок». Технологии Big Data и нейросети позволяют осуществлять поиск лиц и фактов, представляющих оперативный интерес на качественно новом уровне [5]. Обстоятельства подготовки и совершения киберпреступлений имеют свои особенности, которые обусловливают сложность и специфику их раскрытия. К таким специфическим особенностям совершения и раскрытия рассматриваемых преступлений следует отнести следующие: территориальная распределенность злоумышленника и жертвы преступления (зачастую злоумышленники находятся за пределами РФ); отсутствие реального фактического контакта между злоумышленником и жертвой преступления (общение происходит в виртуальной среде или посредством мобильной связи); высокая виктимность киберпреступлений вследствие цифровой безграмотности определенной части населения; доступность для злоумышленников орудий и средств совершения киберпреступлений; предметом преступного посягательства в большинстве случаев являются цифровые данные; формирование в процессе подготовки и совершения преступления электронных следов.

Для создания препятствий правоохранительным органами в раскрытии данных преступлений злоумышленники используют различные способы конспирации, меняют номера сотовых телефонов, адреса своего местонахождения, оформляют сим-карты и открывают счета в банках на подставных лиц, используют электронные кошельки. Особенностью киберпреступлений также является регулярное обновление способов совершения конкретных преступлений, что обусловлено расширением масштабов цифровизации в государстве.

С целью усиления мер противодействия киберпреступности в структуре органов внутренних дел созданы подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий, к основным задачам которых относятся предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе МВД России; анализ данных, содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия преступности [6; 7]. Таким образом, повышению эффективности противодействия киберпреступности в условиях цифровизации могут способствовать следующие меры правового и организационного характера: усиление мер юридической ответственности за совершение киберпреступлений; правовая и техническая возможность доступа оперативных подразделений к цифровым базам данных государственных органов; межрегиональное и международное взаимодействие оперативных подразделений по противодействию киберпреступности; совершенствование методик оперативно-розыскных мер «снятие информации с технических каналов связи» и «получение компьютерной информации»; разработка новых методик проведения оперативно-розыскных мероприятий в виртуальной среде; более активное осуществление оперативного поиска в сети Интернет с применением технологии Big Data; анализ оперативной обстановки по линии киберпреступности с целью своевременного выявления новых

криминальных тенденций и способов совершения преступлений; повышение квалификации сотрудников вновь созданных подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий; достаточная техническая оснащенность и программное обеспечение подразделений специальных технических мероприятий и подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий; внедрение новых форм виктимологической профилактики киберпреступлений, в том числе с использованием современных информационно-телекоммуникационных технологий.

Список литературы:

1.Статистические данные МВД РФ. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics
2.Статистические данные Генпрокуратуры РФ. Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/activity/statistics/office/result
3.Об оперативно-розыскной деятельности : Федеральный закон от 12.08.2023 № 144-ФЗ. СП «Гарант.ру». URL: https://base.garant.ru /10104229/
4.Лагуточкин А.В. Получение компьютерной информации: вопросы теории и практики // Вестник Академии Следственного комитета Российской Федерации. 2023. № 1 (35). С. 75-81.
5.Лагуточкин А.В. Сущность, формирование и перспективы использования нейросетевых технологий в оперативно-розыскной деятельности // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8. № 4. С. 354-365.
6.Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации : Приказ МВД России от 29.12.2022 № 1110. СП «Гарант.ру». URL: https://base.garant.ru/406374891/
7.Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность : Приказ МВД России от 31.03.2023 N 199. СП «Гарант.ру». URL: https://base.garant.ru/407540201/

Khovavko S.M. The influence of the digitization factor on the operational investigative activities of internal affairs bodies // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2023. – T. 9 (75). № 4. – P. 283 – 286.

The article examines the trends of modern digitalization processes, as well as their impact on the operational investigative activities of internal affairs bodies. Statistical data on the structure and dynamics of cybercrimes is provided. A retrospective analysis of criminal legislation is carried out in terms of strengthening liability for crimes committed using the Internet. Characteristics of the peculiarities of committing cybercrimes are given, and new and promising methods for carrying out individual operational investigative activities in the context of digitalization are described. Conclusions are drawn about the main directions for increasing the effectiveness of combating cybercrime in the context of digitalization.

Key words: digitalization, cybercrime, Internet, operational investigative activities.

Spisok literatury:

1. Statisticheskie dannye MVD RF. Oficial'nyj sajt Ministerstva vnutrennih del Rossijskoj Federacii. URL: https://mvd.rf/dejatelnost/statistics
2. Statisticheskie dannye Genprokuratury RF. Oficial'nyj sajt General'noj prokuratury Rossijskoj Federacii. URL: https://epp.genproc.gov.ru/web/gprf/activity/statistics/office/result
3. Ob operativno-rozysknoj deyatel'nosti : Federal'nyj zakon ot 12.08.2023 № 144-FZ. SP «Garant.ru».
4. Lagutochkin A.V. Poluchenie komp'yuternoj informacii: voprosy teorii i praktiki // Vestnik Akademii Sledstvennogo komiteta Rossijskoj Federacii. 2023. № 1 (35). S. 75-81.
5. Lagutochkin A.V. Sushchnost', formirovanie i perspektivy ispol'zovaniya nejrosetevyh tekhnologij v operativno-rozysknoj deyatel'nosti // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2022. T. 8. № 4. S. 354-365.
6. Ob utverzhdenii Polozheniya ob Upravlenii po organizacii bor'by s protivopravnym ispol'zovaniem informacionno-kommunikacionnyh tekhnologij Ministerstva vnutrennih del Rossijskoj Federacii : Prikaz MVD Rossii ot 29.12.2022 № 1110. SP «Garant.ru». URL: https://base.garant.ru/406374891/
7. Ob utverzhdenii Perechnya operativnyh podrazdelenij organov vnutrennih del Rossijskoj Federacii, pravomochnyh osushchestvlyat' operativno-rozysknuyu deyatel'nost' : Prikaz MVD Rossii ot 31.03.2023 N 199. SP «Garant.ru». URL: https://base.garant.ru/407540201/