3. Григорьева, И. В. Хищения государственных бюджетных средств как угроза экономической безопасности Российской Федерации / И. В. Григорьева // Пробелы в рос. законодательстве. – 2017. – № 5. – С. 204–206.

4. Григорьева, И. В. Направления совершенствования уголовно-правовых мер по противодействию хищениям государственной собственности / И. В. Григорьева // Пробелы в российском законодательстве. – 2018. – № 2. – С. 118–121.

5. Сведения ГИАЦ МВД России за 2022–2023 гг. [Электронныйресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/dejatelnost/results/annual_reports – Дата доступа: 05.06.2023.

СОСТОЯНИЕ И ПРОБЛЕМЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Павловская Надежда Владимировна
заведующий лабораторией криминологического обеспечения прокурорской деятельности Научно-исследовательского института Университета прокуратуры Российской Федерации, кандидат юридических наук
korsica@mail.ru

Поиск эффективных способов предупреждения преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ), в последние годы приобретает все большую актуальность и востребованность не только в России, но и в других странах.

Официальные статистические данные показывают значительные масштабы распространения криминальных посягательств данного вида [1]. Так, в 2020–2022 гг. правоохранительными органами в Российской Федерации ежегодно регистрировалось свыше 500 тыс. преступлений, совершенных с использованием ИКТ, в 2023 г. – свыше 600 тыс., а за пятилетний период данный показатель увеличился в 2,3 раза (с 294 тыс. в 2019 г. до 676 тыс. в 2023 г.).

Преступления, совершенные таким способом, занимают все более заметную долю в общей структуре преступности в России. Если пять лет назад на них приходилось лишь 14,5 % всего массива зарегистрированных преступлений, то в 2023 г. – уже более трети (34,8 %), а в некоторых субъектах Российской Федерации данный показатель достигает половины (например, в 2023 г. в Ямало-Ненецком автономном округе она составляет 50,5 %, в Республике Татарстан – 47,9 %, в Республике Марий Эл – 47,2 %, в г. Москва – 45,5 %).

Использование ИКТ становится преобладающим способом совершения для отдельных видов преступлений. Например, сейчас с использованием информационных технологий совершаются две трети

всех деяний, связанных с незаконным производством, сбытом или пересылкой наркотиков, ответственность за которые предусмотрена ст. 228-1 Уголовного кодекса Российской Федерации (далее – УК РФ), свыше 70 % всех случаев вымогательства (ст. 163 УК РФ), более 80 % всех случаев мошенничества (ст. 159 УК РФ).

Чаще всего в преступных целях используются сеть «Интернет» (в 2023 г. – сеть использовалась для совершения 77,8 % всех зарегистрированных преступлений, совершенных с использованием информационно-коммуникационных технологий) и средства мобильной связи (44,7 %).

Наиболее массовым видом преступлений, совершенных с использованием ИКТ, является мошенничество (ст. 159 УК РФ). На них в 2023 г. приходится более половины (52,2 %) всех зарегистрированных преступлений, для совершения которых использовались такие технологии. При этом их количество ежегодно только увеличивается (+32,2 % в 2019 г., +75,6 % в 2020 г., +13,3 % в 2021 г., +4,8 % в 2022 г. и +41,3 % в 2023 г.). Второе место после мошенничества в структуре рассматриваемых преступлений занимают кражи (ст. 158 УК РФ) (17,6 %), а третье – незаконные производство, сбыт или пересылка наркотических средств… (ст. 228-1 УК РФ) (12,0 %). До 5,5 % в 2023 г. увеличился удельный вес преступлений в сфере компьютерной информации, предусмотренных статьями гл. 28 УК РФ.

Разработка системы мер предупреждения преступлений, совершаемых с использованием ИКТ, должна опираться на результаты анализа и изучения особенностей их причинного комплекса, личности современного кибер-преступника, виктимологических характеристик жертв криминальных посягательств. Так, проводимые исследования указывают на определяющее значение в детерминации телефонного и интернет-мошенничества низкого уровня правовой и финансовой грамотности, незнания правил компьютерной гигиены или пренебрежения ими. Так, по данным исследования, проведенного по заказу Банка России, только половина опрошенных респондентов понимают, что чем выше доходность, тем выше риск, а также осведомлены об организациях, занимающихся защитой прав потребителей на финансовом рынке, около половины готовы рискнуть деньгами при инвестировании, пятая часть не использует никакие средства защиты финансов в Интернете, столько же пострадали от взаимодействия с финансовыми, в том числе телефонными, мошенниками [2].

В этих условиях возрастает роль правового и финансового просвещения и информирования в предупреждении преступлений, совершаемых с использованием информационно-коммуникационных технологий. В этом направлении в последние годы российским государством и обществом предпринимаются значительные усилия. Так, распоряжением Правительства Российской Федерации от 25 сентября 2017 г. № 2039-р утверждена Стратегия повышения финансовой грамотности в Российской

Федерации на 2017–2023 годы, распоряжением Правительства Российской Федерации от 22 декабря 2022 г. № 4088-р утверждена Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации, в 2023 г. Банком России одобрены основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов.

В целях повышения эффективности предупреждения кибермошенничества активно совершенствуется российское законодательство. Так, распространенность мошеннических схем, в которых преступники оформляют на граждан кредиты и займы, похищая крупные суммы денежных средств, привела к введению Федеральным законом от 26 февраля 2024 г. № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)» возможности установления гражданами через портал «Госуслуги» или МФЦ запрета на оформление им кредитов. В случае, если кредит все-таки будет выдан, несмотря на установленный запрет, кредитор не сможет потребовать исполнения обязательств по кредиту.

С 25 июля 2024 г. Банк России расширил перечень ранее утвержденных им признаков перевода денежных средств без согласия клиентов. Приказом Банка России от 27 сентября 2018 г. № ОД-2525 к таким сомнительным (мошенническим) операциям относились случаи, когда получатель средств или устройство, с использованием которого производится перевод, находятся в специальной базе данных Банка России; характер, параметры и объем проводимой операции не соответствуют обычным операциям клиента. К этому добавлены случаи переводов на счета, по которым ранее уже совершались мошеннические действия, даже если информации об этом нет в базе данных Банка России; если есть информация о возбужденном уголовном деле в отношении получателя средств; если имеются данные от сторонних организаций, свидетельствующие о мошеннических операциях.

Одновременно с этим вступят в силу нормы Федерального закона от 24 июля 2023 г. № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе», устанавливающие обязанность операторов денежных переводов приостановить операции при обнаружении подобных признаков на два дня (так называемый период охлаждения) и уведомить об этом клиента. Предполагается, что за этот срок клиент может осознать, что перевел деньги мошенникам, и отменить операцию. Если оператор по переводу денежных средств исполнит операцию в нарушение установленных требований, он будет обязан вернуть клиенту – физическому лицу полную сумму похищенных средств в течение 30 дней после получения от него соответствующего заявления.

Одним из действенных способов предупреждения телефонного мошенничества и иных преступлений становится привлечение операторов сотовой связи к административной ответственности за пропуск соединений

с так называемых подменных иностранных номеров. Так, в г. Санкт-Петербург штрафы в 600 тыс. руб. назначены каждому из двух мобильных операторов, допустивших пропуск в свои сети трафика из иностранных государств с номерами российской системы нумерации, которые использовались при совершении дистанционных хищений денежных средств граждан путем обмана в общем размере свыше 1,4 млн руб. [3].

Принимаемые меры могут способствовать более эффективному предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Список цитированных источников

1. Министерство внутренних дел Российской едерации [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/dejatelnost/statistics. – Дата доступа: 13.07.2024.

2. Банк России [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/analytics/szpp/fin_literacy/fin_ed_4/. – Дата доступа: 13.07.2024.

3. Генеральная прокуратура Российской Федерации [Электронный ресурс]. – Режим доступа: https://epp.genproc.gov.ru/web/gprf/search?article=96129384. – Дата доступа:13.07.2024.

ДИФФЕРЕНЦИАЦИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ В НОВЕЛЛАХ ОСОБЕННОЙ ЧАСТИ УК БЕЛАРУСИ 2021–2024 ГГ.

Плетенева Дарья Александровна
старший преподаватель кафедры уголовного права
юридического факультета Белорусского государственного университета
dapleteneva@gmail.com

Законами Республики Беларусь от 26 мая 2021 г. № 112-З; от 14 декабря 2021 г. № 133-З; от 4 января 2022 г. № 144-З; от 5 января 2022 г. № 146-З; от 9 марта 2023 г. № 256-З; от 8 июля 2024 г. № 22-З в УК введены составы 21 вида преступлений.

Это следующие преступления: реабилитация нацизма (ст. 130-1); отрицание геноцида белорусского народа (ст. 130-2); незаконные организация деятельности общественного объединения, религиозной организации или фонда либо участие в их деятельности (ст. 193-1); нарушение законодательства о средствах массовой информации (ст. 198-1); незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203-1); несоблюдение мер обеспечения защиты персональных данных (ст. 203-2); уклонение от исполнения обязанностей налогового агента по перечислению налогов, сборов (ст. 243-1); налоговое мошенничество (ст. 243-2); уклонение от уплаты страховых взносов (ст. 243-3); пропаганда терроризма (ст. 289-1); управление транспортным средством лицом, не имеющим права управления