ТРИБУНА МОЛОДОГО УЧЕНОГО

Научная статья
УДК 343.985.7:[343.7:004](470)

Станислав Николаевич Ущекин
Уфимский юридический институт МВД России, Уфа, Россия, stanislav.ushekin@yandex.ru

НЕКОТОРЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ IT-ТЕХНОЛОГИЙ

Аннотация. В статье исследуются наиболее распространенные способы совершения преступлений в сфере информационных технологий (IT-технологий, и проблемы, связанные с раскрытием и расследованием их органами внутренних дел. Автором отмечено, что в настоящее время IT-технологии занимают главное место в мире, идет необратимый процесс развития общества и государства в целом, происходит переход всех сфер жизнедеятельности в информационное пространство. В связи с изложенным происходит и трансформация преступности, а именно появляются новые способы совершения преступлений, которые ранее правоохранительным органам были не известны.

В работе проанализированы различные негативные моменты, влияющие на расследование и раскрытие указанного вида преступлений. На основании проведенного анализа сделан вывод о том, что, для повышения уровня раскрываемости указанного вида преступлений необходимо как минимум исключить изложенные в указанной статье неблагоприятные факторы и организовать получение дополнительного образования для сотрудников, закрепленных за раскрытием указанного направления преступной деятельности.

Ключевые слова: преступления, информационно-телекоммуникационные технологии, раскрытие преступлений, IT-технологии, негативные факторы.

Для цитирования: Ущекин С. Н. Некоторые проблемные вопросы в борьбе с преступлениями в сфере IT-технологий // Право: ретроспектива и перспектива. 2022. № 2 (10). С. 89–94.

Original Article

Stanislav N. Ushchekin
Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, stanislav.ushekin@yandex.ru

SOME PROBLEM QUESTIONS IN THE FIGHT AGAINST CRIMES IN THE SPHERE OF IT-TECHNOLOGIES

Abstract. The article examines the most common ways of committing crimes in the field of information technology (IT-technologies), and the problems associated with the disclosure and investigation of them by the internal affairs bodies. The author noted that at present, IT-technologies occupy the main place in the world, there is an irreversible process of development of society and the state as a whole, there is a transition of all spheres of life into the information space. In connection with the above, there is also a transformation of crime, namely, there are new ways of committing crimes that were previously unknown to law enforcement agencies.

The paper analyzes various negative aspects that affect the investigation and disclosure of this type of crime. Based on the analysis, it was concluded that, in order to increase the level of detection of this type of crime, it is necessary at least to eliminate the unfavorable factors set forth in this article, and organize additional education for employees assigned to the disclosure of this area of criminal activity.

Keywords: crimes, information and telecommunication technologies, crime detection, IT-technologies, negative factors.

For citation: Ushchekin S. N. Some problem questions in the fight against crimes in the sphere of IT-technologies // Law: retrospective and perspective. 2022. No. 2 (10). P. 89–94.

В настоящее время информационно-телекоммуникационные технологии (IT-технологии) занимают главное место в мире, идет необратимый процесс развития общества и государства в целом, происходит переход всех сфер жизнедеятельности в информационное пространство. В связи с изложенным происходит и трансформация преступности, а именно появляются новые способы совершения преступлений, которые ранее правоохранительным органам были не известны.

С момента введения самоизоляции на территории России число случаев, связанных с телефонным и интернет-мошенничеством за первые 6 месяцев 2020 года увеличилось примерно на 76 %. По итогам 2021 года практически каждое четвертое преступление совершается с использованием IT-технологий. При этом темп роста их количества замедлился.

За четыре месяца текущего года наблюдается снижение количества преступлений, совершенных с использованием IT-технологии. По сравнению с январем–апрелем 2021 года их зарегистрировано на 11,4 % меньше. [1].

Тенденция роста преступлений с использованием IT-технологий напрямую связана с неполноценным освоением информационного пространства, и в частности сети Интернет, правоохранительными органами. Сегодня раскрытие преступлений, совершенных с использованием IT-технологий, является одной из основных задач правоохранительных органов. Неоднократно Президентом Российской Федерации, Министром внутренних дел и иными высокопоставленными должностными лицами акцентировалось внимание на совершенствование способов раскрытия и профилактики указанного вида преступной деятельности. Например, 20 февраля 2019 г. в ежегодном Послании Президента Российской Федерации Федеральному Собранию В. В. Путин определил: «Нам необходимы специалисты, способные работать на передовых производствах, создавать и использовать прорывные технические решения. Для этого нужно обеспечить широкое внедрение обновленных учебных программ на всех уровнях профессионального образования, организовать подготовку кадров для тех отраслей, которые еще только формируются» [2].

Президент Российской Федерации в первую очередь, указывает на необходимость подготовки технических специалистов, которые в будущем будут развивать информационное общество и государство, в связи с чем создаются различные отделы, привлекаются отдельные граждане, обладающие особыми познаниями в области информационных технологий, а также проводится обучения действующих сотрудников органов внутренних дел с целью успешного формирования аппарата противодействия новому виду преступности.

Для наиболее всестороннего исследования проблем раскрытия преступлений, совершенных с использованием IT-технологий, необходимо раскрыть смысл указанной терминологии.

Как нам известно, информация представляет собой различные сведения и данные, независимо от формы их представления, в этой связи под информационно-телекоммуникационными технологиями (IT-технологии) следует понимать различные процессы, способы и методы поиска, сбора, хранения, обработки, предоставления и распространения информации [3].

Изначально задачей информационно-телекоммуникационных технологий было обеспечить общество современными, более простыми, наименее затратными способами и методами поиска, сбора, хранения, обработки, предоставления и распространения информации. Однако лица, осуществляющие преступную деятельность, полноцен-

но освоили данную новацию и принялись осуществлять противозаконные действия с информационными данными, принадлежащими различным людям, независимо от их социального или материального положения.

Исходя из судебной практики, основным объектом совершаемых преступлений является собственность, в частности электронные денежные средства, находящиеся на счетах их владельцев. Основным способом совершения указанных деяний является тайное хищение чужого имущества путем обмана, злоупотребления доверием либо без такового.

Противозаконные деяния, совершаемые с использованием IT-технологий, охватываются рядом составов преступлений, указанных в действующем Уголовной законодательстве Российской Федерации, – это различные виды мошенничества (ст. 159, ст. 159.3, ст. 159.6 Уголовного кодекса Российской Федерации (далее – УК РФ)) краж (п. «г» ч. 3 ст. 158 УК РФ) и иного хищения чужого имущества совершенного с использованием информационно-телекоммуникационных технологий [4].

При расследовании и раскрытии указанных преступлений возникают множество проблемных вопросов, которые в настоящее время решить не представляется возможным. Исходя из анализа практической деятельности, направленной на раскрытие указанного вида преступления, можно сделать вывод о том, что большинство преступлений, совершенных с использованием IT-технологий, годами остаются нераскрытыми.

Повышение статистики раскрываемости по указанному виду преступлений идет за счет «очевидных» преступлений: хищение чужого имущества совершенное с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) и мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ). В большинстве случаев под квалификацию по указанным статьям попадают действия лиц, связанные с обнаружением (находкой) или хищением банковских карт с дальнейшим снятием с них денежных средств либо оплатой различных товаров и услуг [5].

Указанные деяния, на наш взгляд, являются в большинстве случаев очевидными, ведь на всех кассах магазинов и банкоматах имеются камеры видеонаблюдения, при помощи которых можно получить изображение правонарушителя и в дальнейшем с использованием специальных баз данных МВД России получить установочные данные лица. Также имеют место и ситуации, связанные с нерегистрацией указанного вида преступлений, в результате чего заявителю объясняется невозможность раскрытия указанного преступления и бесполезность проведения различных мероприятий по данному факту. В результате изложенные моменты создают мнимую видимость раскрываемости преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

На сегодняшний день существуют различные способы и схемы совершения указанных ранее видов преступлений, наиболее распространенными из них являются:

– двойники интернет-магазинов. Дешевые товары и привлекательные предложения для потенциальных потерпевших. Через поисковые системы пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец получает оплату и пропадает или присылает совершенно иной товар;

– копии сервисов интернет-банкинга. Злоумышленники создают дубликаты сайтов банков. Посредством электронного письма или сообщения на сотовый телефон граждан приглашают пользователей пройти авторизацию. Граждане переходят на фальшивый сайт, регистрируются в личном кабинете, раскрывая логин и пароль для доступа к финансам. Таким образом, лица, вынашивающие противоправный умысел, получают доступ к их банковским счетам;

– фишинговая атака по электронной почте. Рассылка писем с сообщением о выигранном призе или о блокировке счета. Злоумышленники, как правило, просят «по-

бедителя» перевести определенную сумму на указанный ими счет для получения крупного выигрыша или внести оплату для разблокировки карты;

– взлом аккаунтов в социальных сетях и рассылка от их имени сообщений с целью наживы. Мошенники пишут на почту или в соцсети родственникам и знакомым владельца страницы с просьбой срочно перевести деньги, придумывая различные ситуации;

– фальшивые сайты благотворительных организаций, туроператоров, авиакомпаний. Просьба экстренной помощи, заключающейся в сборе денег на лечение больного ребенка, привлекательные цены на путевки;

– «предложения выгодного заработка». Как правило, в данной ситуации злоумышленники предлагают удаленную работу, за которую требуют оплатить взносы на организационные нужды [6].

Помимо выше изложенных, существуют и иные многочисленные способы введения в заблуждение потенциальных потерпевших с целью получения от них денежных средств. Ежедневно лица, совершающие преступления с использованием IT-технологий, развиваются, придумывают новые, ранее не известные способы и схемы обмана.

Недостижение положительных результатов при расследовании и раскрытии преступлений, совершенных в сфере IT-технологий, напрямую зависит от подхода самих сотрудников к расследованию и раскрытию преступления.

С учетом опроса практических работников, а так же анализа юридической литературы и результатов научных трудов других авторов, связанных с тематикой указанного исследования, необходимо выделить следующие неблагоприятные факторы, влияющие на расследование и раскрытие преступлений в сфере информационных технологий:

– нехватка кадров. Со слов Министра внутренних дел Российской Федерации В. А. Колокольцева «Самая серьезная проблема – значительный некомплект» [7]. Множество должностей в органах внутренних дел остаются вакантными достаточно долгое время, в результате чего нагрузка на каждого сотрудника растет, в связи с чем отсутствует реальная временная возможность проведения мероприятий по указанному виду преступлений;

– дефицит специалистов в области информационных и коммуникационных технологий либо низкий уровень владения ими среди сотрудников. В связи с отсутствием необходимых познаний в сфере информационных технологий сотрудники правоохранительных органов в большинстве случаев не могут объективно понять схему совершенного преступления и способ его раскрытия, из-за чего осуществляют формально-минимальное количество мероприятий, и в итоге получить положительный результат не представляется возможным [8];

– необходимость проведения технических мероприятий. В большинстве случаев для раскрытия преступлений, совершенных с использованием информационных технологий, необходимо проведение технических мероприятий, которые, в связи с несовершенством взаимодействия со специальными подразделениями, требуют много времени. Зачастую сотрудники допускают ошибки при подготовке документов на проведение технических мероприятий, в результате чего указанные негативные моменты приводят к тому, что следы преступления скрываются злоумышленниками и положительные результаты получить невозможно;

– упущения в обучении сотрудников правоохранительных органов в расследовании и раскрытии данного вида преступлений. В настоящее время при проведении занятий с сотрудниками оперативных подразделений по раскрытию киберпреступлений полная информация, необходимая для раскрытия и расследования указанных преступлений, не доводится;

– сложившийся стереотип в правоохранительных органах о том, что раскрыть преступление, совершенное с использованием IT-технологий, невозможно. В связи с указанным стереотипом у сотрудников правоохранительных органов отсутствует инициатива при раскрытии указанного вида преступных деяний и перспектива раскры-

тия переходит к наиболее простым, очевидным преступлениям.

Помимо выше изложенных неблагоприятных факторов, влияющих на раскрытие преступлений, совершенных с использованием IT-технологий, существуют и другие, которые напрямую зависят от сотрудников правоохранительных органов и их руководителей.

Таким образом, для повышения уровня раскрываемости указанных преступлений остается актуальным получение дополнительного образования сотрудниками органов внутренних дел.

В настоящее время идет процесс создания новых учебных дисциплин в образовательных организациях системы МВД России. 3 марта 2021 г. в Уфимском юридическом институте МВД России состоялось заседание ученого совета. По итогам было вынесено решение о принятии учебных планов в новой редакции по специальностям «Правоохранительная деятельность», «Правовое обеспечение национальной безопасности». В новую редакцию учебных планов была добавлена учебная дисциплина «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» [9].

Реальная возможность раскрыть преступные деяния, совершенные с использование информационно-телекоммуникационных технологий, имеется лишь ближайшие сутки, после чего все следы преступной деятельности будут бесследно удалены из интернет-пространства. Исходя из этого, необходимо наладить взаимодействие с различными организациями, для того чтобы оптимизировать процесс по получению информации от операторов сотовой связи и IT-телефонии, кредитно-финансовых учреждений, администраций социальных сетей. После того, как удастся исключить долговременный обмен информацией, правоохранительные органы смогут пользоваться актуальной информацией, которая обеспечит успешное расследование преступлений и закрепление доказательственной базы.

В любом случае необходимо не забывать и совершенствовать способы профилактики преступлений, совершаемых с использованием информационных технологий, переходя от листовок с профилактическим материалом и публикаций в средствах массовой информации к чему-то новому, позволяющему блокировать действия правонарушителей, с момента обнаружения негативной активности в информационном пространстве.

СПИСОК ИСТОЧНИКОВ

1. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года. URL: https://мвд.рф/reports/item/30105559 (дата обращения: 19.05.2022).

2. Послание Президента Российской Федерации Федеральному Собранию от 20 февраля 2019 г. // СПС «КонсультантПлюс» (дата обращения: 15.01.2022).

3. Об информации, информационных технологиях и о защите информации: Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. 2006 г. № 31. Ст. 3448. URL: https://base.garant.ru/ (дата обращения: 17.01.2022).

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954. URL: https://base.garant.ru/ (дата обращения: 14.01.2022).

5. Судебная практика. URL: https://sud-praktika.ru/precedent/category/1196.html (дата обращения: 25.01.2022).

6. Сетевое издание «РИА Новости». URL: https://ria.ru/20220118/internet-moshennichestvo-1768431202.html (дата обращения: 25.01.2022).

7. Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации от 17 февраля 2022 г. URL: https://mvdmedia.ru/news/official/vystuplenie-

minsistra-vnutrennikh-del-rossiyskoy-federatsii-generala-politsii-rossiyskoy-federatsii-v/ (дата обращения: 14.02.2022).

8. Загвоздкин Н. Н., Кузора С. А. Преступления в сфере информационных технологий. Особенности совершения, проблемы раскрытия и расследования органами внутренних дел // Закон и право. 2020. № 12. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-informatsionnyh-tehnologiy-osobennosti-sovershenia-problemy-raskrytiya-i-rassledovaniya-organami-vnutrennih (дата обращения: 14.02.2022).

9. Протокол заседания ученого совета Уфимского юридического института МВД России № 8 от 3 марта 2021 г. Республика Башкортостан, г. Уфа.

REFERENCES

1. Brief description of the state of crime in the Russian Federation for January – December 2021. URL: https://mvd.rf/reports/item/30105559 (date of access: 19.05.2022). (In Russ.)

2. Address of the President of the Russian Federation to the Federal Assembly of February 20, 2019 // RLS «ConsultantPlus» (date of access: 15.01.2022). (In Russ.)

3. On information, information technologies and information protection: federal law of the Russian Federation dated July 27, 2006 No. 149-FZ // Collection of legislation of the Russian Federation. 2006 No. 31. Art. 3448. URL: https://base.garant.ru/ (date of access: 17.01.2022). (In Russ.)

4. The Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ // Collection of Legislation of the Russian Federation. 1996. No. 25. Art. 2954. URL: https://base.garant.ru/ (date of access: 14.01.2022).

5. Judicial practice. URL: https://sud-praktika.ru/precedent/category/1196.html (date of access: 25.01.2022). (In Russ.)

6. Network publication «RIA Novosti». URL: https://ria.ru/20220118/internet-moshennichestvo-1768431202.html (date of access: 25.01.2022). (In Russ.)

7. Speech by the Minister of Internal Affairs of the Russian Federation, Police General of the Russian Federation Vladimir Kolokoltsev at an expanded meeting of the board of the Ministry of Internal Affairs of the Russian Federation on February 17, 2022. URL: https://mvdmedia.ru/news/official/vystuplenie-minsistra-vnutrennikh-del -rossiyskoy-federatsii-generala-politsii-rossiyskoy-federatsii-v/ (date of access: 14.02.2022).

8. Zagvozkin N. N., Kuzora S. A. Crimes in the field of information technology. Features of commission, problems of disclosure and investigation by internal affairs bodies // Law and Law. 2020. No. 12. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-informatsionnyh-tehnologiy-osobennosti-sovershenia-problemy-raskrytiya-i-rassledovaniya-organami-vnutrennih (date of access: 14.02.2022). (In Russ.)

9. Minutes of the meeting of the Academic Council of the Ufa Law Institute of the Ministry of Internal Affairs of Russia No. 8 dated March 3, 2021, Republic of Bashkortostan, Ufa. (In Russ.)

Статья поступила в редакцию: 16.03.2022; одобрена после рецензирования: 31.05.2022; принята к публикации: 24.06.2022.

The article was submitted: 16.03.2022; approved after reviewing: 31.05.2022; accepted for publication: 24.06.2022.