УДК 343.721
doi: 10.35750/2071-8284-2021-1-167-171

Кирилл Игоревич Озеров
адъюнкт
ORCID: 0000-0003-3585-712X, ozerov.kir@yandex.ru

Московский университет МВД России имени В.Я. Кикотя
Российская Федерация, 117997, Москва, ул. Академика Волгина, д. 12

Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий

Аннотация: В данной статье рассмотрены проблемы, связанные с раскрытием мошенничеств в сфере информационно-телекоммуникационных технологий, заключающиеся в идентификации и определении местоположения злоумышленников. Отражаются статистические данные по анализируемой проблематике. Исследуются основные средства, используемые для обеспечения анонимности киберпреступников. Наглядно демонстрируются способы совершения мошеннических действий с использованием информационно-телекоммуникационных технологий, в том числе в сети Интернет. Также в данной статье отмечаются мнения различных государственных должностных лиц, научных деятелей и исследователей в области обеспечения противодействия актам кибермошенничества в сфере информационно-телекоммуникационных технологий. В рамках исследования был проведён опрос практических сотрудников, который отражает наглядную картину рассматриваемой проблематики в повседневной жизнедеятельности гражданина и практической работе сотрудников органов внутренних дел, служб информационной безопасности различных организаций. Демонстрируется влияние Covid-19 и его последствий на исследуемую нами преступность. В заключение научной работы были вынесены предложения для наиболее эффективного противодействия мошенническим актам в области информационных технологий, в частности отмечаются необходимые меры профилактики, касающиеся взаимодействия органов внутренних дел как с другими правоохранительными структурами, так и с организациями, обеспечивающими безопасность в киберсреде.

Ключевые слова: мошенничество, информационно-телекоммуникационные технологии, преступление, раскрытие, оперативно-розыскная деятельность

Для цитирования: Озеров К. И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 167–171; doi: 10.35750/2071-8284-2021-1-167-171.

Kirill I. Ozerov
Graduate
ORCID: 0000-0003-3585-712X, ozerov.kir@yandex.ru

Moscow University of the MIA of the Russia named after V. Ya. Kikot
12, str. Academician Volgin, Moscow, 117997, Russian Federation

Disclosure of fraud using information and telecommunications technologies

Abstract: This article discusses the problems associated with the disclosure of information and telecommunications fraud, such as the identification and location of perpetrators. Statistical data on the analyzed issues are reflected. The research conducted on the main means used to ensure the anonymity of cybercriminals. The main methods in which information and telecommunications technologies, including

the Internet, can be used for fraud are clearly demonstrated. The article also notes the opinions of various government officials, scientists and researchers in the field of countering acts of cyber fraud in the field of information and telecommunications technologies. As part of the study, a survey of practical employees was conducted, which reflects a clear picture of the issues under consideration in the daily life of a citizen and the practical work of employees of internal Affairs bodies, information security services of various organizations. The influence of Covid-19 and its consequences on the crime we investigate is demonstrative. At the conclusion of the scientific work, suggestions were made for the most effective counteraction against fraudulent acts in the field of information technology, in particular the necessary preventive measures, are taken with regard to cooperation between the Internal Affairs agencies and other law enforcement agencies and that ensure security in the cyber environment.

Keywords: fraud, information and telecommunication technologies, crime, disclosure, operational detective activity

For citation: Ozerov K. I. Disclosure of fraud using information and telecommunications technologies // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2021. – № 1 (89). – P. 167–171; doi: 10.35750/2071-8284-2021-1-167-171.

В настоящее время наблюдается тенденция массового внедрения информационно-телекоммуникационных систем в повседневную жизнь человека. С их появлением появились негативные моменты.

В силу быстрого темпа развития телекоммуникационных технологий и сложности освоения масштабного программного обеспечения правоохранительными органами, преступная сторона из-за своей заинтересованности и многочисленности атакует киберпространство, совершая мошеннические преступления как против государства, юридических лиц, так и в отношении рядовых граждан страны. В отделах уголовного розыска практически нет работников с техническим образованием, как и оснащения высокотехнологическими средствами, чтобы своими силами предотвращать преступления в рассматриваемой нами сфере.

Дмитрий Медведев на международном форуме «International Cybersecurity Congress» заявил: «Проблема киберпреступности входит в топ-5 по глобальности и наносимому ущербу среди преступлений, её ставят выше порой даже экологических угроз, терроризма и экстремизма».

Мы не можем не согласиться с этим, ведь статистические данные говорят сами за себя. Зарегистрированных мошенничеств с использованием информационно-телекоммуникационных технологий, предусмотренных статьёй 159 УК РФ, – 173 233 случая за отчётный период с января по октябрь 2020 года, из которых раскрыто за данный период всего 10 945. Мошенничеств в сфере компьютерной информации, предусмотренных статьёй 159[6] УК РФ, – 615, раскрытых преступлений – 94. Если рассмотреть аналогичную статистику прошлого 2019 года, то мы увидим, что всего преступлений с использованием компьютерных и телекоммуникационных технологий – 180 153, сейчас же эта цифра достигает 420 662 случаев. Практически втрое увеличилось количество преступлений, совершаемых в киберпространстве.

12 октября 2020 года о росте киберпреступности высказался глава следственного департамента МВД России Сергей Лебедев: «Пандемия коронавирусной инфекции неблагоприятно повлияла на рост информационно-телекоммуникационных мошенничеств, так как многие сферы общества перевели свою деятельность на дистанционный режим». По его словам, на 82 % возросло количество киберпреступлений, совершённых через сеть интернет, а мошенничеств с использованием сотовых телефонов практически в два раза, с использованием же расчётных пластиковых карт приблизительно в 6 раз[1].

Негативная санитарно-эпидемиологическая составляющая стала виновником роста киберпреступности в России. Выявить и раскрыть мошеннические хищения, совершаемые с использованием информационно-телекоммуникационных технологий, крайне сложно, ведь мошенники имеют хорошее техническое оснащение, преобразуются в преступные сообщества, которые порой имеют международное взаимодействие.

Преступления такого рода совершаются дистанционно, причём с использованием атрибутики по сохранению анонимности самого лица и его местоположения. Мошенники пользуются сменой своего IP-адреса (VPN, SSL, TOR), что позволяет вводить в заблуждение правоохранительные органы. К тому же, применяются различные технологии «подставных номеров» с использованием IP-телефонии. Всё это делается для сокрытия следов преступной деятельности и сохранения конфиденциальности данных на протяжении всей подготовки и совершения преступного деяния.

[1] Официальный сайт МВД России [Электронный источник]. – URL: мвд.рф (дата обращения: 10.12.2020).

Основные способы совершения мошенничества с использованием информационно-телекоммуникационных технологий:

1) «претекстинг» и «телефонный фрикинг», когда поступают звонки и смс-сообщения от злоумышленников с просьбой предоставить реквизиты банковской карты или номера кода от онлайн-банка для списания денежных средств, а потерпевший самостоятельно передает запрошенную мошенниками информацию (тесно взаимосвязано с «фишингом»);

2) внедрение вредоносного программного обеспечения в систему онлайн-банка;

3) DDOS-атаки на систему безопасности различных банков или организаций по предоставлению услуг мобильной связи в целях выведения её из строя и получения доступа к счетам клиентской базы или напрямую к системе хранения денежных средств атакуемой компании;

4) взлом учётных данных путём подбора защитных кодов того или иного пользователя;

5) «фишинг», где пользователь, переходя по «спамирующим» сообщениям в виде картинок, телефонных номеров или ссылок на различные Интернет сайты, «передаёт» все свои электронные данные, хранящиеся на устройстве, мошенникам, также «заражая» свой компьютер либо телефон вредоносной программой.

Перед тем как рассмотреть проблемные моменты, связанные с раскрытием мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий, стоит затронуть профилактику подобной преступности.

Так, проведя опрос среди сотрудников отдела уголовного розыска УМВД России по г. Белгороду, мы выяснили, что профилактические мероприятия, в частности инструктажи по мошенничествам, которые совершаются с использованием информационно-телекоммуникационных технологий, проводятся ежедневно. Сотрудники уголовного розыска составляют график и список домов, находящихся на закреплённой территории, затем совершают обход жилых квартир в многоэтажных домах в целях осуществления профилактических бесед с населением, доводя им информацию о том, как чаще всего действуют злоумышленники.

Такие принимаемые практическими работниками меры профилактического воздействия на население, дают положительный результат, граждане действительно слышат о некоторых способах мошеннических актов в области киберпространства впервые.

Сложность и проблемность раскрытия мошенничеств с использованием информационно-телекоммуникационных технологий, предусмотренных статьями 159 и 159[6] УК РФ, состоит в следующем:

1) анонимность и конфиденциальность мошенников является одной из важнейших и серьёзных проблем. Идентифицировать данные о лице и его местонахождении крайне сложно, а при чёткой и слаженной работе мошенников, шансов у правоохранителей совсем мало. Злоумышленники зачастую пользуются иностранным программным обеспечением, IP-адресами, серверами и всем элементным обеспечением, находящимся за пределами Российской Федерации (например, в США). Это говорит о том, что получить оперативно-значимую информацию по тому или иному пользователю невозможно;

2) получение информации, запрошенной правоохранительными органами у банковских организаций, операторов мобильной связи, является долгим процессом и не приносит большой пользы, так как все счета, телефонные номера регистрируются на третьих лиц. Ещё большая сложность возникает, когда нам необходимо запросить информацию по банковскому счету иностранной организации;

3) плохая оснащённость информационно-телекоммуникационными технологиями в органах внутренних дел, особенно находящихся в регионах Российской Федерации, где совершается огромное количество преступлений, но оперативные работники зачастую не имеют компьютера на своём рабочем месте или вовсе личного рабочего места, не говоря уже о высокотехнологичном программном обеспечении;

4) появление новых способов совершения мошенничеств в сфере компьютерной информации и телекоммуникационных средств;

5) быстрое обнаружение и извлечение «цифровых следов» преступления, которые стираются мошенниками по истечении определённого времени (сеансы связи, счета-фактуры, информация в журнале предоставления доступа, лог-сообщения, журналы брандмауэра и т. п.);

6) проблемы внутри- и межведомственного взаимодействия по раскрытию мошеннических действий, связанных с использованием информационно-телекоммуникационных технологий;

7) устаревшие методики раскрытия преступлений, совершаемых дистанционным путём;

8) кадровый «голод» в системе МВД, в частности в оперативных подразделениях, а также недостаток работников с техническим образованием;

9) малочисленность содействующих оперативным подразделениям ОВД граждан, которые владеют оперативной обстановкой в области информационно-телекоммуникационной преступности, а также обладают специальными знаниями для раскрытия преступлений такого рода;

10) нестабильная эпидемиологическая ситуация в государстве, где большинство организаций и учреждений перешли на дистан-

ционную работу, количество пользователей интернета увеличилось, как и количество кибератак со стороны злоумышленников.

Раскрытие мошеннических актов «по горячим следам» целесообразно, так как возможно установить каналы связи злоумышленников, перехватить электронные сообщения и изъять компьютерную информацию, проанализировав «логи» того или иного пользователя, исследовать «кейлогеры», тем самым постараться обнаружить лицо, совершившее преступление [2, с. 26].

Безусловно, первоначальными действиями при раскрытии мошенничеств с использованием информационно-телекоммуникационных технологий будут считаться оперативно-розыскные мероприятия, закреплённые в статье 6 Федерального закона «Об оперативно-розыскной деятельности», которые связаны с использованием технических средств, а именно, прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации. Но не стоит забывать об особенностях таких преступлений, когда оперативным подразделениям для получения эффективного результата зачастую необходимо рассмотреть целый комплекс мероприятий оперативно-розыскного и технического характера, разработанный практиками и теоретиками в области ОРД.

Анализ раскрытия мошенничеств оперативными подразделениями с использованием информационно-телекоммуникационных технологий говорит о том, что отсутствуют механизмы получения оперативно-значимой информации от банковских организаций, интернет-провайдеров, операторов связи, социальных сетей и мессенджеров.

По этой причине необходимо создать электронный документооборот хотя бы с крупнейшими организациями информационного пространства, чтобы без лишних усилий и присутствующих со стороны закона преград, возможно было отслеживать в режиме «онлайн» подозреваемое правоохранительными органами лицо.

Необходимо повышать профессионализм в сфере компьютерной информации, ведь большое количество преступлений переходит в дистанционный режим, следует улучшать методы обучения в образовательной системе России, готовить специалистов с техническим образованием.

Также считаем целесообразным проводить занятия с действующими сотрудниками органов внутренних дел, обучать их работе с существующим комплексом IT-технологий, представляя информацию о том, как работает то или иное программное обеспечение, его особенности, слабые и сильные места конкретного софта на практике.

В качестве положительного примера организации дополнительного образования следует отметить Московский университет МВД России имени В. Я. Кикотя, куда приглашаются специалисты по раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в сфере компьютерной информации, а также работники ПАО «Сбербанк», обеспечивающие кибербезопасность своей организации, специалисты АО «Лаборатория Касперского». Занятия проводятся как в лекционном, так и в практическом формате с привлечением курсантов различных факультетов. Затем лучшие отбираются для участия в международном конгрессе по кибербезопасности (ICC) [10].

В свою очередь, следует обновить методы и меры практического воздействия на мошенничества в сфере информационно-телекоммуникационных технологий.

Для борьбы с киберпреступностью большим корпорациям, изготавливающим софт различной функциональности, следует тесно взаимодействовать с правоохранителями. Законодателю стоит осуществить нормативное закрепление такого сотрудничества, при котором организации, связанные с киберпространством, будут изготавливать программное обеспечение не только в целях своей надобности, для создания безопасности своих ресурсов, но и системы, которые встанут на вооружение органов внутренних дел и позволят отслеживать мошенников, раскрывая их анонимность.

Таким образом констатируем, что тема киберпреступности весьма актуальна в наши дни, особенно это касается мошенничеств с использованием информационно-телекоммуникационных технологий, при которых страдают многомиллионные бюджеты организаций малого, среднего и крупного бизнеса и не только в России, а также наносится огромный материальный ущерб рядовым гражданам.

В последнее время темой ещё больше заинтересовались как практические специалисты, так и теоретики, в связи с санитарно-эпидемиологической ситуацией. Коронавирусная инфекция отправила большинство граждан на дистанционный режим работы, а также подорвала и без того нестабильную экономику России. Мошенники пользуются нынешним положением населения, предприятий и организаций, похищая денежные средства при помощи телекоммуникационных технологий. В свою очередь, правоохранительным органам следует в полной мере заняться исследованием данного вопроса и разработать качественные меры и способы противодействия преступлениям в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий.

Список литературы

1. *Абрамов М. К., Озеров И. Н.* Некоторые проблемы обеспечения законности при осуществлении оперативно-розыскной профилактики преступлений // Проблемы правоохранительной деятельности. – 2014. – №. 1. – С. 12–17.

2. *Афанасьев А. Ю., Репин М. Е.* Некоторые особенности расследования компьютерных преступлений / Студенческие южно-уральские криминалистические чтения: сборник материалов Всероссийской заочной науч.-практ. конф. – Выпуск 3. – Уфа: РИЦ БашГУ, 2015. – С. 26–29.

3. *Батоев В. Б.* Оперативно-разыскное противодействие мошенническим действиям с использованием информационно-телекоммуникационных технологий // Расследование преступлений: проблемы и пути их решения. – 2018. – № 4. – С. 144–149.

4. *Богданов А. В., Ильинский И. И., Хазов Е. Н.* Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. – 2020. – № 1. – С. 15–20.

5. *Гаврилин Ю. В., Шипилов В. В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. – 2013. – № 23. – С. 2–5.

6. *Долгаев В. В., Васильева А. М.* Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий / Уголовное судопроизводство России: проблемы и перспективы развития : материалы Всероссийской научно-практической конференции. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2018. – С. 131–134.

7. *Любан В. Г., Молянов А. Ю., Хазов Е. Н.* Распространённые способы мошенничеств в сфере информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. – 2019. – № 1. – С. 190–194.

8. *Озеров И. Н., Черкасова Е. А., Капустина И. Ю.* Допустимость доказательств в уголовном судопроизводстве: сущность и значение // Проблемы правоохранительной деятельности. – 2016. – № 2. – С. 67–70.

9. *Шхагапсоев З. Л., Тутуков А. Ю.* Особенности выявления мошенничества в сфере компьютерной информации // Социально-политические науки. – 2018. – № 1. – С. 132–134.

10. *Ивлиева Н. В.* Актуальные проблемы противодействия хищениям денежных средств с банковских счетов физических лиц // Научный портал МВД России. – 2019. – №. 3. – С. 68–74.

References

1. *Abramov M. K., Ozerov I. N.* Nekotoryye problemy obespecheniya zakonnosti pri osushchestvlenii operativno-rozysknoy profilaktiki prestupleniy // Problemy pravookhranitel'noy deyatel'nosti. – 2014. – №. 1. – S. 12–17.

2. *Afanas'yev A. Yu., Repin M. Ye.* Nekotoryye osobennosti rassledovaniya komp'yuternykh prestupleniy / Studencheskiye yuzhno-ural'skiye kriminalisticheskiye chteniya: sbornik materialov vserossiyskoy zaochnoy nauch.-prakt. konf. – Vypusk 3. – Ufa: RITS BashGU, 2015. – S. 26–29.

3. *Batoyev V. B.* Operativno-razysknoye protivodeystviye moshennicheskim deystviyam s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy // Rassledovaniye prestupleniy: problemy i puti ikh resheniya. – 2018. – № 4. – S. 144–149.

4. *Bogdanov A. V., Il'inskiy I. I., Khazov Ye. N.* Kiberprestupnost' i distantsionnoye moshennichestvo kak odna iz ugroz sovremennomu obshchestvu // Kriminologicheskiy zhurnal. – 2020. – № 1. – S. 15–20.

5. *Gavrilin Yu. V., Shipilov V. V.* Osobennosti sledoobrazovaniya pri sovershenii moshennichestv v sfere komp'yuternoy informatsii // Rossiyskiy sledovatel'. – 2013. – № 23. – S. 2–5.

6. *Dolgayev V. V., Vasil'yeva A. M.* Moshennichestvo, sovershayemoye s ispol'zovaniyem informatsionno telekommunikatsionnykh tekhnologiy / Ugolovnoye sudoproizvodstvo Rossii: problemy i perspektivy razvitiya: materialy vserossiyskoy nauchno-prakticheskoy konferentsii. – Sankt-Peterburg: Sankt-Peterburgskiy universitet MVD Rossii, 2018. – S. 131–134.

7. *Lyuban V. G., Molyanov A. Yu., Khazov Ye. N.* Rasprostranonnyye sposoby moshennichestv v sfere informatsionno-telekommunikatsionnykh tekhnologiy // Vestnik Moskovskogo universiteta MVD Rossii. – 2019. – № 1. – S. 190–194.

8. *Ozerov I. N., Cherkasova Ye. A., Kapustina I. Yu.* Dopustimost' dokazatel'stv v ugolovnom sudoproizvodstve: sushchnost' i znacheniye // Problemy pravookhranitel'noy deyatel'nosti. – 2016. – № 2. – S. 67–70.

9. *Shkhagapsoyev Z. L., Tutukov A. Yu.* Osobennosti vyyavleniya moshennichestva v sfere komp'yuternoy informatsii // Sotsial'no-politicheskiye nauki. – 2018. – № 1. – S. 132–134.

10. *Ivliyeva N. V.* Aktual'nyye problemy protivodeystviya khishcheniyam denezhnykh sredstv s bankovskikh schetov fizicheskikh lits // Nauchnyy portal MVD Rossii. – 2019. – №. 3. – S. 68–74.

Статья поступила в редакцию 14.12.2020; одобрена после рецензирования 10.02.2021; принята к публикации 02.03.2021.