Владимир Анатольевич МОРОЗКОВ

кандидат юридических наук, доцент, доцент кафедры экономических и учетных дисциплин Сургутского государственного университета, г. Сургут, morozkov_va@surgu.ru

Елена Олеговна ОСТАПОВА

студентка специальности «Экономическая безопасность» Сургутского государственного университета, г. Сургут, ostapova2000@mail.ru

Любовь Александровна ЛУКЬЯНЦЕВА

студентка специальности «Экономическая безопасность» Сургутского государственного университета, г. Сургут, lyuba.q@mail.ru

Алена Игоревна САПУНОВА

студентка специальности «Экономическая безопасность» Сургутского государственного университета, г. Сургут, alena.sapunova2015@mail.ru

ЦИФРОВОЕ МОШЕННИЧЕСТВО КАК УГРОЗА ЛИЧНОЙ ФИНАНСОВОЙ БЕЗОПАСНОСТИ: ОТДЕЛЬНЫЕ АСПЕКТЫ

Аннотация. Посягательства на установленный порядок правоотношений в сфере собственности путем хищения денежные средства, расположенных на банковских картах, электронных кошельках и иных цифровых носителях, в том числе у социально-незащищенных категорий граждан обусловленные обусловлена стремительной компьютеризацией, и недостаточным уровнем защищенности цифровой информации от противоправных посягательств к масштабным хищениям денежных средств.

Проведенный авторами анализ специальной научной литературы, информационно-справочных источников позволил обозначить наиболее проблемные места. Исследованы способы совершения цифрового мошенничества преступления, определены типичные ситуации, в которые попадают потенциальные жертвы и предложен порядок действий держателей банковских карт по преодолению противоправных действий злоумышленников.

Ключевые слова: информационные технологии, цифровое мошенничество, кибератаки, банковская карта, финансовая грамотность, личная финансовая безопасность.

Vladimir Anatolievich MOROZKOV

Candidate of Legal Sciences, Associate Professor of the Department of Economic and Accounting Disciplines, Surgut State University, Surgut, morozkov_va@surgu.ru

Elena Olegovna OSTAPOVA

Student of the specialty "Economic security" of the Surgut State University, Surgut, ostapova2000@mail.ru

Lyubov Alexandrovna LUKYANTSEVA

Student of the specialty "Economic security" of the Surgut State University, Surgut, lyuba.q@mail.ru

Alena Igorevna SAPUNOVA

Student of the specialty "Economic security" of the Surgut State University, Surgut, alena.sapunova2015@mail.ru

DIGITAL FRAUD AS A THREAT TO PERSONAL FINANCIAL SECURITY: SELECTED ASPECTS

Abstract. Encroachments on the established procedure for legal relations in the field of property by stealing funds located on bank cards, electronic wallets and other digital media, including from socially unprotected categories of citizens, are due to rapid computerization and the insufficient level of protection of digital information from illegal encroachments to large-scale embezzlement of funds.

The analysis of special scientific literature, information and reference sources carried out by the authors made it possible to identify the most problematic areas. The ways of committing digital fraud

crimes are investigated, typical situations in which potential victims fall into are identified, and the procedure for bank card holders to overcome the illegal actions of intruders is proposed.
Keywords: information technology, digital fraud, cyber attacks, bank card, financial literacy, personal financial security.

Одной из мировых тенденций развития преступности, как наиболее опасной угрозы экономической безопасности личности, выступает совершенствование форм и видов хищений, предметом которых являются денежные средства, расположенные на банковских картах, электронных кошельках и иных цифровых носителях. Данная преступная направленность обусловлена стремительной компьютеризацией, захватившей практически все стороны жизни нашего общества, роста количества ЭВМ, используемых в России, а также недостаточным уровнем защищенности цифровой информации от противоправных посягательств.

С учетом данных компании RTM Group**,** которая провела анализ материалов следственно-судебной по уголовным делам, связанных с использованием информационных технологий в преступных целях в 2021 г. в России зарегистрировано около 518 тыс. киберпреступлений, что на 1,4% больше, чем за АППГ, но значительно (в 1,8 раза) превосходит показатель 2019 г. [1]. Следует отметить, что рост данного показателя связан не только с низкой финансовой грамотностью населения поскольку, по данным ЦБ России, с 2017 г. уровень финансовой грамотности населения постоянно растет [2]. На наш взгляд, высокая динамика преступлений в цифровой сфере связана прежде всего с тем, что мошенники находят новые пути и способы для совершения противоправных деяний. Поскольку в силу объективно-субъективных факторов нельзя полностью обезопасить себя от мошеннических действий, то представляется, что одна из важнейших задач обеспечения личной финансовой безопасности является — знание основных способов совершения мошенничества в сфере использования цифровой информации, уметь определять основные виды угрозы личности в данной сфере и знать алгоритм типичных действий по обеспечению экономической безопасности, то есть как не попасться на их удочку и что делать, если ты все же столкнулся с мошенниками [3].

Среди основных видов цифрового мошенничества следует выделить: мошенничества с использованием банковских карт, интернет-мошенничества, мобильные мошенничества и финансовые пирамиды.

Также не следует забывать, что мошенничество — это глобальная проблема не только для России, но и для всего мира в целом. Так, по данным информационного канала «Известия», мошенники притворялись благотворительными организациями и собирали деньги якобы на помощь беженцам [4]. Через такие сайты не только похищают деньги, но и заражают вредоносным софтом компьютеры пользователей, поэтому в рамках личной финансовой безопасности важно пользоваться антивирусом, переходить только на проверенные сайты и не переводить деньги неизвестным лицам и организациям, а также проверять организацию, которой собираешься отправить деньги. Например, список всех существующих благотворительных фондов можно найти на сайте «Нужна помощь» и «Добро. Mail.Ru».

Что же касается законодательного регулирования государственного противодействия в данной сфере, то основным источником российского законодательства, регламентирующим цифровое мошенничество как преступление, является Уголовный кодекс Российской Федерации. В 2012 г. в УК РФ была введена ст. 159.6 «Мошенничество в сфере компьютерной информации». Также к нормативно-правовым актам, регулирующие правоотношения связанные с цифровым мошенничеством, следует отнести: Федеральный закон «Об информации, информационных технологиях и о защите информации», а именно следующие статьи: ст. 5 «Информация как объект правовых отношений», ст. 6 «Общедоступная информация», ст. 8 «Право на доступ к информации», ст. 15 «Использование информационно — телекоммуникационных сетей», ст. 16 «Защита информации», ст. 17 «Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации», а также Уголовный кодекс РФ, куда относятся ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Наряду с этим отметим, что высокий рост в цифровом мошенничестве пришелся на период пандемии Covid-19, когда большей части населения пришлось перейти в «дистант».

На официальном сайте Генпрокуратуры мы можем наблюдать, что по большей части рост был за счет телефонного и интернет-мошенничества — за первые полгода 2020 г. число случаев такого мошенничества выросло на 76% по сравнению с первым полугодием 2019 г.

Согласно опубликованной Министерством внутренних дел статистике, в 2020 г. число преступлений с использованием цифровых технологий выросло на 77%, по сравнению с 2019 г. В том числе на 500,2% больше зафиксировали преступлений с платежными картами — 139 597 случаев за первые девять месяцев 2020 года.

Преступления с использованием мобильных телефонов увеличились более чем в два раза — с января по сентябрь их было 155 177 (на 97,7% больше, чем за первые девять месяцев 2019-го). Также за 2020 г. зарегистрировали 209 671 преступление с использованием интернета (их число выросло за год на 93,2%) и 7318 правонарушений с применением программных средств (на 62,8% больше, чем в прошлом году) [5].

Самыми распространенными правонарушениями в IT-сфере оказались мошенничество — 148 322 случаев, кража — 124 408 случая, а число правонарушений по ст. 273 УК РФ (реализация, применение и распространение вредных компьютерных программ) снизилось на 14.4% по сопоставлению с прошлым годом — с января по сентябрь их зарегистрировали 303 [6].

Сотрудники МВД в 2020 г. зафиксировали в Ханты-Мансийском автономном округе (ХМАО) рост на 48,5% до 8 368 количества преступлений, связанных с мошенничеством и кражами денег дистанционным способом, в сравнении, в 2019 г. их было 5 637. За позапрошлый год дистанционным способом с банковских счетов жителей региона мошенники похитили 531 млн руб. ссылка на 7 источник.

Также полиция фиксирует причинение крупного ущерба в случаях, когда люди пытаясь получить «легкие деньги» начинают общаться с лжеброкерами, хотят «сыграть на бирже» и размещают деньги в брокерских конторах. К примеру, одной из частых схем будет то, когда на электронную почту приходит письмо с предложением заработать на инвестициях, человек выходит на лжеброкеров, переводит им средства для «игры на бирже», которые резко возрастают, но при желании их вывести, выясняется, что необходимо оплатить комиссию, а при ее внесении мошенники перестают выходить на связь. Первая сходственная схема была опробована в Югре в январе 2020 г. В итоге один из жителей лишился 3 млн рублей.

Оценить фактические масштабы цифрового мошенничества достаточно сложно. В целях повышения эффективности предупреждения цифрового мошенничества в первую очередь необходимо правильно оформить банковскую страховку как один из охранных инструментов. По закону № 161-ФЗ «О Национальной платежной системе» банк возмещает клиентам сумму операции, которая проведена без его согласия. Это могут быть фишинги, спам, финансовые пирамиды, также при потере карты могут списаны средства.

Когда подделанные документы оказываются в финансовых организациях, провести анализ на подлинность по ним достаточно сложно без соответствующих технических средств. В этом случае можно рассмотреть встраивание отдельных модулей, отвечающих за биометрическую идентификацию клиентов, проверку документов на подлинность либо перенос данных в анкетные данные, либо внедрить в организацию программную платформу.

Также нам необходимо помнить основы финансовой грамотности, чтобы защитить себя, а именно:

– при получении смс-сообщений о списании денежных средств необходимо позвонить в банк и уточнить о прошедшей операции, если эта операция была совершена не вами;

– в случае если вам звонят не с официального номера банка, представляются его сотрудником и говорят, что с вашего счета списываются средства и карту они заблокировали сами, клиент должен спросить полное ФИО и должность звонящего, чтобы проверить, действительно ли этот человек работает в данном банке;

– никогда не сообщать данные своей карты или код из СМС.

В дополнение также разрабатываются множества средств и платформ, которые помогают определять мошенников. Антивирусы регулярно обновляются, стараясь успевать за всевозможными новыми вирусами. Определитель звонков и различные приложения, которые собирают отзывы на незнакомые номера.

Что же касается банковской сферы, то многие банки, с целью идентификации клиента, внедряют программные платформы по биометрии, например, Oz Forensics, основанные на использовании искусственного интеллекта биометрической идентификации личности, помогающая в выявлении фактов мошенничества и фальшивых документов. Данные программы помогают оперативно устанавливать личность получателя банковских услуг. Соответственно,

если в вашем банке используют аналогичную программу, то следует ей пользоваться что позволить значительно снизить угрозу личной финансовой безопасности и не стать жертвой мошенников.

Также в 2021 г. в России запустили платформу «Мышеловка», в которой жертвы мошенников рассказывают о том, как попались на их удочку, а волонтеры передают эту информацию в соответствующие органы. Данные действия помогают оперативно раскрыть новые пути совершения противоправных деяний и оперативно уведомить граждан о новых способах кражи их данных, а также о действиях, которые необходимо принять, чтобы защитить себя [7].

Невозможно полностью обезопасить себя от мошеннических действий, поскольку существующие программы противодействия не дают 100%-й гарантии, поскольку технологии не стоят на месте и в программные продукты IT-индустрию вовлекается все больше участников. Соответственно преступники предпринимают все новые способы и пути для совершения хищений. Все, что может сделать человек для своей финансовой безопасности, это изучить основы мошенничества, использоваться антивирус, следить за сайтами по борьбе с мошенничеством или же смотреть новости, в которых говорят о новых схемах, способах краж и необходимых действий для безопасности, а также соглашаться на новые программы безопасности банков и других организаций. Только внимательность, осторожность и осведомленность может помочь избежать удочки мошенников.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Число киберпреступлений в России // TADVISER Государство.Бизнес.Технологии [сайт] https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 23.02.2022).
2. Центральный банк России. Измерение уровня финансовой грамотности // Центральный Банк [официальный сайт] URL: https://cbr.ru/analytics/szpp/fin_literacy/fin_ed_intro/ (дата обращения 07.03.2022).
3. Финансовое мошенничество: Как себя обезопасить // Клерк [сайт]. URL: https://www.yandex.ru/search/?lr=973&offline_search=1&text=4 (дата обращения 18.004.2022)
4. Мошенническая сцена // Информационное издание «Известия». [сайт] URL: https://iz.ru/1298838/valerii-kodachigov/moshennicheskaia-stcena-aferisty-stali-vymogat-dengi-na-pomoshch-bezhentcam (дата обращения 08.03.2022).
5. Расширенное заседание коллегии МВД России // Официальные сетевые ресурсы Президента России [сайт] URL: http://www.kremlin.ru/events/president/transcripts/67795 (Дата обращения 08.03.2022).
6. Уголовный кодекс Российской Федерации// КонсультантПлюс [официальный сайт]. 1996-2022. URL: http://www.consultant.ru/document/cons_doc_law_10699/ (дата обращения 07.03.2022).
7. Ресурс для борьбы с мошенниками // Информационное издание «Известия». [сайт] URL: https://iz.ru/1166990/anna-kaledina/priiti-v-platformu-v-rossii-poiavilsia-resurs-dlia-borby-s-moshennikami (дата обращения 07.03.2022).