УДК 343.72

А. В. Иванова
Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия

МЕТОДИКА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

научный руководитель: д.ф.н., профессор кафедры истории, философии и социальных наук Золотухин В.М.

В результате активной цифровизации массовое распространение получили электронные средства платежа, в первую очередь банковские карты. Особенно большое влияние на данный факт оказала пандемия COVID-19. Обращение денег в электронной среде представляет массу возможностей для их хищения. Именно поэтому в последние годы появилось большое количество различных видов мошенничества. Проблема расследования мошенничества сегодня стоит достаточно остро, т.к. сотрудникам следственных органов часто не хватает знаний в области обращения и производства карт. Часто преступления даже не доходят до полиции, что значительно искажает статистику и усложняет процесс расследования. Поэтому делается большой упор на профилактические мероприятия и работу с населением в вопросах защиты от мошенничества. В данной работе рассмотрены понятие мошенничества с электронными средствами платежа, состав преступления по статье 159.3 УК РФ, методика расследования данного вида преступлений, а также способы их предупреждения.

Ключевые слова: электронные средства платежа, банковская карта, мошенничество, виды мошенничества, оперативно-розыскные мероприятия, судебная экспертиза, профилактика мошенничества.

XXI век – это век активной цифровизации. В наши дни использование бумажных денег практически отошло на второй план, а массовую популярность приобретают электронные средства платежа. Согласно ст. 3 ФЗ «О национальной платежной системе» под электронными средствами платежа понимаются средства безналичных расчетов с использованием ИКТ и электронных носителей информации [О национальной, 2011]. Наиболее распространёнными ЭСП являются банковские карты. Использование банковских карт значительно упрощает жизнь людей, но существование денежных средств в цифровой среде, как и наличие правовой неопределенности правоприменения [Бахов, Беккер, 2020; Козырева, Тарасенко, 2021] расширяет поле для преступлений. По оценкам экспертов «В 2021 году самый частый вид ущерба — потеря денег с карты или банковского счёта. В типичном случае жертва теряет в результате инцидента до 50 тыс. руб.» [Серебренников, Титаев, 2022, С. 3].

Пользуясь этим, злоумышленники постоянно не только совершенствуют старые, но разрабатывают новые способы и средства хищения, в том числе,

при нарушении антимонопольного законодательства [Скрипко, Скрипко, 2021; Золотухин, Скрипко, 2022] в аспекте дискредитации банковской системы, ее прав на использование банковских карт. Существенным является то, что «господствующие в ту или иную эпоху представления о праве являются итогом консенсуса, согласования позиций членов общества по принципиальным мировоззренческим проблемам» [Разуваев, Шмарко, 2021, С. 68]. В связи с этим, проблема мошенничества с банковскими картами, особенно относительно несовершеннолетних граждан [Козырева, Криони, Морозов, 2019; Золотухин, Козырева, 2021] приобретает актуальность.

Ст. 159 УК РФ закрепляет общее определение мошенничества – это хищение денежных средств путем обмана или злоупотребления доверием [УК РФ, 1996]. Однако по мере развития общества и экономики, расширялась и сфера мошенничества. Поэтому в 2012 г. в УК РФ была введена ст. 159.3 «Мошенничество с использованием электронных средств платежа». Признаки состава данного преступления схожи с другими преступлениями против собственности. Объектом преступления являются общественные отношения, направленные на охрану прав собственности. Предмет преступления – электронные денежные средства, находящиеся на банковских картах. Объективной стороной данного преступления признается хищение денежных средств путем обмана или злоупотребления доверием, как владельца карты, так и организаций, осуществляющих расчет, т.к. злоумышленник выдает себя за владельца карты или денежных средств. Субъектом преступления являются вменяемые граждане в возрасте от 16 лет. Субъективная сторона выражается в том, что данное преступление всегда совершается в форме прямого умысла. [Гладких, Курчеев, 2015, С. 255]

На рисунке 1 представлены данные по количеству эмитируемых карт за последние 5 лет. На графике видно, что за данный период число выпускаемых карт непрерывно растет, причем в 2020г. произошел резкий скачек с 272 604 тыс. ед. в 2019г. до 285 832 тыс. ед. Данный факт можно связать с ограничениями, введенными из-за пандемии COVID-19. Люди стали активнее пользо-

ваться сервисами доставки и интернет – магазинов, а также, в целях безопасности, использовать бесконтактные способы оплаты.

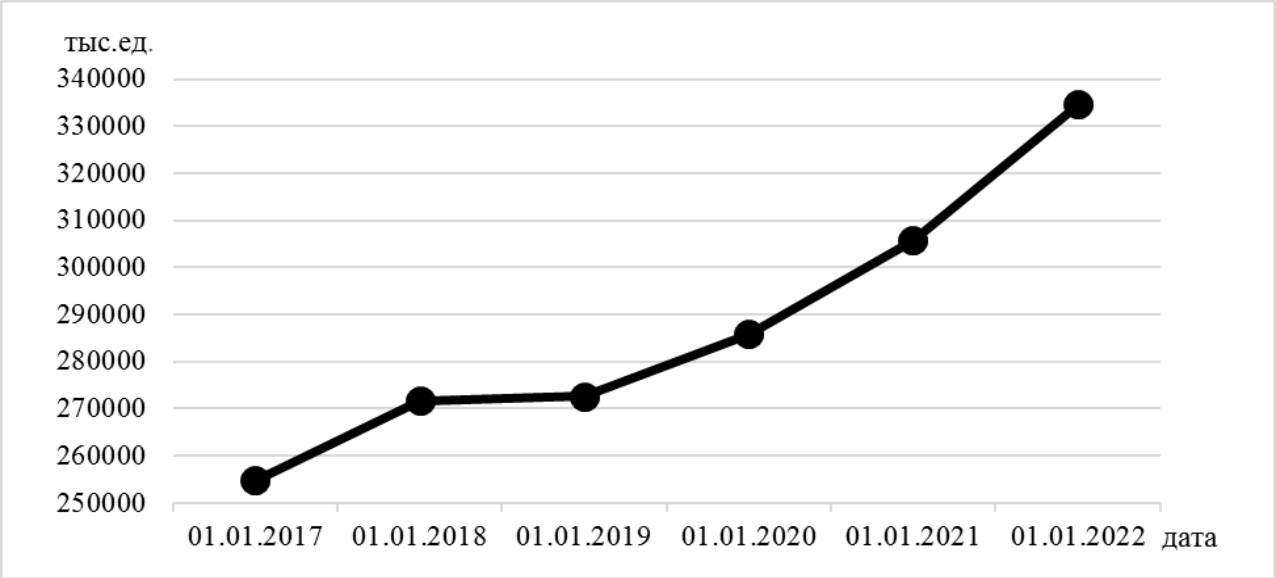

Рис.1 - количество платежных карт, эмитированных кредитными организациями и Банком России [Центральный, 2022]

Вместе с ростом объема выпуска банковских карт, ожидаемо возросло и количество преступлений, связанных с их использованием. Это подтверждается судебной статистикой численности осужденных по статье 159.3 УК РФ (рис.2).

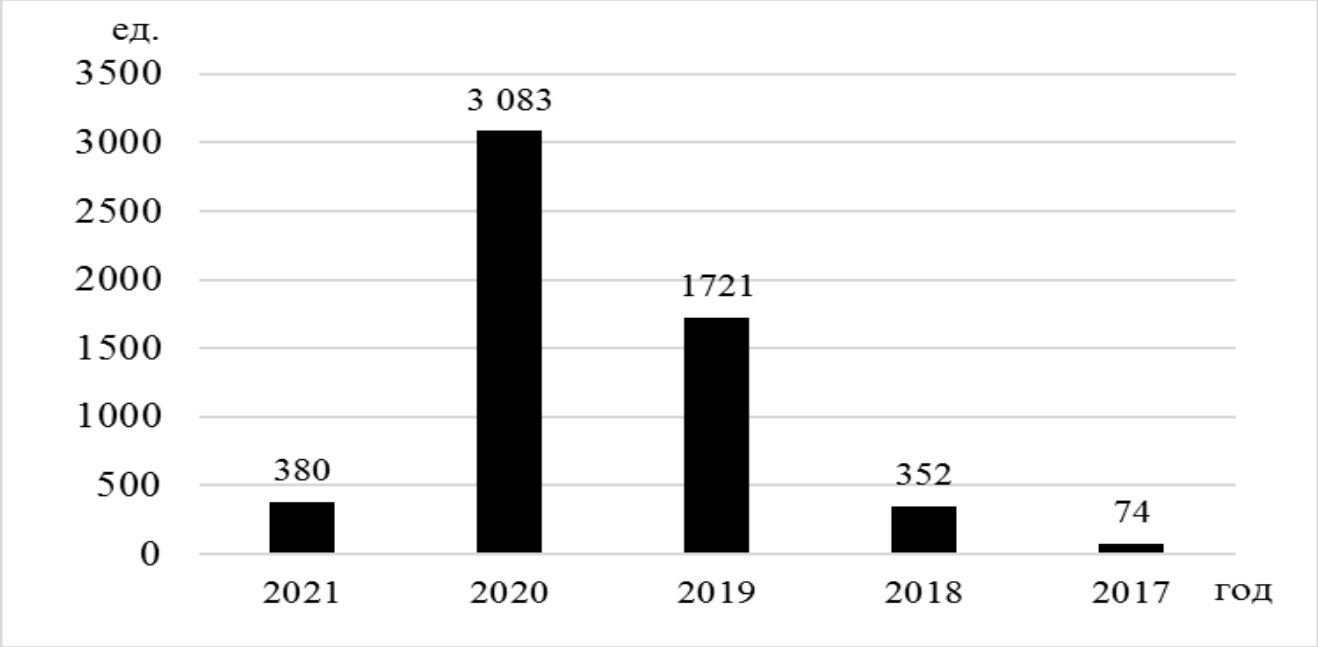

Рис.2 – количество осужденных за мошенничество с использованием электронных средств платежа (Ст. 159.3 УК РФ) [Судебная, 2022]

Согласно данным статистики, количество преступлений с использование электронных средств платежа в 2020 г. было максимальным за последние 5 лет. За год число осужденных по данной статье выросло почти в 2 раза, а по сравнению в 2017 г. почти в 40 раз. Исходя из анализа данных двух рисунков, действительно видна зависимость между объемом эмиссии карт и количество преступлений, связанных с ними.

На сегодняшний день существует около десятка различных видов мошенничества с банковскими картами. Самым распространённым способом обмана являются звонки и СМС. Как правило на телефон поступает СМС с незнакомого номера предположительно от близкого человека, который говорит, что он попал в беду, ему срочно нудны деньги и просит перевести определённую сумму на этот номер телефона или на номер какой-либо карты. Особо доверчивые граждане, как правило это пожилые люди, не задумываясь сами переводят деньги злоумышленникам.

Еще одним вариантом является вишинг или звонок с «банка». Человек, производящий звонок представляется оператором или сотрудником службы безопасности банка, в котором у вас может быть открыт счет и сообщает о подозрительной активности, либо о блокировке карты и просит сообщить CVV – код. Делается это под предлогом блокировки карты, что поможет обезопасить имеющиеся средства, но сообщив этот код, человек снова сам передает деньги мошенникам [Мешкова, 2016]. Причем, если раньше звонки происходили с посторонних номеров, то сегодня мошенники могут звонить с сервисного номера банка (например, с номера 900 – Сбербанк).

Интернет – аналогом вишинга является фишинг. Суть данного способа заключается в создании «зеркальных» сайтов. Как правило, человеку на почту приходит рассылка от банка, государственного органа, интернет – магазина или другого ресурса с ссылкой на их сайт. Чаще всего используется рассылка о выигрыше в конкурсах или лотереях. Переходя по ссылке, человек попадает на сайт абсолютно идентичный официальному, где его просят ввести личные данные, например, ФИО, номер телефона и данные карты на которую якобы будет

выполнен перевод, а далее предлагается войти в личный кабинет банка. Таким образом злоумышленники получают данные карты и ее владельца, а также логин и пароль от онлайн – банка, и тем самым доступ ко всем счётам потерпевшего в данном банке. Также стоит быт внимательным с оплатой покупок или услуг в сети, т.к. сайт также может быть фишинговым и при вводе данных карты они сразу же поступают злоумышленникам [Министерство, 2022].

Следующий способ с появлением чиповых карт постепенно отходит на второй план, но все еще имеет место быть – это скримиинг. Специальное устройство устанавливают на сам банкомат или платёжные терминалы. Устройство считывает все данные карты с ее магнитной ленты, а для распознания пин-кода устанавливается маленькая камера. Таким образам, имея всю информацию о карте и ее владельце, в том числе номер карты и CVV – код, злоумышленники изготавливают карту – клон и пользуются ей при расчетах [Министерство, 2022].

Еще одним способом обмана с помощью банкомата является установка фальшивого устройства. Банкомат может приобрести любой человек, они также продаются в состоянии б/у на таких сайтах, как Avito, и их стоимость составляет от 60 тыс. руб. Поэтому мошеннику не составит труда приобрести банкомат и установить его на видном месте. Предварительно у устройств меняется программная облачка и при вводе пин – кода, данные о карте сохранятся в облачном хранилище или сразу передаются мошенникам. При этом при попытке совершения операций через банкомат, устройство выдаёт ошибку.

Эффективность расследования преступлений, квалифицирующихся по ст. 159.3 УК РФ, зависит не только от практического опыта следователя, но и от его теоретических знаний в сфере банковской безопасности, изготовления и использования банковских карт, особенностям функционирования платежных систем и различных платежных онлайн-сервисов (в т.ч. интернет – банка или мобильный – банк) [Филиппов, 2022].

Расследование преступления начинается с момента поступления заявления в полицию. Тогда ОВД и следственный комитет после проверки на наличие

признаков состава определенного преступления возбуждает уголовное дело. Оперативно-розыскные мероприятия по расследованию дел по ст. 159.3 предполагают: осмотр места преступления; обыск; выемка документов; допрос свидетелей потерпевших и подозреваемых; назначение судебных экспертиз.

Осмотр места происшествия может нести информативный характер только в случае, если преступление совершено с использованием терминалов. Тогда в процессе осмотра собираются все данные о самом устройстве, а именно марка модель, серийный номер, основные элементы (корпус, дисплеи и клавиатура), также печатаемся журнал операций, который в дальнейшем приобщается к делу. При наличии подозреваемых в совершении преступления, следственные органы вправе провести обыск. В случае необходимости изъять банковские карты, чеки, квитанции, записные книжки в которых может содержаться информация о преступлении, а также цифровые носители информации (компьютеры, телефоны, планшеты). Допрос является важной частью расследования любого преступления. При допросе потерпевшего, помимо личных данных, как правило, уточняют, как часто он пользовался картой и в каком формате, где и когда совершал последние операции и предоставлял ли он кому-то данные своей карты [Иванов, Кайгородова, Карагодин, 2018, С. 540].

При расследовании мошенничества с пластиковыми картами могут быть привлечены судебные эксперты для проведения следующих видов экспертиз:

1. технико-криминалистическая – назначается в случае обнаружения подозрительных элементов на изъятой пластиковой карте. Такими следами могут быть начине вмятин на шрифте, смещение букв и цифр. В процессе экспертизы эксперт отвечает на такие вопросы как: каким способом изготовлена изъятая банковская карта, были ли внесены изменения в первичный текс, каким способом были произведены изменения и др.

2. экспертиза материалов, веществ и изделий – необходима в том случае, если все же были обнаружены изменения на в первоначальном тексте изъятой карты для его установления и отвечает на вопросы: каким был первоначальный текст на карте, каким способом он был удален или изменен и др.

3. компьютерно-техническая экспертиза – производится для исследования магнитного носителя карты для установления фактов оригинальности и целостности магнитного носителя, т.к. в поддельных картах чаще всего используются магниты, собранные из кусков [Иванов, Кайгородова, Карагодин, 2018, С. 540].

Проведение экспертиз является способом получения дополнительной информации, которая помогает следствию, но в случае с мошенничеством с пластиковыми картами, ситуация намного сложнее. На сегодняшний день не существует еденной методики расследования преступлений по ст. 159.3 УР РФ, связано это с большим количеством эмитируемых карт на базе разных банков и разных платёжных систем, выпуск карт является бесконтрольным процессом, а преступления совершенный с банковскими картами обладают высокой лестностью, потому что, как правило, совершаются дистанционно.

Расследование любого преступления процесс более сложный, чем его предотвращение. Главное причина по которой растет число хищений путем обмана – это человеческая наивность и неосведомлённость. Именно поэтому МВД РФ и его территориальные органы ведут активную работу с гражданами, на сайте МВД РФ можно найти необходимую информацию о способах мошенничества, о том, как распознать мошенника, и что нужно делать, если человек все же попался на уловку злоумышленника (рис.3). Постоянно сотрудники полиции информируют граждан, проводят классные часы для школьников и читают лекции студентам о существующих способах защиты своих средств. Банки, банковская система в целом, в том числе коммерческие банки, проводят работу с населением и разрабатывают системы безопасности.

Практически на каждом официальном сайте банка можно найти информацию о видах мошенничества и способах их предотвращения. В мобильном приложении «Сбербанк – онлайн» есть целый раздел посвященной данной теме, в нем размещено больше десятка небольших статей и коротких видео о самых популярных способах мошенничества, а также несколько тестов, чтобы проверить насколько полученный материал был усвоен. На официальном сайте

в «разделе ваша безопасность» есть телефон горячей линии, по которому можно обратиться по поводу подозрительных звонков или действий в отношении карты клиента, а также электронные формы с помощью которых можно сообщить о мошеннике или проверить номер телефона на предмет мошенничества. [ПАО «Сбербанк», 2022].

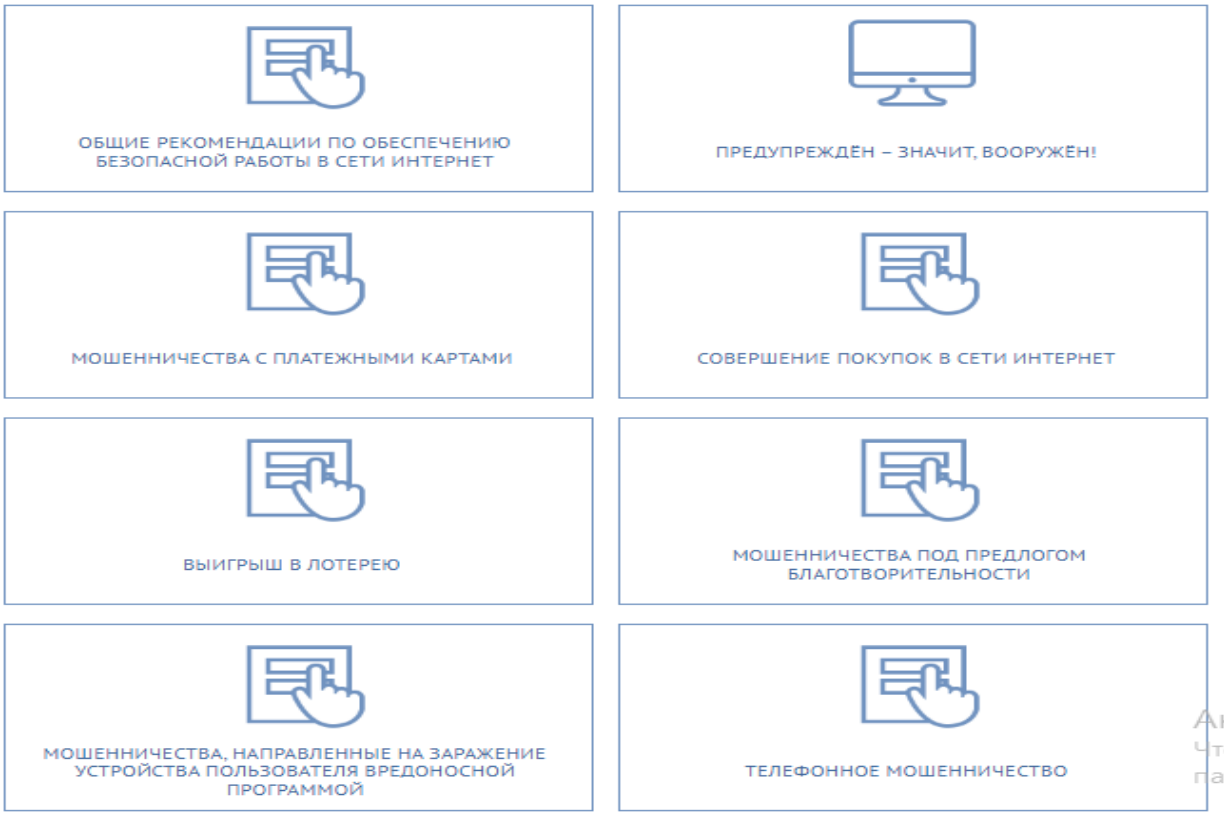

Рисунок 3 – Рекомендации МВД РФ по предупреждению мошенничества [Министерство, 2022]

Со стороны государства можно отметить ужесточение наказания по части 1 ст. 159.3 УК РФ, до 2018 максимальной мерой являлся арест на 4 мес., сегодня за мошенничество с электронными средствами платежа можно получить до 2 лет лишения свободы [УК РФ, 1996]. Довольно активно используется социальная реклама в виде роликов на ТВ и памяток в общественном транспорте или других общественных местах с громким лозунгом «не дай себя обмануть!».

Однако данных мер бывает недостаточно, если вернуться к рисунку 2, можно увидеть спад преступности по данному виду преступления в 2021, но при этом значение за данный год примерно равно значению за 2018. В большей степени это связано с тем, что люди просто игнорируют рекомендации и право-

охранительных органов, и банков. Для защиты своих финансов гражданам необходимо солдат достаточно простые правила: не хранить карты и PIN – коды от них в легкодоступных местах; не сообщать данные карты и личную информацию о себе посторонним лицам, особенно по телефону; следить за транзакциями по счетам, а лучше подключить смс уведомления; в случае звонка из банка сбросить и вручную набрать номер кредитной организации, а лучше все вопросы решать лично в отделении банка; быть внимательным при оплате товаров и услуг через Интернет, обращать внимание на адрес сайта и сертификаты безопасности и желательно использовать антивирус, который блокирует сомнительные сайты [Министерство, 2022].

Со стороны эмитентов платежных карт необходимо ужесточить контроль за их выпуском и оборотом, а также совершенствовать систему безопасности. На сегодняшний день банки вводят биометрическую идентификацию для входа в мобильные приложения и совершения операций через банкоматы, но довольно часто проблема кроется во внутренней безопасности банка [Губарева, 2022, Золотухин, Золотухин, 2022, Теймуров, Штаб, 2022]. Было уже достаточно прецедентов, кода появлялась информация об утечке персональных данных клиентов различных банков.

Для повышения качества расследования данных преступлений необходимо обучать сотрудников следственных органов тонкостям электронного денежного оборота и работы с пластиковыми картами. По мнению О. И. Лепешкиной, «к основным направления государственной политики в области противодействия киберпреступности следуют отнести такие как: обеспечение безопасности персональных данных; повышение уровня защищенности информационной инфраструктуры организаций финансово-банковской системы; развитие культуры информационной безопасности и кибергигиены клиентов — потребителей банковских услуг» [Лепешкина, 2022, С. 69].

Таким образом, проблема мошенничества с банковскими картами на сегодняшний день стоит достаточно остро. Снизить количество преступлений в данной отросли можно, в первую очередь, повышением правовой грамотности

населения. Также в предотвращении и эффективном расследовании преступлений может поспособствовать активное взаимодействие правоохранительных органов с кредитными организациями для повышения качества расследований.

Библиографический список

1. Бахов К. А., Беккер А. Э. Мошенничество с использованием платежных карт. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сб. статей магистрантов и преподавателей КузГТУ. Под редакцией В.М. Золотухина, В.Г. Михайлова. Кемерово, 2020. С. 144-149.

2. Гладких В. И., Курчеев В. С. Уголовное право России. Общая и Особенная части: учебник – М.: Новосибирский государственный университет, 2015 – 614 с.

3. Губарева Ю. С. Влияние значения эксперта на развитие социально-экономических отношения в банковской сфере. // Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сборник статей магистрантов и преподавателей КузГТУ (четвертый выпуск) / под ред. В. М. Золотухина, В. Г. Михайлова ; КузГТУ – Кемерово, 2022. – 507 с. С. 205-212.

4. Золотухин В. М., Золотухин М. В. Проблемы цифровой безопасности в условиях развития технологий. // Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сборник статей магистрантов и преподавателей КузГТУ (IV выпуск) / под ред. В. М. Золотухина, В. Г. Михайлова ; КузГТУ – Кемерово, 2022. – С. 76–84.

5. Золотухин В. М., Козырева М. В. Совершение сделок малолетними гражданами в условиях современного российского правоприменения. // Теория и практика социогуманитарных наук. 2021. – № 1 (13). – С. 83–89.

6. Золотухин М. В., Скрипко В. Е. Обеспечение экологической безопасности в конкурентном социально-экономическом пространстве. / Конкуренция и монополия: сборник материалов V Юбилейной Всероссийской научно-практической конференции студентов, магистрантов, аспирантов, научно-педагогических работников и специалистов в области антимонопольного регулирования (Кемерово, 26-27 октября 2022 г.) / под общ. ред. Ю. С. Якуниной, В. Г. Михайлова; КузГТУ. – Кемерово, 2022. – 283 с. – С. 101–105.

7. Иванов К. Г. Криминалистика: учебник / К. Г. Иванов, О. С. Кайгородова, В. Н. Карагодин [и др.] – Тюмень: – Тюменский государственный университет, 2018. – 652 с.

8. Козырева М. В., Криони А. Е., Морозов Н. В. Социокультурный и правовой аспекты социальной деятельности субъектов в банковской сфере. // Вестник Кемеровского государственного университета. Серия Гуманитарные и общественные науки, 2019. – Т 3. – № 2 (10). – С. 159–164

9. Козырева М. В., Тарасенко А. А. Качество жизни населения и специфика правоприменения в российской социокультурной ментальности. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. – Кемерово, 2021. – С. 82–89.

10. Лепешкина О. И. Киберпреступность как угроза национальной безопасности. Теоретическая и прикладная юриспруденция, 2022. – № 2. – С. 65–69. https://doi.org/10.22394/2686-7834-2022-2-65-69

11. Мешкова Е. В., Митрошина Е. В. Мошенничество с банковскими картами // Контентус, 2016. – № 8 (49). [Электронный ресурс]. Режим доступа: URL: https://cyberleninka.ru/article/n/moshennichestvo-s-bankovskimi-kartami-2 (дата обращения: 19.10.2022).

12. Министерство внутренних дел РФ / Внимание, мошенники! [Электронный ресурс]: официальный сайт. – URL: https://мвд.рф/вопросы/внимание-мошенники/ мошенничества-с-платежными-картами (дата обращения: 19.10.2022).

13. "О национальной платежной системе" ФЗ от 27.06.2011 № 161-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. – 4.07.2011. – № 27. – ст. 3872.

14. ПАО «Сбербанк» / личная безопасность [Электронный ресурс]: официальный сайт. – URL: https://www.sberbank.ru/ru/person/cybersecurity (дата обращения: 20.10.2022).

15. Серебренников Д., Титаев К. Динамика преступности и виктимизации в России 2018–2021 гг. Результаты второго виктимизационного опроса: аналитический обзор. — СПб.: Институт проблем правоприменения при Европейском университете в Санкт-Петербурге, 2022. – (Аналитические обзоры по проблемам правоприменения; вып. 2(2022)). – 34 с. https://enforce.spb.ru/images/rcvs_2021_block_online.pdf (дата обращения 24.11.2022).

16. Скрипко К. В., Скрипко В. Е. Соотношение монополии и конкуренции в современной России. / Конкуренция и монополия: сборник материалов IV Всероссийской научно-практической конференции студентов, магистрантов, аспирантов, научно-педагогических работников и специалистов в области антимонопольного регулирования (Кемерово, 20-21 октября 2021 г.) / под общ. ред. Н. В. Кудреватых, В. Г. Михайлова; КузГТУ. – Кемерово, 2021. – 334 с. С. 242-245.

17. Судебная статистика / Уголовное судопроизводство Данные о назначенном наказании по статьям УК [Электронный ресурс]: официальный сайт. – URL: https://stat.апипресс.рф/stats/ug/t/14/s/17 (дата обращения: 18.10.2022).

18. Разуваев Н. В., Шмарко И. К. Невский форум: секция «Кризис доверия в современном правопорядке» (Санкт-Петербург, июнь 2021 г.). // Теоретическая и прикладная юриспруденция, 2021. – № 4 (10). – С 59–69. DOI 10.22394/2686-7834-2021-4-59-69.

19. Теймуров М.Н., Штаб В.К. Анализ практике неправомерного оборота средств платежей как угроза экономической безопасности Российской Федерации. // Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сборник статей магистрантов и преподавателей КузГТУ (четвертый выпуск) / под ред. В. М. Золотухина, В. Г. Михайлова ; КузГТУ – Кемерово, 2022. – 507 с. С. 289-295.

20. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.09.2022) // Собрание законодательства РФ. – 17.06.1996. – № 25. – ст. 2954

21. Филиппов М. Н. Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов // Ведомости УИС. 2015. №5 (156). URL: https://cyberleninka.ru/article/n/metodika-rassledovaniya-krazh-i-moshennichestv-sovershennyh-s-ispolzovaniem-bankovskih-kart-i-ih-rekvizitov (дата обращения: 20.10.2022).

22. Центральный банк РФ/ статистика национальной платежной системы [Электронный ресурс]: официальный сайт. – URL: https://cbr.ru/statistics/nps/psrf/ (дата обращения: 18.10.2022).

A. V. Ivanova
T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia

METHODS OF INVESTIGATION OF FRAUD WITH BANK CARDS

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

As a result of active digitalization, electronic means of payment, primarily bank cards, have become widespread. The COVID-19 pandemic had a particularly big impact on this fact. The circulation of money in the electronic environment presents a lot of opportunities for their theft. That is why a large number of different types of fraud have appeared in recent years. The problem of fraud investigation is quite acute today, because employees of investigative agencies often lack knowledge in the field of card circulation and production. Often crimes do not even reach the police, which significantly distorts statistics and complicates the investigation process. Therefore, great emphasis is placed on preventive measures and work with the population in matters of fraud protection. This paper examines the concept of fraud with electronic means of payment, the composition of the offense under Article 159.3 of the Criminal Code of the Russian Federation, the methodology of investigation of this type of crimes, as well as ways to prevent them.

Keywords: electronic means of payment, bank card, fraud, types of fraud, operational investigative measures, forensic examination, fraud prevention.