

## **АНАЛИЗ ПРАКТИКИ НЕПРАВОМЕРНОГО ОБОРОТА СРЕДСТВ ПЛАТЕЖЕЙ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

научный руководитель: к.п.н, доцент кафедры истории, философии  
и социальных наук Съедина Н.В.

В статье раскрыта актуальная для системы экономической безопасности Российской Федерации проблема – неправомерный оборот средств платежей, обозначены определения и виды средств платежей, исследована взаимозависимость неправомерного оборота средств платежей и преступлений в сфере компьютерной информации.

**Ключевые слова:** экономическая безопасность, неправомерный оборот, платежи, средства платежа, преступления в сфере компьютерной информации, интернет.

На сегодняшний день практически каждый пользуется платежными картами и другими электронными средствами платежа, будь то оплата покупок в торговых организациях, какие-либо финансовые операции, а также оплата услуг в сети интернет. Это касается как физических лиц, в том числе несовершеннолетних [Золотухин, Козырева, 2021], так и юридических лиц, вступающих в товарно-денежные и/или иные экономические отношения [Козырева, Криони, Морозов, 2019].

В подтверждение вышесказанного можно привести статистику Центрального Банка РФ, согласно которой общее количество эмитированных банковских карт за период 2019-2021 гг. возросло более чем на 50%. Так, если в 2019 г. количество банковских карт составляло – 118 101 тыс., то уже по состоянию на 1 января 2022 г. их количество возросло до – 240 521 тыс. [Платежные карты, 2021].

Кроме того, на сегодняшний день наблюдается повсеместное распространение сервисов, позволяющих осуществлять безналичные платежи без использования непосредственно банковской карты как физического носителя, через смартфон, смарт-часы и иные технические устройства (Apple Pay, Android Pay, Samsung Pay и т.д.). В настоящий момент данную техно-

логию поддерживает большинство производителей смартфонов, при её использовании техническое устройство является своеобразным аналогом банковской карты: лицо, владеющее устройством, просто прикладывает его к POS-терминалу после активации соответствующего сервиса. В некоторых случаях для активации достаточно будет знать пароль, установленный самостоятельно владельцем смартфона, дабы совершать операции, не требующие ввода PIN-кода карты.

Технический прогресс в области безналичной оплаты привел к росту преступности в анализируемой сфере деятельности, хотя отметим, что в 2021 году наметилась тенденция на ее уменьшение. При рассмотрении в динамике можно отметить довольно интенсивный рост с 2019 до 2021 г. преступности такого вида, как неправомерный оборот средств платежей: 26,1% – в 2018 г., 33,1% – в 2019 г., 42,4% – в 2020 г. и 25,5% – в 2021 г. [Платежный рынок, 2021].

При этом отметим, что банки возместили клиентам 935 млн руб. (15% или каждый 7-й похищенный рубль). Текущий уровень возмещения объясняется высокой долей социальной инженерии среди операций без согласия клиентов, которые в результате обмана или злоупотребления доверием нарушают условия договора с кредитными организациями, предусматривающие необходимость сохранения конфиденциальности платежной информации (рисунок 1) [Платежные карты, 2021].

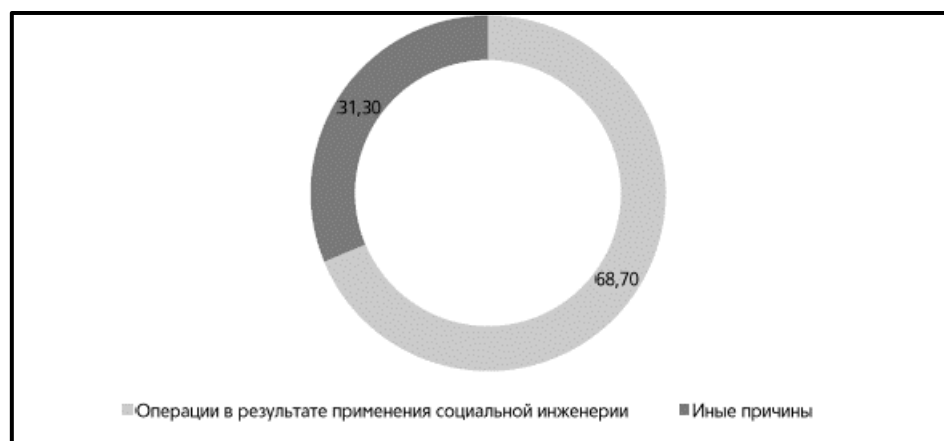


Рисунок – 1 Причины совершения операций без согласия клиентов (%)

По данным Банка России, количество и объем операций по переводу денежных средств с использованием электронных средств платежа (ЭСП) физических лиц составляют 40,3 млрд. единиц и 71,03 трлн. руб. соответственно. Количество и объем операций с использованием платежных карт (в банкоматах и в Интернете) составили 39,2 млрд. единиц и 63,7 трлн. руб. соответственно, аналогичные показатели по операциям в системе дистанционного банковского обслуживания (ДБО) – 1,1 млрд. единиц и 7,3 трлн. руб. соответственно [Информационный, 2021].

Повышение безопасности финансовых услуг является одной из задач, которую Банк России реализует в интересах как их потребителей (повышение уровня и качества жизни [Золотухин, Козырева, 2014; Золотухин, Козырева, 2016]), так и самих кредитно-финансовых организаций [Круковская Левина, 2010; Михайлов, Гегальчий., Михайлова, 2009; Киселева, Михайлов, Михайлова, 2019].

В 2021 г. было зафиксировано 40 тыс. случаев использования платежных карт (за исключением prepaid) без согласия их владельцев в банкомате или терминале. Из них почти четверть (22,4%) произошли в результате использования злоумышленниками приемов социальной инженерии. Общая сумма ущерба по хищениям через банкоматы и терминалы составила свыше 525 млн. руб., при этом банки вернули клиентам более 10% похищенных средств (54,4 млн. руб.). Это связано как с несовершенством законодательной базы и правоприменением [Козырева, Тарасенко, 2020; Zolotukhin, Bikmetov, Shiller, Tarasenko, 2021], так и с проблемами российской ментальности [Золотухин, Казаков, 2014; Gafarov, Gafarova, Belkov, Bikmetov, Zolotukhin, 2021] и трансформацией общественного сознания [Жукова, Жуков, 2018, Zhukova, Zhukov, Zolotukhin, Kazakov, 2019].

Больше всего операций без согласия клиентов – физических лиц пришлось на операции по оплате товаров и услуг в Интернете (CNP-

транзакции). Социальные сети оказывают существенное влияние на уровень распространения киберпреступности и на мировую политику [Селезнев, 2016].

На рисунке 2 представлена информация по распределению операций без согласия клиентов по месту совершения операций [Ключевые, 2021].

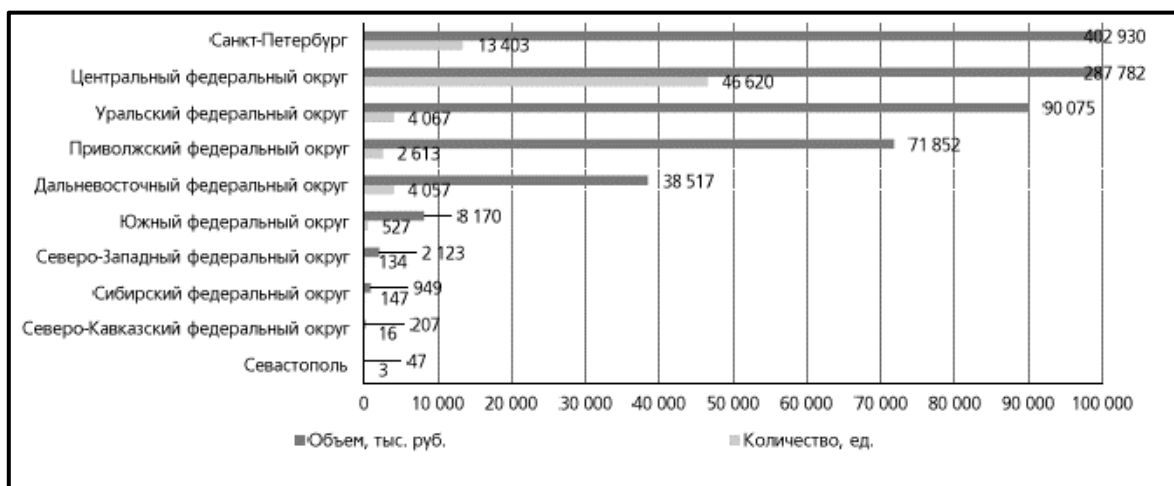


Рисунок 2 – Количество и объем переводов денежных средств без согласия клиента по месту совершения операции (без учета Московского региона)

Учтены только данные об операциях, совершенных в банкоматах (терминалах или импринтерах), а также CNP-транзакции по платежным картам, эмитированным на территории Российской Федерации (за исключением Московского региона, на который приходится 339 522 операции без согласия клиентов на сумму 2594 млн руб.). Особенностью территориального распределения указанных операций является их сосредоточение на территории Центрального федерального округа. Это обусловлено нахождением большинства кредитных организаций, обслуживающих физических лиц.

Кредитным организациям в регионах, необходимо уделять повышенное внимание исполнению подпункта 2.12.3 Положения Банка России № 382-П, обязывающего кредитные организации проводить мероприятия по повышению осведомленности работников и клиентов в области обеспечения защиты информации и рисков получения несанкционированного доступа к электронным денежным средствам [Информационный, 2021].

В 2021 г. отчитывающиеся операторы направили в Банк России информацию о 973 инцидентах, связанных с несанкционированным доступом к их информационной инфраструктуре, на общую сумму 103,8 млн. рублей.

Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры и автоматизированным банковским системам или информации о банковских счетах, стал причиной 877 инцидентов, связанных с переводом денежных средств оператора или его клиентов без их согласия. Объем ущерба в результате таких хищений составил порядка 24,5 млн. рублей.

Хищений, произошедших в результате компьютерных атак или несанкционированного доступа к автоматизированным банковским системам (информации о банковских счетах), было зафиксировано в 15 раз меньше – 58 инцидентов, при этом объем хищений составил 23,2 млн. рублей.

Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, к программно-аппаратному обеспечению банкоматов и электронных терминалов стал причиной 14 хищений на сумму порядка 13,5 млн. руб., в то время как хищений в результате компьютерных атак и несанкционированного доступа было всего 8 (на сумму около 10,6 млн. руб.). Также в 2021 г. произошли 15 компьютерных атак и два случая несанкционированного доступа к программно-аппаратному обеспечению банкоматов, которые стали причиной несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах на сумму 32,2 и 0,9 млн. руб. соответственно [Платежный рынок, 2021].

Общая сумма операционных расходов операторов по переводу денежных средств вследствие списаний (снятий) денежных средств в результате несанкционированного доступа к их информационной инфраструктуре составила 27,4 млн. рублей.

Указанные объемы хищений денежных средств свидетельствуют о достаточно низкой результативности действий злоумышленников в результате атак на кредитные организации. Это может быть обусловлено повышением внимания операторов к вопросам информационной безопасности, включая проводимую ими работу по данному направлению, а также может быть результатом мероприятий Банка России в области защиты информации при осуществлении переводов денежных средств.

Задачей Банка России является снижение социально-экономических рисков от деятельности мошенников, в том числе кибермошенничества и создание благоприятных условий, связанных с защитой информации в организациях кредитно-финансовой сферы, с целью снижения количества атак на данные организации.

#### Библиографический список

Жукова О. И., Жуков В. Д. Воздействие информации на сознание с современной социокультурной реальности. // Современная наука: актуальные проблемы теории и практики. Серия: Познание. 2018. – № 11 (86). – С. 76–79..

Информационный сайт Банка России. Декабрь 2021. [Электронный ресурс]. – Режим доступа: <http://www.cbr.ru/analytics/> (дата обращения 30.01 2022).

Золотухин В. М., Казаков Е. Ф. Особенности «души» русской культуры. // Вестник Кемеровского государственного университета. 2014. – № 4-1 (60). – С. 195–199.

Золотухин В. М., Козырева М. В. Влияние качества жизни и потребностей на формирование среднего класса // Вестник Кемеровского государственного университета, 2014. – № 1–1 (57). – С. 183–18

Золотухин В. М., Козырева М. В. Социокультурные основания реализации и регламентации потребностей в контексте исследования качества жизни. // Вестник Кемеровского государственного университета культуры и искусств, 2016. – № 37-1. – С. 68–75.

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.

Киселева Т. В., Михайлов В. Г., Михайлова Я. С. О подходах к управлению природоохранной деятельностью предприятия с учетом рисков. // Экономика и управление инновациями. 2019. – № 3 (10). – С. 62–68.

Ключевые тренды мирового рынка электронных платежей. Часть 2 [Электронный ресурс]. – Режим доступа: <http://geektimes.ru/company/payonline/blog/273066/> (дата обращения 30.01 2022).

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.

Козырева М.В., Тарасенко А.А. Трансформация российской идентичности и ее влияние на специфику уголовного правоприменения. / В сборнике: Проблемы эконо-

мики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Посвящается 300-летию Кузбасса и 70-летию КузГТУ. под ред. В.М. Золотухина, В.Г. Михайлова. – Кемерово, 2020. – С. 69–75.

Круковская Т. А., Левина Е. И. Анализ влияния факторов на комплексную оценку финансово-хозяйственной деятельности предприятий. // Вестник Кузбасского государственного технического университета. 2010. – № 6 (82). – С. 177–178.

Михайлов В. Г., Гегальчий Н. Е., Михайлова Я. С. Основные риски эффективного функционирования химической промышленности Сибирского федерального округа. // Вестник Кузбасского государственного технического университета, 2009. – № 2 (72). – С. 208–210.

Платежные карты и рост экономики: влияние электронных платежей. [Электронный ресурс]. – Режим доступа: [http://visa.com.ua/ua/ru-ua/aboutvisa/research/pdf/Visa\\_Moodys\\_Fact\\_Sheet\\_RUS.pdf](http://visa.com.ua/ua/ru-ua/aboutvisa/research/pdf/Visa_Moodys_Fact_Sheet_RUS.pdf) (дата обращения 30.01 2022).

Платежный рынок в Российской Федерации в 2021 году краткий обзор // Информационный портал PLUSworld.ru. [Электронный ресурс]. – Режим доступа: <https://www.plusworld.ru/daily/platezhnyj-biznes/platezhnyj-rynok-rossijskoj-federatsii-v-2021-godu-kratkij-obzor/> (дата обращения 30.01 2022).

Селезенев Р.С. Социальные сети в контексте мировой политик: актор или инструмент. // Международные отношения, 2016. – № 3. – С. 215–226.

Gafarov H., Gafarova Iu., Belkov A., Bikmetov R.S., Zolotukhin V.M. Socio-ecological aspects of the realization of the human potential of workers in resourceproducing regions. В сборнике: E3S Web of Conferences. VIth International Innovative Mining Symposium. 2021. С. 03003.

Zolotukhin V.M., Bikmetov R.S., Shiller V.V., Tarasenko A.A. Sociocultural aspect of criminal law enforcement the russian mentality . Rudn conference on legal theory, methodology and regulatory practice (RUDN LTMRP conference 2021/ SHS Web of Conferences (см. в книгах). 2021. № 118. С. 02009.

Zhukova O. I., Zhukov V. D., Zolotukhin V. M., Kazakov E. F. The problem of the impact of information on consciousness and human Identity. / 11 th International Scientific and Theoretical Conference – Communicative Strategies of Information Society Editors: Olga D. Shipunova, Violetta N. Volkova, Alfred Nordmann, Laurent Moccozet. 2019. С. 420-429.

*M. N Teymurov, V. K. Shtab*

*T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia*

## **ANALYSIS OF THE PRACTICE OF ILLEGAL PAYMENT TRAFFIC AS A THREAT TO THE ECONOMIC SECURITY OF THE RUSSIAN FEDERATION**

Scientific adviser: PhD in Pedagogy, Associate Professor at the Department of History,  
Philosophy and Social Sciences Sedina N.V.

The article reveals a problem that is relevant for the system of economic security of the Russian Federation - the illegal circulation of means of payment, defines the definitions and types of means of payment, explores the interdependence of the illegal circulation of means of payment and crimes in the field of computer information.

**Key words:** economic security, illegal turnover, payments, means of payment, crimes in the field of computer information, Internet.