

Дата поступления рукописи в редакцию: 22.01.2026 г.
Дата принятия рукописи в печать: 25.02.2026 г.

DOI: 10.24412/2224-9133-2026-1-524-527

АМИНОВ Ильдар Ринатович,
кандидат юридических наук, доцент,
заместитель начальника научно-исследовательского отдела
Уфимского юридического института МВД России,
e-mail: mail@law-books.ru

ГОЛУБЕВ Игорь Викторович,
преподаватель кафедры организации
охраны общественного порядка Тюменского института
повышения квалификации МВД России,
e-mail: mail@law-books.ru

КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Аннотация. В статье рассматривается актуальная проблема киберпреступности и мошенничества, с использованием электронных средств платежа. Приведена четкая статистика и зафиксировано резкое увеличение совершаемых преступлений данного вида. Рассмотрены детерминанты совершения подобного рода преступлений, определены причины совершения мошенничества с использованием электронных средств платежей, так как причины и порождают возрастание уровня преступности.

Ключевые слова: мошенничество, кража с банковского счета, мошенничество с использованием электронных средств платежа, киберпреступность, закрепление в законодательстве, личность киберпреступника.

AMINOV Ildar Rinatovich,
Candidate of Law, Associate Professor,
Deputy Head of the Research Department Ufa Law Institute
of the Ministry of Internal Affairs of Russia

GOLUBEV Igor Viktorovich,
Lecturer of the Department of Public Order Protection
Tyumen Advanced Training Institute of the Ministry
of Internal Affairs of Russia

CRIMINOLOGICAL ANALYSIS OF E-COMMERCE SCAMMING

Annotation. The article discusses the current problem of cybercrime and fraud using electronic means of payment. Clear statistics are provided and a sharp increase in the number of crimes of this type is recorded. The determinants of committing such crimes are considered, and the causes of committing fraud using electronic means of payment are identified, as these causes contribute to the increase in the level of crime.

Key words: fraud, bank account theft, electronic payment fraud, cybercrime, legal enforcement, cybercriminal identity.

Преступность как свойство человеческого общежития в масштабе мирового уровня его организации имеет место, и, вероятно, будет характеризовать всегда. В условиях многогранности развития всех сфер общественных отношений и их мобильности следует закономерное изменение структуры преступности, ее

усложнение с составлением удельной части в сфере телекоммуникационных технологий [1; с.20].

С развитием информационных технологий наш мир значительно преобразился. Электронные устройства стали доступны каждому, многие привычные сейчас для нас вещи постепенно

перешли из реального в виртуальное пространство. Материальные платежные инструменты уступают место виртуальным финансовым активам. Цифровые деньги и безналичные расчеты становятся неотъемлемой частью современной экономической системы. Научно-технический прогресс открыл множество перспектив для развития общества. Изменились методики передачи данных, введен электронный документооборот и повсеместно внедряются онлайн-коммуникации [2; с.93].

Появились новые схемы мошенничества, поэтому в настоящее время следует быть бдительным и очень внимательным при совершении различных действий с использованием электронных устройств, особенно если это касается выполнения электронных платежей. Ведь при недостаточной осведомленности интернет-пользователь рискует попасть в очень сложное положение, потерять свои финансы или столкнуться с утечкой информации, своих персональных данных.

Отсутствие должной бдительности во время использования современных средств дистанционного банковского обслуживания неизбежно влечет за собой риски возникновения угроз криминального характера. Стоит учитывать, что мошенники используют очень хитрые уловки, проворачивая криминальные хакерские махинации, заставляя потенциальных жертв добровольно раскрывать свои личные данные, информацию о паролях, банковских реквизитах [3; с.109].

Сейчас данная тема очень актуальна, так как преступления подобного рода распространены во всем мире, соответственно в нашей стране ситуация обстоит таким же образом.

25 марта 2019 года состоялось заседание общественного совета, на котором выступил министр внутренних дел Российской Федерации Колокольцев В.А. Он отметил, что за последние годы количество киберпреступлений в стране увеличилось практически в 16 раз. В конце мая Банк России опубликовал статистику по операциям без согласия клиентов за первый квартал 2024 года. Количество мошеннических операций выросло почти на 17% по сравнению с аналогичным периодом прошлого года. Также значительно увеличилось число атак, совершенных через систему быстрых платежей и электронные кошельки. В январе — марте 2024 года через систему быстрых платежей у граждан было похищено 1,13 миллиарда рублей, что в 2 раза превысило показатель первого квартала прошлого года [4]. Каждые полгода статистика растет и это серьезно подрывает общественную и финансовую безопасность как отдельных граждан так и всей страны.

За мошенничество с использованием электронных средств платежа предусмотрена реальная юридическая ответственность, которая регламентируется статьей 159.3 в уголовном законодательстве Российской Федерации. Появление нового вида мошенничества выявило необходимость отграничения на законодательном уровне «обычного, простого» мошенничества от мошенничества с использованием электронных средств платежа. Но ни в науке, ни в правоприменительной практике нет единого подхода к их существенному разграничению. Тяжесть наказания зависит от субъектов фигурируемых в деле. Объективной стороной данного вида мошенничества выступает факт хищения чужого имущества, совершаемого посредством электронных средств платежа. Обязательным признаком таких преступлений является само по себе электронное средство платежа. Определение закреплено в статье 3 Федерального закона «О национальной платежной системе». Субъективная сторона характеризуется виной в форме прямого умысла с корыстной целью. Это вывод сделан на основе суждения, что в случае заполучения денежных средств иного лица, злоумышленник пожелает присвоить их себе и воспользоваться ими.

Обратим внимание на детерминанты совершения преступлений подобного вида. Под детерминантами в криминологической науке понимается совокупность негативных условий, благодаря которым обуславливается высокий уровень преступности. Выделяют причины и условия совершения преступлений, а они действуют совместно, так как причина порождает следствие только с учетом наличия определенных условий в совокупности.

В случае обсуждения данной проблемы, можно выделить следующие причины мошенничества с использованием электронных средств платежа. Первоочередно выступают экономические процессы в стране, практически все население, начиная со школьников, заканчивая пенсионерами, постепенно перешло на электронные кошельки, пластиковые платежные карты. При этом стоит указать, что совсем немногие обладают знаниями о правилах безопасности в киберпространстве. В такой ситуации электронные деньги стали главной предвосхищаемой добычей для мошенников.

Немаловажную роль играют и внешние факторы, например, несовершенство нашего законодательства, все ведь прекрасно понимают, что преступления данного вида являются относительно новыми, так как широкое распространение в нашей стране получили лишь начиная с 2019 года, и, зачастую, случается так, что законодательство немного не успевает подстраиваться под новые тенденции. Конечно, со временем появ-

вились стратегии противодействующие киберпреступности, но они низкоэффективны и ограничены в своем применении. К внешним факторам также можно отнести социально-политическую ситуацию в стране, доступность высшего образования и его качество. Все эти факторы, сливаясь, формируют хорошую базу для осуществления отрицательных побуждений преступников[5; с.322].

Злоумышленники, как правило, обладают специальными квалифицированными знаниями и в сфере IT и в сфере психологии, поэтому у них достаточно легко получается войти в доверие и ввести свою жертву в подвешенное состояние паники и неосведомленности. Им без труда и каких-либо усилий удастся провести неподготовленного человека и заставить его самого же сообщить свои персональные данные.

Личность преступника следует рассматривать не только с точки зрения понимания этого термина в юридическом смысле, как субъекта преступления, но стоит учитывать и общесоциологические и психологические признаки. На формирование осознанного побуждения человека осуществлять преступные замыслы влияет достаточный объем факторов в совокупности. Сюда же относятся и те, что были перечислены выше в виде детерминантов.

Киберпреступниками, как правило, являются лица более молодого возраста, это обуславливается тем, что старшее поколение менее «компьютеризировано», а навыки владения компьютером сейчас формируются уже в подростковом возрасте. Каждый преступник имеет свои личностные особенности, что касается киберпреступников – это люди, склонные к депрессии, тяжелым психологическим переживаниям. Пытаясь все это скрыть, они стараются компенсировать это большим самомнением. Совершая преступления подобного рода, они остаются обезличенными, при этом ощущают чувство превосходства над потерпевшим. Для киберпреступников важно комфортное место откуда они смогут спокойно совершать злодеяния. Дистанционность как раз таки и выступает главным условием совершения преступления. Что снова свидетельствует о неуверенности и, в какой-то степени, даже социофобии. Мошенники перед совершением преступления готовятся к нему, то есть детально изучают психологию потенциальных жертв, а также психологию поведения того лица, за которого они себя выдают. То есть мошенник скорее знакомится и применяет какие-либо профессиональные характеристики свойственные представителям определенной деятельности, для того чтобы быстро установить контакт и повысить степень доверия. Некоторые «наиболее подготовленные» специально ограничиваются кру-

гом лиц, схожими по социальным характеристикам, например жертвы примерно одного возраста и схожего социального статуса. Делается это для того, чтобы облегчить или упростить сам процесс совершения преступления, ради экономии времени и извлечения наибольшей выгоды.

Как правило, на уловки мошенников чаще всего попадают люди в возрасте. Это обусловлено их социальным статусом и возрастом, пожилые люди излишне доверчивы, обладают меньшей стрессоустойчивостью и более тревожны. В силу возраста и эмоционального состояния, они, как правило, не способны защитить свои права. Скорее это связано с тем, что люди данной категории находятся в некой изоляции от различных новшеств в сфере компьютеризации всех процессов. Со времени пандемии практически все сервисы перешли в электронный формат. Естественным образом, все, что связано с современными технологиями понимается и признается пожилыми людьми довольно сложно, поэтому они готовы поверить кому угодно и отдать все свои сбережения, чтобы, как им кажется на первый взгляд, обезопасить себя. Часты случаи, анонимных звонков пенсионерам от лжепредставителей банка, пенсионного фонда или лжесотрудников полиции с требованием перевести накопления на безопасный счет. Несомненно влияет на общую ситуацию факт доверчивости и наивности пенсионеров. Ведь они зачастую не имеют рядом близких родственников, которые могли бы оказать им поддержку и позаботиться о них. Поэтому легко входят в контакт с незнакомыми людьми. Вообще, пенсионеры, пожилые люди в целом являются наиболее незащищенной категорией граждан. Даже дети находятся под большей защитой государства, в нашей стране права несовершеннолетних в наиболее усиленной форме охраняются законом.

Таким образом, мы проанализировали основные аспекты мошенничества с использованием электронных средств платежа. Можно заключить, что данный вид мошенничества относительно недавно получил распространение, но уже представляет собой значительную опасность и требует проведения серьезных мер, направленных на недопущение и уменьшения статистики противоправных действий. В современных реалиях электронные средства платежа, платежные карты хоть и подвержены атакам мошенников, но так и остаются самым удобным на данный момент способом расчета. Развитие в этой сфере должно сопровождаться созданием эффективной системы управления, усовершенствованием нормативно-правовой базы в плане безопасности пользователей, а также усиления ответственности за совершение мошеннических действий с использованием электронных средств платежа.

Список литературы:

[1] Аминов, И. Р. К вопросу о предупреждении противоправного поведения в сфере информационно- телекоммуникационных-технологий / И. Р. Аминов // Современные проблемы уголовного процесса: пути решения : Сборник материалов Международной научно-практической конференции, Уфа, 03–04 апреля 2025 года. – Уфа: Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2025. – С. 20-23. – EDN AJLTJJ.

[2] Аминов, И. Р. Криптовалюта как предмет преступлений коррупционной направленности / И. Р. Аминов, С. В. Трусов // Международный научный вестник. – 2025. – № 1. – С. 93-97. – DOI 10.24412/2782-3849-2025-1-93-97. – EDN MFDHNE.

[3] Гречишников, В. А. Детерминанты мошенничества с использованием электронных средств платежа и способы его предупреждения / В. А. Гречишников // Закон и право. – 2020. – № 1. – С. 109-111. – DOI 10.24411/2073-3313-2020-10025. – EDN AEZGJV.

[4] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств https://www.cbr.ru/statistics/ib/review_1q_2024/

[5] Кодзокова, Л. А. Противодействие мошенничеству с использованием электронных средств платежа в Российской Федерации / Л. А.

Кодзокова // Пробелы в российском законодательстве. – 2020. – Т. 13, № 4. – С. 322-325. – EDN INRM CZ.

References:

[1] Aminov, I.R. On the prevention of unlawful behavior in the field of information and telecommunication technologies/I.R. Aminov//Modern problems of the criminal process: solutions: Collection of materials of the International Scientific and Practical Conference, Ufa, April 03-04, 2025. - Ufa: Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation, 2025. - S. 20-23. – EDN AJLTJJ.

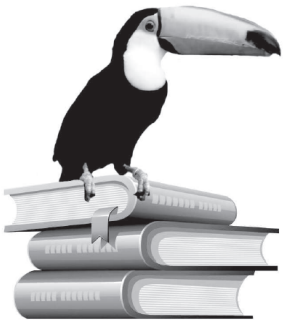
[2] Aminov, I.R. Cryptocurrency as the subject of corruption-related crimes/I.R. Aminov, S.V. Trusov//International Scientific Bulletin. – 2025. – № 1. - S. 93-97. – DOI 10.24412/2782-3849-2025-1-93-97. – EDN MFDHNE.

[3] Grechishnikov, V. A. Determinants of fraud using electronic means of payment and ways to prevent it/V. A. Grechishnikov//Law and Law. – 2020. – № 1. - S. 109-111. – DOI 10.24411/2073-3313-2020-10025. – EDN AEZGJV.

[4] Overview of Information Security Incidents Reporting for Funds Transfers https://www.cbr.ru/statistics/ib/review_1q_2024/

[5] Kodzokova, L. A. Countering fraud using electronic means of payment in the Russian Federation/L. A. Kodzokova//Gaps in Russian legislation. – 2020. - T. 13, NO. 4. - S. 322-325. – EDN INRM CZ.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.