

УДК 330.3

РИСКИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ В ОТМЫВАНИИ ДЕНЕГ И ФИНАНСИРОВАНИИ ТЕРРОРИЗМА

Мамаева Ю. А., студентка гр. Э-Б-О-202, 3 курс

Научный руководитель Ворошило В. В., к.э.н., доцент

Крымский Федеральный Университет им. В. И. Вернадского
г. Симферополь

В настоящее время электронные платежи стали неотъемлемой частью нашей жизни. Они удобны, быстры и доступны в любое время и из любой точки мира. Однако использование электронных платежей также имеет свои риски, особенно в отношении отмывания денег и финансирования терроризма.

В литературе понятие электронный платеж определяется как платеж, совершаемый с помощью электронных телекоммуникаций и электронных платежных инструментов. Он осуществляется с помощью средств. Так в Федеральном законе № 161 «О национальной платежной системе» дается понятие электронных средств платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств [4]. Представим в таблице 1 виды и их содержание.

Таблица 1 – Средства электронных платежей

Виды	Описание видов
Кредитные карты	Один из самых популярных видов электронных платежей. Пользователи могут использовать кредитные карты для оплаты товаров и услуг онлайн, а также для снятия наличных денег в банкоматах.
Дебетовые карты	Дебетовые карты являются альтернативой кредитным картам и позволяют пользователям снимать деньги со своих банковских счетов для оплаты товаров и услуг.
Электронные кошельки	Электронные кошельки позволяют пользователям хранить деньги и осуществлять платежи в Интернете. Они могут быть связаны с банковскими счетами или использоваться независимо от них.
Банковские переводы	Банковские переводы являются классическим способом отправки денег через банк. В Интернете существуют специальные сервисы, которые позволяют осуществлять банковские переводы онлайн.
Предоплаченная карта	Платежная карта, предоставляемая клиенту оператором электронных денежных средств, используемая для перевода электронных денежных средств, а также для осуществления

	иных операций, предусмотренных статьей 7 настоящего Федерального закона.
Криптовалюты	Цифровые валюты в соответствии с российским законодательством, а также цифровые финансовые активы, которые могут использоваться в иностранной юрисдикции для платежей (денежные суррогаты).

Источник: составлено автором на основе [4, 5].

Электронные виды платежей могут быть использованы для отмывания денег, так как они предоставляют возможность быстро и эффективно перемещать деньги через различные страны и юрисдикции. Отмывание денег - это процесс, в котором «грязные» деньги преобразуются в «чистые» деньги. Это может быть достигнуто путем перевода денег через различные счета, чтобы скрыть их происхождение. С использованием электронных платежей эти операции могут быть осуществлены быстрее и более анонимно, что делает их более привлекательными для преступников. Террористическое финансирование - это финансирование, предназначеннное для поддержки террористических деятельности. Использование электронных платежей может помочь террористам собирать деньги из разных источников и передавать их на различные счета по всему миру. Для наглядности в таблице 2 представлены виды риска, связанные с использованием электронных платежей.

Таблица 2 – Риски, связанные с использованием электронным платежей.

Вид риска	Описание
Риск отмывания денег	Процесс перевода незаконных доходов в законные средства путем их интеграции в легальную экономическую систему.
Риск финансирования терроризма	Использование электронных платежей для перевода денежных средств, которые затем используются для финансирования террористических действий
Риск мошенничества	Использование электронных платежей для осуществления мошеннических операций, таких как кража идентификационных данных, взлом счетов и перевод денег на фиктивные счета.
Риск потери конфиденциальности	Возможность разглашения конфиденциальной информации при использовании электронных платежей, такой как информация о кредитных картах, банковских счетах, адресах электронной почты и других личных данных.
Риск ошибок	Возможность возникновения ошибок при проведении электронных платежей, таких

	как неправильный перевод денег или задержка в проведении операции.
Риск несанкционированного доступа	Возможность несанкционированного доступа к электронным счетам и кредитным картам, что может привести к краже денежных средств и потере конфиденциальной информации.

Источник: составлено автором на основе [3].

В таблице 3 приведены возможные угрозы и их описания, связанные с электронными средствами платежами.

Таблица 3 - Угрозы использования электронных средств платежей

Угрозы	Описание
1. Анонимность	Одной из главных угроз является возможность совершения платежей без идентификации пользователей. Некоторые платежные системы не требуют полной идентификации пользователей, что позволяет им скрывать свою личность при совершении операций. Это может быть использовано для сокрытия источника денег и финансирования нелегальных деятельности.
2. Сложность отслеживания	Электронные платежи могут совершаться в любой точке мира, их маршрут может быть неясен и сложен для отслеживания. Это может быть использовано для сокрытия факта финансирования террористических групп или других нелегальных организаций.
3. Масштабы	Электронные платежи могут быть совершены в огромных масштабах за короткое время. Это может быть использовано для сокрытия больших сумм денег, полученных из нелегальных источников.
4. Проблемы с безопасностью	Электронные платежи могут стать объектом кибератак и взлома, что может привести к утечке конфиденциальной информации и потере денег.
5. Уголовная ответственность	Могут использоваться в расчетах за наркотики и последующем отмывание денег полученным ПОД/ФТ.

Источник: составлено автором на основе [6, 9].

В России электронные платежи стали популярными в последние годы, особенно после запрета на использование анонимных электронных кошельков. Электронные средства платежа – это иногда источники финансирования незаконной деятельности. Повышенное внимание к таким финансовым институтам связано с большим количеством нарушений закона [8]. Это обусловлено тем, что электронные платежи позволяют переводить деньги в другие страны, это, в свою очередь, увеличивает риск использования этих систем для международного отмывания денег и финансирования терроризма.

Один из примеров отмывания денег через электронные платежи в России был связан с использованием онлайн-казино. Как правило, в таких случаях,

злоумышленники используют электронные платежные системы для передачи денег на счета онлайн-казино. Затем они играют в казино и выигрывают некоторую сумму, после чего эти выигрыши переводят обратно на свои счета в электронных платежных системах.

Таким образом, злоумышленники могут получить деньги, которые выглядят как законные выигрыши в онлайн-казино. Это позволяет им "отмыть" деньги и использовать их для своих незаконных целей, например, для финансирования террористических организаций или других преступных группировок.

Однако, в России принимаются меры для борьбы с отмыванием денег и финансированием терроризма, они приведены в таблице 4.

Таблица 4 - Способы уменьшения рисков использования электронных платежей в отмывании денег и финансировании терроризма

Способы уменьшения рисков	Описание
Внедрение систем идентификации пользователей	Платежные системы должны требовать полной идентификации пользователей при совершении операций, что поможет уменьшить возможность скрытого финансирования.
Введение лимитов на суммы переводов	Ограничение сумм переводов может помочь уменьшить возможность сокрытия больших сумм денег.
Установление лимитов	На суммы переводов является одним из способов борьбы с отмыванием денег и финансированием терроризма при использовании электронных платежей. Введение ограничений на максимальную сумму перевода может ограничить возможность сокрытия больших денежных средств, а также уменьшить вероятность перевода средств на террористические организации.

Источник: составлено автором на основе [2].

В целях дальнейшего совершенствования мер по борьбе с кибермошенничеством и киберворовством в апреле 2018 года был принят Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». Законом усиlena уголовная ответственность за хищение чужого имущества, совершенное с банковского счета, а равно электронных денежных средств (лишение свободы на срок до 6 лет) [1]. Так, внесены изменения в статью УК РФ, предусматривающую наказание за мошенничество с использованием платежных карт. Уточнено наименование. Речь идет о мошенничестве с использованием электронных средств платежа. Введен новый квалифицирующий признак – «с банковского счета, а равно электронных денежных средств».

Скорректированы санкции за мошенничество в сфере компьютерной информации. Вместо ареста на срок до 4 месяцев за мошенничество с

использованием ЭСП предусмотрено лишение свободы на срок до 3 лет. Снижены пороговые суммы крупного и особо крупного размеров в целях применения соответствующих статей УК РФ.

Однако следует отметить, что установление лимитов на суммы переводов также может негативно повлиять на бизнес-процессы, связанные с электронными платежами. Это может быть связано с ограничением возможности проведения крупных сделок, а также с увеличением времени на проведение переводов. Таким образом, при установлении лимитов на суммы переводов необходимо учитывать не только риски отмывания денег и финансирования терроризма, но и возможные негативные последствия для бизнеса.

Федеральным законом от 27.06.2018 от №167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» установлена обязанность операторов по переводу денежных средств при выявлении ими признаков перевода денежных средств без согласия клиента приостанавливать выполнение такой операции на срок до 2 рабочих дней [7].

В России делается все возможное для того, чтобы уменьшить риски, связанные с отмыванием доходов и финансированием терроризма с использованием виртуальных валют. Для борьбы с этими рисками необходимо совместное усилие со стороны государственных органов, финансовых учреждений и самих пользователей электронных переводов.

В заключении можно сказать, что электронные платежи имеют множество преимуществ, но их использование также связано с рисками отмывания денег и финансирования терроризма. Использование электронных платежей сегодня представляет собой серьезную угрозу в плане отмывания денег и финансирования терроризма. Электронные платежи позволяют легко и быстро переводить деньги, обходя налоговые и другие ограничения, что делает их привлекательным инструментом для преступников. Однако в России существует широкий спектр мер и контролей, которые предназначены для предотвращения этих незаконных действий.

Список литературы

1. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств: федеральный закон от 27.06.2018 от №167-ФЗ // КонсультантПлюс: информационно-правовая система. - URL: https://www.consultant.ru/document/cons_doc_LAW_301060/ (дата обращения: 08.03.2023).
2. О внесении изменений в Уголовный кодекс Российской Федерации: федеральный закон от 23 апреля 2018 г. № 111-ФЗ // КонсультантПлюс: информационно-правовая система. - URL: https://www.consultant.ru/document/cons_doc_LAW_37863/ (дата обращения: 08.03.2023).

3. О национальной платежной системе" (с изм. и доп., вступ. в силу с 11.01.2023): федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 28.12.2022) // КонсультантПлюс: информационно-правовая система. - URL: https://www.consultant.ru/document/cons_doc_LAW_115625/4f41fe599ce341751e4e34dc50a4b676674c1416/ (дата обращения: 15.03.2023).
4. О национальной оценке рисков ОД/ФТ (вместе с "Публичным отчетом. Национальная оценка рисков легализации (отмывания) преступных доходов. Основные выводы 2017 – 2018: информационное письмо Банка России от 14.08.2018 N ИН-014-12/54 // КонсультантПлюс: информационно-правовая система. - URL: https://www.consultant.ru/document/cons_doc_LAW_304897/110eb8df9e21705d49ab460da9944050e87fca3c/ (дата обращения: 21.03.2023).
5. Национальная оценка рисков легализации (отмывания) преступных доходов: публичный отчет Росфинмониторинга // Сайт Росфинмониторинг – URL: <https://www.fedsfm.ru/special/fm/risksml/elpay> (дата обращения: 08.03.2023).
6. Борьба с финансированием терроризма (БФТ): финансовая энциклопедия: официальный сайт. - URL: <https://nesrakonk.ru/combating-financing-terrorism-cft/> (дата обращения: 08.03.2023).
7. Криптовалюты: тренды, риски, меры // Банк России: официальный сайт – 2022. - URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 08.03.2023). – Текст электронный.
8. Апелляционное определение от 7 августа 2018 г. по делу № 2-37/2018 : Судебные и нормативные акты РФ // Верховный суд Российской Федерации - URL: <https://sudact.ru/vsrf/doc/aT0fzm5VqpZm/> (дата обращения: 22.03.2023). – Текст электронный.
9. Мир познаний: Что такое идентификация клиента в банке // URL: <https://deepcloud.ru/articles/chto-takoe-identifikatsiya-klienta-v-banke> (дата обращения: 22.03.2023). – Текст электронный.