pISSN 2073-039X
eISSN 2311-8725

Эффективность бизнеса

УПРАВЛЕНИЕ ПОДОЗРИТЕЛЬНЫМИ ФИНАНСОВЫМИ ОПЕРАЦИЯМИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИЧЕСКИХ ОТНОШЕНИЙ

Аксана Альбековна ТУРГАЕВА [a,•],

Валерия Алексеевна ЧАПЛЫГИНА [b]

[a] кандидат экономических наук, доцент департамента экономической безопасности и управления рисками, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
a_turgaeva@mail.ru
https://orcid.org/0000-0002-8374-1706
SPIN-код: 8718-4901

[b] студентка магистратуры факультета экономики и бизнеса, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
valerika.chapl2015@yandex.ru
ORCID: отсутствует
SPIN-код: 4912-9886

[•] Ответственный автор

История статьи:
Рег. № 481/2023
Получена 25.09.2023
Получена в доработанном виде 16.10.2023
Одобрена 27.10.2023
Доступна онлайн 28.12.2023

Специальность: 5.2.3

УДК 332.055.2
JEL: G22, M41, M42, M49

Ключевые слова:
цифровизация, риски, легализация доходов, экономические преступления, индикаторы подозрительности

Аннотация

Предмет. Управление подозрительными финансовыми операциями в условиях цифровизации.

Цели. Представить основные этапы государственной информатизации и цифровой трансформации в России. Уточнить индикаторы подозрительных финансовых операций в период развития цифровых и информационных технологий. Определить критерии оценки индикаторов подозрительности как инструмент управления рисками в условиях цифровизации экономических отношений.

Методология. Применялись методы систематизации, группировки, рассуждения и абстракции.

Результаты. Представлена эволюция государственной информатизации и цифровой трансформации в России. Определены индикаторы подозрительных финансовых операций в период развития цифровых и информационных технологий. Предложены критерии оценки индикаторов подозрительности. Подтверждена необходимость контроля подозрительных финансовых операций в целях управления рисками, связанными с отмыванием денег, полученных преступным путем, а также финансовых потерь, связанных с цифровыми технологиями.

Выводы. Анализируя этапы цифровизации экономических отношений, складывающихся в России, можно проследить развитие подозрительных финансовых операций и на этой основе выявить риски потерь, разработать контрольные мероприятия по управлению этими рисками, используя предлагаемые индикаторы и критерии их оценки. В результате возможно актуализировать перечень типичных подозрительных финансовых операций для осведомленности руководителей организаций для принятия своевременных управленческих решений по минимизации рисков.

Для цитирования: Тургаева А.А., Чаплыгина В.А. Управление подозрительными финансовыми операциями в условиях цифровизации экономических отношений // Экономический анализ: теория и практика. – 2023. – Т. 22, № 12. – С. 2332 – 2351.
https://doi.org/10.24891/ea.22.12.2332

Специфической чертой современного этапа развития общества является цифровизация. Цифровые технологии и системы оказывают влияние на окружающую реальность, становясь неотъемлемой составляющей жизни во всех сферах. При этом основная задача внедрения цифровых технологий – повышение удобства и скорости получения, обработки, хранения и передачи информации. Развитие цифровых технологий лежит в основе достижения общественного прогресса.

Термин «цифровизация» в узком смысле следует понимать как процесс преобразования данных для представления их в цифровом виде, что, как правило, приводит к уменьшению величины издержек, повышению степени удобства и улучшению восприятия данных. Чаще всего представление имеющихся данных в цифровом виде приводит к благоприятным последствиям, в результате чего делается вывод о цифровизации как о положительном явлении, ведущем к ее проникновению во все сферы жизни общества [1–4].

В широком смысле термин «цифровизация» означает сложившийся по всему миру достаточно сильный тренд в глобальных процессах развития экономической системы и общественной жизни, в соответствии с которым перевод данных в цифровой формат представления в итоге ведет к качественному повышению уровня жизни граждан и уровня управляемости экономики и государственной сферы, а также росту общественного благосостояния. Основные этапы государственной информатизации и цифровой трансформации в России представлены в *табл. 1*.

Процесс цифровизации, начало которому было положено в 1966–1970 гг., прошел довольно долгий путь. Основным нормативно-правовым актом, регулирующим государственную информатизацию в стране, является Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

С развитием цифровизации экономических отношений преступники все более часто используют новые технологии для легализации доходов, полученных незаконным путем. Одной из перспективных форм легализации доходов является использование криптовалют, которые в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» названы цифровыми финансовыми активами, при этом они не могут служить средством платежа. С ростом популярности криптовалют, мошенники все чаще используют их для обхода законодательства и легализации своих доходов. Для борьбы с этим явлением необходимо развивать новые методы и технологии, которые позволят государству

контролировать операции с криптовалютами и предотвращать их использование для легализации доходов, полученных незаконным путем.

Еще одной формой легализации доходов является использование банковских операций. Преступники могут использовать различные схемы, чтобы скрыть происхождение своих доходов и легализовать их через банковские операции. Для борьбы с этим явлением необходимо развивать новые методы и технологии, которые позволят банкам более эффективно контролировать операции своих клиентов и предотвращать легализацию доходов, полученных незаконным путем. Также важно развивать новые методы и технологии для борьбы с финансовыми преступлениями в целом. Например, использование искусственного интеллекта и машинного обучения может помочь банкам и другим финансовым учреждениям более эффективно обнаруживать и предотвращать финансовые преступления.

В условиях информационной экономики можно предположить, что способы отмывания преступных доходов будут все совершенствоваться. Преступники будут использовать новые технологии и методы для скрытия происхождения своих доходов, полученных незаконным путем. В свою очередь использование преимуществ современных технологий позволит правоохранительным органам и уполномоченным структурам эффективно выявлять, нейтрализовать и устранять все случаи незаконного оборота преступных денег. Развитие технологий искусственного интеллекта и алгоритмов машинного обучения может помочь в борьбе с легализацией доходов, позволяя автоматически выявлять подозрительные транзакции и операции. Также с увеличением количества данных, которые собираются и обрабатываются в цифровой экономике, возможно усиление роли аналитических инструментов и экспертных систем в выявлении рисков.

Преступный элемент приспосабливается к новым условиям и активно пользуется предоставленными благами информационного общества. У каждой инновации две стороны – одну используют во благо, другая может нести негативные последствия при неправильном применении. Так, цифровизация общественных отношений массово улучшает жизнь и быт человечества, подняв научный прогресс на небывалый ранее уровень. Однако это неизбежно повлекло за собой то, что злоумышленники приспособили передовые технологии под свои нужды, извлекая из благ цивилизации свою незаконную выгоду. Но из-за этого не стоит отказываться от предоставленных возможностей, главное – правильно их применять. Разработка и внедрение эффективных механизмов контроля в сфере финансовых транзакций, а также повышение уровня правовой культуры в обществе могут стать ключевыми инструментами в этой борьбе.

Росфинмониторинг представил справочник кодов видов необычных операций, на которые необходимо обращать внимание при проведении сделок или других

финансово-хозяйственных операций[1]. Банк России постоянно обновляет индикаторы подозрительности финансовых операций, использующиеся частным сектором, для выявления рисков, связанных в том числе с цифровыми возможностями.

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) представила индикаторы подозрительных операций[2]. Критерии оценки для каждого индикатора следующие:

- низкий уровень (зеленый): 1–2;
- средний уровень (желтый): 3–4;
- высокий уровень (красный): более 4.

Низкий уровень – указанное значение до 2 позволит снизить количество обрабатываемых сигналов, большинство из которых были бы ложными.

Средний уровень –диапазон 3–4 указывает на возможность реализации схем с использованием нескольких счетов, но четко не указывает на это. Целесообразно производить мониторинг лиц, попадающих в данный диапазон.

Высокий уровень – управление более, чем 4 счетами с одной группы IP-адресов прямо указывает на запутанный характер деятельности.

По каждому индикатору обоснуем критерии оценки.

Индикатор 1. Дистанционное управление финансовыми операциями по нескольким (множеству) счетам осуществляется с одной группы IP-адресов.

Критерии оценки:

- количество денежных переводов, осуществляемых с одной группы IP-адресов. Чем больше количество переводов, тем выше индикатор подозрительности;
- частота денежных переводов, осуществляемых с одной группы IP-адресов. Чем чаще происходят переводы, тем выше индикатор подозрительности;
- соответствие объема денежных переводов виду деятельности компании, которой принадлежит группа IP-адресов. Если объем переводов значительно превышает

[1] Описание структур наименования, служебной и информационной частей ФЭС, описание кодов признаков, указывающих на необычный характер операций (сделок), и требования к технологическим электронным документам, направление которых регламентировано Особенностями представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», утвержденными приказом Федеральной службы по финансовому мониторингу от 08.02.2022 № 18. URL: https://fedsfm.ru/search?searchText=описание+кодов+признаков%2C+указывающих+на+необычный+характер+операций

[2] Посредники, предоставляющие профессиональные услуги отмывания денег. URL: cbr.ru›content/document/file/66453/translate.docx

типичный для данной компании, это может свидетельствовать о нарушениях в сфере противодействия отмыванию доходов и финансированию терроризма (ПОД/ФТ);

- использование нескольких счетов для осуществления денежных переводов с одной группы IP-адресов. Если компания использует несколько счетов для осуществления переводов, это может быть признаком скрытой деятельности или попытки уклонения от налогов.

Обоснование: если операции осуществляются с одной группы IP-адресов, это может указывать на связь между различными счетами и на то, что операции могут быть связаны с отмыванием денег.

Индикатор 2. Дистанционное управление финансовыми операциями по нескольким (множеству) счетам осуществляется с одного устройства (мобильного телефона, ноутбука и т.д.).

Критерии оценки:

- количество счетов, управляемых с одного устройства. Чем больше счетов, тем выше индикатор подозрительности;
- частота операций по каждому счету. Если операции проводятся слишком часто или слишком редко, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;
- суммарный объем финансовых операций, проводимых с разными счетами с одного устройства. Чем больше сумма операций, тем выше индикатор подозрительности;
- соответствие местоположения устройства и местоположения счетов. Если устройство находится в другой стране или регионе, чем счета, это может быть признаком наличия нарушений в сфере ПОД/ФТ;
- использование нескольких устройств для управления одними и теми же счетами. Если компания использует несколько устройств для управления одними и теми же счетами, это может быть признаком скрытой деятельности или попытки уклонения от налогов.

Обоснование: операции осуществляются с одного устройства, это может указывать на связь между различными счетами на одном устройстве, существует вероятность использования нескольких устройств у одного пользователя в целях мошеннических схем.

Индикатор 3. Дистанционное управление финансовыми операциями по счетам компаний, зарегистрированных в разных странах, открытых в разных банках,

принадлежащих разным собственникам и управляемых разными директорами, осуществляется с одной группы IP-адресов.

Критерии оценки:

- количество счетов, управляемых с одной группы IP-адресов. Чем больше счетов, тем выше индикатор подозрительности;
- частота операций по каждому счету, осуществляемых с одной группы IP-адресов. Если операции проводятся слишком часто или слишком редко, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;
- соответствие местоположения группы IP-адресов и местоположения счетов. Если группа IP-адресов находится в другой стране или регионе, чем счета, это может быть признаком наличия нарушений в сфере ПОД/ФТ;
- использование нескольких групп IP-адресов для управления одними и теми же счетами. Если компания использует несколько групп IP-адресов для управления одними и теми же счетами, это может быть признаком скрытой деятельности или попытки уклонения от налогов.

Обоснование: так как финансовыми операциями управляет один пользователь, что невозможно в нескольких компаниях в нескольких государствах, то данный пользователь может быть задействован в преступных переводах.

Индикатор 4. Одно лицо является распорядителем по счетам множества компаний.

Критерии оценки:

- количество компаний, управляемых одним лицом. Чем больше компаний, тем выше индикатор подозрительности;
- частота операций по каждой компании, управляемой одним лицом. Если операции проводятся слишком часто или слишком редко, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;
- соответствие местоположения компаний и местоположения распорядителя. Если распорядитель находится не в той стране или регионе, где работают компании, это может быть признаком мошенничества или легализации доходов;
- соответствие типа операций виду деятельности компаний, которыми распоряжается одно лицо. Если тип операций не соответствует типичной деятельности компаний, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;
- использование нескольких идентификационных данных для управления одними и теми же компаниями. Если распорядитель использует несколько

идентификационных данных для управления одними и теми же компаниями, это может быть признаком скрытой деятельности или попытки уклонения от налогов.

Обоснование: если данное лицо не является владельцем данных компаний (что тоже не является верным показателем), возможен хакерский взлом, подложный доступ к счетам, это сигнализирует о преступной деятельности.

Индикатор 5. Транзитный характер движения денежных средств по счетам (денежные средства, поступающие на счета, списываются в течение того же дня, баланс по счету к концу операционного дня нулевой).

Критерии оценки:

- частота транзакций по счетам. Если транзакции проводятся слишком часто или слишком редко, это может свидетельствовать о мошенничестве;
- объем денежных средств, проходящих через счета. Если объем слишком большой или не соответствует типичной деятельности клиента, это может быть признаком нарушений в сфере ПОД/ФТ;
- соответствие типа операций виду деятельности клиента. Если тип операций не соответствует типичной деятельности клиента, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;
- использование нескольких идентификационных данных для открытия счетов. Если клиент использует несколько идентификационных данных для открытия счетов, это может быть признаком скрытой деятельности или попытки уклонения от налогов.

Обоснование: данный счет может быть задействован в удлинении цепочки перевода денежных средств, что является сегментом отмывочной схемы.

Индикатор 6. Регулярные трансграничные операции со счетов компаний с признаками фиктивности, связанные с оплатой за услуги или предоставлением займов.

Критерии оценки:

- несоответствие объема трансграничных операций и типа деятельности компании. Если объем операций значительно превышает типичный для данного вида деятельности компании, это может свидетельствовать о фиктивности операций;
- наличие нескольких счетов, используемых для проведения трансграничных операций. Если компания использует несколько счетов для проведения трансграничных операций, это может свидетельствовать о попытке скрыть фиктивность операций;

- отсутствие документального подтверждения проведения услуг или предоставления займов. Если компания не предоставляет документальное подтверждение проведения услуг или предоставления займов, это может свидетельствовать о фиктивности операций.

Обоснование: регулярные трансграничные операции со счетов компаний с признаками фиктивности, связанные с оплатой за услуги или предоставлением займов, могут быть использованы для вывода капитала за рубеж или для сокрытия доходов от налоговых органов. Если компании, от имени которых происходят операции, имеют признаки фиктивности, это может указывать на возможность незаконных мотивов операции. Если оплата за услуги или предоставление займов не подтверждается документально, это также может указывать на незаконные мотивы операции.

Индикатор 7. Переводы денежных средств за рубеж по импортным договорам, при этом фактические поставки товаров не осуществляются.

Критерии оценки:

- объем переводов денежных средств за рубеж по импортным договорам. Критерий оценивает, какие суммы переводятся за рубеж по импортным договорам, при этом фактические поставки товаров не осуществляются. Чем больше суммы переводов, тем выше индикатор подозрительности;

- частота переводов денежных средств за рубеж по импортным договорам. Критерий оценивает, как часто происходят переводы денежных средств за рубеж по импортным договорам, при этом фактические поставки товаров не осуществляются. Чем чаще происходят переводы, тем выше индикатор подозрительности;

- соответствие объема переводов денежных средств за рубеж по импортным договорам и объему импортируемых товаров. Критерий оценивает соответствие объема переводов денежных средств за рубеж по импортным договорам и объему импортируемых товаров. Если объем переводов значительно превышает объем импортируемых товаров, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;

- соответствие цен, указанных в импортных договорах, рыночным ценам на аналогичные товары. Критерий оценивает соответствие цен, указанных в импортных договорах, рыночным ценам на аналогичные товары. Если цены значительно отличаются от рыночных, это может свидетельствовать о нарушениях в сфере ПОД/ФТ;

- отсутствие документов, подтверждающих фактическую поставку товаров. Критерий оценивает наличие или отсутствие документов, подтверждающих

фактическую поставку товаров. Если такие документы отсутствуют, это может свидетельствовать о нарушениях в сфере ПОД/ФТ.

Обоснование: переводы денежных средств за рубеж по импортным договорам без сопутствующих операций по экспорту товаров или услуг могут быть использованы для вывода капитала за рубеж или для сокрытия доходов от налоговых органов. В таких случаях операция может быть незаконной и подлежать проверке со стороны правоохранительных органов.

Индикатор 8. Оплата по договорам купли-продажи недвижимого имущества и дорогостоящих активов осуществляется со счетов оффшорных компаний.

Критерии оценки:

- количество оффшорных компаний, используемых для оплаты недвижимости и дорогостоящих активов. Чем больше оффшорных компаний используется для оплаты, тем выше индикатор подозрительности;
- частота использования оффшорных компаний для оплаты недвижимости и дорогостоящих активов. Критерий оценивает, как часто оффшорные компании используются для оплаты недвижимости и дорогостоящих активов. Чем чаще происходит использование, тем выше индикатор подозрительности;
- связи между оффшорными компаниями, используемыми для оплаты недвижимости и дорогостоящих активов. Критерий оценивает, есть ли связь между оффшорными компаниями, используемыми для оплаты недвижимости и дорогостоящих активов (например, использование одного и того же адреса или контактных данных). Если есть связи, это может свидетельствовать о мошенничестве;
- общая сумма операций на счетах оффшорных компаний, используемых для оплаты недвижимости и дорогостоящих активов. Критерий оценивает, какие суммы вносятся (снимаются) при операциях на счетах оффшорных компаний, используемых для оплаты недвижимости и дорогостоящих активов. Чем больше суммы, тем выше индикатор подозрительности.

Обоснование: оплата по договорам купли-продажи недвижимости и дорогостоящих активов со счетов оффшорных компаний может быть использована для вывода капитала за рубеж или для сокрытия доходов от налоговых органов. Оффшорные компании могут использоваться для скрытия и перераспределения доходов, что может указывать на незаконные мотивы операции. Если оплата происходит через несколько оффшорных компаний, это может указывать на скрытый характер операции и необходимость дополнительного анализа. Важно учитывать также реальность деятельности оффшорных компаний, так как некоторые из них могут существовать только на бумаге и не иметь реального бизнеса.

Индикатор 9. Оплата за товары, поставляемые в третьи страны, осуществляется со счетов компаний, не являющихся стороной по договору.

Критерии оценки:

- количество компаний, используемых для оплаты товаров в третьи страны. Чем больше компаний используется для оплаты товаров, тем выше индикатор подозрительности;
- частота использования компаний для оплаты товаров в третьи страны. Критерий оценивает, как часто компании используются для оплаты товаров в третьи страны. Чем чаще происходит использование, тем выше индикатор подозрительности;
- общая сумма операций на счетах компаний, используемых для оплаты товаров в третьи страны. Критерий оценивает, какие суммы вносятся (снимаются) при операциях на счетах компаний, используемых для оплаты товаров в третьи страны. Чем больше суммы, тем выше индикатор подозрительности;
- связи между компаниями, используемыми для оплаты товаров в третьи страны. Критерий оценивает, есть ли связь между компаниями, используемыми для оплаты товаров в третьи страны (например, использование одного и того же адреса или контактных данных). Если есть связи, это может свидетельствовать о нарушениях в сфере ПОД/ФТ.

Обоснование: оплата за товары, поставляемые в третьи страны, осуществляется со счетов компаний, не являющихся стороной по договору, может свидетельствовать о наличии незаконных операций, в том числе связанных с отмыванием денег или сокрытием доходов.

Индикатор 10. Юрисдикции регистрации компаний, расположение банков и нахождения бенефициаров (распорядителей) по счетам не совпадают, при этом по счетам компаний совершаются финансовые операции по основаниям, не связанным с заявленным видом деятельности компаний.

Критерии оценки:

- количество компаний, зарегистрированных в юрисдикции, отличной от места расположения банка. Чем больше компаний зарегистрировано в другой юрисдикции, тем выше индикатор подозрительности;
- частота изменения юрисдикции регистрации компании. Критерий оценивает, как часто компании меняют свою юрисдикцию регистрации. Чем чаще происходит замена, тем выше индикатор подозрительности;
- общая сумма операций на счетах компаний, зарегистрированных в другой юрисдикции. Критерий оценивает, какие суммы вносятся (снимаются) при

операциях на счетах компаний, зарегистрированных в другой юрисдикции. Чем больше суммы, тем выше индикатор подозрительности;

- связи между компаниями, зарегистрированными в разных юрисдикциях. Критерий оценивает, есть ли связь между компаниями, зарегистрированными в разных юрисдикциях (например, использование одного и того же адреса или контактных данных). Если есть связи, это может свидетельствовать о мошенничестве;

- отсутствие связи между юрисдикцией регистрации компании и ее заявленным видом деятельности. Критерий оценивает, соответствует ли заявленный вид деятельности компании ее юрисдикции регистрации. Если нет соответствия, это может свидетельствовать о мошенничестве.

Обоснование: если финансовые операции компании соответствуют одному или нескольким из указанных критериев, то это может свидетельствовать о подозрительной операции, требующей дополнительного анализа и, возможно, обращения в правоохранительные органы.

Индикатор 11. Подозрительные операции проводятся по счетам компаний, зарегистрированных через одного регистрирующего агента или по одному адресу.

Критерии оценки:

- количество компаний, зарегистрированных через одного регистрирующего агента. Чем больше компаний зарегистрировано через одного регистрирующего агента, тем выше индикатор подозрительности;

- частота изменения регистрирующего агента. Критерий оценивает, как часто компании меняют своего регистрирующего агента. Чем чаще происходит замена, тем выше индикатор подозрительности;

- общая сумма операций на счетах компаний, зарегистрированных через одного регистрирующего агента. Критерий оценивает, какие суммы вносятся (снимаются) при операциях на счетах компаний, зарегистрированных через одного регистрирующего агента. Чем больше суммы, тем выше индикатор подозрительности;

- связи между компаниями, зарегистрированными через одного регистрирующего агента. Критерий оценивает, есть ли связь между компаниями, зарегистрированными через одного регистрирующего агента (например, использование одного и того же адреса или контактных данных). Если есть связи, это может свидетельствовать о нарушениях в сфере ПОД/ФТ.

Обоснование: если финансовые операции компании соответствуют одному или нескольким из указанных критериев, то это может свидетельствовать о

подозрительной операции, требующей дополнительного анализа и, возможно, обращения в правоохранительные органы.

Индикатор 12. Операции по внесению или снятию наличных денежных средств осуществляются систематически через одни и те же банкоматы (незначительные временные интервалы между операциями по внесению (снятию) наличных денежных средств с разных банковских карт могут свидетельствовать о том, что операции совершаются одним и тем же лицом).

Критерии оценки:

- частота операций. Критерий оценивает, как часто происходят операции по внесению (снятию) наличных денежных средств через одни и те же банкоматы. Чем чаще происходят такие операции, тем выше индикатор подозрительности;
- временные интервалы между операциями. Критерий оценивает, насколько значительны временные интервалы между операциями по внесению/снятию наличных денежных средств с разных банковских карт. Чем меньше интервалы, тем выше индикатор подозрительности;
- количество карт. Критерий оценивает, сколько различных банковских карт используется для операций по внесению (снятию) наличных денежных средств через одни и те же банкоматы. Чем больше карт используется, тем выше индикатор подозрительности;
- сумма операций. Критерий оценивает, какие суммы вносятся (снимаются) при операциях через одни и те же банкоматы. Чем больше суммы, тем выше индикатор подозрительности.
- регион операций. Критерий оценивает, в каком регионе происходят операции по внесению (снятию) наличных денежных средств через одни и те же банкоматы. Если операции происходят в разных регионах, это может свидетельствовать о нарушениях в сфере ПОД/ФТ.

Обоснование: если операции по внесению или снятию наличных денежных средств соответствуют одному или нескольким из указанных критериев, то это может свидетельствовать о подозрительной операции, требующей дополнительного анализа и, возможно, обращения в правоохранительные органы.

Индикатор 13. Банковские счета, электронные кошельки и банковские карты используются на протяжении короткого периода времени, затем заменяются на новые финансовые реквизиты.

Критерии оценки:

- частота замены финансовых реквизитов. Оценка частоты замены финансовых реквизитов может помочь выявить, насколько часто происходят подобные случаи и какие меры можно принять для предотвращения нарушений в сфере ПОД/ФТ;
- идентификация пользователей. Оценка процессов идентификации пользователей может помочь выявить возможные слабые места в системе безопасности, которые могут использоваться для получения доступа к финансовым реквизитам;
- мониторинг транзакций. Оценка системы мониторинга транзакций может помочь выявить необычные или подозрительные операции, связанные с заменой финансовых реквизитов;
- связи между замененными реквизитами. Критерий оценивает, есть ли связь между замененными финансовыми реквизитами (например, использование одного и того же телефонного номера или электронной почты). Если есть связи, это может свидетельствовать о нарушениях в сфере ПОД/ФТ.

Обоснование: использование финансовых реквизитов на короткий период времени и их частая замена может свидетельствовать о том, что мошенники пытаются скрыть свою деятельность и избежать выявления. Необычный объем и частота транзакций, необычные схемы транзакций и использование счетов, кошельков или карт на разных территориях могут указывать на то, что злоумышленники используют эти реквизиты для совершения мошеннических операций.

Успешное противодействие легализации доходов, полученных преступным путем, возможно только при совместных усилиях государства, бизнеса и общественности. Только так можно обеспечить настоящую прозрачность и законность в экономической сфере и создать условия для устойчивого развития общества.

Таблица 1
Основные этапы государственной информатизации и цифровой трансформации в России

Table 1
The main stages of State informatization and digital transformation in Russia

Год	Основные направления, законодательные акты	Примечания
1966	Первый проект по развитию автоматизации в СССР: аванпроект государственной сети вычислительных центров	Основные программные документы в сфере государственной информатизации
1985	О мерах по обеспечению компьютерной грамотности учащихся средних учебных заведений и широкого внедрения электронно-вычислительной техники в учебный процесс: постановление ЦК КПСС и Совета Министров СССР от 28.03.1985 № 271	Основной нормативно-правовой акт, регулирующий государственную информатизацию
1986	Государственный комитет СССР по вычислительной технике и информатике (ГКВТИ СССР)	Структуры, ответственные за информатизацию и цифровизацию в государственном секторе
1991	Комитет по информатизации при Кабинете Министров СССР	
1992	Комитет по информатизации при Минкомсвязи России	
1994	Об основах государственной политики в сфере информатизации: Указ Президента РФ от 20.01.1994 № 170	Основной нормативно-правовой акт, регулирующий информационно-телекоммуникационное обеспечение органов государственной власти
1995	Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов: одобрена решением Президента РФ от 23.11.1995 № Пр-1694)	Основной программный документ в сфере государственной информатизации
1996	Комитет при Президенте РФ по политике информатизации	Структура, ответственная за информатизацию и цифровизацию в государственном секторе
2002	О Федеральной целевой программе «Электронная Россия (2002–2010)»: постановление Правительства РФ от 28.01.2002 № 65	Основной программный документ в сфере государственной информатизации
	Об электронной цифровой подписи: Федеральный закон от 10.01.2002 № 1-ФЗ	Основной нормативно-правовой акт, регулирующий использование электронной цифровой подписи
2004	О Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года и плане мероприятий по ее реализации: распоряжение Правительства РФ от 27.09.2004 № 1244-р	Основной программный документ в сфере государственной информатизации
2006	Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ	Основной нормативно-правовой акт в сфере государственной информатизации
	О создании системы мониторинга использования информационных технологий в деятельности федеральных органов государственной власти: постановление Правительства РФ от 18.05.2006 № 298	Основной нормативно-правовой акт в сфере государственной информатизации (утратил силу 10 июля 2012 года на основании постановления Правительства РФ от 26.06.2012 № 644)
	Проект «Электронный гражданин» – обучение граждан навыкам работы с компьютером для получения госуслуг	Основные события в сфере государственной информатизации

Год	Основные направления, законодательные акты	Примечания
2007	Проект Минкомсвязи России «Компьютер в каждый дом»	
	Начал работу первый региональный портал госуслуг «Портал государственных и муниципальных услуг Санкт-Петербурга»	
2008	О Концепции формирования в Российской Федерации электронного правительства до 2010 года: распоряжение Правительства РФ от 06.05.2008 № 632-р	Основной программный документ в сфере государственной информатизации
	Созданы крупные государственные информационные системы (ГАС «Управление», ГИАС КСО, «Система-112»), технологии ИКТ с доступом в Интернет массово внедрены в работу госслужащих	Основные события в сфере государственной информатизации
	Начал работу Единый портал государственных и муниципальных услуг	
	О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (вместе с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года): распоряжение Правительства РФ от 17.11.2008 № 1662-р	Основной программный документ в сфере государственной информатизации
2009	Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в электронном виде, а также услуг, предоставляемых в электронном виде учреждениями субъектов Российской Федерации и муниципальными учреждениями: распоряжение Правительства РФ от 17.12.2009 № 1993-р	Основные события в сфере государственной информатизации
2010	О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов: постановление Правительства РФ от 24.05.2010 № 365	Основной нормативно-правовой акт, регулирующий государственную информатизацию (утратил силу)
	Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ	Основной нормативно-правовой акт, регулирующий государственную информатизацию
	Создана система межведомственного электронного взаимодействия (СМЭВ)	Основные события в сфере государственной информатизации
2011	Введена в эксплуатацию АИС «Управление ведомственной и региональной информатизацией»	
2013	О Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности: постановление Правительства РФ от 26.08.2013 № 735	Структура, ответственная за информатизацию и цифровизацию
2014	Об утверждении государственной программы Российской Федерации «Информационное общество»: постановление Правительства РФ от 15.04.2014 № 313	Основной программный документ в сфере государственной информатизации
	Внедрена система электронного документооборота между федеральными и региональными органами власти	Основные события в сфере государственной информатизации
2015	Сформирована инфраструктура электронного правительства	
	О федеральной государственной информационной системе координации информатизации (вместе с Положением о федеральной государственной	Структура, ответственная за информатизацию и цифровизацию в

Год	Основные направления, законодательные акты	Примечания
	информационной системе координации информатизации): постановление Правительства РФ от 14.11.2015 № 1235	государственном секторе
	Создана федеральная государственная информационная система координации информатизации	Основные события в сфере государственной информатизации
2016	О приоритетных направлениях использования и развития информационно-коммуникационных технологий в федеральных органах исполнительной власти и органах управления государственными внебюджетными фондами и о внесении изменений в некоторые акты Правительства Российской Федерации: постановление Правительства Российской Федерации от 05.05.2016 № 392	Структура, ответственная за информатизацию и цифровизацию в государственном секторе
2017	Об утверждении программы «Цифровая экономика Российской Федерации: распоряжение Правительства РФ от 28.07.2017 № 1632-р	Основной программный документ в сфере государственной информатизации
2018	О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации от 07.05.2018 № 204	Основной нормативно-правовой акт в сфере государственной информатизации
	Преобразование региональных органов власти, ответственных за информатизацию и развитие электронного правительства, в органы цифрового развития	Структура, ответственная за информатизацию и цифровизацию в государственном секторе
2020	О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21.07.2020 № 474	Основной нормативно-правовой акт в сфере государственной информатизации
	О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами: постановление Правительства РФ от 10.10.2020 № 1646	
	Назначение в высших исполнительных органах государственной власти ответственных за цифровую трансформацию	Структура, ответственная за информатизацию и цифровизацию в государственном секторе
	О внесении изменений в часть вторую Налогового кодекса Российской Федерации: Федеральный закон от 31.07.2020 № 265-ФЗ	У ИТ-компаний существенно снижается финансовая нагрузка
	Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: Федеральный закон от 31.07.2020 № 258-ФЗ	Особые правовые режимы, позволяющие тестировать в реальных условиях технологии, которые пока существуют вне правового поля
	О новой редакции паспорта федерального проекта «Нормативное регулирование цифровой среды» национальной программы «Цифровая экономика Российской Федерации»: письмо Минэкономразвития России от 14.08.2020 № 26355-ВФ/Д31и	Основной нормативно-правовой акт в сфере государственной информатизации
	О внесении изменений в Федеральный закон «О стандартизации в Российской Федерации»: Федеральный закон от 30.12.2020 № 523-ФЗ	Основной программный документ в сфере государственной информатизации
	О внесении изменений в Федеральный закон «О персональных данных»: Федеральный закон от 30.12.2020 № 519-ФЗ	

Год	Основные направления, законодательные акты	Примечания
	Об утверждении Правил перевозок грузов автомобильным транспортом и о внесении изменений в пункт 2.1.1 Правил дорожного движения Российской Федерации: постановление Правительства РФ от 21.12.2020 № 2200	Возможность формирования в электронном виде транспортных накладных и других перевозочных документов
	О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях: Федеральный закон от 08.12.2020 № 407-ФЗ: Федеральный закон от 31.07.2020 № 265-ФЗ	Удаленная работа регламентирована законодательно
	О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ	Установлено, что криптовалюта не может быть средством платежа. Цифровые финансовые активы можно продавать, покупать, обменивать на другие цифровые финансовые активы, передавать по наследству

Источник: Регуляторный ландшафт стратегии и «цифры»: обзор нормативных правовых актов. URL: https://strategy.cdto.ranepa.ru/a3-regulirovanie-v-sfere-it-i-cifrovoj-transformacii; Новые российские законы: что изменится в IT-сфере в 2021 году? URL: https://tproger.ru/articles/novye-rossijskie-zakony-chto-izmenitsja-v-it-sfere-v-2021-godu/

Source: The regulatory landscape of strategy and "digit": A review of regulations]. URL: https://strategy.cdto.ranepa.ru/a3-regulirovanie-v-sfere-it-i-cifrovoj-transformacii; New Russian laws: What will change in the IT sphere in 2021?. URL: https://tproger.ru/articles/novye-rossijskie-zakony-chto-izmenitsja-v-it-sfere-v-2021-godu/

Список литературы

1. *Халин В.Г., Чернова Г.В.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. 2018. № 10. С. 46–63. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-ee-vliyanie-na-rossiyskuyu-ekonomiku-i-obschestvo-preimuschestva-vyzovy-ugrozy-i-riski?ysclid=lnu9zh7sc0369670924

2. *Прасолов В.И., Фешина С.С.* Влияние цифровой трансформации на процессы выявления легализации доходов, полученных преступным путем // Экономика: вчера, сегодня, завтра. 2020. Т. 10. № 8А. С. 130–145. URL: http://www.publishing-vak.ru/file/archive-economy-2020-8/13-prasolov.pdf

3. *Хабриева Т.Я.* Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики: стратегические задачи и правовые решения // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 459–466. URL: https://cyberleninka.ru/article/n/protivodeystvie-legalizatsii-otmyvaniyu-dohodov-poluchennyh-prestupnym-putem-i-finansirovaniyu-terrorizma-v-usloviyah-tsifrovizatsii?ysclid=lnua6q7ajl252461939

4. *Тургаева А.А., Кочеткова Н.Н., Иглина Н.А.* Применение цифровых возможностей в страховом бизнесе // Экономический анализ: теория и практика. 2023. Т. 22. Вып. 2. С. 254–263. URL: https://doi.org/10.24891/ea.22.2.254

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-039X
eISSN 2311-8725

Business Performance

MANAGEMENT OF SUSPICIOUS FINANCIAL TRANSACTIONS IN THE CONTEXT OF DIGITALIZATION OF ECONOMIC RELATIONS

Aksana A. TURGAEVA [a,•],

Valeriya A. CHAPLYGINA [b]

[a] Financial University under Government of Russian Federation,
Moscow, Russian Federation
a_turgaeva@mail.ru
https://orcid.org/0000-0002-8374-1706

[b] Financial University under Government of Russian Federation,
Moscow, Russian Federation
valerika.chapl2015@yandex.ru
ORCID: not available

• Corresponding author

Article history:
Article No. 481/2023
Received 25 Sept 2023
Received in revised form
16 Oct 2023
Accepted 27 Oct 2023
Available online
28 Dec 2023

JEL classification: G22, M41, M42, M49

Keywords: digitalization, risk, money laundering, economic crime, suspicious activity indicator

Abstract

Subject. The article addresses the management of suspicious financial transactions in conditions of digitalization.

Objectives. The aim is to present the main stages of State informatization and digital transformation in Russia, clarify indicators of suspicious financial transactions in the period of development of digital and information technologies, define evaluation criteria for suspicion indicators as a risk management tool under digitalization of economic relations.

Methods. We employed methods of systematization, grouping, reasoning, and abstraction.

Results. The paper presents the evolution of State informatization and digital transformation in Russia, defines indicators of suspicious financial transactions, suggests criteria to assess suspicion indicators. We confirmed the need for monitoring suspicious financial transactions to manage risks associated with money laundering from criminal proceeds, and financial losses related to digital technologies.

Conclusions. The analysis of stages of digitalization of economic relations in Russia enables to trace the development of suspicious financial transactions and, on this basis, identify risk of losses, formulate control measures to manage these risks, using the proposed indicators and criteria for their assessment. As a result, it is possible to update the list of typical suspicious financial transactions for the awareness of heads of organizations to make timely management decisions on risk minimization.

Please cite this article as: Turgaeva A.A., Chaplygina V.A. Management of Suspicious Financial Transactions in the Context of Digitalization of Economic Relations. *Economic Analysis: Theory and Practice*, 2023, vol. 22, iss. 12, pp. 2332–2351.
https://doi.org/10.24891/ea.22.12.2332

References

1. Khalin V.G., Chernova G.V. [Digitalization and its impact on the Russian economy and society: Advantages, challenges, threats and risks]. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*, 2018, no. 10, pp. 46–63. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-ee-vliyanie-na-rossiyskuyu-ekonomiku-i-obschestvo-preimuschestva-vyzovy-ugrozy-i-riski?ysclid=lnu9zh7sc0369670924 (In Russ.)

2. Prasolov V.I., Feshina S.S. [Impact of digital transformation on the processes of identifying the legalization of illegal income]. *Ekonomika: vchera, segodnya, zavtra = Economics: Yesterday, Today and Tomorrow*, 2020, vol. 10, no. 8A, pp. 130–145. URL: http://www.publishing-vak.ru/file/archive-economy-2020-8/13-prasolov.pdf (In Russ.)

3. Khabrieva T.Ya. [Counteraction to the legalization (laundering) of proceeds from crime and the financing of terrorism in the context of the digitization of economy: Strategic objectives and legal solutions]. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 4, pp. 459–466. URL: https://cyberleninka.ru/article/n/protivodeystvie-legalizatsii-otmyvaniyu-dohodov-poluchennyh-prestupnym-putem-i-finansirovaniyu-terrorizma-v-usloviyah-tsifrovizatsii?ysclid=lnua6q7ajl252461939 (In Russ.)

4. Turgaeva A.A., Kochetkova N.N., Iglina N.A. [Application of digital capabilities in the insurance business]. *Ekonomicheskii analiz: teoriya i praktika = Economic Analysis: Theory and Practice*, 2023, vol. 22, iss. 2, pp. 254–263. (In Russ.) URL: https://doi.org/10.24891/ea.22.2.254

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.