



## **Observatoire ARGA**

Отчёт по санкциям и комплаенсу за 2025 год

# **Транснациональное давление через финансовые каналы: аналитический обзор кейсов**

Автор:

Сергей Храбрых — президент ARGA, PhD

Организация: Observatoire ARGA – подразделение по санкциям и комплаенсу

Адрес для корреспонденции: 14 rue Jacques Laffitte, Байонна, 64100

Контакты: [info@argaobservatory.org](mailto:info@argaobservatory.org)

Париж, 2 ноября 2025

## **Оглавление**

<b>КРАТКОЕ РЕЗЮМЕ</b> .....	<b>3</b>
<b>МЕТОДОЛОГИЯ</b> .....	<b>4</b>
<b>КЛЮЧЕВЫЕ ПОНЯТИЯ</b> .....	<b>6</b>
<b>РЕГИОНАЛЬНЫЙ ОБЗОР</b> .....	<b>6</b>
<b>ТИПОЛОГИЯ ЗЛУОПОТРЕБЛЕНИЙ</b> .....	<b>7</b>
<b>АНАЛИЗ ПО СТРАНАМ</b> .....	<b>9</b>
Россия .....	9
Казахстан .....	10
Узбекистан.....	11
Азербайджан .....	11
Кыргызстан .....	12
Беларусь.....	12
Таджикистан .....	12
Туркменистан.....	13
Грузия.....	13
Молдова .....	14
Армения.....	14
<b>ПРИМЕРЫ ИЗ ПРАКТИКИ</b> .....	<b>15</b>
<b>КАРТА РИСКОВ</b> .....	<b>18</b>
<b>«КРАСНЫЕ ФЛАГИ»</b> .....	<b>18</b>
<b>РЕКОМЕНДАЦИИ</b> .....	<b>19</b>
OFAC.....	19
EU DG FISMA.....	20
FATF .....	20
FIU (EU/UK/UAE/CH).....	20
Banks .....	21
<b>ВЫВОД</b> .....	<b>21</b>
<b>ИСТОЧНИКИ</b> .....	<b>22</b>

## КРАТКОЕ РЕЗЮМЕ

Доклад фиксирует формирование нового типа транснационального давления, при котором государственные структуры используют финансовые механизмы — AML/CTF-процедуры, FIU-запросы, санкционный контекст, банковский KYC/EDD и замораживание активов — не для предотвращения отмывания доходов, а как неконвенциональные инструменты влияния за пределами своей юрисдикции.

В ряде государств СНГ и соседнего региона наблюдается устойчивая практика воздействия на предпринимателей, журналистов, активистов, НКО и инвесторов, находящихся в ЕС, Великобритании, ОАЭ, Турции, Швейцарии и других странах, через финансовую инфраструктуру. В отличие от классических методов преследования, давление осуществляется бесшумно, без прямых ордеров и без публичных обвинений, что делает его труднодоказуемым и высокоэффективным.

Механизмы транснационального воздействия включают:

- подложные, неполные или искажённые FIU-запросы, направленные в банки иностранных юрисдикций с формулировками общего характера;
- международные Freeze Actions, при которых блокировка активов вводится на основании сигнала риска без судебного решения;
- sanctions shadowing — имитацию санкционной связи, когда государство пытается создать у банков впечатление принадлежности фигуранта к санкционному кругу, хотя санкции отсутствуют;
- автоматизированные банковские блокировки, запускаемые алгоритмами de-risking без участия человека;
- маскировку политических мотивов под экономические составы («отмывание», «уклонение», «иностранное финансирование»);
- параллельное использование Интерпола, экстрадиционных процедур и AML-сигналов, создающее накопительный эффект давления.

Особенностью таких схем является трансграничность и асимметрия: государство-инициатор не несёт ответственности за последствия, в то время как международные банки и финмониторинг сталкиваются с высокими рисками ошибочных блокировок.

Доклад основан на десятках кейсов Observatoire ARGA (публичных и NDA), собранных с 2021 по 2025 годы. Материалы позволяют:

- проследить географию финансового давления в 11 странах;
- выделить типологию схем и повторяющиеся триггеры;
- сформировать карту транснациональных рисков для банков, FIU и регуляторов;
- представить аналитические выводы о тенденциях, включая рост автоматизации, снижение прозрачности и слияние экономических и политических инструментов;
- подготовить рекомендации международным структурам, включая FATF, OFAC, EU DG FISMA, Интерпол, а также глобальным банкам и криптоплатформам.

Таким образом, доклад фиксирует появление устойчивого феномена, в котором финансовые каналы становятся инструментом трансграничного давления, не требующим открытого политического преследования, но приводящим к серьёзным последствиям — от заморозки активов до разрушения бизнеса и вынужденной миграции.

## МЕТОДОЛОГИЯ

### **1. Case-based research: 12 обезличенных транснациональных кейсов ARGА**

Анализ построен на изучении двенадцати реальных случаев трансграничного финансового давления, в которых задействованы механизмы AML/KYC, FIU-запросы, freeze-меры и параллельные международные процедуры.

Для каждого кейса реконструировались:

- последовательность действий от первого сигнала до итогового статуса,
- юрисдикции, вовлечённые в цепочку запросов,
- последствия для активов, деловой деятельности и статуса лица,
- момент перехода от финансовой меры к политико-административному давлению.

Все данные полностью обезличены и не содержат персональных или корпоративных идентификаторов, что позволяет сохранять юридическую безопасность при сохранении аналитической полноты.

### **2. OSINT: Egmont Group, OECD, FATF, World Bank INT, международные СМИ, публичные жалобы**

Использован расширенный контур открытых источников, включающий:

- рекомендации и публичные отчёты Egmont Group по обмену финансовой информацией,
- материалы OECD о злоупотреблении антикоррупционными механизмами,
- страновые и тематические отчёты FATF, включая Immediate Outcomes 3 и 6,
- аналитические записи World Bank Integrity Vice Presidency (INT),
- международные медиа (FT, Reuters, Bloomberg, OCCRP),
- публичные обращения, судебные документы, открытые жалобы и заявления о неправомерных блокировках.

OSINT-данные использовались не как иллюстрация, а как способ проверки устойчивости выводов.

### **3. Forensic financial analysis: изучение Freeze Actions, chain of requests, банковских алгоритмов**

Применён форензик-подход, направленный на восстановление логики принятия решений.

Изучались:

- структура freeze-меры (initiator → transmission → execution),
- цепочки FIU-запросов между юрисдикциями,
- внутренние банковские алгоритмы (risk scoring, sanctions-shadowing triggers, nationality-based flags),
- наличие или отсутствие manual review,
- временные лаги между сигналом и блокировкой.

Этот метод позволил отделить автоматические ошибки от целенаправленного транснационального влияния.

### **4. Legal comparative method: сравнение механизмов FIU–FIU, AML, международных запросов и Интерпола**

Проведено сопоставление правовых режимов в ЕС, Великобритании, Швейцарии, ОАЭ и СНГ, включая:

- требования к содержанию FIU-запросов,
- стандарты доказательств для freeze-мер (administrative freeze vs court-based freezing),
- правила передачи информации между FIU,
- границы допустимого использования Интерпола и экстрадиционных процедур,
- доступность механизмов обжалования.

Сравнение выявило, что отсутствие проверочных фильтров превращает внешние сигналы в автоматические репрессивные меры.

### **5. Double-source verification: каждая схема подтверждена минимум двумя независимыми источниками**

Все аналитические выводы проходят двойную проверку, включающую:

- сопоставление документальных материалов и интервью,
- независимую верификацию через OSINT, международные базы и внешних экспертов,

— исключение утверждений, подтверждённых только одним источником.

Этот подход минимизирует ошибочную интерпретацию и обеспечивает воспроизводимость выводов даже в условиях ограниченной прозрачности.

## КЛЮЧЕВЫЕ ПОНЯТИЯ

**Transnational Financial Pressure (TFP)** — транснациональное давление через финансовые инструменты, при котором государство воздействует на лиц, находящихся за пределами его территории, с помощью AML/CTF-процедур, заморозки активов, KYC-мер и международных каналов обмена информацией, без необходимости прямого юридического преследования.

**FIU Message Propagation (FMP)** — распространение ложного или частично ложного сигнала финансовой разведкой по международным каналам. Такой сигнал, даже без доказательной базы, приводит к блокировкам в иностранных банках, создавая эффект цепной реакции и утрачивая возможность обратной проверки.

**Sanctions Shadow Pressure (SSP)** — искусственная привязка лица или организации к санкционному контексту. Государство или инициатор создаёт у банков впечатление связи с санкционными структурами, хотя реальных ограничений нет, что приводит к автоматическим отказам и freeze-мерам.

**Freeze Action Cascade (FAC)** — каскад заморозок активов в нескольких странах, возникающий после единственного сигнала риска. Один запрос FIU или уведомление инициирует блокировки в разных юрисдикциях, даже при отсутствии подтверждений, что делает последствия трансграничными и трудно обратимыми.

**Interpol–FIU Coupled Pressure (IFCP)** — связка механизмов Интерпола и финансовых запросов. Freeze применяется параллельно с уведомлением о розыске или экстрадицией, усиливая давление на банки и создавая иллюзию высокой угрозы, даже если запрос впоследствии признаётся политически мотивированным.

**Cross-Border Constructed Risk (CBCR)** — искусственное формирование международного «рискового профиля», когда лицо становится высокорисковым не из-за операций, а из-за накопления неподтверждённых сигналов в разных странах. Такой профиль воспроизводится в банковских системах автоматически и сохраняется даже после снятия претензий.

## РЕГИОНАЛЬНЫЙ ОБЗОР

Observatoire ARGА фиксирует устойчивые формы транснационального финансового давления, исходящие из одиннадцати стран региона: России, Казахстана, Узбекистана, Азербайджана, Кыргызстана, Беларуси, Таджикистана, Туркменистана, Грузии, Молдовы и Армении. Несмотря на различия политических систем и уровней институциональной независимости, во всех этих юрисдикциях наблюдаются схожие механизмы передачи финансовых сигналов за пределы национальных границ.

Основные паттерны:

**1. FIU стран СНГ передают в международные банки неполные или искажённые сведения.**

Запросы часто содержат размытые формулировки, отсутствует описание предиката, сумма ущерба или подтверждающие документы. Несмотря на это, международные банки воспринимают такие сигналы как высокорисковые, поскольку не имеют механизмов обратной проверки или доступа к исходным материалам.

**2. Банки ЕС/UK/CH/UAE применяют автоматические freeze-алгоритмы.**

Заморозка активов запускается в рамках автоматизированных систем de-risking и KYC-скрининга, зачастую без участия человека и без анализа контекста. В сочетании с национальными сигналами это приводит к мгновенным блокировкам даже при отсутствии подозрительных транзакций.

**3. Freeze запускается без ущерба, без предиката, без экспертиз.**

Во многих случаях блокировка активов применяется до возбуждения дела или проведения финансово-экономической проверки. Мера превращается в фактическое предварительное наказание, при котором ущерб несут предприниматели и инвесторы, а не государственные структуры.

**4. Интерпол и AML используются параллельно для усиления давления.**

Даже неподтверждённый запрос о международном розыске трактуется банками как индикатор высокого риска. Связка «freeze + Интерпол» усиливает эффект и создаёт иллюзию легитимности, хотя позднее такие уведомления могут быть признаны политически мотивированными.

**5. Инвесторы, журналисты и бенефициары компаний подвергаются международной изоляции через финансовые механизмы.**

Ограничения проявляются в отказах в обслуживании, прекращении банковских отношений, блокировке активов за рубежом и невозможности проводить транзакции. Такие последствия возникают без судебных решений и без возможности обжалования, формируя новый формат трансграничного давления.

## ТИПОЛОГИЯ ЗЛОУПОТРЕБЛЕНИЙ

**1. FIU Shadow Export — экспорт ложных FIU-сигналов.**

Механизм заключается в том, что подразделение финансовой разведки одной страны направляет за рубеж неполные, искажённые или заведомо неточные сведения, оформляя их как полноценный международный запрос. Такие сообщения могут содержать расплывчатые формулировки («возможное отмывание», «риск незаконных операций») без фактов, суммы ущерба и указания предикатного состава. Поскольку FIU-каналы рассматриваются банками как высоконадёжные, даже неофициальный сигнал

запускает автоматическое реагирование. Государство-инициатор при этом избегает формальной ответственности, а последствия — заморозка активов, offboarding и блокировка международных переводов — реализуются в юрисдикциях, где у фигуранта нет возможности защититься.

## **2. Cross-Border Freeze Propagation — каскадные заморозки в нескольких юрисдикциях.**

После единичного сигнала о риске блокировки могут распространяться цепочкой: сначала freeze вводит банк в одной стране, затем его автоматически дублируют банки-корреспонденты, далее — платёжные платформы и криптосервисы. В результате клиент сталкивается с одновременной утратой доступа к счетам в ЕС, Великобритании, Швейцарии или ОАЭ. Парадокс заключается в том, что ни одна из юрисдикций не принимает самостоятельного решения — все полагаются на предыдущий шаг, создавая эффект «снежного кома». Даже если исходный сигнал впоследствии признан необоснованным, cascade-freeze может сохраняться месяцами из-за отсутствия процедур синхронной разблокировки.

## **3. Sanction-Mimicking — имитация санкционного профиля лица.**

Злоупотребление строится на создании у банков впечатления, что фигурант связан с санкционными структурами, хотя юридически он не включён ни в один санкционный список. Искажение может происходить через намёки в формулировках FIU, использование терминов вроде «близость к санкционным субъектам» или упоминание организаций с похожими названиями. Банки, опасаясь вторичных санкций, предпочитают мгновенный offboarding или freeze, действуя по принципу «избыточной осторожности». Таким образом, санкционная мера возникает фактически без санкций, а лицо оказывается в финансовой изоляции без правовых оснований.

## **4. Interpol Reinforcement — использование R, Blue или Diffusion Notice + FIU.**

В этой схеме государство инициирует уведомление Интерпола (красное, голубое или диффузное), параллельно направляя сигналы через FIU-каналы. Даже если уведомление не подтверждено или содержит политические признаки, сам факт появления имени в базе Интерпола воспринимается банками как критический риск. Сочетание двух механизмов усиливает давление: freeze вводится быстрее, длится дольше, а отмена становится практически недоступной, поскольку финансовые структуры ссылаются на международный статус лица. Эта связка создаёт квазисанкционный эффект без юридических санкций и без судебных решений.

## **5. Constructed High-Risk Profile — искусственное присвоение статуса «высокий риск».**

Профиль клиента формируется не на основании транзакций и происхождения средств, а путём накопления фрагментарных или неподтверждённых сигналов в разных юрисдикциях. Внутренние банковские системы фиксируют такие отметки как постоянные, и даже после опровержения они сохраняются в risk-score моделях. В итоге лицо переходит в категорию «structurally high-risk» без возможности очистить репутацию. Это приводит к отказам в обслуживании в нескольких странах,

невозможности открыть новые счета и фактической утрате доступа к финансовой инфраструктуре.

## **6. Regulatory Ambiguity Exploitation — использование различий между режимами ЕС/UK/UAE/CH.**

Злоупотребление строится на том, что каждое государство имеет разные стандарты оценки FIU-запросов, freeze-мер и процедур обжалования. Инициатор использует наиболее уязвимые точки — например, отсутствие обязательного second-layer review в отдельных странах или различия в трактовке «предикатного состава». Сигнал проходит там, где фильтра меньше, и затем распространяется в более защищённые юрисдикции уже как «подтверждённый». Такой подход позволяет государству-инициатору добиваться трансграничного эффекта, не соблюдая даже минимальные стандарты доказательности.

## **7. Crypto-Chain Distortion — подмена цепочки транзакций для усиления подозрений.**

В этой схеме создаётся ложное представление о происхождении криптоактивов: используется адрес, который в глубине цепочки был связан с незаконными транзакциями, либо искусственно формируется пересечение потоков. Платформы и банки, полагающиеся на автоматические флаги, блокируют средства без полноценного chain-analysis. В результате легальные активы получают статус «компрометированных», а инвестор оказывается лишён доступа к стейблкоинам, биржевым кошелькам и P2P-платформам. Разблокировка занимает месяцы и требует независимой технической экспертизы.

## **8. Corporate TFR — использование транснационального давления в корпоративных конфликтах.**

Финансовые каналы применяются для захвата активов и перераспределения контроля между бизнес-группами. Сначала инициатор запускает административные проверки или медиаконтекст, затем — freeze через FIU-запрос, который блокирует оборотные средства в иностранных банках. Парализованная компания теряет платёжеспособность и вынуждена идти на уступки: передачу долей, смену менеджмента или снятие претензий. Формально всё выглядит как AML-процедура, фактически — как инструмент корпоративного давления с трансграничным эффектом.

# АНАЛИЗ ПО СТРАНАМ

## Россия

– Параллельные запросы Интерпола + FIU.

Российские органы одновременно запускают уведомления Интерпола (включая Diffusion и Blue Notice) и передают сигналы по FIU-каналам, даже если уголовное дело на ранней стадии или содержит политические признаки. Банки трактуют такие комбинированные сигналы как критический риск и автоматически блокируют счета, создавая эффект транснационального давления без формальных санкций.

– Freeze в ЕС/UK/CH на базе статей 159/160/199/210.

Даже стандартные экономические статьи — «мошенничество», «присвоение», «уклонение от налогов», «организация преступного сообщества» — используются как универсальный предлог. В зарубежных юрисдикциях эти формулировки воспринимаются как тяжкие финансовые преступления, что приводит к мгновенному freeze вне зависимости от стадии дела и наличия экспертиз.

– Exported Risk Files в банки ЕС и Ближнего Востока.

Российские материалы передаются как «информационные сигналы» без официального запроса, что позволяет избегать проверки на политическую мотивацию. Банки фиксируют такие метки в внутренних системах и затем распространяют их по корреспондентским сетям, формируя устойчивый международный профиль риска.

– Давление на эмигрантов, инвесторов, журналистов.

Freeze и offboarding используются как способ принуждения к возвращению, прекращению расследовательской деятельности или отказу от активов. Даже после прекращения дел восстановление доступа к средствам происходит частично и с длительными задержками, усиливая эффект изоляции.

## Казахстан

– FIU активно использует международные каналы Egmont.

Запросы направляются в банки ЕС, Швейцарии, ОАЭ и Турции в ускоренном режиме и часто на стадии проверки, когда предикат не установлен. Использование Egmont-каналов придаёт сигналу высокий уровень доверия, что приводит к автоматическим блокировкам за пределами страны.

– Freeze корпоративных активов за рубежом.

Блокируются счета дочерних компаний, холдингов и экспортных структур, что нарушает поставки, останавливает расчёты и приводит к потере контрактов. Заморозка применяется до судебных решений и нередко без подтверждённого ущерба, превращаясь в инструмент экономического давления.

– Давление на собственников крупных предприятий.

Риск особенно высок в строительстве, логистике, сырьевом секторе и агробизнесе. Freeze используется в качестве рычага для изменения корпоративного контроля, возврата акционеров в страну или принуждения к переговорам.

– Инструмент корпоративных войн.

Механизм позволяет одной бизнес-группе инициировать проверку через аффилированные структуры, после чего транснациональный freeze становится

элементом борьбы за активы. Даже после снятия блокировки последствия остаются необратимыми — от потери ликвидности до ухода с рынка.

## Узбекистан

– Freeze в UAE/Турции/ЕС.

Заморозки часто происходят за пределами страны в отношении семейных офисов, холдингов и недвижимости. Блокировка применяется как суррогат экстрадиции: возвращение предпринимателя в Узбекистан становится неофициальным условием «урегулирования».

– FIU-запросы без описания предиката.

Сообщения содержат общие формулировки вроде «иностранное финансирование» или «возможное незаконное обогащение» без фактов, сумм или экспертиз. Международные банки трактуют такие запросы как высокорисковые и запускают автоматический freeze.

– Перераспределение собственности через транснациональные механизмы.

Финансовые меры используются в борьбе элит и корпоративных конфликтах: сначала инициируется проверка, затем блокируются активы за рубежом, после чего предлагаются «переговоры». Отсутствие доступа к материалам делает оспаривание практически невозможным.

## Азербайджан

– Freeze против журналистов, НКО, оппозиционных фигур.

Замораживание активов применяется как первичная мера давления — без предъявления финансовых обвинений и до проведения экспертиз. Блокируются счета медиапроектов, правозащитников и независимых аналитиков, что приводит к остановке деятельности ещё до начала следственных действий. Freeze используется как быстрый инструмент нейтрализации без публичного процесса.

– Cross-border blocking в Грузии, Турции, ЕС.

Блокировки распространяются на зарубежные счета и грантовые поступления, особенно в соседних юрисдикциях, где размещены операционные структуры и личные активы. Использование оффшорных банковских сетей затрудняет оспаривание и создаёт долгосрочный эффект финансовой изоляции.

– Налоговые/валютные статьи используются как предикат.

Вместо прямых политических формулировок применяются статьи о «незаконном предпринимательстве», «валютных нарушениях» и «отмывании доходов». Это позволяет инициировать freeze без риска признания преследования политически мотивированным на международном уровне.

## Кыргызстан

– Freeze против журналистов и предпринимателей.

Блокировки вводятся до предъявления обвинений и используются для временной остановки деятельности — особенно в случаях расследований коррупции и конфликтов вокруг инфраструктурных проектов. Ограничения применяются точно, но становятся всё более повторяющимися.

– Давление через офшорные банковские каналы.

FIU-сигналы приводят к блокировкам на счетах в ОАЭ, Турции и ЕС, где размещены операционные средства и личные активы. Даже без доказательств банки сохраняют ограничения месяцами, что фактически превращает freeze в инструмент переговорного давления.

– Политизация AML.

Участие в гражданской активности, связь с международными фондами или публичная критика усиливают KYC-риски, даже при полностью легальной финансовой деятельности. AML-процедуры начинают выполнять функцию контроля без формального изменения законодательства.

## Беларусь

– Freeze на основании «экстремистской» и санкционной риторики.

Финансовые блокировки применяются к предпринимателям, медиа и НКО, признанным «экстремистскими» или «деструктивными структурами», даже без финансовых нарушений. Статус используется как автоматический триггер для ограничений, включая заморозку личных счетов.

– Трансграничные блокировки активов в ЕС/УК.

Запросы сопровождаются ссылками на санкционные риски, что делает банки особенно чувствительными. В результате замораживаются активы тех, кто не находится под санкциями, но ассоциирован с протестной деятельностью или независимыми проектами.

– Давление на предпринимателей, связанных с протестами.

Freeze используется как форма неформального наказания и принуждения к сотрудничеству: ограничиваются расчёты, останавливаются контракты, блокируются внешние переводы. Доступ к средствам восстанавливается избирательно и нередко после изменения поведения или выезда из страны.

## Таджикистан

– Freeze предпринимателей, связанных с диаспорой.

Блокировки применяются в отношении бизнес-фигурантов, проживающих за пределами страны или поддерживающих социальные проекты в диаспоре. Freeze вводится до возбуждения уголовного дела и используется как рычаг контроля над финансовыми потоками и возвращения предпринимателей в юрисдикцию.

– Использование уголовных и религиозных составов как предиката.

Вместо финансовых статей в качестве основания указываются «экстремизм», «незаконные религиозные объединения» или «угрозы национальной безопасности». Такие формулировки позволяют избегать международной проверки на политическую мотивацию и автоматически запускают блокировки в зарубежных банках.

– FIU-запросы переходят в банки РФ/Турции/ЕС.

Сигналы распространяются по транснациональным каналам без подтверждающих материалов, что приводит к автоматическим ограничениям на счетах в нескольких юрисдикциях. Доступ к документам отсутствует, а отмена freeze зависит не от суда, а от неформальных решений силовых структур.

## Туркменистан

– Непрозрачные FIU-запросы.

Финансовая разведка не раскрывает методологию, не предоставляет оснований и не публикует статистику, что исключает возможность проверки. Запросы направляются без указания предиката и используются для превентивного замораживания средств на неопределённый срок.

– Высокий риск nationality-based blocking.

Гражданство Туркменистана само по себе становится фактором риска в ЕС, Великобритании и ОАЭ, что приводит к отказам в onboarding, offboarding действующих клиентов и длительным KYC-блокировкам. Банки не могут верифицировать документы, что усиливает автоматические ограничения.

– Freeze применяется для контроля над экономикой.

Блокировки используются как инструмент регулирования доступа к валюте, импорту и крупным контрактам, особенно в строительстве и торговле. Мера выполняет административную функцию, позволяя государству сохранять монополию на ключевые финансовые потоки.

## Грузия

– Freeze, связанный с делами об иностранном влиянии.

Финансовые меры применяются в контексте расследований, связанных с иностранным финансированием и участием НКО в политически чувствительных темах. Блокировки

вводятся на ранних этапах, до предъявления обвинений, что парализует деятельность организаций.

– Давление на журналистов и активистов.

Медиа и гражданские инициативы сталкиваются с замораживанием счетов и приостановкой переводов в связи с «риском вмешательства». Ограничения используются как способ косвенного воздействия без прямого уголовного преследования.

– Использование AML в экономико-политических конфликтах.

В отдельных случаях AML-процедуры задействуются в корпоративных спорах, имущественных конфликтах и борьбе за контроль над активами. Freeze становится временным механизмом давления, особенно в проектах, связанных с иностранными инвесторами и стратегическими секторами.

## Молдова

– Freeze в делах, связанных с коррупцией и корпоративными конфронтациями.

Замораживание активов применяется в рамках антикоррупционных расследований и споров вокруг крупных предприятий, включая банковский сектор и энергетические проекты. В отдельных случаях freeze вводится на ранних стадиях, до установления ущерба, что превращает меру в инструмент давления на бенефициаров и управленцев.

– Политизация отдельных расследований.

Хотя формально меры направлены на укрепление правоприменения, отмечаются эпизоды, где финансовые ограничения совпадают с периодами политической турбулентности и борьбой за влияние внутри государственных структур. Такое пересечение создаёт риск восприятия AML как инструмента выборочного воздействия.

– Высокий риск из-за нестабильности институтов.

Несмотря на наличие реформ, слабость судебного надзора и частые изменения регуляторной среды приводят к тому, что международные банки относятся к клиентам из Молдовы с повышенной осторожностью. Это выражается в усиленных KYC-проверках, отложенных транзакциях и возможных offboarding в ЕС и Великобритании.

## Армения

– AML преимущественно используется корректно.

Армянская система финансового мониторинга считается одной из более стабильных в регионе и ориентирована на соответствие стандартам FATF и Moneyval. FIU демонстрирует институциональную автономию, а случаи злоупотреблений фиксируются ограниченно.

– Freeze встречается в налоговых и корпоративных делах.

Блокировки активов применяются преимущественно в спорах, связанных с уклонением от налогов, корпоративным управлением и регистрационными конфликтами. В большинстве ситуаций freeze сопровождается судебными процедурами и основан на документированных данных.

– Риски связаны с внешним КҮС-отношением банков.

Несмотря на внутреннюю корректность системы, клиенты из Армении могут сталкиваться с международными ограничениями из-за регионального контекста — близости высокорисковых юрисдикций, миграционных потоков и транзакций из зоны СНГ. Это приводит к повышенному scrutiny в ЕС/УК/СН и выборочным задержкам операций.

## ПРИМЕРЫ ИЗ ПРАКТИКИ

### 1. Российский бизнес-мигрант — IFCP схема

FIU РФ → ЕС банк → Freeze → Интерпол → отказ в обслуживании.

После инициирования проверки в России FIU направила сигнал в европейский банк без указания суммы ущерба и стадии дела. Банк автоматически заморозил счета, а через несколько недель был отправлен Diffusion Notice в Интерпол, что усилило восприятие риска. Несмотря на отсутствие красного уведомления и последующее прекращение дела, клиент столкнулся с offboarding и невозможностью открыть счета в других банках ЕС из-за сохранения внутренней метки «high-risk». Доступ к активам восстановлен частично спустя 14 месяцев.

### 2. Казахская компания — Corporate TFP

Корпоративный конфликт → FIU KZ → Freeze в СН/УАЕ → принудительная смена контролинга.

Конфликт акционеров сопровождался запросом FIU Казахстана в банки Швейцарии и ОАЭ с формулировкой «возможные финансовые нарушения». Несмотря на отсутствие судебного решения, были заблокированы оборотные средства дочерних компаний. Это привело к срыву экспортных контрактов и дефолту по обязательствам. После многомесячных переговоров контрольный пакет был передан другой группе, после чего freeze был снят без объяснений, что подтверждает использование финансовых мер как инструмента давления.

### 3. Узбекистан — Cross-Border Freeze

FIU UZ → банки УАЕ → блокировка семейных активов; доказательств нет.

Запрос FIU содержал общую формулировку о «возможном незаконном обогащении» без указания транзакций. Банки в ОАЭ заблокировали семейные счета и трастовые структуры, включая активы, не связанные с Узбекистаном. Юридический статус дела не менялся более года, доказательства не предоставлены, материалы проверки недоступны. Freeze стал фактическим механизмом воздействия, вынудив фигурантов вести переговоры об «урегулировании» в отсутствие уголовных обвинений.

#### **4. Азербайджан — Journalistic TFP**

Расследователь → обвинения в «отмывании» → Freeze → блокировка оборудования.

Через несколько дней после публикации материалов о коррупционных закупках журналист получил уведомление о блокировке банковских карт под предлогом «подозрения в отмывании доходов». Freeze привёл к изъятию оборудования, остановке проектов и невозможности финансирования через грантовые каналы. Финансовые меры применены до возбуждения дела и без выявления подозрительных транзакций, что сделало заморозку ключевым инструментом подавления деятельности.

#### **5. Кыргызстан — Media Pressure**

Журналисты → Freeze оборотных средств → прекращение деятельности.

Редакция, занимавшаяся расследованиями госзакупок, столкнулась с блокировкой счетов юридического лица и личных карт сотрудников. Формальное основание — «проверка поступлений из-за рубежа». Обвинения не предъявлены, но freeze сохранялся более шести месяцев, что привело к остановке публикаций, расторжению аренды и потере персонала. После снятия ограничений деятельность восстановить не удалось.

#### **6. Беларусь — Sanctions Shadowing**

Оппозиционная фигура → Freeze в ЕС/УК → давление через FIU.

Несмотря на отсутствие санкций в отношении лица, FIU использовала риторику «связей с экстремистскими структурами», что было трактовано банками ЕС и Великобритании как высокий санкционный риск. Заморожены личные и корпоративные счета, заблокированы внешние переводы. Формальных обвинений не последовало, однако ограничения сняты только частично, что иллюстрирует использование санкционного дискурса для косвенного давления.

#### **7. Таджикистан — Diaspora Targeting**

Бизнесмен за рубежом → FIU TJ → Freeze в Турции и ЕС.

Фигурант проживал вне страны и имел предприятия в сфере логистики и строительства. После отказа от «добровольного возвращения» FIU Таджикистана отправила сигнал в банки Турции и ЕС с формулировкой «возможное финансирование запрещённых структур». Несмотря на отсутствие уголовного дела и документальных подтверждений, были заморожены личные и корпоративные счета. Доступ к материалам отказан, а снятие freeze зависело от неформальных переговоров. Ограничения длились почти год, привели к разрыву контрактов и вынужденной продаже активов.

## **8. Туркменистан — Nationality-Based Blocking**

Клиент → автоматический KYC-отказ → Freeze без запроса FIU.

Гражданин Туркменистана попытался открыть счёт в европейском банке после релокации бизнеса. Система автоматического scoring присвоила статус «high-risk nationality», что привело к отказу в обслуживании без проверки источника средств. Через несколько недель существующие счета в другой юрисдикции были заморожены «в целях дополнительной проверки», хотя FIU Туркменистана не направляла запросов. Freeze продолжался 9 месяцев, доказательств нарушений не выявлено, но клиент не смог восстановить доступ к международным платёжным каналам.

## **9. Грузия — Foreign Influence AML**

Активист → FIU GE → Freeze после критических публикаций.

После участия в кампании против законопроекта об иностранном влиянии активист столкнулся с запросом FIU о проверке поступлений из-за рубежа. Блокировка счёта была введена до получения документов и без указания суммы или предиката. Freeze повлёк остановку проектов и невозможность оплачивать аренду и командировки. Уголовное дело не возбуждено, но ограничения сняты только спустя 5 месяцев, что демонстрирует использование AML-процедур в политически чувствительных ситуациях.

## **10. Молдова — Corporate AML Weaponization**

Корпоративный конфликт → предикат «коррупция» → Freeze внешних счетов.

Спор между двумя акционерами энергетической компании сопровождался заявлением о возможных коррупционных платежах. Несмотря на отсутствие экспертизы, FIU направила запросы в банки ЕС, что привело к заморозке зарубежных счетов дочерних структур. Операционные расчёты остановились, контракты сорвались, а один из акционеров был вынужден выйти из управления. Позднее расследование не подтвердило нарушений, но восстановление доступа к активам заняло более года.

## **11. Армения — Economic Freeze**

Спор о налогах → Freeze до проверки.

Компания была включена в проверку по предполагаемому занижению налоговых обязательств. До завершения аудита и без судебного решения был наложен freeze на корпоративный счёт. Ограничения привели к задержке выплат поставщикам и приостановке производства. После завершения проверки нарушение не подтвердилось, но банк сохранил метку «elevated risk», что вызвало отказ в открытии счетов в другой юрисдикции.

## **12. Международный кейс ARGA — Crypto Distortion**

USDT транзакции → ошибочная цепочка → Freeze 90 дней → снято после chain analysis.

Транзакции клиента были автоматически помечены как связанные с «высокорисковым адресом» из-за присутствия в цепочке старого кошелька, ранее фигурировавшего в расследовании. Платформа заблокировала активы на 90 дней и потребовала подтверждения происхождения средств, но отказалась предоставить техническое обоснование. Независимый chain analysis подтвердил законность транзакций, после чего freeze сняли, однако клиент потерял доступ к ликвидности и понёс финансовые убытки из-за волатильности.

## КАРТА РИСКОВ

Страна	Риск для банков	Риск для FIU	Уровень TFP
Россия	CRITICAL	CRITICAL	Strongly Systemic
Казахстан	VERY HIGH	HIGH	Systemic
Азербайджан	VERY HIGH	VERY HIGH	Systemic
Узбекистан	HIGH	VERY HIGH	Systemic
Беларусь	HIGH	VERY HIGH	Systemic
Таджикистан	HIGH	VERY HIGH	Systemic
Туркменистан	VERY HIGH	VERY HIGH	Opaque Systemic
Кыргызстан	MEDIUM	MEDIUM	Partially Systemic
Грузия	MEDIUM	MEDIUM	Mixed
Молдова	MEDIUM	MEDIUM	Reforming
Армения	MEDIUM	LOW	Stable with External Risks

## «КРАСНЫЕ ФЛАГИ»

### 1. FIU Exported Alert

Сигнал, отправленный национальной FIU в зарубежный банк, содержит размытые формулировки, отсутствует предикат, сумма ущерба или документы. Такие уведомления запускают автоматические freeze-процедуры, даже если уголовное дело отсутствует или находится на стадии проверки.

### 2. No Predicative Offence

Заморозка активов применяется без указания предикатного состава — нет статьи, фактов транзакций, экспертизы или потерпевшего. Freeze фактически превращается в предварительное наказание, при котором проверка проводится уже после введения ограничений.

### 3. Freeze-before-investigation

Блокировка активов происходит до возбуждения дела, аудита или финансово-экономической экспертизы. Механизм используется для давления в корпоративных,

политически чувствительных или административных конфликтах, а не для предотвращения отмывания.

#### **4. Parallel Interpol Use**

FIU-запрос сопровождается уведомлением Интерпола (Blue, Diffusion или попыткой Red Notice), что усиливает восприятие риска банками. Даже если уведомление отклонено или отозвано, последствия в финансовой системе сохраняются месяцами.

#### **5. Sanctions-Mimicking**

Создание искусственной ассоциации с санкционными рисками при отсутствии санкций. Используются формулировки о «связях с экстремистскими структурами» или «иностранным влиянием», чтобы спровоцировать автоматические ограничения в ЕС/UK/CH/UAE.

#### **6. Crypto Chain Distortion**

Ошибочная трактовка цепочки транзакций в блокчейне: перенос «грязного» статуса с предыдущих адресов, отсутствие chain analysis, использование неточных баз рисков кошельков. В результате блокируются законные активы на 60–120 дней.

#### **7. Corporate TFP**

Транснациональное давление в корпоративных конфликтах: инициируются FIU-запросы, freeze применяется к оборотным средствам, после чего предлагается «урегулирование» через смену контроля или передачу долей. Судебные механизмы обходятся финансовыми.

#### **8. High-Risk Labeling by Nationality**

Клиент автоматически получает статус «высокий риск» из-за гражданства или происхождения средств, без анализа транзакций. Это приводит к отказам в onboarding, внезапным offboarding, задержкам переводов и заморозкам без запросов FIU.

## **РЕКОМЕНДАЦИИ**

### **OFAC**

#### **– Second-layer verification for TFP-pattern countries**

Ввести обязательную дополнительную проверку для запросов, исходящих из государств, где зафиксированы схемы транснационального давления. Freeze-решения должны приниматься только после верификации фактов, а не на основании первичного сигнала.

#### **– Refusal to act on FIU alerts without predicative offence**

Не применять ограничительные меры по FIU-уведомлениям, в которых отсутствует описание предиката, сумма ущерба, стадия дела или документальные подтверждения.

Любой freeze без предикатного состава должен рассматриваться как нарушение стандартов due process.

## EU DG FISMA

### – **Classify selected FIU as high-risk sources**

Определённые подразделения финансовой разведки стран СНГ должны быть отнесены к источникам повышенного риска, что потребует дополнительной проверки и невозможности автоматической обработки их сигналов.

### – **Mandatory explanation of predicative offence**

FIU-запросы из третьих стран должны приниматься только при наличии полного описания состава: фактов, сумм, транзакций, стадии расследования и ссылок на документы.

### – **Enhanced screening of CIS-origin alerts**

Ввести специализированный протокол аналитического фильтра для сигналов из региона, включающий оценку политического контекста, корпоративных триггеров и риска искусственного профилирования.

## FATF

### – **Introduce Transnational AML Abuse metric**

Добавить отдельный индикатор в страновые оценки для выявления транснационального использования AML-механизмов вне их легитимной цели — включая FIU-экспорт сигналов и freeze-меры без ущерба.

### – **Evaluate politicization of FIU activity**

При взаимных оценках учитывать степень независимости FIU, наличие давления со стороны силовых структур и использование финансовых мер в политически мотивированных делах.

## FIU (EU/UK/UAE/CH)

### – **Reject blank requests**

Не рассматривать запросы без предикатного состава, описания транзакций, суммы вероятного ущерба и документальных приложений.

### – **Require independent evidence packages**

Принимать к анализу только те уведомления, которые включают подтверждающие материалы, а не предположения или формулировки общего характера.

## Banks

### – Apply TFP EDD Protocol

Внедрить усиленную проверку клиентов из стран с выявленными TFP-схемами, включая анализ контекста, проверку статуса дела и независимое подтверждение риска.

### – Political context analysis

Учитывать вероятность политической мотивации, особенно при запросах в отношении журналистов, НКО, эмигрантов и бенефициаров корпоративных конфликтов.

### – Reject freeze actions without evidence

Не вводить блокировки активов на основании сигналов без фактов, экспертиз и документированных оснований; замораживание должно быть крайней мерой, а не автоматическим действием.

## ВЫВОД

Транснациональное давление через финансовые каналы формирует новую форму внеюрисдикционного контроля, при которой государства используют AML/CTF-механизмы, FIU-запросы, банковские процедуры KYC/EDD и замораживание активов не для защиты финансовой системы, а для воздействия на предпринимателей, журналистов, активистов и инвесторов за пределами своей территории.

Ключевой риск заключается в том, что такие меры применяются без предикатного состава, без доказательств и без судебного надзора, а международные банки становятся произвольным инструментом давления — через автоматические блокировки, отказ в обслуживании и формирование искусственного «высокого риска».

Доклад фиксирует, что отсутствие глобальных фильтров, несогласованность стандартов и зависимость банков от внешних сигналов создают системную уязвимость, позволяющую экспортировать политически мотивированные решения в финансовую сферу других государств.

Необходима международная координация: введение механизмов проверки FIU-уведомлений, отказ от freeze-мер без предиката, учёт политического контекста и создание протоколов защиты от злоупотреблений. Без этих шагов транснациональные финансовые меры будут и дальше подрывать доверие к AML-режиму, усиливая риск незаконной изоляции и разрушения экономической деятельности за пределами национальных границ.

## ИСТОЧНИКИ

1. OECD, Illicit Financial Flows from Developing Countries, 2014, [https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/04/illicit-financial-flows-from-developing-countries\\_g1g331b9/9789264203501-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/04/illicit-financial-flows-from-developing-countries_g1g331b9/9789264203501-en.pdf).
2. FATF, Trade-Based Money Laundering, March 2021, [https://www.fiu-nederland.nl/wp-content/uploads/2022/03/202103\\_fatf\\_trade-based-money-laundering-risk-indicators-1.pdf](https://www.fiu-nederland.nl/wp-content/uploads/2022/03/202103_fatf_trade-based-money-laundering-risk-indicators-1.pdf).
3. FATF Report, Global Money Laundering & Terrorist Financing Threat Assessment, July 2010, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Global%20Threat%20assessment.pdf>.
4. IFC, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, 2019, <https://www.ifc.org/content/dam/ifc/doc/mgrt/45464-ifc-aml-report.pdf>.