

AML нашего времени

Успех финансового мониторинга в условиях новых угроз зависит от построения контура цифровой устойчивости и системного подхода к развитию IT-инфраструктуры и кадрового потенциала



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Прошло уже полтора года с момента сообщения МВД о совместном со Сбербанком выявлении и задержании сотрудниками спецслужб в начале 2025 года организаторов нелегальной платежной системы Rapidpay. По информации «Ъ», через нее прошло около 700 млн рублей, а ее услугами пользовались интернет-казино, пункты обмена криптовалют, букмекерские конторы, колл-центры мошенников и даже блогеры. Во время обысков у фигурантов обнаружили реквизиты более 8,5 тыс. банковских карт, оформленных на дропперов.

А в июне 2025 года, после того, как прокуратура США предъявила сильно политизированные обвинения россиянину **Юрию Гугнину,** основа-

телю криптовалютной компании Evita, в отмывании 530 млн долларов США, стало понятно еще одно обстоятельство. И заключается оно в том, что по обе стороны океана стражи закона начали больше полагаться на мощные AML-системы, нежели на классические «аналоговые» методы финансовой разведки как в фиатном, так и криптовалютном секторах.

Италия получила карту, а Казахстан — по ломбарду

И только в марте 2026 года Федеральная служба по финансовому мониторингу (Росфинмониторинг) начала осторожно в назидание и в предостережение «джентльменам удачи» приоткрывать свои секреты. Но чтобы понять масштаб проблем и сложность задач, финансовая разведка на своих информационных ресурсах дает анализ международного контекста, по которому можно судить о тенденциях и внутри нашей страны. Вот некоторые факты за первое полугодие 2026 года.

- Исполнительный директорат Контртеррористического комитета СБ ООН (КТИД) провел брифинг о роли пропаганды в привлечении средств для финансирования терроризма и в борьбе с этой угрозой. Эксперты рассказали о совместной работе с ФАТФ по изучению тенденций финансирования терроризма, в том числе в контексте обновленного в 2025 году Отчета о рисках. Отмечено, что пропаганда направлена на привлечение доноров и распространение инструкций о том, как внести финансовый вклад. Информационные кампании проводятся через соцсети, приложения, СМИ и личный контакт.
- По результатам взаимной оценки ФАТФ, которая проводилась с июня по июль 2025 года, установлено, что Италия не уделяет должного внимания мерам противодействия финансированию терроризма. В частности, речь идет о переводах небольших сумм и использовании преступниками собственных средств. Отмечается, что прокуроры успешно добиваются обвинительных приговоров по таких делам, однако санкции, налагаемые на преступников, не имеют сопоставимой с нарушениями жесткости. Италия получила дорожную карту, где описаны меры, которые стране необходимо предпринять в течение трех лет для устранения всех недочетов.
- Агентство Республики Казахстан по финансовому мониторингу (АФМ) окончило расследование по факту незаконной предпринимательской деятельности в ломбардной сфере. Фигурант организовал систему предоставления займов населению под залог техники без обязательной лицензии. Деятельность велась под видом комиссионных магазинов, что позволяло обходить регулирование со стороны уполномоченных органов. Злоумышленник устанавливал завышенные процентные ставки, достигающие 3,7% в день, что в 12 раз превышало законодательно установленный предел 0,3%. Но это еще не всё! АФМ 29 апреля 2026 года заморозила цифровые активы на сумму более 9,7 млн USDT по делу одного из крупнейших теневых криптосервисов СНГ RAKS Exchange. Установлено, что через данный обменник проходили транзакции более 200 наркомаркетов, действовавших на территории Казахстана, России, Украины и Молдовы, а общий оборот платформы превысил 224 млн долларов. В ходе масштабного крипторасследования по принципу Follow the Money осуществлен блокчейн-анализ свыше 4 тыс. криптокошельков, связанных с незаконным оборотом наркотических средств и деятельностью даркнет-площадок.
- Управление по финансовому регулированию и надзору Великобритании (FCA) провело первую скоординированную операцию по пресечению незаконной торговли криптовалютой. Проведены проверки в отношении восьми компаний в Лондоне, по итогам которых выданы предписания о прекращении деятельности. Власти отмечают риски, связанные с использованием цифровых активов для отмывания преступных доходов.

В глобальном масштабе картина в докладе ФАТФ «Кибермошенничество. цифровизация и риски ОД/ФТ/ФРОМУ», опубликованном в феврале 2026 года, выглядит так: «В 156, или в 90%, оцененных юрисдикций прямо указывают мошенничество как значительный риск отмывания денег. Масштабы мошенничества продолжают расти. Например, только в Сингапуре число случаев кибермошенничества увеличилось на 61% за два года. В Соединенном Королевстве мошенничество в настоящее время составляет более 40% всех преступлений. В ряде стран до 15% взрослого населения становились жертвами кибермошенничества, что подчеркивает широкий масштаб и растущий характер этой угрозы. Хотя общий объем потерь от мошенничества, включая ущерб, причиненный физическим лицам, предприятиям и государственным финансам, невозможно точно определить, только в Соединенных Штатах Америки он составляет как минимум десятки миллиардов долларов ежегодно».

Почем безопасность?

С 27 по 30 апреля 2026 года в Новосибирске в Межрегиональном управлении Росфинмониторинга по Сибирскому федеральному округу прошел семинар по вопросам организации проведения финансовых расследований, на котором была обнародована некоторая информация.

Открывая семинар, первый заместитель директора ведомства **Олег Крылов** подчеркнул важность развития межведомственного сотрудничества, единого понимания рисков и объединения усилий по их минимизации, а также важность обмена практиками в сфере борьбы с отмыванием денег

В Сингапуре число случаев кибермошенничества увеличилось на 61% за два года. В Соединенном Королевстве мошенничество в настоящее время составляет более 40% всех преступлений. В ряде стран до 15% взрослого населения становились жертвами кибермошенничества

и финансированием терроризма в контексте подготовки российской антиотмывочной системы к очередному раунду взаимных оценок ФАТФ.

«Развитие цифровых технологий ставит перед финансовой разведкой новые задачи. Сегодня мы отмечаем такие тенденции, как использование цифровых активов, криптовалют при совершении преступлений, в том числе связанных с отмыванием денег и финансированием терроризма. Для борьбы с новыми вызовами в антиотмывочной сфере необходимо консолидировать усилия … внедрять инновационные решения и подходы в работу Службы», — сказал Олег Крылов.

Среди ключевых рисков были выделены:

- транснациональная организованная преступность, в том числе мошенничество, хищение бюджетных средств и коррупция;
- незаконный оборот наркотических средств;
- терроризм и экстремизм.

Встает вопрос: какова цена этих рисков и насколько оправданы инвестиции в построение впечатляющих своими масштабами и производительностью AML-систем?

На этот вопрос в 49-м выпуске журнала «Финансовая безопасность» от 2026 года ответил **Антон Лисицын,** заместитель директора Росфинмониторинга: «Массовые утечки данных, рост числа дипфейк-атак и телефонного мошенничества подрывают доверие граждан к цифровым финансовым сервисам. Это создает системный риск для цифровизации финансового сектора — стратегического приоритета государственной политики. Для Росфинмониторинга это означает, что мы рискуем не только данными, но и национальной безопасностью — согласно экспертным данным, один час простоя AML-системы (ЕИС Росфинмониторинга) обходится в 500 млн рублей (по данным за 2022 год)».

Понятно, что все это предъявляет принципиально новые требования к национальной системе противодействия отмыванию доходов и финансированию терроризма и заставляет регуляторов создавать цифровую оборону нового поколения, которая выстраивается на основе цифровой трансформации национальной системы ПОД/ФТ как стратегический приоритет на 2024–2026 годы. Это отражено в официальной декларации «Стратегические цели Росфинмониторинга на 2024–2026 годы».

Среди задач:

- развитие цифровых сервисов в сфере ПОД/ФТ;
- повышение эффективности аналитических инструментов;
- совершенствование информационных технологий финансового мониторинга;
- развитие оценки рисков и кадрового потенциала.

По мнению экспертов Службы, основной вызов на ближайшие годы — стремительное развитие технологий. Современные инструменты, такие как генеративный искусственный интеллект, дипфейки, решения на базе Web3 и модель «Cybercrime-as-a-Service», значительно упрощают доступ преступников к сложным атакам и повышают их эффективность.

В этих условиях отечественная государственная система обладает потенциалом не только оперативно реагировать на возникающие угрозы, но и выстраивать проактивную защиту финансового суверенитета в условиях цифровой трансформации. Ключевыми факторами успеха станут скорость внедрения передовых технологий, качество межведомственного взаимодействия и повышение финансовой грамотности граждан.

Что «под капотом»?

Резюмируя публикацию Антона Лисицына, касающуюся деталей IT-инфраструктуры, которая обеспечивает финансовую безопасность страны, можно выделить следующие факты.

В последние годы единая информационная система Росфинмониторинга трансформировалась из базового инструмента сбора и обработки данных в полноценную цифровую экосистему, поддерживающую все ключевые задачи ведомства. Внедрены инновационные IT-решения, включая собственную языковую модель ИИ (2025 год), что позволило автоматизировать анализ больших объемов информации, выявлять признаки финансовых нарушений и минимизировать человеческий фактор.

Сегодня система функционирует как самостоятельная экосистема, обеспечивающая интеграцию с ведомственными базами данных, оперативный

Один час простоя AML-системы Росфинмониторинга обходится в 500 млн рублей

обмен информацией и анализ транзакций на предмет отмывания денег и финансирования терроризма. В планах — расширение международного взаимодействия, внедрение машинного обучения и развитие Международного центра оценки рисков (МЦОР), который аккумулирует лучшие практики и укрепляет сотрудничество со странами СНГ.

Особое внимание уделено технологиям блокчейна и сервису «Прозрачный блокчейн», позволяющему идентифицировать участников криптовалютных операций и отслеживать их активность. Это стало важным инструментом для мониторинга оборота криптовалют и подготовки законодательного регулирования.

Для безопасного обмена чувствительной информацией с зарубежными партнерами создана уникальная защищенная система обмена данными, исключающая компрометацию информации. В ближайшее время круг участников этой системы будет расширен для повышения эффективности международного сотрудничества.

В числе вызовов — дефицит квалифицированных кадров в сфере кибербезопасности и финансовой разведки. Для решения этой задачи реализуются масштабные образовательные инициативы, включая Международную олимпиаду по финансовой безопасности.

Мы видим и в «цифровой тени»

Понятно, что в одиночку даже с такой продвинутой IT-инфраструктурой Росфинмониторинг один в поле не воин, он всегда действует в кооперации с другими силовыми подразделениями, в частности с киберразведкой, о деятельности которой в публичном пространстве сведений меньше, чем о самих финансовых разведчиках.

Но так уж случилось, что 49-й номер упоминавшегося журнала украсила статья **Сергея Кондратьева** (старшего оперуполномоченного по особо важным делам отдела по противодействию имущественным преступлениям, совершенным в сфере компьютерной информации, МВД, подполковника полиции) и **Артема Чозгияна** (оперуполномоченного этого же отдела МВД, лейтенанта полиции) «Киберпатрулирование и мониторинг даркнета». В этой публикации представители МВД России акцентировали внимание на том, что одним из ключевых инструментов обогащения преступников сегодня является даркнет — анонимизированный сегмент интернета. Здесь размещаются предложения о так называемых бизнес-проектах, под прикрытием которых вербуются российские граждане для оказания локальной поддержки преступной инфраструктуре, в том числе для вывода крупных денежных средств за границу. Кроме того, в даркнете можно найти предложения о продаже банковских карт, оформленных на подставных лиц, а также существуют тематические сообщества, где происходят обмен опытом и распространение новых схем мошенничества.

Для противодействия этим угрозам в структуре МВД России действует специализированное подразделение — Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России). Это головное подразделение по борьбе с киберпреступностью, которое применяет современные методы работы, в том числе киберпатрулирование.

Данная практика представляет собой систематический и непрерывный мониторинг, анализ и контроль противоправной активности в цифровой среде, включая даркнет. Такой подход позволяет не только реагировать на уже совершенные преступления, но и выявлять и пресекать их на стадии подготовки.

Особую эффективность киберпатрулированию придает использование собственного специализированного ПО. IT-системы способны анализировать большие массивы данных, выявлять скрытые связи между участниками преступных сетей и прогнозировать их дальнейшие действия. Благодаря высоким технологиям (Hi-Tech) правоохранительная деятельность приобретает проактивный характер и позволяет действовать на опережение.

Результаты такой работы уже очевидны: в 2025 году впервые в современной истории России было зафиксировано снижение количества массовых финансовых преступлений, совершаемых с использованием информационно-коммуникационных технологий (ИКТ). Этот успех напрямую связан с переходом от реактивного реагирования к постоянному технологически оснащенному мониторингу цифрового пространства.

В завершение представители МВД подчеркнули, что в условиях, когда финансовая преступность все глубже уходит в «цифровую тень», эффективная защита общества и государства возможна только при переходе к проактивной модели противодействия. Киберпатрулирование и мониторинг даркнета с использованием собственных ИКТ-решений становятся не просто инструментами раскрытия преступлений, а стратегическим ресурсом обеспечения национальной финансовой безопасности. Снижение уровня массовых киберпреступлений — наглядное подтверждение того, что технологически оснащенное правоохранительное присутствие в даркнете способно разрушать преступную инфраструктуру еще до того, как она нанесет ущерб гражданам и экономике страны.

Итак, работа проводится колоссальная. Чего удалось достичь? «Банки и финорганизации России в 2025 году предотвратили вывод в теневой оборот более 400 млрд рублей благодаря принятым заградительным мерам. Финансовый сектор хорошо исполняет требования антиотмывочного законодательства, активно сотрудничает с финансовой разведкой и передает ей данные о подозрительных операциях», — заявил статс-секретарь, заместитель директора Росфинмониторинга **Герман Негляд.** Б.О