



ПРЕЗИДЕНТ РОССИЙСКОЙ
АКАДЕМИИ НАУК

**ГЕННАДИЙ
КРАСНИКОВ:**

«Мы являемся свидетелями того, как научно-технологический прогресс меняет привычный окружающий нас мир. Огромное значение обретает просветительство в вопросах внедрения новых технологий, применение опыта наших разработчиков, исследователей»

ВСТУПИТЕЛЬНОЕ СЛОВО



ЮРИЙ ЧИХАНЧИН

Директор Росфинмониторинга,
председатель редакционного совета



УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Сегодня мы не можем представить мир без высоких технологий. Они проникли практически во все сферы жизни, стали частью нашей повседневной деятельности. Финансовые технологии позволяют нам совершить покупку в один клик, не посещая магазин, перевести деньги, оплатить услуги, оформить кредит. Это удобно и экономит время.

Тренд на цифровизацию напрямую затронул и деятельность государственных органов. Росфинмониторинг, как большинство других ведомств, в своей работе активно использует возможности ИТ-инструментов.

Например, наша Служба взаимодействует с субъектами антиотмывочной системы через личный кабинет на сайте Росфинмониторинга. Ежедневно мы получаем от них порядка миллиона сообщений и уже в течение нескольких часов с момента поступления даем обратную связь. Конечно, такой объем информации невозможно обработать вручную.

Но надо понимать, что за этими технологиями стоят люди, которые их создали. Искусственный интеллект, какими бы колоссальными возможностями ни обладал, — это только помощник. Решение всегда принимает человек.

Вместе с развитием высоких технологий значительно воз-

росли и риски их использования в противоправных целях. ИИ и другие ИТ-разработки взяли на вооружение злоумышленники, применяя их в хищении средств, отмывании денег, финансировании терроризма, незаконном обороте наркотиков, оружия и при совершении других деяний. При этом масштабы киберпреступности приобрели транснациональный характер.

Поэтому сегодня так важно объединять усилия международного сообщества, органов государственной власти, частного сектора и гражданского общества в борьбе с новыми вызовами и угрозами.

На страницах этого журнала представлены практики применения цифровых инструментов и искусственного интеллекта в работе госорганов и банков в России и за рубежом, отдельные аспекты регулирования рынка финансовых услуг, опыт выявления и пресечения правонарушений, совершаемых в киберпространстве и с использованием высоких технологий. Также обсуждаются актуальные вопросы информационной безопасности и использования криптовалют.

Мы предлагаем читателям погрузиться в мир высоких технологий и еще раз задуматься об их роли в нашей жизни.



СОДЕРЖАНИЕ

6 ГЕННАДИЙ КРАСНИКОВ

Приветствие читателям
журнала «Финансовая
безопасность»

Высокие технологии на службе финансовой безопасности

8 АНТОН ЛИСИЦЫН

Борьба с легализацией
преступных доходов
и финансированием
терроризма в мире цифровых
технологий: вызов времени

11 Г-Н КЕШАВ АНАНД, Г-ЖА М. ШАНМУГА ПРИЯ

Развитие финтеха в Индии:
курс на инновации,
финансовую безопасность и
борьбу с киберпреступностью

15 ЮРИЙ КОРОТКИЙ:

«Финансовый мониторинг —
это в своем роде финансовая
томография»

19 ОТАБЕК РАХМАНОВ

Регулирование рынка
финансовых технологий
в контексте ПОД/ФТ: опыт
Узбекистана

24 ВИКТОРИЯ КАПАРЧУК, ЯНА БАЙРАЧНАЯ, АЛЕКСАНДР КУРЬЯНОВ

Использование цифровых
технологий в надзорной
деятельности

31 ДИНАРА МУСИНА

Реестр бенефициарных
собственников: опыт
Казахстана

Искусственный интеллект и финтех: о настоящем и будущем

35 СВЕТЛАНА ОРЛОВА:

«Цифровые продукты
и решения — это
уверенные шаги
к развитию государственного
финансового аудита»

39 ВИКТОР ДОСТОВ

Искусственный интеллект
в финансах и его влияние
на некоторые аспекты
ПОД/ФТ



11

Г-Н КЕШАВ АНАНД, Г-ЖА М. ШАНМУГА ПРИЯ

Развитие финтеха в Индии: курс на инновации,
финансовую безопасность и борьбу
с киберпреступностью

15

ЮРИЙ КОРОТКИЙ:

«Финансовый
мониторинг —
это в своем роде
финансовая
томография»



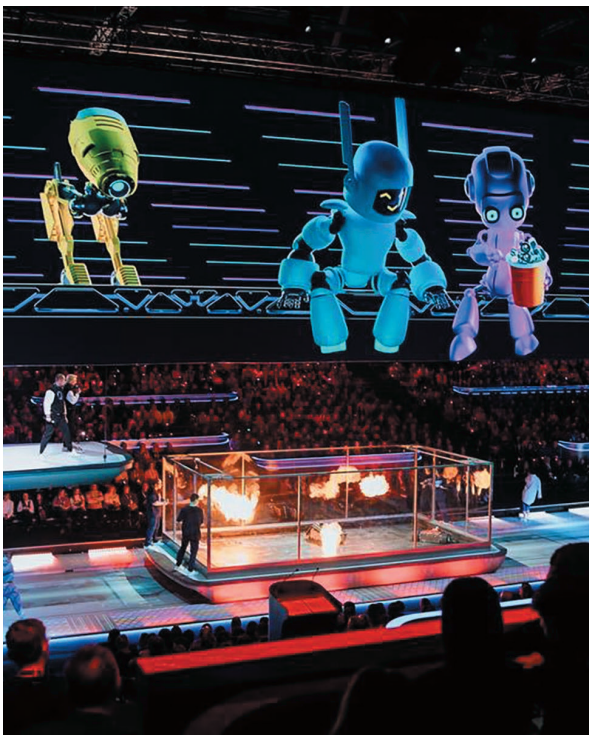
35

СВЕТЛАНА ОРЛОВА:

«Цифровые продукты
и решения —
это уверенные
шаги к развитию
государственного
финансового аудита»



68 **ОЛЬГА ТИСЕН**
Правовое регулирование оборота виртуальных активов и противодействия их использованию в целях ОД/ФТ в отдельных странах ЕАГ



43 **МИХАИЛ ПРОНИН**
Применение искусственного интеллекта в работе службы финансового мониторинга банка

46 **АЛЕКСЕЙ ГЕЛЕТА:**
«Финтех-рынок России можно назвать одним из наиболее инновационных и технологически продвинутых в мире»

Выявление и пресечение киберпреступлений

50 **БОГДАН ШАБЛЯ**
Противодействие «дропам» и высокорисковым р2р-операциям — приоритетный вектор финансового мониторинга

53 **ВАДИМ УВАРОВ**
Информационная безопасность на финансовом рынке: вопросы противодействия кибермошенничеству при переводах денежных средств

57 **АНТОН РАСТАЩЕНОВ**
Досудебное ограничение доступа в сети Интернет к информации, распространение которой на территории Российской Федерации запрещено

60 **РОМАН МУХЛЫНОВ**
Актуальные тренды на рынке нелегальных поставщиков финансовых услуг

63 **ОЛЕГ КИПКАЕВ**
Использование цифровых технологий в сборе, обработке и обобщении информационно-аналитических и иных данных, используемых в прокурорской деятельности, на примере функциональных возможностей информационно-аналитической системы «Электронный кабинет прокурора»

Криптовалюта: в поисках решений

68 **ОЛЬГА ТИСЕН**
Правовое регулирование оборота виртуальных активов и противодействия их использованию в целях ОД/ФТ в отдельных странах ЕАГ

73 **ДМИТРИЙ МАЧИХИН**
AML-расследования в WEB3-индустрии

77 **ШОН МУНИР**
Работа с цифровыми активами: криптовалюта, NFT и финансовая безопасность

Трибуна молодых специалистов

80 **СОФЬЯ РУДКОВИЧ**
О необходимости правового регулирования деятельности провайдеров услуг виртуальных активов в целях ПОД/ФТ во всех странах мира

Новости антиотмывочной системы

84 «Игры Будущего». Победители турнира «Кубок четырех континентов» посетили Казань

85 Состоялось первое заседание Совета БРИКС по противодействию отмыванию доходов и финансированию терроризма в расширенном составе

85 Вопросы финансовой безопасности обсудили на Всемирном фестивале молодежи

84 **«ИГРЫ БУДУЩЕГО». ПОБЕДИТЕЛИ ТУРНИРА «КУБОК ЧЕТЫРЕХ КОНТИНЕНТОВ» ПОСЕТИЛИ КАЗАНЬ**

ПРИВЕТСТВИЕ ЧИТАТЕЛЯМ ЖУРНАЛА «ФИНАНСОВАЯ БЕЗОПАСНОСТЬ»



ГЕННАДИЙ КРАСНИКОВ,
президент РАН,
академик РАН



УВАЖАЕМЫЕ ЧИТАТЕЛИ!

В этом году Российская академия наук отмечает 300 лет со дня своего основания. Празднуя этот значимый юбилей, мы вспоминаем не только славные страницы истории отечественной науки, но и смотрим в будущее. Наши ученые трудятся над задачами, связанными с укреплением научно-технологического суверенитета России, достигают важных результатов в самых передовых областях науки.

Отмечу, что сегодня все мы являемся свидетелями того, как научно-технологический прогресс меняет привычный окружающий нас мир. Огромное значение обретает просветительство в вопросах внедрения новых технологий, применение опыта наших разработчиков, исследователей.

В этой связи очень важно, что журнал «Финансовая безопасность» ориентирован не только

на профильных специалистов. Он также позволяет и широкому кругу читателей разобраться в сложнейших темах обеспечения кибербезопасности, узнать о перспективах использования искусственного интеллекта в финансовой сфере, а также о рисках, которые несет его широкое внедрение.

Рассчитываю, что на страницах этого издания читатели найдут статьи ведущих отечественных и зарубежных исследователей, экспертов, представителей органов государственной власти, а также смогут больше узнать о том, как в дальнейшем будут развиваться процессы цифровизации экономики и финансов.

Желаю вам здоровья, новых ярких успехов и, конечно, всего самого доброго.





ВЫСОКИЕ ТЕХНОЛОГИИ НА СЛУЖБЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

8 АНТОН ЛИСИЦЫН

Борьба с легализацией преступных доходов и финансированием терроризма в мире цифровых технологий: вызов времени

11 Г-Н КЕШАВ АНАНД, Г-ЖА М. ШАНМУГА ПРИЯ

Развитие финтех в Индии: курс на инновации, финансовую безопасность и борьбу с киберпреступностью

15 ЮРИЙ КОРОТКИЙ:

«Финансовый мониторинг — это в своем роде финансовая томография»

19 ОТАБЕК РАХМАНОВ

Регулирование рынка финансовых технологий в контексте ПОД/ФТ: опыт Узбекистана

24 ВИКТОРИЯ КАПАРЧУК, ЯНА БАЙРАЧНАЯ, АЛЕКСАНДР КУРЬЯНОВ

Использование цифровых технологий в надзорной деятельности

31 ДИНАРА МУСИНА

Реестр бенефициарных собственников: опыт Казахстана

БОРЬБА С ЛЕГАЛИЗАЦИЕЙ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА В МИРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ВЫЗОВ ВРЕМЕНИ

Цифровизация всех процессов в обществе становится все более значимой в современном мире, принося одновременно новые возможности и вызовы для различных отраслей и секторов экономики. Рост и развитие цифровых технологий, таких как интернет, мобильные приложения, облачные вычисления, большие данные и искусственный интеллект, приводят к изменениям в жизни граждан, в способах работы и взаимодействия внутри компаний, функционирования государственного сектора



АНТОН ЛИСИЦЫН,
заместитель директора
Росфинмониторинга

Финансовая сфера также претерпевает значительные изменения под влиянием цифровых технологий. Онлайн-банкинг, мобильные платежи и цифровые кошельки упрощают и ускоряют процессы банковских операций и платежей, а блокчейн-технология и криптовалюты предоставляют новые возможности.

Инновации и цифровая трансформация становятся ключевыми факторами для развития государств в условиях цифровой экономики, способствуют созданию новых отраслей и рабочих мест, повышению производительности и улучшению качества

жизни. Применение цифровых технологий в государственном управлении позволяет упростить и автоматизировать процессы, повысить доступность государственных услуг для граждан, улучшить эффективность и прозрачность работы государственных органов, а также адаптироваться к изменяющимся условиям.

Искусственный интеллект и автоматизация имеют огромный потенциал для улучшения бизнес-процессов и повышения эффективности в цифровой экономике. ИИ может помочь автоматизировать рутинные задачи, анализировать большие объемы данных, принимать решения на основе алгоритмов

и улучшать производительность, открыть новые возможности в области анализа данных и разработки интеллектуальных систем.

Говоря о цифровизации механизмов работы Федеральной службы по финансовому мониторингу, нельзя не отметить, что концепцией развития Единой информационной системы Росфинмониторинга предусмотрена реализация ряда направлений, где использование механизмов ИИ оправдано и должно обеспечить прирост производительности труда сотрудников.

Данные, аккумулированные в информационной системе Службы за годы ее существования, представляют собой значительный объем информации, необходимый для осуществления аналитической деятельности.

Зачастую сведения, полученные из многочисленных разнородных внешних источников, бывают представлены в неструктурированном и неформализованном виде, что влечет за собой необходимость дополнительной обработки или обогащения.

При обработке указанной информации первостепенное значение приобретает ее разметка, позволяющая идентифицировать хозяйствующие субъекты для последующего обнаружения признаков противоправной деятельности, а также формирования признакового пространства для классификации по категориям рисков. Анализ такого объема данных невозможен без использования машинной обработки. Росфинмониторинг разработал и успешно применяет на практике несколько методов искусственного интеллекта, включая компонент, позволяющий разрабатывать, обучать и применять математические модели для анализа поведения экономических субъектов. Этот компонент включает в себя модель классификации, которую можно обучать, и которая позволяет на практике, например, выявлять среди миллионов хозяй-

ствующих субъектов организации с номинальными учредителями и руководством или же номинальных физических лиц, которые занимаются обналичиванием средств, а также иные признаки подозрительной или противоправной деятельности.

В части обработки естественного языка реализуется функция идентификации платежных реквизитов, выявленных в результате обработки сообщений, публикуемых в социальных сетях и имеющих признаки сбора денежных средств на противоправные цели.

Аналогичным образом анализируется русскоязычный сегмент глобальной сети Интернет. Компонент извлекает и анализирует субъекты, представляющие интерес для Федеральной службы по финансовому мониторингу, и выявляет их взаимосвязи. Полученные данные обогащают информационное пространство Росфинмониторинга, дополняя уже имеющиеся сведения о субъектах.

В эпоху цифровой экономики колоссальные объемы данных, аккумулируемые и хранимые в настоящее время, открывают уникальные возможности для извлечения ценной информации и играют ключевую роль в вопросах принятия решений, построения новых моделей с опорой на скрытые паттерны и тенденции, а также при оптимизации рабочих процессов.

На основе больших данных Росфинмониторинг реализует проект международной платформы для подразделений финансовой разведки семи стран: Республики Армения, Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации, Республики Таджикистан и Республики Узбекистан.

Созданная по инициативе Росфинмониторинга в рамках Содружества Независимых Государств (СНГ) технологическая площадка — Международный центр оценки рисков (МЦОР) — предлагает

своим партнерам использовать новаторские методы для координации и укрепления международного сотрудничества в сфере выявления и снижения уровня межнациональных угроз, что становится критически значимым элементом работы в условиях мировой турбулентности.

Создание МЦОР обусловлено наличием общих для всех государств рисков, связанных с ОД/ФТ, и необходимостью совместных действий по их минимизации. К таким рискам относятся, в частности, подозрительные транснациональные финансовые потоки, использование фиктивных компаний или индивидуальных предпринимателей, операции с обналичиванием денежных средств, транснациональная наркоторговля, перемещение капитала на общие зарубежные площадки для его отмывания.

➤ «СОЗДАННАЯ ПО ИНИЦИАТИВЕ РОСФИНМОНИТОРИНГА В РАМКАХ СНГ ТЕХНОЛОГИЧЕСКАЯ ПЛОЩАДКА — МЕЖДУНАРОДНЫЙ ЦЕНТР ОЦЕНКИ РИСКОВ (МЦОР) — ПРЕДЛАГАЕТ СВОИМ ПАРТНЕРАМ ИСПОЛЬЗОВАТЬ НОВАТОРСКИЕ МЕТОДЫ ДЛЯ КООРДИНАЦИИ И УКРЕПЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ВЫЯВЛЕНИЯ И СНИЖЕНИЯ УРОВНЯ МЕЖНАЦИОНАЛЬНЫХ УГРОЗ»

Объединение информации о финансовых потоках всех государств-участников СНГ в рамках единого



информационного пространства позволяет проводить комплексный анализ финансовых операций на территории содружества, а также создавать условия для эффективного прогнозирования потенциальных рисков с целью применения общих предупредительных и заградительных мер.

Единообразное восприятие рисков, технологически совершенный и быстрый обмен данными позволят членам Совета руководителей подразделений финансовой разведки государств – участников Содружества Независимых Государств (СРПФР) эффективно применять инструменты реагирования для снижения уровня общих угроз, акцентируя усилия непосредственно на борьбе с преступностью и укреплении взаимодействия в контексте противодействия незаконной деятельности.

Важным аспектом взаимодействия стран в рамках МЦОР является повышение качества аналитической работы ПФР за счет использования данных, которыми располагают страны-партнеры. Обладание актуальной информацией о состоянии и динамике трансграничных финансовых операций и связанных с ними рисках ОД/ФТ позволит проводить тематические международные оперативно-профилактические операции с участием ПФР и других национальных органов государств — членов СРПФР.

Еще один элемент, способствующий обеспечению финансового мониторинга для защиты национальных интересов государства, — это Национальный «Пояс финансовой безопасности». В данном случае технологии Big Data служат инструментом поддержки процесса принятия решений и соответствующих методических, программных и аппаратных средств, необходимых для качественного усовершенствования управляющих систем. Национальный «Пояс финансовой безопасности» — это

система, объединяющая в себе комплекс методических подходов к систематизации и анализу информации, методов обработки данных и программно-аппаратных решений для хранения, исследования и визуализации информации.

Национальный «Пояс финансовой безопасности» выполняет следующие основные функции:

- анализ данных по различным направлениям;
- выявление взаимосвязей и получение новых знаний между различными областями мониторинга;
- использование полученной информации для своевременного принятия превентивных, защитных или заградительных мер.

По сути это междисциплинарный анализ событий в различных областях мониторинга. Данный анализ позволяет идентифицировать точки концентрации риска и новые факторы риска. Интеграция такой системы в процессы стратегического планирования обеспечивает основу для принятия мер, направленных на снижение рисков.

Важно отметить также технологии блокчейн, которые изменили способы ведения бизнеса и обеспечили доверие в условиях цифровой экономики. Блокчейн как технология гарантирует безопасность и прозрачность криптовалютных транзакций в современном мире. Однако при всей доступности исходных данных (адреса отправителя и получателя криптовалют, объем и время транзакции), как правило, отсутствует информация, которая позволила бы идентифицировать личности участников.

Для решения этой проблемы в настоящее время Службой в своей деятельности используется сервис по анализу криптовалютных транзакций «Прозрачный блокчейн», в основе которого лежит разметка участников криптовалютного рынка, позволяющая проводить мониторинг и отслеживание их активности.

Несмотря на то, что «Прозрачный блокчейн» относительно свежий продукт, уже сейчас доступ к сервису имеют более 7 тысяч пользователей из числа сотрудников российских правоохранительных органов и зарубежных подразделений финансовой разведки. У Службы уже имеются успешные примеры проведения структурными подразделениями финансовых расследований совместно с правоохранительными органами по тематике противодействия использованию криптовалюты в противоправной деятельности, результатом которых являются уголовные дела. На текущий момент активно ведутся работы по обеспечению бесперебойного функционирования сервиса и его динамичному развитию, и можно утверждать, что он станет одним из ключевых элементов цифровой экосистемы Росфинмониторинга.

С развитием цифровых технологий возникают новые требования к образованию и навыкам, необходимым для успешной адаптации и профессионального развития в этом быстро меняющемся мире. Цифровая грамотность становится неотъемлемой частью образования. Это подразумевает умение эффективно использовать цифровые технологии, обрабатывать информацию, работать с данными и использовать цифровые инструменты для решения задач. Образовательные программы должны стать более гибкими и адаптивными, чтобы обеспечить обучение актуальным навыкам и знаниям. Необходимо обновлять учебные планы и методы обучения, чтобы отражать новейшие тенденции и требования цифровой экономики.

В этих условиях Служба как никогда заинтересована в сотрудниках, имеющих высокий уровень компетенций в области машинного обучения, Data Science, программирования на Python.

РАЗВИТИЕ ФИНТЕХА В ИНДИИ: КУРС НА ИННОВАЦИИ, ФИНАНСОВУЮ БЕЗОПАСНОСТЬ И БОРЬБУ С КИБЕРПРЕСТУПНОСТЬЮ

В последние годы сектор цифровых и мобильных банковских услуг в Индии стремительно растет, чему способствуют правительственные инициативы по расширению доступа к финансовым услугам, а также развитие интернета и повсеместное распространение доступных смартфонов



Г-Н КЕШАВ АНАНД,
заместитель директора
ПФР Индии



Г-ЖА М. ШАНМУГА ПРИЯ,
содиректор
ПФР Индии

Ежегодный приток технических специалистов и финансовых экспертов — выпускников престижных университетов и колледжей Индии в сочетании с государственной политикой благоприятствования стартапам и устойчивым ростом ВВП страны создает динамичную экосистему, которая за-

кладывает основу для быстрого развития финтех-стартапов.

Значительный подъем произошел благодаря внедрению Единого платежного интерфейса (Unified Payments Interface — UPI) — мобильного сервиса мгновенных платежей. С января 2019 по январь 2024 года это увеличило число транзакций с 672 млн до

невероятных 12 203 млн, а сумму транзакций — со 109 932 крор инд. рупий (около 15,5 млрд долл. США) до 1 841 084 крор инд. рупий (около 221,5 млрд долл. США)¹.

Несмотря на продвижение финансовых услуг среди широких слоев населения, развитие финтеха породило и новые риски для финансовой стабильности.

¹ <https://www.npci.org.in/what-we-do/upi/product-statistics>.



Особенно стоит отметить возросшую вероятность финансовых киберпреступлений. Регулирующие и правоохранительные органы, разведслужбы и представители финтех-индустрии осознают эти риски. Сегодня ведется совместная работа по противодействию им, принимаются меры по их устранению и повышению уровня информированности о них.

АНОНИМНОСТЬ, СЕТЕВАЯ ДОСТУПНОСТЬ И РОСТ КИБЕРПРЕСТУПНОСТИ

Рост киберпреступности обусловлен анонимностью, которую обеспечивает развитие технологий и интернета. Даже при минимальных технических навыках человек может получать деньги незаконным путем, не выходя из дома. Несмотря на надежные меры кибербезопасности, в системах остаются отдельные уязвимости, чем пользуются злоумышленники. Кибератаки основаны на этих недостатках, и скрытое слежение позволяет обнаружить подобные тактики вторжения. Благодаря сетевой доступности киберпространство позволяет практически беспрепятственно действовать на глобальном уровне.

РИСК ДЛЯ ФИНАНСОВОЙ СТАБИЛЬНОСТИ

В ноябре 2022 года в результате национальной оценки рисков в Индии выяснилось, что кибермошенничество и изъятия в системе безопасности создают значительные риски для финансовой стабильности. Особенно это касается банковских операций, кредитования, платежей, ценных бумаг и денежных рынков. Кибермошенничество не только подрывает репутацию банков, но и создает ряд

рисков: сбои в работе, ограничение ресурсов, финансовые убытки, проблемы с ликвидностью. Участвовавшие в последнее время случаи кибермошенничества представляют собой серьезную угрозу для финансового сектора с точки зрения уязвимости в сфере ПОД.

ТРЕНДЫ КИБЕРПРЕСТУПНОСТИ: РОСТ СЛУЧАЕВ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Согласно отчету I4C² за 2-й квартал 2022 года, опубликованному в журнале *Cyber Pravaha*, количество киберпреступлений, зарегистрированных на Национальном портале регистрации киберпреступлений Индии (NCRP), выросло до 237 658 против 97 179 за аналогичный период предыдущего года. Доминирующей категорией стало финансовое мошенничество в интернете — 67,9% от всех зарегистрированных киберпреступлений. Среди платежных платформ наиболее резко возросло число случаев мошенничества, связанных с UPI: с 18 864 до 84 145 во 2-м квартале по сравнению с предыдущим годом. Кроме того, за тот же период значительно увеличилось число случаев мошенничества с дебетовыми и кредитными картами: с 8 628 до 26 793, как и жалоб на мошенничество в сфере интернет-банкинга: с 5 104 до 19 267.

СТРАТЕГИЧЕСКИЙ АНАЛИЗ ИНСАЙТОВ

Группа стратегического анализа Подразделения финансовой разведки (ПФР) Индии провела обширный анализ сообщений о подозрительных операциях (СПО), связанных с киберпреступлениями, за период с апреля 2018 года

по декабрь 2022 года. Отмечен 12-кратный рост числа таких сообщений. Основные виды киберпреступлений: мошенничество с кредитными картами, фишинг, аферы трудового найма, кража личных данных и фальшивые кредитные/игровые/азартные приложения.

Для выявления и тщательной проверки физических и юридических лиц, причастных к киберпреступлениям, разработана новая методология, основанная на оценке рисков. Этот метод учитывает разнообразие субъектов, сообщающих о подозрительных операциях, частоту этих сообщений и набор первичных преступлений.

Кроме того, на основе пространственного анализа были приняты предупредительные и оперативные меры по выявлению и устранению очагов киберпреступности.

По результатам стратегического анализа на основе оценки рисков разработаны планы действий в отношении групп высокого риска киберпреступности. Сюда относятся оперативный анализ таких групп, обучение и постоянный диалог с сообщающими субъектами для понимания и устранения возникающих моделей киберпреступности, а также для совершенствования стратегий борьбы с отмыванием денег в условиях роста числа случаев киберпреступности.

МЕРЫ ПО УСТРАНЕНИЮ РИСКОВ

Борьбе с кибермошенничеством и отмыванием денег способствует мониторинг мошеннических приемов, выполняемый ПФР Индии

² Индийский координационный центр по борьбе с киберпреступностью (I4C) учрежден Министерством внутренних дел Индии.

в сотрудничестве с правоохранительными органами и финансовыми организациями. Специальная рабочая группа разработала и внедрила «красные флаги» — типичные признаки кибермошенничества. При этом особое внимание было уделено мошенническим операциям и схемам по целому спектру мошеннических приложений, в том числе связанных с кредитами, ставками, азартными играми, инвестициями, трудоустройством, знакомствами. Усиленные меры теперь предусматривают мониторинг рисков приложений, изменение процедуры проверки благонадежности, проверку IP-адресов и географических данных для более

эффективной борьбы с этими преступлениями.

В сотрудничестве с сообщаемыми организациями ПФР Индии ведет регулярный тщательный контроль приложений, сайтов и платформ социальных сетей, которые, как известно, подвергают опасности ничего не подозревающих людей, применяя различные тактики киберпреступлений. Собранные благодаря этим мерам сведения распространяются среди сообщаемых организаций, других разведывательных служб и правоохранительных органов, с тем чтобы предпринять дальнейшие действия. Кроме того, анализ современных стратегий киберпре-

ступности служит для повышения информированности населения, а также для содействия сообщаемым организациям в выявлении таких незаконных схем и реагировании на них через свои системы противодействия легализации доходов, полученных преступным путем.

Банк RBI принял ряд мер по снижению рисков и выпустил для банков рекомендации по борьбе с мошенничеством и киберпреступлениями. Также в специальных рекомендациях подробно описаны методы, которые используют мошенники, включая атаку на банковские счета и кошельки prepaid-инструментов (Prepaid Instrument — PPI). Банкам предписано оперативно решать эти проблемы, анализируя тактику мошенничества и разрабатывая стратегии по устранению обнаруженных уязвимостей.

Банк RBI выпустил и указания для банков в отношении мошенничества и киберпреступлений в сферах инвестиционных афер, предложений частичной занятости и финансовых пирамид. RBI подчеркивает необходимость:

- а) создания надежной системы выявления и мониторинга предполагаемых дроповых счетов;
- б) совершенствования процедур проверки благонадежности клиента, мер противодействия отмыванию денег, включая комплексную юридическую оценку, проверку личности, профилирование рисков, мониторинг в режиме реального

ПФР ИНДИИ СОВМЕСТНО С ФИНАНСОВЫМ РЕГУЛЯТОРОМ — РЕЗЕРВНЫМ БАНКОМ ИНДИИ (RESERVE BANK OF INDIA — RBI) И НЕКОТОРЫМИ ДРУГИМИ БАНКАМИ СФОРМИРОВАЛО РАБОЧУЮ ГРУППУ ПО БОРЬБЕ С ДРОПОВЫМИ СЧЕТАМИ КИБЕРПРЕСТУПНИКОВ. БЫЛИ СОСТАВЛЕНЫ РЕКОМЕНДАЦИИ:

1. Стандартизировать процесс выявления и предотвращения дроповых счетов с помощью оценки рисков, процедуры оценки благонадежности и технологических мер.
2. Стимулировать обмен информацией между финансовыми учреждениями, чтобы предотвратить миграцию мошеннических средств.
3. Внедрить поведенческую биометрию для более эффективного обнаружения преступлений.
4. Присваивать счетам рейтинг риска.
5. Создать систему отслеживания сетей для счетов кибермошенников.





времени и работу со счетами, которые, предположительно, используются в незаконных целях;

в) обеспечения эффективного контроля и мониторинга цифровых операций, в том числе в UPI, и сообщения о подозрительной деятельности в ПФР Индии, даже если операциями управляют сторонние поставщики услуг.

ВЕДОМСТВЕННЫЕ ИНИЦИАТИВЫ ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

В 2019 году Министерство внутренних дел Индии создало Индийский координационный центр по борьбе с киберпреступностью (I4C). Национальный портал регистрации киберпреступлений позволяет круглосуточно сообщать о преступлениях, особенно против женщин и детей. Система сообщений о киберпреступлениях населением (Citizen Financial Cyber Fraud Reporting and Management System) способствует оперативному принятию мер против кибермошенников благодаря горячей линии «1930» для жалоб в режиме онлайн.

На портале CyTrain правоохранные органы проходят онлайн-обучение по расследованию

и преследованию киберпреступлений. В то же время объединенные координационные группы по борьбе с киберпреступлениями способствуют укреплению межведомственного сотрудничества.

Кроме того, национальная лаборатория криминалистики киберпреступлений предоставляет передовые возможности судебной экспертизы для расследования таких преступлений.

Группа реагирования на компьютерные инциденты (CERT-In) занимается устранением инцидентов, связанных с ИТ-безопасностью, и способствует внедрению передовых практик. Инициатива «Кибербезопасность Индии» (Cyber Surakshit Bharat) связана с обучением правительственного ИТ-персонала по вопросам киберугроз, а программа CyberDost обеспечивает информированность населения о кибербезопасности.

Таким образом, ПФР Индии совместно с финансовым регулирующим органом и другими подразделениями правительства Индии, участвующими в борьбе с киберпреступностью, прилагает постоянные усилия для предотвращения кибермошенничества и снижения финансового ущерба, наносимого кибермошенниками.

Скоординированные усилия подразделений финансовой разведки Индии и других стран, а

также контролируемых организаций по пресечению движения незаконных средств на банковских счетах киберпреступников позволили предотвратить финансовые убытки множества граждан и, соответственно, обезопасить финансовую экосистему страны.

Благодаря инициативам правительства Индии по борьбе с киберпреступностью Индия уверенно идет к устранению в ближайшем будущем этой угрозы.

➤ **«СКООДИНИРОВАННЫЕ УСИЛИЯ ПОДРАЗДЕЛЕНИЙ ФИНАНСОВОЙ РАЗВЕДКИ ИНДИИ И ДРУГИХ СТРАН, А ТАКЖЕ КОНТРОЛИРУЕМЫХ ОРГАНИЗАЦИЙ ПО ПРЕСЕЧЕНИЮ ДВИЖЕНИЯ НЕЗАКОННЫХ СРЕДСТВ НА БАНКОВСКИХ СЧЕТАХ КИБЕРПРЕСТУПНИКОВ ПОЗВОЛИЛИ ПРЕДОТВРАТИТЬ ФИНАНСОВЫЕ УБЫТКИ МНОЖЕСТВА ГРАЖДАН И, СООТВЕТСТВЕННО, ОБЕЗОПАСИТЬ ФИНАНСОВУЮ ЭКОСИСТЕМУ СТРАНЫ»**

ЮРИЙ КОРОТКИЙ: «ФИНАНСОВЫЙ МОНИТОРИНГ — ЭТО В СВОЕМ РОДЕ ФИНАНСОВАЯ ТОМОГРАФИЯ»

➤ **Юрий Короткий**
об эволюции
информационных систем
Росфинмониторинга, идеальной
ИТ-системе будущего
и криптокомплаенсе

Юрий Короткий, заслуженный юрист Российской Федерации, международный эксперт в сфере противодействия отмыванию доходов и финансированию терроризма, к. ю. н.



Поступив на службу в Комитет по финансовому мониторингу практически с момента его основания, Юрий Федорович трудился в финансовой разведке на протяжении 22 лет. Под его руководством был усовершенствован аналитический арсенал, разработаны и внедрены новые инструменты анализа, методология построения рабочего процесса управления рисками ОД/ФТ.

В эксклюзивном интервью «Финансовой безопасности» Юрий Короткий рассказал, как развивалась ИТ-система в российской финансовой разведке, какие методы анализа наиболее эффективны и почему так важно регулировать оборот криптовалют.

— Юрий Федорович, более 20 лет посвятив Росфинмониторингу, вы стояли у истоков информационных систем Службы. С чего все начиналось?

— Любая информационная система (ИС) — это сочетание трех компонент: «информация» + «железо» + «мозги». На языке информационных технологий — это информационный ресурс, аппаратно-программный комплекс и аналитика. К моему приходу в Службу, а это декабрь 2001 года (в то время еще не Служба, а Комитет финансового мониторинга), части «информации» и «железа», то есть система сбора, хранения и обработки информации в своей основе уже были сформированы. И справедливости ради надо отметить,

что заслуга в этом принадлежит не мне. Не могу не назвать имена таких замечательных пионеров нашей ИС, как Александр Егоркин, Юрий Гребенщиков, Валерий Макешин и многие другие.

Что касается третьего, аналитического компонента, то здесь мне и в самом деле довелось внести определенный вклад. А начиналось все с системы спецучета. В то время она именовалась «СДП» — спецделопроизводство — и подробно регламентировала поводы, основания, порядок заведения, производства по делам финансовых расследований и их реализации. То есть были заданы алгоритмы всего процесса аналитической работы. Эта компонента актуальна по сей день, и по своей сути за 20 с лишним лет мало изменилась. Сменила, правда, название на «КОФР» — компонента обеспечения финансовых расследований.

— Мы знаем, что вы автор методологии построения рабочего процесса управления рисками ОД/ФТ. Одна из ее ключевых идей — оценка рисков в рамках контекстов. В чем преимущество именно такого подхода?

— Скажу больше. На мой взгляд, это не просто преимущество, это единственно верный подход, потому что подозрительна не сама операция, а обстоятельства ее проведения. Поэтому и оценить подозрительность операции можно только через контекст, в котором она совершается. По-моему, данный вывод очевиден. Например, чтобы оценить подозрительность операций, совершаемых в бюджетной сфере, надо изучить детали госконтракта, механизм ценообразования, особенности конкурсных процедур, обоснованность выбора поставщика, возможную аффилированность исполнителя с заказчиком и многие другие аспекты, представляющие собой контекст операций по расходованию бюджетных средств.



» «ИТ-СИСТЕМА БУДУЩЕГО БУДЕТ НАПОМИНАТЬ ТЕХНОЛОГИЮ АВТОМАТИЧЕСКОГО МНОГОПОЛОСНОГО СКАНИРОВАНИЯ ОПЕРАТИВНОЙ ОБСТАНОВКИ С ИСПОЛЬЗОВАНИЕМ ТЫСЯЧ ИНДИКАТОРОВ И БОЛЬШИХ ДАННЫХ»

— Финансовая разведка — ведомство, для которого необходимы современные финансовые информационные технологии ввиду ежедневного анализа большого массива данных. Какими свойствами должна обладать система, чтобы она быстро приспосабливалась к вызовам и угрозам? Возможна ли быстрая системная адаптация?

— Да, способность быстро адаптироваться к изменениям обстановки и оперативно реагировать на постоянно меняющиеся вызовы и угрозы — это, бесспорно, очень важное требование к системе. Но этого недостаточно. Такая система обречена на постоянные «догонялки» и реагирование постфактум. Система должна работать на упреждение. Как? Возвращаю вас к предыдущему вопросу — через контекст. Мы не знаем, что именно предпримет завтра преступник и

кем он является. Но мы знаем, где и каким образом он вероятнее всего себя проявит. Не буду раскрывать всех секретов и риск-индикаторов, по которым мы выделяем области усиленного мониторинга, где система заранее сориентирована на возможные признаки и факты еще до их появления и готова на них среагировать. Ожидать противника в засаде — это и есть упреждение. Но для этого нужна предиктивная аналитика.

— Какая она, идеальная ИТ-система будущего для целей укрепления антиотмывочной системы?

— Предлагаете помечтать? Я давно заметил много общего между предназначением системы финансового мониторинга и компьютерной томографией в медицине. Ведь задачи у них идентичны: своевременно диагностировать болезнь

или распознать симптомы заболевания. Финансовый мониторинг — это в своем роде финансовая томография. ИТ-система будущего будет напоминать технологию автоматического многополосного сканирования оперативной обстановки с использованием тысяч индикаторов и больших данных. На выходе, как в медицине, — оценка состояния здоровья, диагностика заболеваний, выработка курса лечения. И все это с использованием искусственного интеллекта. Как вам такая картина будущего?

— Звучит интересно и многообещающе. А какой инструментарий, на ваш взгляд, наиболее полезен для оценки внешних угроз и внутренних уязвимостей страны?

— Если коротко, то никакой отдельно взятый инструмент не способен на это. Нужен арсенал средств и система автоматического выбора того инструментария, который настроен а) на данный вид конкретно выявленной угрозы/уязвимости и б) на особенности той предметной области, где данная угроза/уязвимость имеют место быть.

— Какие текущие тенденции в развитии ИТ-систем в целях мониторинга вы можете выделить?

— Сейчас много говорят о цифровизации. На курсах руководителей цифровой трансформации кто-то из преподавателей сказал, что оцифровать можно и помойку. Но мы получим не цифровизацию, а цифровую помойку. И это верно. Трансформация сначала должна произойти в головах у тех, чей труд подлежит цифровизации. Есть такое понятие — «цифровая зрелость», которую система и ее субъекты должны достичь. Этот процесс нельзя миновать или как-то обойти. Но его можно и должно ускорить. Как раз сейчас, на мой взгляд, мы проходим этап «цифрового созревания». В чем это заключается? В трех основных тенденциях, которые зафиксирова-

ны в нашей Концепции, и ничего нового я тут не открою:

- осмысление и формализованное представление структуры предметной области ПОД/ФТ (онтология);
- процессный подход, то есть пошаговое описание процесса достижения конечных результатов и целевых показателей эффективности;
- переход от технологии управления данными к извлечению и управлению знаниями.

— От метода «расширяющегося зрачка» к автоматизации: какие, на ваш взгляд, методы анализа высокорисковых операций из наиболее современных доказали свою эффективность?

— Мы с иронией и улыбкой вспоминаем метод «расширяющегося зрачка», с чего мы начинали разбор входного потока сообщений. А ведь по сути сам принцип не изменился. Как тогда, 20 лет назад, так и сейчас, в основе лежит то, что мы называем индикаторы риска. Просто раньше на них реагировал зрачок аналитика, а сейчас компьютерные технологии позволяют не просто снимать риск-сигнал, но и замерять скоринги, выделять зоны по уровням риска (так называемый «светофор»), создавать тепловые карты оперативной обстановки с выделением тех факторов, которые образуют «красные зоны». Разработанная нами «матрица рисков» еще не до конца внедрена в практику ситуационного анализа и национальной оценки рисков, но, я убежден, за ней будущее, и именно здесь широкое поле для применения искусственного интеллекта.

— Росфинмониторинг продолжает международное сотрудничество и расширяет его географию. При этом ИТ-системы финразведок отличаются. Каковы основные механизмы для выстраивания взаимодействия, в том числе с новыми

техническими продуктами, в условиях национальной специфики? Могут ли информационные технологии выступить как инструмент углубления сотрудничества?

— Последовательность здесь такова: сначала нарабатываются алгоритмы совместной работы, одновременно под них подводится нормативная база, и только потом подключаются совместные ИТ-проекты. Так что в данном случае первично наличие воли и совместных наработок. Если этот базис сложится — за айтишниками не заржавеет. Вопросы адаптации и интеграции разных систем — технически непростые, но вполне решаемые проблемы. Главное — формирование единого оперативного пространства и общих подходов к его освоению.

➤ **«РАЗРАБОТАННАЯ НАМИ "МАТРИЦА РИСКОВ" ЕЩЕ НЕ ДО КОНЦА ВНЕДРЕНА В ПРАКТИКУ СИТУАЦИОННОГО АНАЛИЗА И НАЦИОНАЛЬНОЙ ОЦЕНКИ РИСКОВ, НО, Я УБЕЖДЕН, ЗА НЕЙ БУДУЩЕЕ, И ИМЕННО ЗДЕСЬ ШИРОКОЕ ПОЛЕ ДЛЯ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»**

— Каким вы видите развитие комплаенса с учетом необходимости регулирования криптоактивов?

— Compliance переводится как «соответствие правилам». Поэтому развитие системы комплаенс в сфере оборота криптоактивов напрямую зависит от того, как скоро мы придем к полноценной системе регулирования криптовалютного рынка. На нынешнем этапе, когда комплаенс функционирует



исключительно в сфере оборота фиатных валют, мы должны дополнить действующую систему внутреннего контроля методиками и инструментами вскрытия «связок» между банковскими операциями клиентов и их криптовалютными транзакциями. Надо научиться распознавать эту связь через так называемые «дропы», P2P-платежи и прочие стыки между двумя разными операционными системами:

фиатной и криптовалютной. Как раз этой проблемой в соответствии

с поручением Президента Российской Федерации в рамках проекта «Прозрачный блокчейн» мы сейчас и занимаемся.

Что касается перспектив регулирования отечественного рынка криптовалюты, убежден, оно должно идти не по пути «выдавливания» криптотранзакций в теневой оборот, а напротив, по пути повышения их прозрачности. И второе важное направление — сфера криптовалютного посредничества. Здесь требуется «импортозамещение» иностранных поставщиков услуг виртуальных активов (ПУВА) и становление отечественного рынка криптовалютных услуг с собственной системой криптокомплаенс. Кроме этого, у нас есть опыт «приземления» крупных иностранных ИТ-вендоров на условиях соблюдения российского законодательства, в том числе налогового и антиотмывочного. Следовало бы применить этот опыт и в отношении ПУВА-нерезидентов. Беспрепятственная активность иностранных криптообменников на территории России, оставаясь вне российской юрисдикции, а точнее, в зоне «регуляторных дыр» российского законодательства, — такое положение дел несет в себе еще большие риски, чем сама криптовалюта. Ликвидация этих «дыр» неоправданно долго затягивается.

**» «ЧТО КАСАЕТСЯ ПЕРСПЕКТИВ РЕГУЛИРОВАНИЯ
ОТЕЧЕСТВЕННОГО РЫНКА КРИПТОВАЛЮТЫ,
УБЕЖДЕН, ОНО ДОЛЖНО ИДТИ НЕ ПО ПУТИ
"ВЫДАВЛИВАНИЯ" КРИПТОТРАНЗАКЦИЙ В ТЕНЕВОЙ
ОБОРОТ, А НАПРОТИВ, ПО ПУТИ ПОВЫШЕНИЯ ИХ
ПРОЗРАЧНОСТИ»**



РЕГУЛИРОВАНИЕ РЫНКА ФИНАНСОВЫХ ТЕХНОЛОГИЙ В КОНТЕКСТЕ ПОД/ФТ: ОПЫТ УЗБЕКИСТАНА



ОТАБЕК РАХМАНОВ,
заместитель начальника
управления Центрального банка
Республики Узбекистан

Общее население Узбекистана составляет 36,5 млн человек. 25 млн из них — молодое население в возрасте от 15 лет и старше. Это создает потенциальную базу для расширения использования финансовых технологий, учитывая тенденцию молодых людей к принятию новых цифровых решений

ОБЗОР РЫНКА ФИНАНСОВЫХ ТЕХНОЛОГИЙ — СУБЪЕКТЫ

На рынке присутствует 35 банков с сетью из 2510 филиалов и офисов банковских услуг. Это обеспечивает широкий охват территории страны и доступность финансовых услуг для населения.

В Узбекистане действует 49 платежных организаций, что свидетельствует о разнообразии предлагаемых финансовых услуг. Кроме того, есть 12 систем электронных денег и 6 платежных систем, что способствует разнообразию и конкуренции на рынке.

На рынке присутствуют 3 оператора платежных систем, обеспечивающих инфраструктуру для эффективного осуществления денежных переводов и транзакций.

Эти данные подчеркивают значимость финансового сектора в Узбекистане и говорят о том, что страна обладает развитой инфраструктурой для осуществления различных финансовых операций, что в свою очередь создает благоприятные условия для развития финансовых технологий.

ОБЗОР РЫНКА ФИНАНСОВЫХ ТЕХНОЛОГИЙ — ОБЪЕКТЫ

В стране функционирует более 427 тысяч точек терминалов для продаж (POS), что является значительным показателем и свидетельствует о широком распространении систем безналичных платежей в торговых и сервисных точках.



Количество банкоматов и информационных киосков превышает 24 тысячи единиц. Это означает высокий уровень доступности финансовых услуг для населения, учитывая, что такие объекты часто располагаются как в банковских отделениях, так и в общественных местах.

В обращении находится 42,4 миллиона платежных карт, что свидетельствует о широком использовании электронных средств расчета в стране. Это создает удобство для потребителей и способствует развитию безналичных платежей.

Среди платежных карт 6,7 миллиона относятся к международным платежным системам, таким как Visa, UnionPay, Mastercard. Это показывает интеграцию узбекской финансовой системы в мировой экономический контекст и обеспечивает возможность совершения международных транзакций для граждан и бизнеса.

Таким образом, объекты финансовых технологий в Узбекистане обладают широким диапазоном и позволяют предоставлять разнообразные услуги как национального, так и международного уровня.

РЫНОК ФИНАНСОВЫХ ТЕХНОЛОГИЙ — РЕГУЛЯТИВНЫЕ ОСНОВЫ

В Узбекистане регулирование рынка финансовых технологий основывается на ряде законодательных актов и правил, которые направлены на обеспечение безопасности и противодействие преступной деятельности. Одним из ключевых документов является Закон Республики Узбекистан «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения» № 660-II от 26 августа 2004 года. Этот за-

кон определяет основные меры по борьбе с финансовыми преступлениями и устанавливает ответственность за их совершение.

Дополнительные меры по реализации указанного закона были утверждены Постановлением Кабинета Министров № 402 от 29 июня 2021 года, что свидетельствует о постоянном совершенствовании правовой базы в этой области. Эти меры включают в себя конкретные положения и инструкции для эффективной борьбы с легализацией доходов, финансированием терроризма и распространением оружия массового уничтожения.

Важным аспектом регулирования являются правила внутреннего контроля, утвержденные Центральным банком и Подразделением финансовой разведки. Эти правила предназначены для банков, операторов платежных систем, операторов систем электронных денег и платежных организаций и направлены на усиление мер по противодействию финансовым преступлениям.

Для обеспечения безопасности транзакций и идентификации клиентов были установлены положения о порядке цифровой идентификации клиентов, утвержденные Постановлением Центрального банка № 3322 от 30 сентября 2021 года. Это позволяет эффективно проверять личность клиентов в онлайн-среде и снижать риск финансовых мошенничеств.

НОВЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ — ЭТАПЫ ВНЕДРЕНИЯ В ДЕЛОВУЮ ПРАКТИКУ

Внедрение новых финансовых технологий в деловую практику

представляет собой многоэтапный процесс, требующий основательного анализа и мер предосторожности для обеспечения безопасности и эффективности операций.

Первый этап — это обследование продукта, которое включает в себя детальное изучение его функциональности, возможностей и потенциальных преимуществ для бизнеса и клиентов. Затем происходит определение рисков, угроз и уязвимостей, связанных с новым продуктом, чтобы иметь ясное представление о возможных негативных последствиях его использования. После этого проводится анализ рисков, который включает в себя оценку вероятности возникновения различных угроз и их потенциального воздействия на бизнес и клиентов. На основе результатов анализа разрабатываются стратегии по уменьшению рисков, которые могут включать в себя изменения в продукте, в процессах его использования или в политике безопасности компании.

Важным шагом является уведомление Центрального банка до запуска нового продукта. Это требуется для обеспечения согласованности с законодательством и регулированием финансового рынка. После уведомления Центральный банк может провести свой собственный анализ продукта и дать рекомендации по его улучшению или дополнительным мерам безопасности.

Наконец, после получения рекомендаций и одобрения со стороны Центрального банка происходит запуск нового продукта на рынок. Однако процесс не заканчивается на этом. Не реже одного раза в год проводится повторное выявление рисков предыдущих и действующих продуктов в контексте противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма. Это

позволяет оперативно реагировать на изменения в среде и вносить коррективы в стратегии безопасности и управления рисками.

ФИНАНСОВЫЕ ТЕХНОЛОГИИ — РЕШЕНИЯ ПО ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Финансовые технологии играют ключевую роль в обеспечении безопасности и эффективности финансовых операций, а цифровая идентификация является одним из важных компонентов этого процесса. В Узбекистане были разработаны национальные решения цифровой идентификации, которые предоставляют возможность проведения идентификации только для резидентов страны.

Одним из ключевых механизмов, используемых в цифровой идентификации, является Liveness Detection. Этот механизм обеспечивает защиту от спуфинга, используя глубоко обученные нейронные сети для проверки — принадлежит ли представленное фото «живому» пользователю.

Другим важным аспектом является Face Recognition, который позволяет сравнивать одно лицо со всеми фотографиями лиц, хранящимися в базе данных. Этот метод обеспечивает идентификацию одного лица среди множества, что увеличивает точность идентификации.

Face Comparison — это еще один важный метод, который позволяет проверить вероятность того, что два фото лица принадлежат одному и тому же человеку. Этот подход особенно полезен при подтверждении личности в случае использования различных фотографий или изображений.

В процессе цифровой идентификации могут использоваться различные методы, включая как автоматизированные процессы без участия человеческого фактора,

так и методы, включающие участие человека. В обоих случаях важно обеспечить высокую точность и безопасность процесса идентификации для защиты интересов клиентов и обеспечения соблюдения регулирующих требований.

ФИНАНСОВЫЕ ТЕХНОЛОГИИ — ПОРОГИ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ

Правила внутреннего контроля по противодействию лега-

лизации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ) в Республике Узбекистан устанавливают ряд конкретных порогов и критериев для определения подозрительных финансовых операций. Эти правила направлены на обеспечение безопасности финансовых транзакций и предотвращение их использования для незаконных целей.

ОСНОВНЫЕ ПОРОГИ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ СОГЛАСНО ПРАВИЛАМ ВНУТРЕННЕГО КОНТРОЛЯ ПО ПОД/ФТ В УЗБЕКИСТАНЕ МОГУТ ВКЛЮЧАТЬ СЛЕДУЮЩИЕ АСПЕКТЫ:

- перевод клиентом денежных средств с банковской карты через мобильное приложение на одну (один) или несколько банковских карт или электронных кошельков одновременно или многократно в течение срока, не превышающего 30 дней, на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины;
- получение клиентом на банковскую карту денежных средств с одной (одного) или нескольких банковских карт или электронных кошельков на общую сумму, равную или превышающую 500-кратный размер базовой расчетной величины, одновременно или многократно в течение срока, не превышающего 30 дней;
- перевод денежных средств через мобильное приложение с одной (одного) банковской карты (электронного кошелька) на 5 и более иностранных банковских карт или электронных кошельков одновременно или многократно в течение срока, не превышающего 30 дней;
- поступление денежных средств с 5 и более иностранных банковских карт или электронных кошельков на 1 банковскую карту (электронный кошелек) одновременно или многократно в течение срока, не превышающего 30 дней;
- поступление денежных средств одновременно или многократно в течение срока, не превышающего 30 дней;



РЫНОК ПЛАТЕЖНЫХ ОРГАНИЗАЦИЙ

Рынок платежных организаций в Узбекистане характеризуется широким спектром мер и инструментов, принимаемых и используемых для минимизации рисков операций с опасностью легализации доходов и финансирования терроризма (ОД/ФТ). В целях обеспечения безопасности и надежности финансовой системы страны платежные организации внедряют разнообразные методы и процедуры.

Системы CDD (Customer Due Diligence) и KYC (Know Your Customer): эти системы позволяют идентифицировать клиентов и проверять их на предмет соответствия нормам и требованиям регулирующих органов. Они включают в себя e-KYC (электронную систему контроля клиентов), которая позволяет более эффективно и быстро проводить процедуры идентификации.

Внутренние порядки и процедуры: платежные организации разрабатывают внутренние правила и процедуры для взаимодействия своих сотрудников, агентов и субагентов с клиентами. Это включает в себя определение порядка работы с рискованными клиентами — публичными должностными лицами (ПДЛ).

Системы мониторинга за операциями клиентов: платежные организации используют специализированные системы мониторинга, которые автоматически отслеживают и анализируют операции клиентов для выявления подозрительных транзакций.

Системы выявления и передачи подозрительных операций: платежные организации имеют механизмы для обнаружения и передачи подозрительных операций соответствующим органам надзора и контроля.

Системы анализа и мониторинга рисков: платежные организа-

ции регулярно проводят анализ, оценку и мониторинг рисков, связанных с проводимыми операциями. Они разрабатывают и применяют стратегии снижения уровня рисков в соответствии с выявленными угрозами.

Разработка и обновление внутренних правил: платежные организации регулярно обновляют свои внутренние правила и процедуры с учетом выявленных рисков и изменений в законодательстве. Это позволяет им эффективно реагировать на новые угрозы и требования регуляторов.

Все эти меры и инструменты способствуют обеспечению эффективного противодействия легализации преступных доходов и финансированию терроризма в финансовом секторе Узбекистана, обеспечивая таким образом стабильность и безопасность финансовой системы страны.

СИСТЕМЫ ЭЛЕКТРОННЫХ ДЕНЕГ

Системы электронных денег играют важную роль в современной финансовой инфраструктуре Узбекистана. В соответствии с законодательством страны эмитентами электронных денег могут выступать исключительно банки, что обеспечивает дополнительный уровень надежности и контроля за операциями с электронными средствами.

Однако следует отметить, что в некоторых случаях проведение надлежащей проверки клиентов не осуществляется. Например, если сумма одной транзакции по электронным деньгам не превышает определенного порога (например, 1 базовая расчетная величина) либо если сумма электронных денег в кошельке клиента остается невысокой (например, менее 5 базовых расчетных величин). Эти ограничения направлены на упрощение и ускорение

мелких и частых операций, сокращая при этом бюрократическую нагрузку на клиентов.

Для минимизации рисков, связанных с операциями по электронным деньгам, установлены лимиты как на отдельные транзакции, так и на общие объемы операций в определенный период времени. Например, могут быть установлены максимальная сумма одной транзакции по электронным деньгам, максимальная сумма электронных денег, которые могут находиться в кошельке клиента, максимальная сумма транзакций по электронным деньгам в течение месяца, а также максимальная сумма транзакций по карте за месяц. Эти лимиты позволяют банкам и регуляторам контролировать и ограничивать потенциальные риски, связанные с использованием электронных денег, и обеспечивают безопасность и стабильность финансовой системы.

НОВЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ: NFC, QR-КОДЫ, TAP-TO-PHONE

В последние годы новые финансовые технологии, такие как NFC, QR-коды и Tap-to-phone, стали неотъемлемой частью современной платежной системы. Позволяя проводить операции быстрее и удобнее, они стали предпочтительным способом оплаты для многих пользователей.

Платежи по технологии NFC являются одним из самых популярных способов бесконтактной оплаты. Объемы операций по этой технологии значительно возросли за последние несколько лет, что свидетельствует о растущей популярности этого метода. Например, в 2021 году объем операций составил 12,2 трлн сум, а в 2023 году уже достиг 31,6 трлн сум. Несмотря на это, финансовые учрежде-

ния должны соблюдать стандарты надлежащей проверки клиентов, особенно в случае сомнительных операций. Если невозможно провести такую проверку, финансовые учреждения обязаны уведомить соответствующие государственные органы и отказаться от сотрудничества с клиентом.

Платежи по технологии QR-кодов также стали популярным способом онлайн-платежей. Технология Tap-to-phone позволяет использовать мобильные устройства в качестве POS-терминалов, что снижает затраты и увеличивает удобство для предпринимателей. Однако усиленные меры по надлежащей проверке клиентов становятся необходимыми. Это включает получение информации об источниках денежных средств, а также изучение целей, запланированных или проведенных клиентом операций.

ОБЪЕМ И КОЛИЧЕСТВО ТРАНЗАКЦИЙ ПО QR-КОДАМ ЗНАЧИТЕЛЬНО УВЕЛИЧИЛИСЬ ЗА ПОСЛЕДНИЕ ГОДЫ

Например, в 2023 году объем операций составил 315 млрд сум, а количество транзакций достигло 93,8 тыс. Такой рост требует повышенное внимание к обеспечению безопасности и предотвращению мошенничества, особенно в отношении нерезидентов, ПДЛ, а также клиентов, осуществляющих подозрительные операции.

В целом развитие новых финансовых технологий открывает новые возможности для пользователей, но требует от финансовых учреждений постоянного внимания к вопросам безопасности и соблюдения законодательства.

НОВЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ: FACE PAY, ATTO И PALM PAY

В сентябре 2023 года была внедрена инновационная технология бесконтактной оплаты, которая представляет собой значительный шаг в области финансовых технологий. Эта технология, известная как FacePay, предлагает удобный и безопасный способ совершения платежей с использованием биометрических данных лица. Специальная камера считывает уникальные черты лица пользователя и автоматически ассоциирует их с привязанной к системе банковской картой, обеспечивая безопасность и защиту данных.

Кроме того, в сфере транспортных услуг было внедрено решение под названием ATTO, которое представляет собой бесконтактную пластиковую карту с технологией NFC. Карты ATTO могут быть приобретены через специальные картоматы или в точках продаж проездных билетов, что делает их доступными для широкого круга пользователей. Эта технология также поддерживает оплату услуг проезда через мобильное приложение, используя как протокол NFC, так и QR-коды, обеспечивая удобство для пассажиров.

Инновационные банки также внедрили новые методы оплаты услуг с использованием биометрии лица и ладони. Так, технологии FacePay и PalmPay позволяют клиентам совершать платежи и операции в банковских учреждениях с помощью сканирования лица или ладони, что усиливает уровень безопасности и идентификации. Эти методы оплаты особенно полезны для клиентов, которые ценят простоту и удобство при совершении финансовых операций.

**➤ «РАЗВИТИЕ
НОВЫХ ФИНАНСОВЫХ
ТЕХНОЛОГИЙ ОТКРЫВАЕТ
НОВЫЕ ВОЗМОЖНОСТИ
ДЛЯ ПОЛЬЗОВАТЕЛЕЙ,
НО ТРЕБУЕТ ОТ
ФИНАНСОВЫХ УЧРЕЖДЕНИЙ
ПОСТОЯННОГО ВНИМАНИЯ
К ВОПРОСАМ БЕЗОПАСНОСТИ
И СОБЛЮДЕНИЯ
ЗАКОНОДАТЕЛЬСТВА»**



ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ

Цифровые технологии, автоматизированные решения обработки больших массивов данных становятся неотъемлемым элементом надзорной деятельности в сфере противодействия легализации (отмывания) преступных доходов и финансирования терроризма (ПОД/ФТ), реализации в ней риск-ориентированного подхода, оценки эффективности и коммуникаций с поднадзорными субъектами, автоматизации отдельных бизнес-процессов. Целями цифровизации выступают: повышение оперативности взаимодействия с контролируемыми лицами, снижение административной нагрузки на бизнес и высвобождение ресурсов надзорных органов



Виктория Капарчук,
советник Управления организации
надзорной деятельности
Росфинмониторинга



Яна Байрачная,
ведущий специалист-эксперт
Управления организации
надзорной деятельности
Росфинмониторинга



Александр Курьянов,
начальник Управления
организации надзорной
деятельности
Росфинмониторинга, к. э. н.

По некоторым экспертным оценкам в мире интенсивность внесения изменений в нормативные акты, регулирующих кредитно-финансовую сферу за последнее десятилетие выросла более чем в 5 раз. При этом наблюдается увеличение случаев привлечения

участников рынка к ответственности, все более частыми и существенными становятся штрафы за несоблюдение обязательных требований. Оптимизировать процесс соблюдения обязательных требований в условиях постоянного роста числа регуляторных требований способствуют RegTech

(Regulatory Technology) решения. Активная разработка RegTech началась в 2017-2019 гг., период роста регуляторной нагрузки и одновременного развития технологий искусственного интеллекта.

ЭКСПЕРТАМИ ОТМЕЧАЕТСЯ РЯД ПРЕИМУЩЕСТВ РЕГТЕХ РЕШЕНИЙ:

Повышение эффективности

Технологии способны обрабатывать с высокой скоростью большие объемы данных, например, быстро анализировать необработанный юридический текст и извлекать необходимую для надзорных целей информацию.

Повышенная точность и полнота

Ручные разрозненные процессы обычно создают пробелы в обеспечении соблюдения требований, что приводит к человеческим ошибкам и повышенному регуляторному риску. Внедрение RegTech, а также продуманная интеграция этих технологий позволяют устранить пробелы и упрощают процесс обеспечения соответствия нормативным актам.

Внутренняя согласованность и скоординированность

Технологические инструменты обеспечивают большую прозрачность всего бизнеса, объединяя когда-то разрозненные процессы и персонал. В результате формируется единая информационная среда, объединяющая различные подразделения в организации. Это позволяет быстрее обмениваться данными, что также приводит к повышению уровня соответствия требованиям.

Качественное управление рисками

Многие RegTech инструменты помогают эффективно снижать различные виды рисков, включая злоупотребления на рынке, кибератаки и мошенничество, путем мониторинга и оповещения о подозрительной активности.

Оптимизации исполнению обязательных требований также способствуют SupTech (*Supervisory Technology*) решения.

Под SupTech подразумевается использование цифровых инструментов, включая аппаратное и программное обеспечение, регулируемыми и надзорными органами для реализации своих функций¹.

Востребованность такого рода технологий, способных в том числе собирать, хранить, анализировать и визуализировать различ-

ные информационные массивы обусловлена ростом интенсивности и объема создания как структурированных, так и неструктурированных данных. Например, в дополнение к традиционным формам отчетности от подотчетных субъектов, компетентные ведомства активно используют информацию из открытых источников (например, публикации в социальных сетях) для расширения своих знаний.

Поскольку регулирующие, надзорные и правоохранительные органы полагаются на данные, внутренние процедуры и рабочие инструменты, а также человеческие и другие ресурсы, все они

сталкиваются с общими проблемами – хотя и в разной степени – связанными с низким качеством данных и трудоемкими ручными процессами. SupTech решения могут содействовать компетентным органам решить эти проблемы, повысив их возможности, эффективность и результативность сбора и анализа данных, в том числе обеспечивая автоматизацию рутинных задач, разработку новых аналитических методов и формирование обработанной информации.

Понятие SupTech трактуется по-разному, но в основном используется для обозначения надзорной практики в отношении участников рынка ценных бумаг. Так, ОЭСР отмечает эффективность SupTech решений для более эффективного выявления фактов инсайдерской торговли, манипулирования рынком и др.²

В настоящее время концепция SupTech рассматривается для более широкого круга надзорных органов, в том числе осуществляющих контроль в сфере обеспечения конкуренции, за соблюдением антикоррупционных требований и др. Экспертами отмечается, что SupTech, улучшая надзорные, аналитические, а также правоприменительные возможности компетентных органов, обеспечивают положительное влияние на финансовую стабильность, целостность рынка и благосостояние потребителей³. Инструменты SupTech также расширяют возможности надзорных ведомств в сборе и управлении данными, содействуя повышению их качества, что само по себе является предпосылкой для расширенного анализа данных.

Практика применения SupTech позволяет выделить основные преимущества их внедрения надзорными органами.

¹ Going Digital: Shaping Policies, Improving Lives / OECD Publishing. URL: Mode of access: <https://doi.org/10.1787/9789264312012-en>.

² Using digital technologies to improve the design and enforcement of public policies // OECD. URL: <https://dx.doi.org/10.1787/99b9ba70-en>.

³ The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: <https://www.fsb.org/wp-content/uploads/P091020.pdf>.



Улучшение возможностей обнаружения нарушений

Имеющиеся данные свидетельствуют о том, что надзорные органы, в том числе осуществляющие контроль за рынком ценных бумаг, соблюдением антимонопольных требований, а также правоохранительные органы, участвующие в борьбе с коррупцией, все чаще используют инструменты SupTech, чтобы лучше выявлять следующие преступления:

- факты отмыwania денег и финансирования терроризма, инсайдерской торговли и иные виды неправомерных действий (таких как неправомерные продажи и мошенничество);
- антиконкурентное поведение;
- факты взяточничества и коррупции за рубежом.

Приложения SupTech, в том числе базирующиеся на использовании искусственного интеллекта, особенно актуальны для этих целей, поскольку надзор основан на анализе больших массивов детализированных, срочных и неструктурированных данных из разрозненных источников. При этом цифровые технологии сами по себе способствуют возникновению новых форм ОД и ФТ, недобросовестных практик на финансовом рынке, мошенничества и антиконкурентного поведения, необходимы новые инструменты для их обнаружения и борьбы с ними.

Инструменты искусственного интеллекта используются в работе подразделений финансовой разведки для анализа входящего информационного потока: сортировки, объединения и определения приоритетности данных, указанных в сведениях о подозрительных операциях или деятельности клиента.

Органы контроля внедряют инструменты искусственного интеллекта для выявления нарушений в государственных закупках и проверки сообщений о коррупции. Например, в Бразилии технологии искусственного интеллекта используют для отбора поступающих сообщений о коррупции и для принятия решения о том, какие кейсы заслуживают дальнейшего расследования, а также анализа сигналов, которые позволяют выявлять незаконные процедуры государственных закупок до заключения контрактов.

Повышение эффективности правоприменительных действий

Инструменты искусственного интеллекта могут значительно повысить эффективность правоприменительных действий, поскольку расследования и судебные преследования, как правило, связаны с большими затратами времени и ресурсов. На этом фоне инструменты искусственного интеллекта могут быть полезны для анализа больших массивов данных, обеспечивая соответствие представленных материалов требованиям к формату и структуре, а также анализируя доказательства с использованием методов машинного обучения, таких как обработка текстов на естественном языке (*Natural Language Processing*). В целом инструменты искусственного интеллекта особенно хорошо подходят для стандартизации процедур и повторяющихся задач, связанных с большими объемами данных.

Улучшение сбора данных

Поскольку обязательная отчетность становится все более сложной, органы контроля сталкиваются с проблемами, связанными

со сбором запоздалых и некачественных отчетных данных, что, в свою очередь, может повлиять на их способность осуществлять мониторинг и надзор. Одновременно подотчетные организации несут существенные издержки на формирование отчетности для надзорных ведомств.

В целях улучшения сбора данных органы контроля в последние годы начали внедрять так называемые «вытягивающие» технологии, позволяющие органам власти получать сведения от регулируемого субъекта по мере необходимости. API-интерфейсы значительно облегчают предоставление данных подотчетными организациями, снижая соответствующие затраты и обеспечивая более эффективные коммуникации между сторонами⁴. Надзорные ведомства изучают способы перевода инструкций по составлению отчетов в машиночитаемый формат, чтобы автоматизировать регулятивную отчетность и еще больше облегчить соблюдение требований.

Повышение эффективности управления данными

Три основные задачи в рамках управления данными включают валидацию, консолидацию и визуализацию, каждая из которых относится к конкретным целевым точкам цикла управления данными. Валидация относится к проверке полноты, правильности и непротиворечивости данных в соответствии с правилами отчетности, в то время как консолидация относится к агрегированию данных из нескольких источников и в различных форматах, а визуализация предполагает представление информации наглядным образом⁵.

⁴ The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: <https://www.fsb.org/wp-content/uploads/P091020.pdf>.

⁵ The Suptech Generations // di Castri, S. et al. URL: <https://www.bis.org/fsi/publ/insights19.htm>.

Применительно к надзорной деятельности в сфере ПОД/ФТ можно выделить следующие направления использования цифровых решений:

- дистанционный мониторинг деятельности контролируемых лиц для последующего использования полученной информации в моделях оценки рисков;
- содействие проведению качественной надлежащей проверки клиентов и оценки их рисков;
- предоставление обратной связи, автоматизированное доведение до контролируемых лиц риск-оценки, сведений о наблюдаемых признаках нарушений ими обязательных требований;
- организация профилактических мероприятий (размещение обучающих материалов, в том числе видеокурсов, анкетирование, формирование разделов faq) и др.

Интересными представляются примеры внедрения SupTech и RegTech в деятельность надзорных органов зарубежных стран, в том числе государствах-членах ЕАГ.



Так, Агентство Республики Казахстан по финансовому мониторингу, используя возможность онлайн-сервиса «Личный кабинет» на своем портале, на ежедневной основе проверяет работу субъектов первичного финансового мониторинга и имеет возможность оперативно реагировать на признаки нарушений по ПОД/ФТ. Личный кабинет используется для направления сообщений в ПФР, а также доведения перечней для применения

целевых финансовых санкций по ФТ, обучения субъектов первичного финансового мониторинга (антиотмывочное законодательство, рекомендации, памятки, аналитические справки, описание типологий и др.), публикации различных отчетных данных по тематике ПОД/ФТ, а также предоставления обратной связи. Внедрение в практику Личного кабинета позволило оптимизировать взаимодействие с частным сектором, в том числе снизить объем документооборота.



Мексиканская CNBV (Comision Nacional Bancaria y de Valores), осуществляющая контроль (надзор) в сфере ПОД/ФТ реализует проект, включающий облачные вычисления для обработки больших объемов данных, связанных с соблюдением обязательных требований по ПОД/ФТ, что позволяет увеличить объем и гибкость хранения, мобильность и вычислительную мощность. Платформа также позволяет разрабатывать как базовую, так и расширенную перспективную аналитику для повышения эффективности мониторинга и лучшего выявления нетипичных моделей поведения.



В Сингапуре внедрены ИТ-решения для ранжирования организаций по уровню риска. Подход к оценке присущего риска банков обычно включает регулярный сбор некоторых агрегированных данных от каждого банка для оценки соответствующего уровня риска ОД/ФТ. Часто этот трудоемкий и длительный процесс, включающий в себя сравнение данных по сопоставимым банкам, может потребовать значительное количество качественных оценок.

Надзорный орган Сингапура во взаимодействии со специалистами по анализу данных составил исчерпывающий список индикаторов риска ОД/ФТ, разработал

форму для сбора необходимых данных в машиночитаемом формате, и разработал методологию оценки рисков для ее последовательного применения.

Сегодня имеется возможность оперативно сформировать интегральную риск-оценку ОД/ФТ каждого банка вместе с отчетом о ее основных факторах после получения соответствующих данных. Это позволило надзорным органам лучше выявлять финансовые организации с более высоким уровнем риска. Кроме того, если в конкретных банках на постоянной основе выявляются неожиданные существенные изменения в профиле рисков, в отношении них могут быть инициированы в оперативном порядке надзорные мероприятия.

В Сингапуре в надзорной деятельности в сфере ПОД/ФТ активно применяются методы анализа сетевых связей. Одним из источников данных являются сообщения о подозрительной деятельности (СПД). Используя методы сетевого анализа, надзорные органы разработали аналитический инструмент для выявления сетей юридических и физических лиц, которые связаны через различные СПД, поданные в разные периоды времени различными подотчетными субъектами. Такие данные сопоставляются со сведениями и профилем компании из так называемого корпоративного реестра (например, информация о деловой активности, руководителях и бенефициарных владельцах). Реализуя сетевой анализ этого многомерного набора данных, контрольные органы могут определять области повышенного риска и финансовые организации для проведения адресных надзорных мероприятий.

Технологии также могут изменить способ проведения выездных инспекций. Например, надзорные ведомства используют



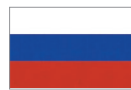
автоматизированный аналитический инструментарий для изучения всего пула транзакций проверяемой организации за 2-3 предшествующих года. Технология избавляет инспекторов от необходимости вручную проверять операционные данные для выявления аномалий. В конечном счете это позволяет контрольному органу уделять во время проверок большее внимание зонам повышенного риска и способствует более предметному диалогу с контролируемым лицом и его руководством по вопросам управления рисками и внутреннего контроля с обсуждением примеров из практики.



В Тунисе надзорными органами используется технология Blockchain для оценки рисков трансграничной перевозки наличных денег и адресного надзора за организациями. По результатам Национальной оценки рисков, проведенной в Тунисе в 2017 году международная перевозка наличных средств и контрабанда были отнесены к деятельности с высоким уровнем риска. В результате власти Туниса, включая ПФР, Центральный банк, таможенные органы и Министерство внутренних дел, в партнерстве с частным сектором (банки и пункты обмена валюты) разработали национальную платформу, использующую технологию блокчейн под названием «Ганнибал» для сбора, хранения и совместного анализа данных. Платформа формирует динамические информационные панели, позволяющие более эффективно анализировать риски ОД/ФТ, связанные с трансграничной перевозкой наличных денег. Это также помогает ПФР, правоохранительным органам, банкам и обменным пунктам выявлять и обнаруживать сети курьеров наличных.

Развитие автоматизированных систем, используемых для оценки рисков поднадзорных субъектов, а также онлайн-сервисов для вза-

имодействия с частным сектором выступают приоритетом надзорной деятельности, осуществляемой Росфинмониторингом.



Одним из таких RegTech решений, объединяющим более 60 тыс. подотчетных организаций (ИП), выступает Личный кабинет на сайте финансовой разведки. Сейчас это не только канал передачи сообщений в Службу и доведения информации о лицах, причастных к террористической деятельности и ФРОМУ, по сути это самостоятельный инструмент контроля, позволяющий решать целый ряд задач по повышению уровня осведомленности о требованиях законодательства и рисках, менять поведение контролируемого лица в антиотмывочном контуре.

Ключевым элементом данного механизма выступает система дистанционного доведения до подотчетных субъектов риск-оценки, формируемой по результатам дистанционного мониторинга. Эффективность таких корректирующих мер достаточно высокая, большим плюсом являются охват, невысокая затратность с точки зрения администрирования и возможность гибкой настройки и выбора критериев риск-оценки. Ежегодно несколько тысяч подотчетных субъектов снижают риски неисполнения обязательных требований по ПОД/ФТ в результате такого взаимодействия. Система позволяет не только снизить административную нагрузку на контролируемых лиц, но и перераспределить ресурсы надзорного органа на решение сложных аналитических задач, требующих профессионального суждения и опыта.

Функционал Личного кабинета ориентирован и на повышение уровня знаний субъектов ПОД/ФТ, их осведомленности о требованиях законодательства, результатах национальной оценки рисков, новых трендах и схемах противоправной деятельности.

НА ТЕКУЩИЙ МОМЕНТ В ЛИЧНОМ КАБИНЕТЕ РАЗМЕЩЕНО ОПИСАНИЕ БОЛЕЕ 60 ТИПОЛОГИЙ, ВКЛЮЧАЯ ПРИЗНАКИ ДЛЯ ИХ ВЫЯВЛЕНИЯ.

Также реализован функционал дистанционного обучения, размещен ряд учебных курсов, по результатам изучения которых пользователь имеет возможность оценить свои знания через тестирование. Имеется возможность автоматического предоставления разъяснений требований законодательства по типовым вопросам.

В контексте развития механизмов коммуникаций с частным сектором в 2022 году введен в эксплуатацию Личный кабинет профессионального сообщества (ассоциаций, гильдий), функционал которого позволяет в том числе доводить материалы, касающиеся выполнения подотчетными организациями требований законодательства о ПОД/ФТ, уведомлять о проводимых мероприятиях для организации участия в них членов соответствующих профессиональных сообществ и др.

В целях эффективного использования Личного кабинета в процедурах НПК создан агрегатор информации о проверяемом клиенте из максимально возможного количества источников в единую консолидированную форму.

Через Личный кабинет надзорного органа предоставлена возможность в онлайн режиме видеть результаты проводимого Росфинмониторингом дистанционного мониторинга, это обеспечивает оперативность реагирования органами контроля (надзора) в сфере ПОД/ФТ на риски в дея-

тельности своих поднадзорных субъектов, способствует применению единообразных подходов при планировании контрольной деятельности. Кроме того, через этот ресурс в режиме онлайн доводится макро-аналитика, позволяющая надзорному органу увидеть не только динамику параметров законопослушности сектора и вовлеченности его представителей в проведение подозрительных операций, но и его подверженность конкретным рискам. Среди задач на ближайшую перспективу – интеграция в Личный кабинет панели руководителя надзорного органа.

Такая панель, впервые разработанная для руководителей территориальных органов Росфинмониторинга (рисунок 1), предоставляет дополнительные аналитические данные, в том числе по эффективности применяемых мер надзорного реагирования в различных аналитических срезах (в разрезе инструментов контроля, отдельных регионов и видов деятельности). Это позволяет корректи-

ровать работу надзорного блока, выбирая наиболее эффективные подходы в осуществлении контрольной деятельности.

Личный кабинет также выполняет функции «обратной связи». Начиная с 2019 года обратная связь по направленным кредитными организациями сведениям о подозрительных операциях (СПО) доводится до подотчетных субъектов через Личный кабинет на сайте Росфинмониторинга в виде Индекса качества информационного потока (рисунок 2). На основе определенных алгоритмов формируется оценка по наиболее значимым критериям, характеризующим эффективность информационного взаимодействия подотчетных субъектов и Росфинмониторинга. В настоящее время оцениваются следующие параметры взаимодействия: оперативность направления СПО, фокус поступающих сведений на актуальные риски, характеристика взаимодействия с ПФР (направление сведений о рисках (типологиях), ответы на запросы ПФР,

нарушение сроков представления сведений в ПФР).

На основе данных критериев рассчитывается интегральная оценка, характеризующая качество взаимодействия субъекта с ПФР. В качестве результатов такого формата обратной связи: увеличение оперативности выявления сомнительных операций, повышение качества СПО, их фокуса на риски.

Важным условием повышения качества информационного потока от подотчетных субъектов выступает своевременная ориентация субъектов финансового мониторинга на актуальные риски и тренды в кредитно-финансовой сфере.

Одним из примеров такой практики является доведение до кредитных организаций типологий и признаков сомнительных операций через функционал Личного кабинета. В контексте ПОД/ФТ под типологией принимается проявление различных схем проведения сомнительных операций с использованием инфраструктуры

► Рисунок 1. Панель руководителя





финансовых учреждений, имеющих систематический или повторяющийся характер. Системность их проявления, как правило, связана с различными уязвимостями систем внутреннего контроля субъектов первичного финансового мониторинга.

Источниками информации о новых типологиях могут служить результаты финансового анализа как ПФР, так и субъектов финансового мониторинга. Например, Росфинмониторинг совместно с кредитными организациями – членами Совета комплаенс (консультативного органа при Межведомственной комиссии по ПОД/ФТ) регулярно рассматривает примеры финансового анализа, которые зачастую ложатся в основу типологий, доводимых через функционал Личного кабинета. Следует отметить, что информирование о рисках в таком формате также учитывается при расчете Индекса качества информационного потока.

Анализ поступившей информации, в том числе с указанием идентификатора типологий (для каждой из которой присваивается уникальный номер для направления СПО в случае выявления подозрительной операции, попадающей под соответствующие признаки) позволяет Росфинмониторингу делать в онлайн-режиме различные тематические выбор-

► Рисунок 2. Индекс качества информационного потока



ки, что упрощает анализ операционного потока.

В целом развитие ИТ-инфраструктуры позволяет надзорным органам выйти на качественно новый уровень работы, расширяя экспертные знания и оперативность выработки решений.

Ключевая цель развития цифровых технологий в надзорной деятельности в ближайшей пер-

спективе видится в содействии внедрению стандартов клиентоцентричности, обеспечивающих не только снижение регуляторной нагрузки, но и формирование за счет более адресных коммуникаций уникальной атмосферы партнерства и доверия между государством и частным сектором.



РЕЕСТР БЕНЕФИЦИАРНЫХ СОБСТВЕННИКОВ: ОПЫТ КАЗАХСТАНА

*В соответствии со статьями 6-1 Закона Республики Казахстан
«О противодействии легализации (отмыванию) доходов, полученных
преступным путем, и финансированию терроризма» Агентство Республики
Казахстан по финансовому мониторингу уполномочено вести Реестр
бенефициарных собственников юридических лиц (далее — Реестр)*



ДИНАРА МУСИНА,
руководитель Департамента
оперативного анализа
Агентства по финансовому
мониторингу Республики
Казахстан

Предоставление информации и сведений из Реестра о бенефициарном собственнике юридического лица осуществляется:

- 1) государственным органам Республики Казахстан, осуществляющим в пределах своей компетенции контроль за соблюдением субъектами финансового мониторинга законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, по подконтрольным им субъектам;
- 2) правоохранительным и специальным государственным органам;
- 3) субъектам финансового мониторинга.

В статье мы рассмотрим подходы, разработанные Агентством по финансовому мониторингу, по созданию и ведению Реестра,

а также его функционал, реализованный в личном кабинете для государственных органов — регуляторов, правоохранных органов и субъектов финансового мониторинга.

ПОДХОДЫ ПО СОЗДАНИЮ И ВЕДЕНИЮ РЕЕСТРА РЕАЛИЗУЮТСЯ НА ОСНОВЕ ТРЕХ ФАКТОРОВ:

- итоги проведенной оценки рисков юридических лиц, то есть степень их вовлеченности в предикатные преступления и отмывание денег;
- наличие доступа у Агентства к различным базам данным и ИТ-возможности по их обработке;
- актуализированные Рекомендации ФАТФ.



БИЗНЕС-ПРОЦЕСС РЕЕСТРА
БЕНЕФИЦИАРНЫХ
СОБСТВЕННИКОВ

Согласно Рекомендации ФАТФ, информация о бенефициарных собственниках должна быть полной, точной и актуальной, поэтому самым важным этапом разработанного бизнес-процесса стал сбор информации из различных источников.

Следовательно, начало бизнес-процесса включает в себя сбор информации о бенефициарных собственниках, заявленных самими юрлицами. Тут источниками информации являются:

- **Министерство юстиции**, которое консолидирует все регистрационные данные страны;
- **субъекты финансового мониторинга**, на которых возложена обязанность идентификации и фиксации бенефициарных собственников своих клиентов (реестр крупных акционеров, реестр бенефициарных собственников, ведомый по участникам Международным финансовым центром «Астана»);

- **Комитет государственных доходов**, которому в рамках исполнения налоговых обязательств резиденты представляют декларации о контроле иностранных компаний;
- **Агентство по финансовому мониторингу**, которое имеет полномочия запрашивать и получать информацию о бенефициарных собственниках.
- **Министерство энергетики и Министерство индустрии и инфраструктурного развития**, которые являются уполномоченными органами по получению и хранению информации о бенефициарных собственниках недропользователей (международный стандарт прозрачности в добывающих отраслях).

Итак, первый этап — это сбор из нескольких источников всех данных, заявленных самими юрлицами о своих бенефициарных собственниках.

Большая часть этой информации доступна Агентству по финансовому мониторингу в онлайн-режиме. Соответственно, сбор и ее консолидация являются автоматизированным процессом.

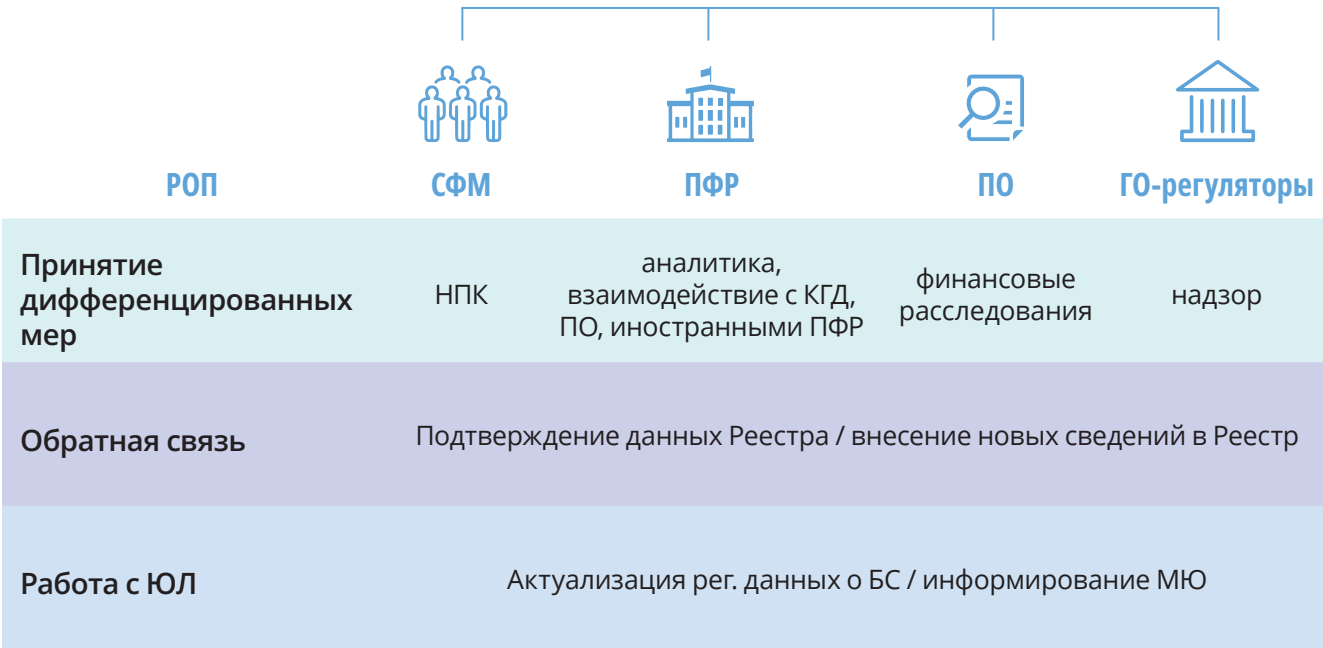
ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ
ДАННЫХ

Далее с целью перепроверки данной информации осуществляется сбор сведений из дополнительных источников информации, таких как:

- сообщения по пороговым и подозрительным операциям — от субъектов финансового мониторинга;
- налоговые декларации — от Комитета государственных доходов;
- родственные и корпоративные связи — от Министерства юстиции;
- электронные счета-фактуры — от Комитета государственных доходов;
- сведения иностранных подразделений финансовой разведки — история запросов;
- открытые источники данных в интернете.

СТАТУСЫ БЕНЕФИЦИАРНЫХ
СОБСТВЕННИКОВ

На базе совокупности сведений разработана детализированная методология алгоритмов обра-



ботки этих данных в части определения бенефициарных связей. Алгоритмы обработки данных автоматизированы. На сегодняшний день это 19 алгоритмов, которые уже применяются и показывают свою эффективность.

**ИТОГОМ РАСЧЕТОВ
ТАКИХ АЛГОРИТМОВ
ЯВЛЯЕТСЯ ПРИСВОЕНИЕ
ФИЗИЦАМ ОДНОГО ИЗ
СЛЕДУЮЩИХ СТАТУСОВ:**

- «Регистрационный бенефициарный собственник»
- «Предполагаемый бенефициарный собственник»

Регистрационными признаются только сведения о собственниках, представленные в Министерство юстиции, остальные признаются предполагаемыми.

Каждый алгоритм определения «предполагаемого бенефициарного собственника» исходит из отдельной методики и источника информации, имеет свой вес, свой балл достоверности. На сегодня достоверность имеет экспертную балльную шкалу от 1 до 4, где 1 — это низкая вероятность достоверности, 4 — высокая.

Каждый алгоритм запускается по расписанию. Итоги каждого запуска алгоритмов сохраняются.

Пользователями Реестра являются участники антиотмывочной системы: государственные органы — регуляторы, правоохранные органы, субъекты финансового мониторинга, подразделение финразведки.



**С УЧЕТОМ
ПРОВЕДЕННОЙ
ПРОФИЛЬНОЙ РАБОТЫ
ПОЛЬЗОВАТЕЛЬ РЕЕСТРА
ИМЕЕТ ВОЗМОЖНОСТЬ
ВНЕСТИ В РЕЕСТР ПО
ПРЕДПОЛАГАЕМЫМ
БЕНЕФИЦИАРНЫМ
СОБСТВЕННИКАМ СВОЮ
ПОЗИЦИЮ, А ИМЕННО:**

1. Подтвердить либо не подтвердить гипотезу подразделения финансовой разведки.
2. Добавить свою гипотезу — дополнительного предполагаемого бенефициарного собственника с описанием своего алгоритма/схемы.

Каждая обратная связь участника антиотмывочной системы ценна и способствует совершенствованию и расширению действующих 19 алгоритмов.

Кроме того, в ходе проведения профильной работы с клиентами, с объектами анализа, с объектами контроля пользователи стимулируют актуализацию регистрационных данных самими юридическими лицами.

Таким образом, активно используя Реестр бенефициарных собственников в своей деятельности, каждый участник антиотмывочной системы вносит вклад в наше общее дело по предотвращению и пресечению вовлечения юридических лиц в предикатные преступления и отмывание денег.



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ФИНТЕХ: О НАСТОЯЩЕМ И БУДУЩЕМ

35 СВЕТЛАНА ОРЛОВА:

«Цифровые продукты и решения — это уверенные шаги к развитию государственного финансового аудита»

39 ВИКТОР ДОСТОВ

Искусственный интеллект в финансах и его влияние на некоторые аспекты ПОД/ФТ

43 МИХАИЛ ПРОНИН

Применение искусственного интеллекта в работе службы финансового мониторинга банка

46 АЛЕКСЕЙ ГЕЛЕТА:

«Финтех-рынок России можно назвать одним из наиболее инновационных и технологически продвинутых в мире»

СВЕТЛАНА ОРЛОВА:

«ЦИФРОВЫЕ ПРОДУКТЫ И РЕШЕНИЯ — ЭТО УВЕРЕННЫЕ ШАГИ К РАЗВИТИЮ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО АУДИТА»



О мерах по внедрению искусственного интеллекта в сфере государственного контроля (аудита), возможностях новых технологий для совершенствования государственного управления, а также актуальных цифровых решениях в профильной области редакции журнала «Финансовая безопасность» рассказала аудитор Счетной палаты Российской Федерации Светлана Орлова

— Светлана Юрьевна, благодарю вас за выделенное время в вашем плотном рабочем графике. Тема этого номера связана в том числе с развитием искусственного интеллекта. На ваш взгляд, как возможности ИИ реализовать в сфере государственного финансового контроля (аудита)?

— Для начала я хотела бы отметить, что мы работаем в векторе,

данном Президентом России Владимиром Путиным на Петербургском международном экономическом форуме в июне 2023 года. Он звучит так: «Ключевое направление экономики предложений касается активной автоматизации и освоения технологий искусственного интеллекта. Нужно активно внедрять и использовать эти разработки, поддерживать подготов-

ку отечественного программного обеспечения в сфере больших данных, запускать проекты в области искусственного интеллекта».

В феврале 2024 года Президентом Российской Федерации внесены ключевые дополнения в Национальную стратегию развития искусственного интеллекта на период до 2030 года. В частности, федеральным органам исполни-

тельной власти (ФОИВ) необходимо руководствоваться положениями данной стратегии при разработке и реализации отраслевых документов стратегического планирования. Таким образом, после внесенных изменений деятельность ФОИВ будет в определенном смысле ориентироваться на технологии искусственного интеллекта.



Неизменность этой стратегической линии была озвучена в Послании Президента Российской Федерации Федеральному Собранию. Счетная палата на протяжении последних лет работает в этом направлении. Прежде всего над цифровизацией деятельности инспекторского состава.

Безусловно, отдельные технологии искусственного интеллекта уже используются в смартфонах, медицине, образовании, системах умных домов и промышленности.

Важные элементы, необходимые для создания и использования технологий искусственного интеллекта, — это большие данные,

умение их анализировать, используя технологии нейронных сетей.

В сфере государственного финансового аудита (контроля) из названных элементов искусственного интеллекта особое значение имеет качество больших данных и особенно их достоверность. Именно на организации анализа больших данных первоначально и было сосредоточено наше внимание. В рамках цифровых решений, созданных в Счетной палате при помощи цифровых инструментов сбора, анализа и визуализации данных (дата-аналитики), эта задача в основном была решена. На конец 2023 года реестр цифровых решений и продуктов Счетной палаты содержит данные о более чем 300 цифровых решениях и продуктах.

Эти решения выводят проведение аудита на новый уровень с применением современных технологий и методов.

Кроме того, цифровые решения как минимум на треть снижают время работы инспектора по анализу данных объекта аудита (контроля). За счет минимизации человеческого фактора риск ошибок практически равен нулю. И третье — значительно расширен диапазон проверяемой информации.

Конечно, это было бы невозможно без масштабной работы по цифровой трансформации аудита, проводимой в Счетной палате.

В рамках направления аудита государственного управления, которое я возглавляю, мы способствуем цифровой трансформации и в наших объектах аудита.

— *Светлана Юрьевна, раз уже есть результаты работы в этом направлении, прошу вас более детально на этом остановиться.*

— В качестве примера могу привести совместную работу по внедрению современных информационных технологий в судопроизводство.

В 2023 году мы провели 4 расширенных совещания с 15 министерствами и ведомствами — лидерами цифровизации, в том числе Минцифры России, Минюстом России, Федеральным казначейством, Федеральной налоговой службой, Федеральной службой судебных приставов, Росимуществом и другими ведомствами. С ними мы обсудили лучшие практики внедрения современных информационных технологий в судопроизводство, межведомственное взаимодействие государственных органов и судебной системы, в том числе совершенствование процесса работы с депозитными счетами арбитражных судов.

Эти вопросы мы поднимали на встрече с коллегами из Правительства Российской Федерации, Верховного Суда Российской Федерации и Совета Федерации Федерального Собрания Российской Федерации.

При нашем участии в конце 2023 года Судебным департаментом при Верховном Суде Российской Федерации, Минцифры России и Федеральным казначейством заключено соглашение о намерениях выработки общих подходов в сфере внедрения современных информационных и коммуникационных технологий в процесс судопроизводства и судебного делопроизводства.

Результатом этого взаимодействия должно стать создание удобного для граждан и бизнеса сервиса, включенного в судебный процесс, который позволит упростить внесение участниками судопроизводства денежных средств, повысит прозрачность их движения и сведет на нет возможности злоупотребления этими денежными средствами.

Сейчас этот проект находится на стадии проработки технических решений, и мы полагаем, что его пилотная реализация может начаться уже в ближайшее время на базе Арбитражного суда города Москвы.

тического мероприятия «Анализ администрирования лицевых (депозитных) счетов для учета операций с денежными средствами, поступающими во временное распоряжение арбитражных судов, в 2012–2022 годах и истекшем периоде 2023 года».

Основная цель цифрового решения — сопоставить платежные документы по средствам, поступающим во временное распоряжение арбитражных судов, с количеством принятых к рассмотрению дел за 11 лет и проверить исполнение положений Регламента организации деятельности федеральных судов и управлений Судебного департамента в субъектах Российской Федерации по работе с лицевыми (депозитными) счетами для учета операций со средствами, поступающими во временное распоряжение.

А теперь исходные данные: количество платежных документов — около 9 млн; количество арбитражных дел — свыше 27 млн.

Сложно представить, сколько потребовалось бы инспекторов и времени на обработку и анализ этого массива информации и цифр.

При этом еще имелись сложности, которые заключались в том, что данные характеризовались существенной неопределенностью: денежные средства вносились одними лицами, а могли выплачиваться иным лицам, в том числе не участвующим в судебном процессе, а также неполнотой данных в части поступавших на депозитный счет суда денежных средств (где вместо ИНН суда указаны ИНН управления федерального казначейства).

Разработанное цифровое решение позволило решить эту задачу. И самое главное:

- по результатам этого мероприятия подтверждена необходимость реализации пилотного проекта по оптимизации и автоматизации процессов распоряжения денежными средства-



ми, находящимися на лицевых счетах, открытых в органах Федерального казначейства, внесенными гражданами и организациями в соответствии с процессуальным законодательством;

- предложено внести изменения в Регламент организации деятельности федеральных судов и управлений Судебного департамента в субъектах Российской Федерации по работе с лицевыми (депозитными) счетами для учета операций со средствами, поступающими во временное распоряжение.

— Над каким цифровым решением трудятся ваши сотрудники в настоящее время?

— Сегодня, получив обратную связь от ряда департаментов Счетной палаты, мы дорабатываем цифровое решение, разработанное в рамках реализации наших Методических рекомендаций по выявлению и оценке коррупционных рисков.

Доработка решения проводится с помощью новой технологии —

так называемого «генеративного» искусственного интеллекта.

Для тех, кто с этим еще не столкнулся, поясню, технология подразумевает возможность обучения собственного алгоритма поиска информации в соответствии с заданными критериями.

После доработки и апробации решения результаты анализа госконтракта будут отображать не только указание на возможные рискованные зоны, но и описание риска, совокупности причин, по которым выявлены риски возможного нарушения.

Кроме того, когда проект будет готов, мы сможем анализировать не только выборочно контракты, а планируем пакетную загрузку документов в любом машиночитаемом формате.

Автоматизированный процесс выявления рискованных зон позволит в разы сократить время обработки и анализа документов.

Особо хочу обратить внимание, что никакой искусственный интеллект не заменит работу инспектора и может являться только его помощником.

➤ «ОСОБО ХОЧУ ОБРАТИТЬ ВНИМАНИЕ, ЧТО НИКАКОЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НЕ ЗАМЕНИТ РАБОТУ ИНСПЕКТОРА И МОЖЕТ ЯВЛЯТЬСЯ ТОЛЬКО ЕГО ПОМОЩНИКОМ»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ФИНАНСАХ И ЕГО ВЛИЯНИЕ НА НЕКОТОРЫЕ АСПЕКТЫ ПОД/ФТ



Виктор Достов,
председатель Ассоциации
«Электронные деньги»,
старший научный сотрудник
Финансового университета
при Правительстве Российской
Федерации, к. ф.-м. н.

Искусственный интеллект стал, вероятно, самым громким технологическим прорывом двух последних лет. Несомненно, качественный скачок в его развитии позволит нам пересмотреть традиционные подходы к решению множества интеллектуальных задач, ранее требовавших для решения участия человека, и расширить круг задач, решаемых без человеческого участия

Согласно недавнему консультативному докладу ЦБ РФ¹, финансовая сфера стала одним из наиболее активных потребителей новой технологии. В данной статье мы весьма кратко попытаемся рассмотреть суть этого технологического прорыва и его возможное влияние на развитие сектора с особым вниманием на аспекты ПОД/ФТ.

ВВЕДЕНИЕ В ТЕХНОЛОГИЮ

В формате статьи невозможно дать исчерпывающее введение в столь широкую технологию, как ИИ, обладающую к тому же многолетней историей разработки и использования. Мы ограничимся формулировкой ключевых моментов, связанных с магистральными на нынешний момент нейронны-

ми сетями и большими языковыми моделями (LLM, Large Language Models) на их основе. Слово «языковой» не должно вводить в заблуждение — любой объект, переводимый в последовательность нулей и единиц, — книга, оцифрованная фотография, скоринговые данные, платежные графы криптовалют или колебания их курсов, видео и прочее — с точки зрения

¹ <https://cbr.ru/press/event/?id=17177>.



ИИ представляет собой высказывания на специализированных языках.

Очень упрощенно нейронная сеть представляет собой последовательность преобразований столбцов исходных значений (векторов) в конечный вектор-результат. Например, типичная LLM берет исходный текст, то есть столбец (или более привычно, строку) буквенных символов и превращает их в столбец (строку) на выходе. Текст этой статьи ИИ тоже видит как длинный столбец из букв. Можно подать его на вход ИИ, добавив к нему столбец-вопрос, и получить ответ Да/Нет или ответ в развернутой форме, или перевод на другой язык. В виде столбца символов можно представить множество объектов — например картинки, видео, данные научного эксперимента, наборы транзакций и многое другое.

Само по себе преобразование на удивление просто. Мы берем первый столбец, преобразуем его во второй по простому правилу: каждая ячейка в столбце-результате представляет собой сумму всех значений в первом столбце, помноженную на произвольные коэффициенты A_{ij} , образующие таблицу (матрицу). Далее полученные значения в каждой ячейке второго столбца преобразуются при помощи несложных формул, которые уменьшают маленькие значения и увеличивают большие, повышая, так сказать, контрастность результата. Дальше из второго столбца по такому же правилу при помощи следующей матрицы A_{ij} делается третий столбец и так далее, до столбца ответа. Матрица коэффициентов вместе с формулой преобразования и столбцом образуют слой, необходимое число слоев на удивление мало. В 1958 году Розенблатт показал, например, что для любой задачи классификации образов (распознавание цифр и букв, выделение машин и пешеходов и

множество других задач) достаточно нейросети с тремя слоями.

Откуда ИИ берет матрицы A_{ij} ? Тут тоже все просто — его нужно обучать. Процесс обучения незамысловат. Сначала коэффициенты выбираются случайно, и ИИ показывает входную строку с известным ответом — например, вопрос, про который известен ответ Да или Нет. ИИ выдает ответ, для начала тоже случайный. Если он угадал, то ему задают следующий вопрос. Если не угадал — матрицу немного меняют и повторяют вопрос, потом еще немного меняют и повторяют снова, пока не получится правильный ответ. Такой подбор повторяют невообразимое множество раз, пока правильный ответ не будет получаться в подавляющем большинстве случаев (или всегда). Тогда ИИ считают обученным и выпускают в реальную жизнь отвечать на новые вопросы.

Человечество очень давно мечтало о создании искусственного интеллекта. Говоря о языковых моделях, первые идеи были предложены российским математиком Марковым в 1913 году. Однако только около 2022 года набралась критическая масса программных, аппаратных и контекстных возможностей для обучения мощного искусственного интеллекта и стремительно стали появляться модели для обработки текстов и изображений.

При этом оказалось, что LLM на базе нейросетей обладают свойством универсальности. Исторически разработки в области ИИ велись по множеству относительно несвязанных направлений. Для анализа текстов использовались совсем другие алгоритмы, чем для игр или управления беспилотниками. Нейронные сети с

глубоким обучением оказались всеядными — они успешно решали любые классы задач, каким-то образом преобразованные в вектора данных. Это позволило уйти от распыления ресурсов и сконцентрироваться на одном прорывном направлении. Использование ИИ немедленно стали диффундировать в самые разнообразные области человеческой деятельности — от цифрового искусства до медицины. Разумеется, финансовая область не стала исключением.

ИИ В ФИНАНСАХ

В силу первоначальной концентрации на языковых моделях самые быстрые внедрения были связаны с общением с клиентом. К ним можно отнести чат-боты поддержки, аналитику по обращениям, контроль над работой персонала колл-центров и так далее. Туда же относится, например, оптимизация описаний продуктов. Здесь используются общие языковые модели, финансовая специфика появляется только в контексте.

На анализе поведения клиентов основано и использование ИИ для оптимизации самих продуктов. Обучение в данном случае производится на линейке различных параметров продукта, например, депозита, и ИИ обучается оптимизировать эти параметры для достижения нужного результата — например, уровня продаж. Предпринимались и более амбициозные попытки по анализу и оптимизации поведения клиента в целом, но удивительным образом поведение клиентов оказалось плохо управляемым.

Отдельным направлением является скоринг. ИИ позволяет рейтинговать клиентов на основе достаточно нетривиальных подходов и связей между различными параметрами, позволяя, например, более успешно выдавать кредиты.

Большие надежды возлагаются на использование ИИ в информационной безопасности банков. Любой внешний запрос к автоматической банковской системе (АБС) может рассматриваться ИИ с точки зрения того, происходит ли он от легитимного клиента или это компьютерная атака. Объектом обучения служат большие записи истории с разбивкой на добросовестные запросы и попытки атак.

Это весьма краткий список примеров, он постоянно растет с точки зрения разнообразия сегментов применения.

ИИ и ПОД/ФТ

На практическую важность использования ИИ в ПОД/ФТ аналитики обратили внимание достаточно давно. Еще в 2018 году KPGM и Ассоциация сертифицированных специалистов по борьбе с отмыванием средств (ACAMS) отметила резкое ускорение внедрения ИИ для борьбы с отмыванием. На это же, в частности, обратило внимание и ФАТФ в своей аналитической записке². На данный момент мы видим следующие ключевые направления:

1. Анализ риска клиентов при постановке на обслуживание

В этом случае ИИ обучается на большой базе прошлых клиентов банков (юридических и физических лиц), по которым а posteriori известно их качество. Обучение позволяет гораздо более эффективно ранжировать клиентов по степени риска, решая в значительной мере проблему дерискинга. По данным Сбербанка и HSBC, таким образом удастся поставить на обслуживание достаточно значительную часть клиентов, которые при традиционной процедуре рас-

смотрения получали немотивированный отказ.

2. Анализ текущих операций

Классический анализ операций оперирует заданными паттернами, например дроблением платежей, консолидацией, использованием подозрительных посредников и так далее. Однако реальные схемы часто бывают более изощренными и не подпадают под формальный анализ. ИИ позволяет уйти от ограничений формальных критериев и более эффективно отслеживать и рапортовать о подозрительных операциях. Такие методы уже используются ВТБ, Сбербанком, Standard Chartered, JPMorgan Chase, Danske Bank и другими. Следует отметить, что такие механизмы эффективны и для контроля над распределенными платежными системами. В частности, уже в августе 2020 года Росфинмониторинг сообщил о разработке прототипа системы анализа криптовалютных транзакций, основанной на технологии искусственного интеллекта. Система получила название «Прозрачный блокчейн» и в феврале 2021 года заработала.

3. Построение графов аффилированности

Важнейшей технической задачей ПОД/ФТ является нахождение скрытых бенефициарных и аффилиационных связей между участниками сложных платежных конструкций. ИИ позволяет анализировать как платежные операции, так и внешнюю информацию (записи в реестрах юридических лиц, информацию о собственниках из внешних источников и так далее) для построения графов, где в узлах находятся юридические и физические лица, а связи между узлами отражают степень аффилированности. На основе этого успешно выявляются формальные и неформальные отношения между внешне независимыми участниками платежных операций.

4. Мониторинг человеческого комплаенса

Данная модель впервые была опробована на работе «человеческих» колл-центров (например, решения JustAI). Существует ряд клиентских проблем, которые на современном уровне ИИ решить не может. Однако, анализируя тек-



² Opportunities and challenges of new technologies for AML/CFT <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf>.



стовые и голосовые диалоги, он может дать оценки и рекомендации по качеству работы людского персонала. Аналогично, ИИ может мониторить работу «человеческого» комплаенса, вычлняя типовые ошибки, ранжируя персонал по качеству и давая соответствующие рекомендации.

5. Анализ изменений в законодательстве

Определенные надежды возлагаются на использование ИИ при автоматической обработке нормативных документов. Это потенциально позволяет оптимизировать внутренние политики банка при изменении требований регулятора.

6. Анализ контрактов

В деятельности комплаенса значительное время занимает анализ документов, предоставляемых для подтверждения происхождения средств и целей транзакции. Это достаточно большая нагрузка в силу специфичности и разнообразия данных документов. ИИ способен анализировать данные документы на предмет их подлинности и соответствия целям сделки.

7. Построение базовых показателей

Как указывалось выше, ИИ может изменить модель комплаенса путем перехода от фиксированного набора критериев к анализу полного набора операций. Возможен и обратный переход — можно обучить ИИ на наборе сомнительных операций, поручив ему выбрать наиболее эффективный ограниченный набор критериев для быстрого анализа.

8. Идентификация

Отдельный блок задач связан с идентификацией клиента. Эти задачи не являются специфичными для финансового сектора и скорее связаны с общей задачей иденти-

фикации личности. Сюда относятся анализ фотографий клиента и фотодокументов, анализ речи и видеозаписей и любые другие методики, повышающие достоверность идентификации личности как удаленно, так и в режиме присутствия.

УЯЗВИМЫЕ СТОРОНЫ ИИ ПРИМЕНИТЕЛЬНО К ПОД/ФТ

При всех преимуществах ИИ обладает спецификой, несущей потенциальную угрозу в любой области применения и особенно в финансовой. В отличие от алгоритмических подходов, допускающих анализ принятия решений ИИ, нейросеть в принципе не допускает интерпретации в терминах алгоритма. Мы не можем, например, при анализе подозрительных операций вычлнить участки матриц A_{ij} , отвечающие за поиск дробления и консолидации, и так далее. Поэтому мы не можем проверить надежность работы алгоритма иначе как статистически, давая ему большое количество задач и проверяя качество. Даже при этом существует ряд типовых проблем, например:

- галлюцинации, когда на основании правильных данных ИИ создает артефакты, не имеющие отношения к действительности. Были случаи, когда ИИ изобретал судебные прецеденты или предлагал несуществующие скидки;
- минные поля, когда ИИ при незначительной модификации исходных данных выдает абсолютно неправильные ответы. Природа этого явления окончательно непонятна, что затрудняет борьбу с ним;
- переобучение, когда повышение объема и качества входных данных необъяснимо приводит к деградации качества ответов, и целый ряд других.

Относительно эффективным средством является использование многокомпонентных систем, в которых одна нейронная сеть проверяет результаты другой. Тем не менее окончательного решения для этих проблем на сегодня нет.

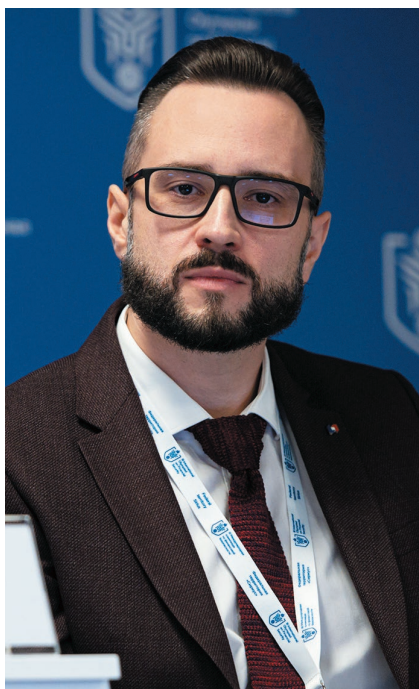
ИСПОЛЬЗОВАНИЕ ИИ С ЦЕЛЬЮ ОД/ФТ

Разумеется, такой мощный инструмент неизбежно привлеч внимание криминального сообщества. У нас пока нет типизации применения ИИ для отмывания денег или финансирования терроризма, однако мы можем достаточно уверенно рассмотреть следующие возможности: использование ботов для общения с банками при онбординге, изготовление фальшивых идентификаторов личности, симуляция личности при удаленной идентификации, оптимизация скриптов для социального инжиниринга, оптимизация графов криминальных транзакций и так далее. Эта тема заслуживает отдельной статьи.

Нет никаких сомнений, что ИИ найдет эффективное применение в банковской сфере в целом и в ПОД/ФТ в частности. На взгляд автора, сейчас практические возможности ИИ преувеличены, и в ближайшее время они будут критически переоценены. Тем не менее анализ возможностей ИИ и разработка методологии борьбы с криминальными использованиями ИИ должны стать одним из приоритетов аналитиков и практиков в сегменте ПОД/ФТ.

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОТЕ СЛУЖБЫ ФИНАНСОВОГО МОНИТОРИНГА БАНКА

Сегодня тема применения искусственного интеллекта стала мейнстримом для любых областей деятельности. При этом банковская сфера часто выступает своеобразным локомотивом для продвижения новых высокотехнологичных ИТ-продуктов и решений



➤ МИХАИЛ ПРОНИН,
вице-президент —
директор Департамента
финансового мониторинга
ПАО «Промсвязьбанк», к. э. н.

Мы видим большое количество успешных решений в кредитовании, транзакционном обслуживании клиентов и особенно по направлениям, где экспертиза во многом строится на автоматизированном анализе клиентских данных и клиентского поведения.

В этой логике формируется впечатление, что противомошенническая сфера, сосредоточенная на выявлении подозрительной активности клиентов, идеально подходит для применения инструментов машинного обучения, одного из подмножеств области искусственного интеллекта.

В аналитической работе подразделения по финансовому мониторингу Банка ПСБ эксперименты с применением инструментов машинного обучения мы начали проводить в 2020 году. Основной акцент делался на различные математические модели поиска аномалий в платежном поведении клиентов.

Были достигнуты определенные качественные результаты за счет использования алгоритма, сочетающего в себе дерево решений и логистическую регрессию. Однако значительных успехов, когда работа такой модели по эффективности была на порядок лучше, чем рабо-

та экспертов-аналитиков, мы долго не могли получить.

Зато мы получили важный опыт, который в дальнейшем позволил определить стратегию наших действий.

Во-первых, мы выявили интересную закономерность. В большинстве случаев платежное поведение подозрительных клиентов не является аномальным по отношению к клиентской базе в целом. Это связано с тем, что подозрительные клиенты, для того чтобы не быть обнаруженными, вынуждены постоянно «мимикрировать».

Такое приспособление и подражание нормальному поведению добропорядочных клиентов приводит к тому, что математические модели относят к аномальному поведению не подозрительных клиентов, а поведение той части добропорядочных клиентов, которые не ведут себя стандартным образом. Такая специфика свойственна, например, молодым начинающим предпринимателям или редким сферам бизнеса, для которых нетиповое платежное поведение обосновано особенностями функционирования самой сферы деятельности.

Во-вторых, отмеченная нами постоянная подстройка поведения высокорисковых клиентов к стан-



дартному нормальному поведению приводит к постоянным изменениям самих аналитических данных. В результате модели, которые прекрасно работали вчера, очень быстро теряют эффективность и требуют замены на новые. Причем чем интенсивнее мы подвергаем эту область мониторингу с использованием инструментов машинного обучения и сложных аналитических моделей, тем быстрее она начинает меняться.

Этим внедрение инструментов искусственного интеллекта в финансовом мониторинге разительно отличается от их внедрения в других областях. Например, в том же ритейле модель универсального поведения покупателя в магазине при анализе на большом объеме данных достаточно точна и последовательна. Благодаря этому поведение покупателя в магазине может успешно прогнозироваться.

Поэкспериментировав в том, насколько непроста будет в решении задача внедрения искусственного интеллекта в финансовом мониторинге, мы поняли, что в самой экспертизе рисков ОД/ФТ мы разбираемся хорошо, а вот в применении инструментов машинного обучения у нас своей внутрикомандной экспертизы нет, и в 2022 году мы приняли решение начать нанимать аналитиков данных непосредственно в подразделение по ПОД/ФТ.

Важно понимать, что от привычного нам клиентского аналитика, ведущего противолегализаци-

онные расследования, аналитик данных отличается разительно. Это совсем иной работник, требующий индивидуальной коммуникации и специальных профессиональных инструментов. Так в нашей операционной деятельности появились «песочницы» с данными, мощные компьютеры, программирование на Python и BI-инструменты визуализации данных.

Далее мы создали партнерскую среду, в которой клиентские аналитики смогли без ограничений выдвигать поисковые гипотезы по возможному новым методам выявления подозрительных клиентов, а аналитики данных оцифровывать такие гипотезы в соответствующие модели. Полученные модели ставились в регламентный режим, а результаты их работы вновь возвращались на верификацию к клиентским аналитикам. Если эффективность работы моделей снижалась, то клиентский аналитик формулировал гипотезу по ее уточнению, либо совсем новую гипотезу в этой же тематике риска, которая по ранее описанному циклу уходила в реализацию к аналитику данных.

Формирование общей коммуникативной среды клиентских аналитиков и аналитиков данных привело не только к синергетическим результатам совместного труда, но и к интенсивному встречному повышению квалификации работников и развитию у них новых компетенций. Аналитики данных стали погружаться в предметную

область. Да, перед ними не стояла задача превращения в клиентских аналитиков, ведь такие специалисты у нас уже есть. Но сближение помогло им начать понимать, как сфера противодействия легализации преступных доходов представлена именно в части подходов к работе с данными. Как итог, аналитики данных начали под разные гипотезы подбирать наиболее подходящие инструменты обработки данных.

Не отставали и клиентские аналитики. Если раньше вопросы, связанные с информационными технологиями, казались им чем-то сложным и недоступным, то, посмотрев, как все устроено, отдельные части функционала работы аналитика данных они стали забирать на себя. Дополнительно знакомство с инструментами аналитики данных позволило классическим клиентским аналитикам начать формулировать более сложные гипотезы выявления риска.

В целом это достаточно интересный опыт, который мы определили для себя как коллаборацию естественного интеллекта и интеллекта искусственного.

Описанный цикл работ мы поставили на конвейер, что позволяет:

1. Оперативно реагировать на новые риски и типологии подозрительной активности клиентов, о которых мы узнаем от Банка России и Росфинмониторинга. Тестовая настройка новых моделей риска занимает не более 2 рабочих дней.

» «ПОЭКСПЕРИМЕНТИРОВАВ В ТОМ, НАСКОЛЬКО НЕПРОСТА БУДЕТ В РЕШЕНИИ ЗАДАЧА ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ФИНАНСОВОМ МОНИТОРИНГЕ, МЫ ПОНЯЛИ, ЧТО В САМОЙ ЭКСПЕРТИЗЕ РИСКОВ ОД/ФТ МЫ РАЗБИРАЕМСЯ ХОРОШО, А ВОТ В ПРИМЕНЕНИИ ИНСТРУМЕНТОВ МАШИННОГО ОБУЧЕНИЯ У НАС СВОЕЙ ВНУТРИКОМАНДНОЙ ЭКСПЕРТИЗЫ НЕТ, И В 2022 ГОДУ МЫ ПРИНЯЛИ РЕШЕНИЕ НАЧАТЬ НАНИМАТЬ АНАЛИТИКОВ ДАННЫХ НЕПОСРЕДСТВЕННО В ПОДРАЗДЕЛЕНИЕ ПО ПОД/ФТ»



▲ Панельная дискуссия на финале III Международной олимпиады по финансовой безопасности

2. Постоянно повышать эффективность применяемых аналитических правил онлайн- и офлайн-мониторинга клиентских операций. Благодаря этому при постоянном росте клиентской базы мы можем позволить себе не наращивать численность персонала.

3. В большом количестве апробировать собственные гипотезы выявления новых видов и обновленных вариаций старых схем подозрительных операций. Ежеквартально не менее 10 гипотез проходят путь от идеи до работающего алгоритма.

Поделюсь еще одним интересным наблюдением. В октябре 2023 года в рамках Международной олимпиады по финансовой безопасности мы проводили мастер-класс для студентов, на ко-

тором рассказывали про наш аналитический проект «Паттерны». Это такой внутренний проект по разработке нового высокоэффективного инструмента выявления подозрительных операций в деятельности клиентов.

Фактически сама возможность нам в этот проект войти возникла благодаря накопленным работам в машинном обучении с участием аналитиков данных и обретенному нашими клиентскими аналитиками навыку формулирования аналитических гипотез.

И вот мы перед студентами делимся этим впечатлением об успешном симбиозе и фантазируем, как было бы прекрасно, если в будущем эти навыки могли бы быть воплощены в одном работнике, который анализирует клиентов, синтезирует гипотезы, потом

их самостоятельно программирует и применяет для выявления высокорисковых операций.

И получаем вопросы из зала, почему это еще не так. Представьте себе, что именно такими специалистами в будущем представляют себя наши сегодняшние студенты — участники Олимпиады. И не только представляют, но и последовательно готовят себя к такому формату работы, накапливая знания и развивая необходимые навыки.

С таким молодым поколением нас ждет прекрасное будущее в сфере противомонополизационного мониторинга. Будущее, в котором естественный и искусственный интеллект будут эффективно взаимодействовать и развиваться.



АЛЕКСЕЙ ГЕЛЕТА:

«ФИНТЕХ-РЫНОК РОССИИ МОЖНО НАЗВАТЬ ОДНИМ ИЗ НАИБОЛЕЕ ИННОВАЦИОННЫХ И ТЕХНОЛОГИЧЕСКИ ПРОДВИНУТЫХ В МИРЕ»



Перед внедрением в жизнь финтех-инициативы проходят независимую экспертизу. Проекты оцениваются на предмет возможных рисков и угроз, а также насколько они полезны гражданам, государству и бизнесу. Такую экспертизу проводит Группа цифрового комплаенса Аналитического центра при Правительстве Российской Федерации. Чем еще занимается подразделение и какую роль сегодня играет финансовая грамотность: об этом редакция журнала побеседовала с руководителем Группы Алексеем Гелетой.



— Росфинмониторинг сотрудничает с Аналитическим центром при Правительстве Российской Федерации по самым разным направлениям. В том числе были реализованы проекты с Группой цифрового комплаенса, которую вы возглавляете. Расскажите, что входит в задачи Группы, и как лично вы познакомились с этой отраслью.

— В 2020 году по инициативе Правительства Российской Федерации на базе Аналитического центра при Правительстве Российской Федерации было создано новое для государственного сектора экспертное направление — «цифровой комплаенс». Его основными задачами стали межведомственная координация при проработке финтех-инициатив и предоставление комплексной и независимой аналитическо-правовой экспертизы, в том числе с учетом международного опыта. Мы работаем по направлениям, связанным как с выяв-

лением рисков и угроз, так и с развитием финтех-рынка с учетом потребностей государства, бизнеса и граждан.

Мое же знакомство с функционированием системы комплаенса началось еще со студенческой скамьи. Я выпускник профильной кафедры Института финансовой и экономической безопасности НИЯУ МИФИ, созданной при поддержке Росфинмониторинга. Преподавателями были штатные сотрудники ведомства, что помогло получить не только теоретические знания, но и практические, в том числе в процессе прохождения стажировки в Росфинмониторинге. Фундаментальный и разносторонний опыт в сфере комплаенса я получил, работая в банковском секторе. Я участвовал в построении и автоматизации систем управления регуляторными (комплаенс) рисками и ПОД/ФТ на уровне головного банка и дочерних организаций, необходимо было обеспечить соблюдение

единых стандартов комплаенс банковской группы, при этом учитывать особенности локального законодательства страны регистрации дочерней организации.

— Какие сферы являются профильными для Группы цифрового комплаенса в настоящее время?

— Можно выделить три основных направления:

1. Сферы, которые находятся в «серой» зоне и требуют формирования комплексной экспертизы и рекомендаций для дальнейшего принятия управленческих решений как на федеральном, так и на региональном уровнях. В том числе к ним можно отнести майнинг и оборот цифровых валют. Приходится погружаться в конкретные проекты, иницилируемые представителями бизнеса, связанные с развитием автоматизированных систем, блокчейн-технологий, платежных механизмов.

2. Выявление рисков и угроз для национальной финансовой системы и социально-экономической сферы. Прорабатывались активно, связанные с выявлением незаконных банковских транзакций (мискодинг), мошенничества под видом социальных выплат и кешбеков, незаконных ресурсов в период COVID-19 и многие другие. В детали рабочего процесса и результаты погружаться не будем, но от нас требовалось четкое понимание основных причин возникновения угроз, построение клиентских путей и бизнес-процессов, выявление наиболее уязвимых зон, формирование потоков данных, построение аналитических панелей, участие в межведомственных активностях, подготовка аналитических отчетов, содержащих рекомендации по минимизации или устранению выявленных угроз.

3. Участие в развитии платежных механизмов. Несмотря на попытки внешнего давления финтех-рынок России можно назвать одним из наиболее инновационных и тех-

нологически продвинутых в мире. Однако у нас есть зоны роста и, как следствие, необходимость актуализации консервативных подходов или создания новых регуляторных условий для развития финансовой системы. При решении таких задач важна постоянная коммуникация и понимание между представителями бизнеса, предлагающими новые идеи для развития национальной финансовой системы, и органами власти, которые обеспечивают безопасность финансовой системы в рамках своих компетенций.

Достичь понимания между участниками процесса без лишних бюрократических барьеров и существенно продвинуться в разрешении актуальных вопросов удается на площадке Координационного центра Правительства Российской Федерации.

— Какие процессы в сфере финтеха вы считаете консервативными?

— Вопросы идентификации граждан, в частности при открытии банковского счета. В различных социально-экономических сферах мы видим успешную цифровизацию процессов, людям стало удобнее и быстрее решать свои бытовые и рабочие вопросы за счет удаленных сервисов, чего не скажешь об открытии банковского счета.

Все же нам удалось продвинуться в данном направлении. По результатам поступивших обращений представителей банковского сектора, на площадке Координационного центра совместно с Банком России, Росфинмониторингом и иными профильными ведомствами инициирована проработка механизмов удаленной идентификации иностранных граждан при открытии банковского счета в российской кредитной организации, в народе данный проект получил название «Карта туриста». Благодаря слаженной работе удалось внести соответствующие изменения в национальное антилегаліза-

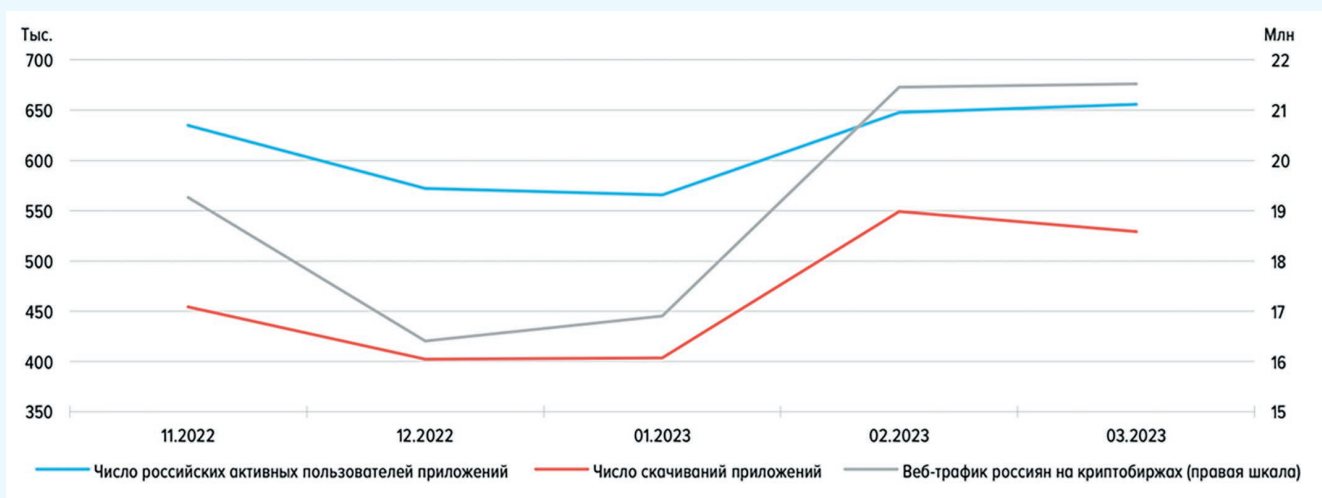
ционное законодательство. Теперь при соблюдении определенных критериев и условий иностранные граждане могут удаленно открыть банковский счет в российской кредитной организации, получить виртуальную карту МИР и начать осуществлять сопутствующие траты до приезда в Россию. Тем не менее уже поступает обратная связь от кредитных организаций о возникающих сложностях, которые необходимо совместно прорабатывать.

Вопросы регулирования майнинга и оборота криптовалют также являются острой темой на протяжении многих лет. Все ведомства понимают, что криптовалюта несет в себе риски и угрозы, вот только нет единого мнения, как с ними бороться. Фактически сформировалось два лагеря: одни считают, что для минимизации рисков и угроз необходимо запретить оборот криптовалют с участием российской финансовой системы, а другие считают, что надо создать четкие регуляторные условия для всех участников российского крипторынка. На экспертном уровне и с учетом увеличения интереса граждан к данному цифровому продукту я больше склонен к подходу риск-ориентированного регулирования крипторынка, который позволит разделить участников на добропорядочных и нет. Ведь все запретить — самое простое решение, но как в дальнейшем органам власти и кредитными организациями обеспечить эффективное соблюдение запрета — большой вопрос, который может привести к штрафам для кредитных организаций и нерабочим законодательным нормам.

В рамках межведомственной проработки ведомства все ближе к тому, чтобы найти «золотую середину» в подходах регулирования. Но необходимо учитывать, что субъекты регулирования могут стать объектом внешних санкций, самый актуальный пример — операторы платформ по выпуску цифровых финансовых активов.



► Активность российских пользователей на криптобиржах



Источник: https://www.cbr.ru/Collection/Collection/File/44007/4q_2022_1q_2023.pdf

— На ваш взгляд, новые технологии могут усилить защиту пользователей финансовых услуг от мошенников? Или, напротив, это скорее дополнительный инструмент для преступников?

— А вот тут возникает парадокс: новые технологии могут как усилить безопасность, так и стать дополнительным инструментом для преступников. Практика показывает, что мошенники начинают использовать новые технологии намного раньше, чем на них обращают внимание органы власти. Чтобы не быть голословным, как минимум можно ознакомиться со случаями мошенничества с использованием технологий Deepfake и подмены голоса. Негативный тренд есть, и он будет только развиваться.

— Какова роль финансовой грамотности в условиях цифровизации: проводил ли Аналитический центр тематические исследования? Какие проекты в этой сфере кажутся вам перспективными?

— Текущая статистика неутешительная — из года в год потери граждан от мошенничества с использованием цифровых сервисов растут. По данным Банка России, в 2023 году кибермошенники похи-

тили у россиян 15,8 млрд рублей, что следует¹ из Обзора операций, совершенных без согласия клиентов финансовых организаций. В 2023 году объем операций без согласия клиентов увеличился по сравнению с 2022 годом на 11,48%.

В России различными ведомствами наработана большая база знаний по повышению финансовой грамотности. В частности, Росфинмониторинг успешно проводит Международную олимпиаду по финансовой безопасности, накоплен колоссальный опыт и практические кейсы, которые будут полезны гражданам в условиях интенсивной цифровизации. Обучение можно реализовывать в виде интернет-игр, квизов и других цифровых форматов, которые могут быть рекомендованы для внедрения в образовательных и государственных организациях, предприятиях и иных учреждениях.

— Цифровой комплаенс в России: есть ли уникальные особенности?

— Если вы спрашиваете про функцию цифрового комплаенса в российских кредитных организациях, то лучше подразделений комплаенса этих банков никто не расскажет. Предлагается рассмотреть возможность обсуждения данного вопро-

са в рамках Совета по комплаенсу, организованного Росфинмониторингом. С удовольствием принял бы участие.

Относительно возглавляемого мной подразделения можно отметить следующие уникальные особенности: Группа цифрового комплаенса функционирует на площадке Координационного центра Правительства Российской Федерации и является независимым экспертным хабом для Правительства Российской Федерации при принятии управленческих решений.

► **«ВОПРОСЫ РЕГУЛИРОВАНИЯ МАЙНИНГА И ОБОРОТА КРИПТОВАЛЮТ ТАКЖЕ ЯВЛЯЮТСЯ ОСТРОЙ ТЕМОЙ НА ПРОТЯЖЕНИИ МНОГИХ ЛЕТ. ВСЕ ВЕДОМСТВА ПОНИМАЮТ, ЧТО КРИПТОВАЛЮТА НЕСЕТ В СЕБЕ РИСКИ И УГРОЗЫ, ВОТ ТОЛЬКО НЕТ ЕДИНОГО МНЕНИЯ, КАК С НИМИ БОРОТЬСЯ»**

¹ <https://www.cbr.ru/press/event/?id=18419>



ВЫЯВЛЕНИЕ И ПРЕСЕЧЕНИЕ КИБЕРПРЕСТУПЛЕНИЙ

50 БОГДАН ШАБЛЯ

Противодействие «дропам» и высокорисковым P2P-операциям — приоритетный вектор финансового мониторинга

53 ВАДИМ УВАРОВ

Информационная безопасность на финансовом рынке: вопросы противодействия кибермошенничеству при переводах денежных средств

57 АНТОН РАСТАЩЕНОВ

Досудебное ограничение доступа в сети Интернет к информации, распространение которой на территории Российской Федерации запрещено

60 РОМАН МУХЛЫНОВ

Актуальные тренды на рынке нелегальных поставщиков финансовых услуг

63 ОЛЕГ КИПКАЕВ

Использование цифровых технологий в сборе, обработке и обобщении информационно-аналитических и иных данных, используемых в прокурорской деятельности, на примере функциональных возможностей информационно-аналитической системы «Электронный кабинет прокурора»

ПРОТИВОДЕЙСТВИЕ «ДРОПАМ» И ВЫСОКОРИСКОВЫМ P2P-ОПЕРАЦИЯМ — ПРИОРИТЕТНЫЙ ВЕКТОР ФИНАНСОВОГО МОНИТОРИНГА



БОГДАН ШАБЛЯ,
директор Департамента
финансового мониторинга
и валютного контроля
Банка России

Банк России отмечает нарастание рисков, связанных с использованием российского банковского сектора для проведения P2P-операций физических лиц, обеспечивающих расчеты граждан с теневым бизнесом. Эти риски напрямую связаны с обслуживанием банками подставных физических лиц, так называемых «дропов», по счетам которых проводятся P2P-операции. Банк России в плотном взаимодействии с банками разрабатывает и внедряет подходы по противодействию таким операциям, включающие меры по повышению оперативности выявления счетов физических лиц — «дропов», а также реагированию на выявляемые риски

Практика надзорной деятельности и мониторинга операций кредитных организаций указывает на использование недобросовестными субъектами P2P-сервисов кредитных организаций для проведения высокорисковых операций. Такие операции позволяют принимать деньги теневому бизнесу, для которого доступ к легальному банковскому обслуживанию запрещен. Под теневым бизнесом имеются в виду онлайн-казино и букме-

керские конторы, финансовые пирамиды, продавцы пиратского контента, нарушающие авторские права, различного рода мошеннические сайты, продавцы запрещенных товаров, криптообменники и P2P-сервисы криптобирж, использующие «дропов».

Мы исходим из того, что вовлечение граждан в такие операции несет для них риски не только потери своих сбережений из-за различного рода мошенничества, но и риски вовлечения в противоправную де-

ятельность, результатом которого может быть уголовная ответственность. Для банков же проведение таких операций, учитывая высокие объемы операций данного теневого бизнеса, может привести к ситуации, угрожающей интересам кредиторов и вкладчиков.

В 2020–2022 гг. такие операции проводились с использованием эквайринговых услуг банковского сектора и концентрировались в основном в небольших кредитных организациях, специализирую-

щихся на оказании теневого банковских услуг. Расчеты, как правило, проводились через счета иностранных поставщиков платежных услуг, юридических лиц и индивидуальных предпринимателей, специально создаваемых для таких операций, недобросовестных финансовых организаций, ведущих нелегальную деятельность под видом, например, микрозаймов.

Банком России проведена работа по вытеснению из банковского сектора высокорисковых операций и финансовых организаций, системно вовлеченных в их проведение.

ЗАПУСК ПЛАТФОРМЫ «ЗНАЙ СВОЕГО КЛИЕНТА»

значительно затруднил использование для таких операций счетов юридических лиц и индивидуальных предпринимателей. Уход из России международных платежных систем, ранее проводивших высокорисковые операции через иностранные банки-эквайеры, также заставил теневой платежный рынок значительно измениться.

В результате в 2023 году мы отмечаем переток объемов высокорисковых операций в схему прямых P2P-расчетов по платежным картам и счетам «дропов», которые открывают на свое имя в банке счет или банковскую карту, а затем передают их в распоряжение участников теневого бизнеса. В качестве примеров P2P-операций можно привести переводы денежных средств «с карты на карту», «с кошелька на кошелек», «со счета абонента оператора связи на кошелек или карту и обратно».

Объем высокорисковых P2P-операций в банковском секторе,



как и количество вовлеченных в их проведение «дропов», на текущий момент нами оценивается как высокий и требующий с нашей стороны комплексных мер реагирования. Руководством Банка России данное направление работы определено как приоритетное.

С одной стороны, использование схем P2P-расчетов с гражданами для теневого бизнеса, по нашим оценкам, сложнее и дороже, чем эквайринговых операций, в том числе в связи с необходимостью поддержания инфраструктуры из ИТ-составляющей, автоматизирующей проведение и учет операций, и многочисленных счетов подставных физических лиц — «дропов». С другой стороны, ряд факторов способствовал переориентированию участников теневого бизнеса на использование указанной схемы:

- простота и доступность открытия банковских карт и электронных кошельков, позволяющих практически без ограничений и с минимальными комиссиями проводить P2P-операции в значительных объемах. С одной стороны, это делает удобными такие банковские продукты для

населения и бизнеса. С другой стороны, простотой «входа» и доступностью банковских продуктов пытаются пользоваться участники теневого банковского бизнеса. Например, так называемые «дроповоды», открывающие счета для такого бизнеса. Они обращаются к менее осведомленным гражданам, которые, не зная всех последствий, передают открытый только что счет (кошелек) в управление постороннему лицу. К счету привязываются десятки виртуальных карт, по которым в считанные дни проводятся значительные суммы;

- возможность идентификации физических лиц при открытии электронных кошельков с привлечением сторонних организаций (например, банковских платежных агентов, операторов связи), которые зачастую могут формально подходить к исполнению требований по идентификации, поскольку от количества открытых ими физическим лицам электронных кошельков зависит размер полученного ими дохода. Действующее законодательство позволяет при проведении



идентификации (упрощенной идентификации) в целях выдачи электронных кошельков подтверждать достоверность представленных сведений с использованием государственных информационных систем без личного присутствия и предоставления оригиналов документов. Мы выявляли случаи открытия кредитными организациями электронных кошельков с использованием персональных данных физических лиц без их ведома и проведения по ним операций, что создавало значительные риски для граждан;

- некоторые публично доступные Р2Р-сервисы кредитных организаций в сети Интернет имеют технические уязвимости. Организаторы теневого бизнеса используют на своих сайтах в сети Интернет фиктивные платежные Р2Р-формы, на которых «роботы» собирают данные банковских карт граждан и автоматически перенаправляют их на реальную интернет-страницу кредитной организации для совершения Р2Р-операции.

В целях предотвращения указанных рисков Банком России изданы методические рекомендации от 06.09.2021 № 16-МР¹ и от 12.10.2023 № 13-МР².

В методических рекомендациях № 16-МР кредитным организациям рекомендовано выявлять операции по переводу денежных средств (электронных денежных средств) между физическими лицами с применением электронных средств платежа (в частности, платежных карт и электронных кошельков), обладающие признаками, нехарактерными для обычных

расчетов, и применять противомонополизационные меры, а также обеспечивать необходимую информационную защиту собственных Р2Р-сервисов от роботизированного использования.

Для снижения рисков использования эквайринговых услуг в обмен методических рекомендаций № 16-МР Банком России опубликованы методические рекомендации № 13-МР, в которых кредитным организациям — эквайерам в том числе рекомендовано контролировать зачисление средств на счета того торгового-сервисного предприятия, где совершалась покупка (это закрывает так называемую «ресторанную схему»), а также обращать повышенное внимание на признаки нехарактерных переводов в пользу торгового-сервисных предприятий, не осуществляющих реальной хозяйственной деятельности.

Сейчас мы в плотном взаимодействии с банками разрабатываем и внедряем новые современные инструменты противодействия высокорисковым Р2Р-операциям. Они предусматривают и повы-

шение оперативности выявления счетов и операций физических лиц — «дропов» вплоть до выявления в онлайн-режиме, и дополнительные контрольные процедуры при оформлении банковских карт и использовании некоторых банковских продуктов.

Цель данной работы, — во-первых, затруднить деятельность теневого бизнеса, чтобы использование банковского сектора и Р2Р-операций было для него максимально неудобным и затратным.

Во-вторых, привить финансовым организациям и населению нулевую терпимость к деятельности «дропов». Этому должны способствовать развитие банковским сектором комплаенс-процедур, пресекающих возможности обслуживания счетов подставных физических лиц, и проводимая Банком России и кредитными организациями совместно с правоохранительными органами информационно-просветительская работа по информированию граждан о последствиях такой деятельности и формированию негативного отношения к ней.

➤ «СЕЙЧАС МЫ В ПЛОТНОМ ВЗАИМОДЕЙСТВИИ С БАНКАМИ РАЗРАБАТЫВАЕМ И ВНЕДРЯЕМ НОВЫЕ СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ ПРОТИВОДЕЙСТВИЯ ВЫСОКОРИСКОВЫМ Р2Р-ОПЕРАЦИЯМ. ОНИ ПРЕДУСМАТРИВАЮТ И ПОВЫШЕНИЕ ОПЕРАТИВНОСТИ ВЫЯВЛЕНИЯ СЧЕТОВ И ОПЕРАЦИЙ ФИЗИЧЕСКИХ ЛИЦ — «ДРОПОВ» ВПЛОТЬ ДО ВЫЯВЛЕНИЯ В ОНЛАЙН-РЕЖИМЕ, И ДОПОЛНИТЕЛЬНЫЕ КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ПРИ ОФОРМЛЕНИИ БАНКОВСКИХ КАРТ И ИСПОЛЬЗОВАНИИ НЕКОТОРЫХ БАНКОВСКИХ ПРОДУКТОВ»

¹ О повышении внимания кредитных организаций к отдельным операциям клиентов — физических лиц.

² В отношении деятельности кредитных организаций и платежных агрегаторов по осуществлению расчетов с организациями товаров (услуг) по операциям, совершенным с использованием электронных средств платежа.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ФИНАНСОВОМ РЫНКЕ: ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ ПРИ ПЕРЕВОДАХ ДЕНЕЖНЫХ СРЕДСТВ



➤ ВАДИМ УВАРОВ,
директор Департамента
информационной безопасности
Банка России

Повсеместное распространение и использование цифровых платежных технологий принципиальным образом изменило отношение общества к проблеме обеспечения информационной безопасности. В условиях бурного развития дистанционного банковского обслуживания отсутствие надлежащих мер по защите клиентов банков от кибермошенников может привести к негативным социально значимым последствиям¹. Поэтому сегодня способность эффективно противостоять рискам хищения денежных средств со счетов граждан является одним из ключевых факторов защиты прав потребителей финансовых услуг и повышения уровня доверия к цифровым технологиям

Противодействие кибермошенничеству в кредитно-финансовой сфере является одним из приоритетных направлений деятельности Банка России. По результатам системной работы, проводимой регулятором во взаимодействии с представителями отрасли, в 2023 году банки

отразили почти 34,8 млн попыток совершения мошеннических операций. Это позволило не допустить хищения 5,8 трлн рублей, принадлежащих клиентам кредитных организаций.

Вместе с тем на протяжении последних нескольких лет Банк России фиксирует ежегодное увеличение

объема успешных операций, совершенных без согласия клиентов банков. В 2023 году злоумышленники похитили 15,8 млрд рублей. По сравнению с прошлым годом объем похищенных денег вырос на 11,5%. Количество мошеннических операций увеличилось на 33% и превысило 1,1 млн случаев².

¹ Согласно официальным данным МВД России, в 2023 году каждое третье преступление в нашей стране было совершено с использованием информационно-телекоммуникационных технологий. В этой сфере зарегистрировано на 29,7% больше уголовно наказуемых деяний, чем в 2022 году (<https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/>).

² Ежегодные обзоры операций, совершенных без согласия клиентов финансовых организаций, опубликованы на официальном сайте Банка России (http://www.cbr.ru/analytics/ib/operations_survey/2023/).

МОШЕННИЧЕСКИЕ ОПЕРАЦИИ: СТАТИСТИКА



Одним из факторов, не позволяющих кардинально переломить ситуацию с противодействием мошенничеству и социальной инженерии, является постоянное совершенствование злоумышленниками схем и сценариев воздействия на граждан. В настоящее время наблюдается тренд на персонализированные атаки, реализации которых предшествует детальное изучение личной информации потенциальных жертв, в том числе самостоятельно размещаемой гражданами на различных ресурсах в сети Интернет.



В целях противодействия деятельности телефонным и интернет-мошенникам Банк России проводит комплексную работу. Система принимаемых мер включает совершенствование законодательства, регламентирующего деятельность финансовых организаций, информационно-просветительскую работу с гражданами, а также взаимодействие с правоохранительными, надзорными органами, регистраторами доменных имен и операторами связи.

В июле 2024 года вступит в силу разработанный при участии Банка России закон о совершенствовании

механизмов противодействия хищению денежных средств клиентов банков³. Он предусматривает:

- введение двухдневного «периода охлаждения» — обязательной для банка процедуры приостановки денежных переводов по реквизитам, информация о которых содержится в базе данных Банка России «О случаях и попытках осуществления переводов денежных средств без согласия клиента» (далее — база данных Банка России). За два дня человек сможет обдумать, оценить совершаемые действия и отказаться от перевода на подозрительный счет;

- обязанность банка отключать доступ к электронным средствам платежа «дропам», если информация о совершенных ими противоправных действиях поступила в базу данных Банка России от МВД России. Если же информация поступила в базу данных Банка России от финансовой организации, то отключение электронных средств платежа клиенту будет являться правом банка;
- обязанность банка возместить клиенту деньги в течение 30 дней в том случае, если банк допустил перевод средств на мошеннический счет, который находится в базе данных Банка России, без выполнения обязательных действий по защите клиента.

Результаты проведенного Банком России в 2023 году опроса населения о степени удовлетворенности безопасностью финансовых услуг показали, что почти 62% граждан, которые пострадали от мошенников, обратились с соответствующим заявлением в банк и/или в полицию. Развитие информационного обмена о мошеннических операциях между банками и правоохранительными органами принципиально важно.



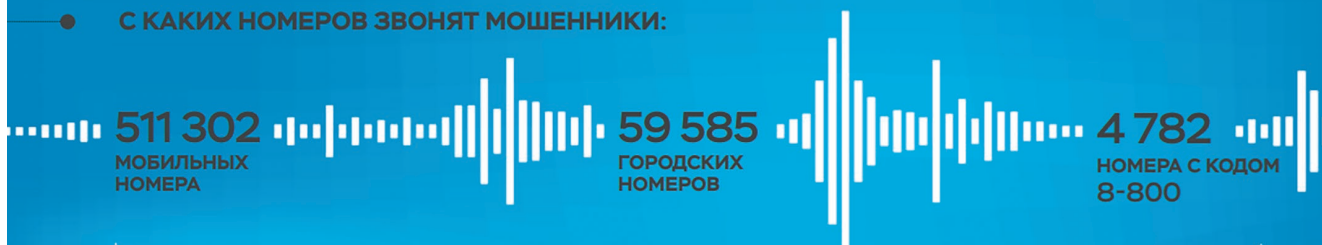
ПОРТРЕТ ПОСТРАДАВШЕГО



³ Федеральный закон от 24 июля 2023 года № 369-ФЗ «О внесении изменений в Федеральный закон "О национальной платежной системе"».

ТЕЛЕФОННЫЙ ЗВОНОК – ОСНОВНОЙ ИНСТРУМЕНТ ЗЛОУМЫШЛЕННИКОВ

● С КАКИХ НОМЕРОВ ЗВОНЯТ МОШЕННИКИ:



ЗЛОУМЫШЛЕННИКИ МИГРИРУЮТ В МЕССЕНДЖЕРЫ И ВСЕ ЧАЩЕ ИСПОЛЬЗУЮТ ИХ ДЛЯ ОБМАНА ЛЮДЕЙ

В октябре 2023 года вступил в силу закон об информационном взаимодействии Банка России и МВД России⁴, который создал условия для автоматизированного обмена данными об операциях без согласия клиентов между ведомствами. Теперь правоохранительные органы могут в максимально сжатые сроки получать необходимую для расследования фактов мошенничества и уголовных дел информацию из базы данных Банка России. В свою очередь, сведения, которые Банк России получает от МВД России, банки могут учитывать в своих антифрод-системах для предотвращения новых мошеннических операций.

В целях противодействия противоправным действиям в сети Интернет Банк России взаимодействует с Генеральной прокуратурой Российской Федерации⁵ и регистраторами доменных имен. В их адрес в 2023 году регулятор

направил более 38,3 тысячи интернет-ресурсов, с помощью которых осуществлялась противоправная деятельность, в целях их блокировки. Основная часть этих ресурсов (55%) — фишинговые сайты, главной целью которых является хищение данных клиентов финансовых организаций. Кроме того, инициировано ограничение доступа к 4,5 тысячи страниц (групп) в социальных сетях и к 35 приложениям, которые преимущественно использовались злоумышленниками для осуществления безлицензионной деятельности и фишинга под видом действующих кредитных организаций.

В адрес операторов связи Банком России на блокировку направлены 575,7 тысяч номеров телефонов, используемых мошенниками для хищения средств у граждан.

С учетом результатов проводимого Банком России мониторинга,

в текущем году в фокусе внимания регулятора две тенденции, имеющие негативные социальные последствия для граждан: это значительный объем кредитного мошенничества и вовлечение граждан, особенно молодежи, в «дроперство».

Проблема кредитного мошенничества опасна не только тем, что увеличивается средний чек хищений. Граждане, которые под влиянием злоумышленников оформляют кредит и самостоятельно передают им заемные средства, на многие годы попадают в «долговую яму». В целях защиты граждан и повышения ответственности кредитных организаций Банк России прорабатывает соответствующие инициативы. К ним относится «период охлаждения» между одобрением кредита и перечислением средств заемщику: в первую очередь эта мера должна касаться тех случаев, когда заемщик оформ-

⁴ В соответствии с Федеральным законом от 20 октября 2022 года № 408-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе».

⁵ В рамках полномочий, предусмотренных статьей 6.2 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

ляет кредит на крупную сумму. Не менее важно интегрировать в кредитный конвейер антифрод-процедуры для того, чтобы при выдаче заемных средств банк понимал, находится человек под воздействием третьих лиц или нет.

Также Банк России ведет активную борьбу с «дроперством» — деятельностью по выводу и обналичиванию денежных средств, полученных преступным путем, в том числе с использованием электронных средств платежа вовлекаемых в нее граждан. Существуют различные варианты вовлечения в «дроперство». В одних случаях люди участвуют в этой деятельности сознательно, хотя иногда и не понимают возможных для себя последствий. В других случаях они не знают, что оказались вовлеченными в противоправную деятельность: передавая кому-то свои данные, размещая их в общем доступе, например в социальных сетях, они могут стать соучастниками преступления. Наиболее уязвимые возрастные группы — подростки и молодежь (основной возраст «дропов» — 17–19 лет).

Для решения этой проблемы Банк России в апреле 2022 года дал рекомендации кредитным организациям об отключении электронных средств платежа лицам, чьи платежные карты используются для вывода и обналичивания похищенных денежных средств⁶. Поэтому банки уже сейчас имеют право

временно приостанавливать онлайн-доступ к управлению счетом при осуществлении клиентом подозрительных операций.

После вступления в силу в июле 2024 года вышеуказанного закона о совершенствовании механизмов противодействия хищению денежных средств клиентов банков требования по ограничению дистанционного банковского обслуживания «дропа» ужесточатся. Банки будут обязаны приостанавливать использование клиентом электронного средства платежа, если информация о совершенных им противоправных действиях поступила в базу данных Банка России от МВД России. С учетом того, что эта информация направляется всем кредитным организациям, дистанционные операции по счетам «дропа» будут приостановлены во всех банках.

Эта мера будет способствовать созданию условий для того, чтобы злоумышленникам стало экономически невыгодно осуществлять свою противоправную деятельность.

Для активизации информационной работы кредитных организаций с клиентами Банк России подготовил и согласовал с МВД России соответствующие Методические рекомендации⁷. В них указаны конкретные мероприятия по повышению осведомленности клиентов в целях противодействия вовлечению в «дроперство». Основные

цели информационно-просветительской работы — информирование об ответственности и последствиях участия в «дроперской» деятельности, формирование у граждан осознания ее противоправного характера и негативного образа «дропа».

Концепция борьбы банковской отрасли с различными проявлениями кибермошенничества, включая кредитное мошенничество и дроперство, в значительной степени базируется на высоком качестве данных о подозрительных операциях, которые банки направляют в базу данных Банка России, а регулятор в свою очередь распространяет среди всех участников информационного обмена. От полноты, достоверности и своевременности предоставления этих сведений зависит скорость и эффективность противодействия злоумышленникам, а также качество работы антифрод-систем в банках. Поэтому обеспечение надлежащего репортинга данных в Банк России сегодня является одним из ключевых приоритетов деятельности регулятора, в том числе надзорной. Это крайне важно для того, чтобы механизмы противодействия хищению денежных средств, предусмотренные принятыми законами, обеспечивали защиту прав и интересов граждан — потребителей финансовых услуг.

⁶ Информационное письмо Банка России от 15.04.2022 № 01-56-5/3143 о реализации кредитными организациями мероприятий по противодействию осуществлению переводов денежных средств без согласия клиентов.

⁷ Методические рекомендации от 28.02.2024 № 3-МР по усилению кредитными организациями информационной работы с клиентами в целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента, а также заключению договоров на получение кредитных (заемных) денежных средств под влиянием обмана или при злоупотреблении доверием и осуществлению операций с использованием указанных денежных средств, а также вовлечению граждан в деятельность по выводу и обналичиванию средств, полученных преступным путем.

ДОСУДЕБНОЕ ОГРАНИЧЕНИЕ ДОСТУПА В СЕТИ ИНТЕРНЕТ К ИНФОРМАЦИИ, РАСПРОСТРАНЕНИЕ КОТОРОЙ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ЗАПРЕЩЕНО

В последние годы проблема преступлений, совершаемых с использованием информационно-коммуникационных технологий, остается одной из самых актуальных и несет серьезную угрозу национальной безопасности Российской Федерации



АНТОН РАСТАЩЕНОВ,
начальник отдела
по предупреждению
распространения и выявлению
деструктивной и запрещенной
информации в сети Интернет
Управления по организации
борьбы с противоправным
использованием информационно-
коммуникационных технологий
МВД России, подполковник
полиции

Ускоренное внедрение в повседневную жизнь общества достижений информационных технологий позволяет преступникам оставаться вне поля зрения правоохранительных органов.

Согласно официальным статистическим сведениям, в январе — декабре 2023 года органами внутренних дел зарегистрировано 677 тысяч преступлений, совершенных с использованием информационно-коммуникационных технологий, что на 29,7% больше, чем годом ранее.

Неуклонный рост количества преступлений указанной категории свидетельствует о необходимости поиска наиболее оптимальных и эффективных форм, методов и средств их выявления, предупреждения, пресечения, раскрытия и расследования.

В комплексе оперативно-розыскных мероприятий по нейтрализации интернет-преступности важную роль занимают меры превентивного характера, направленные на противодействие

противоправным информационным ресурсам, используемым криминальными элементами как в качестве рекламных и пропагандистских площадок, так и платформ, предназначенных для отмывания преступных доходов и финансирования уголовной среды.

В соответствии с действующим законодательством МВД России совместно с Роскомнадзором реализуется функция по ограничению доступа к интернет-ресурсам, содержащим запрещенную информацию, в том числе сведения о наркотиках, оружии, а также материалы экстремистского характера.

В 2023 году совместными усилиями указанных ведомств ограничен доступ к более 330 тысячам сайтов и страниц с информацией такого содержания.

Отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, а также обеспечении защиты инфор-

мации регулируются Федеральным законом от 27 июля 2006 г. № 149-ФЗ¹.

Как правило, источниками распространения запрещенной информации являются специально созданные ресурсы в сети Интернет, представляющие собой специализированные сайты и страницы форумов, а также тематические группы в социальных сетях. При этом лица, участвующие в создании вышеперечисленных площадок, могут находиться за рубежом, используя инструменты и ресурсы для модерации.

Статьей 15.1 Федерального закона № 149-ФЗ, вступившей в силу с 1 ноября 2012 года, регламентирован механизм блокировки интернет-ресурсов, под которым понимается совокупность мер организационно-технического характера, призванных ограничить доступ к запрещенной информации, распространяемой в сети Интернет.

Частью 2 статьи 15.1 Федерального закона № 149-ФЗ предусмотрено, что в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено»² включаются доменные имена и

(или) указатели страниц сайтов в сети Интернет, а также сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

В соответствии с частью 5 статьи 15.1 Федерального закона № 149-ФЗ основаниями для включения в ЕАИС «Единый реестр» таких интернет-ресурсов являются решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации³, а также решение суда о признании распространяемой посредством сети Интернет информации, запрещенной в Российской Федерации.

Подпунктами «а» — «м» пункта 1 части 5 статьи 15.1 Федерального закона № 149-ФЗ установлен исчерпывающий перечень запрещенной информации, в отношении которой уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти в пределах их компетенции принимаются соответствующие решения.

В частности, подпункты «б» и «к» пункта 1 части 5 статьи 15.1 Федерального закона № 149-ФЗ определяют основанием для включения в ЕАИС «Единый реестр» интернет-ресурсов, распространяющих информацию:

- о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их

прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

- о способах, методах самодельного изготовления взрывчатых веществ и взрывных устройств, незаконного изготовления или переделки оружия, основных частей огнестрельного оружия, а равно незаконного изготовления боеприпасов, за исключением информации о способах, методах самостоятельного снаряжения патронов к гражданскому огнестрельному длинноствольному оружию.

Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31.12.2015 № 683, деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, отнесена к одной из основных угроз государственной и общественной безопасности.

В этой связи одним из основных направлений обеспечения информационной безопасности является противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии и идей национальной исключительности.

Федеральными законами от 28.12.2013 № 398-ФЗ⁴ и от 25.11.2017 № 327-ФЗ⁵ Федеральный закон № 149-ФЗ дополнен статьей 15.3, регламентирующей порядок ограничения доступа к обнаруженной в информационно-телекоммуни-

¹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Далее — Федеральный закон № 149-ФЗ.

² Далее — ЕАИС «Единый реестр».

³ Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено». Далее — постановление № 1101.

⁴ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"».

⁵ «Об информации, информационных технологиях и о защите информации» и статью 6 Закона Российской Федерации «О средствах массовой информации».



кационных сетях, в том числе в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также информационным материалам иностранной или международной неправительственной организации, деятельность которой признана нежелательной на тер-

ритории Российской Федерации, и сведениям, позволяющим получить доступ к указанным информации или материалам.

В соответствии с частью 1 статьи 15.3 Федерального закона № 149-ФЗ при поступлении от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан уведомлений о распространении

в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации указанного характера Генеральный прокурор Российской Федерации или его заместители вправе направить в Роскомнадзор требование о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Роскомнадзор на основании требования Генерального прокурора Российской Федерации или его заместителей незамедлительно направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу или к информации, размещенной на нем, после получения которого оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, обязан незамедлительно ограничить доступ к такому информационному ресурсу. Сведения об информационном ресурсе вносятся Роскомнадзором в отдельный реестр.

Предусмотренный порядок позволяет оперативно реагировать на случаи распространения в сети Интернет подобной информации, что достигается обязательным указанием в требовании Роскомнадзора доменного имени сайта в сети Интернет, сетевого адреса, указателей страниц сайта в сети Интернет, позволяющих идентифицировать такую информацию.



АКТУАЛЬНЫЕ ТРЕНДЫ НА РЫНКЕ НЕЛЕГАЛЬНЫХ ПОСТАВЩИКОВ ФИНАНСОВЫХ УСЛУГ

Обеспечение сохранности доходов населения и защита потребителей от вовлечения в нелегальную деятельность на финансовом рынке — одна из важнейших задач финансовых регуляторов



▶ РОМАН МУХЛЫНОВ,
заместитель директора
Департамента небанковского
кредитования Банка России

Банк России предпринимает шаги по консолидации усилий всех заинтересованных сторон для того, чтобы уберечь сбережения граждан от мошенников и противостоять недобросовестным и незаконным практикам.

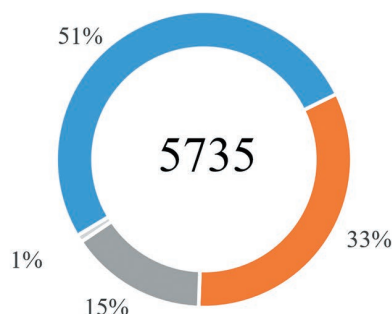
В 2023 году Банк России выявил 5 735 субъектов (компаний, проектов, индивидуальных предпринимателей и других) с признаками нелегальной деятельности, в том числе с признаками финансовых пирамид. Это на 15,5% больше, чем годом ранее, но «срок жизни» таких проектов стал короче, а «средний чек» уменьшился. Информация по всем выявленным фактам для пресечения деятельности направляется в правоохранительные органы, Росфинмони-

торинг, ФАС России, Роскомнадзор. Однако мошенники каждый год используют новые схемы и инструменты, и потому требуется особое внимание при выявлении таких практик — как со стороны регулятора, правоохранителей, общественников, так и со стороны финансовых организаций.

Наиболее яркими трендами за последние годы стали переход к онлайн-взаимодействию и использованию криптотематики мошенниками и нелегальными поставщиками финансовых услуг. Банк России неоднократно подчеркивал, что распространение криптовалют в Российской Федерации сопряжено с высокими рисками для благосостояния граждан и стабильности финансовой системы, а также рисками вовле-

► **Распределение субъектов, имеющих признаки нелегальной деятельности, в 2023 году**

- Финансовые пирамиды
- Нелегальные кредиторы
- Нелегальные профессиональные участники рынка ценных бумаг
- Иные формы



чения клиентов финансовых организаций в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма¹. Чтобы купировать ситуацию, были разработаны рекомендации, направленные на снижение таких рисков для клиентов банков и других финансовых организаций².

Не менее опасно то, что растет количество нелегальных участников финансового рынка, которые привлекают инвестиции в криптовалюту. В 2022 году криптовалюту привлекал каждый второй псевдоинвестиционный проект, в 2023 — предлагали вложение во внутренние токены или принимали взносы в крипте почти все пирамиды и нелегальные форекс-клубы.

Использование криптовалют в нелегальной деятельности несет высокие риски ввиду трудностей отслеживания транзакций в криптовалюте, что может осложнить поиск конечного бенефициара преступной схемы. Преступники быстро адаптируются к новым условиям, постоянно усложняя способы вывода средств из мошеннических проектов в криптовалюту. Из 2944 финансовых пирамид, выявленных за 2023 год, более 45% предлагали «инвесторам» для пе-

ревода средств воспользоваться системами зарубежных поставщиков платежных услуг. Почти 1500 мошеннических проектов принимали взносы в криптовалюте, что, помимо прочего, помогает организаторам и бенефициарам схем сохранять анонимность.

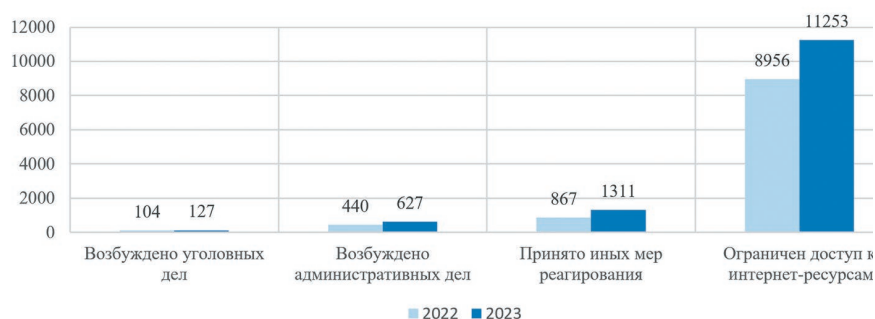
На фоне стабильного роста интереса потребителей к получению финансовых услуг дистанционно и формирования устойчивого доверия к информации, получаемой из социальных медиа, большинство финансовых пирамид, псевдоброкеров и даже нелегальных кредиторов действуют через интернет, поэтому все большее количество потребителей могут столкнуться с недобросовестными практиками и мошенничеством.

Безусловно, Банк России постоянно совершенствует настройки си-

стемы мониторинга информационного пространства. В прошлом году, например, была автоматизирована оценка публикуемого контента, годом ранее в систему мониторинга были добавлены соцсети и мессенджеры. Это позволило улучшить качество и оперативность обнаружения нелегальных поставщиков финансовых услуг. Нелегальные ресурсы по инициативе Банка России блокируются, но организаторы таких проектов в ответ создают новые. Нередко мошенники создают ресурсы с одинаковым контентом после блокировки основного сайта. Чтобы блокировка была более комплексной, с 2023 года Банк России стал инициировать меры, которые позволяют одновременно ограничивать доступ не только к доменам, но и ко всем субдоменам, которые используются субъектами нелегальной деятельности.

За 2023 год по инициативе Банка России был ограничен доступ к более 11,2 тыс. интернет-ресурсов, включая страницы в социальных сетях «ВКонтакте» и «Одноклассники» и мессенджере Telegram (более 3000 страниц, каналов, чат-ботов и т. п.), которые использовались нелегальными участниками финансового рынка и финансовыми пирамидами. Общая аудитория

► **Меры в отношении нелегальных организаций и финансовых пирамид, принятые по обращениям Банка России**



¹ Информация о рисках и угрозах, сопутствующих распространению криптоактивов (виртуальных валют, криптовалют), размещена на официальном сайте Банка России в информационно-телекоммуникационной сети Интернет (пресс-релиз от 27.01.2014 «Об использовании при совершении сделок "виртуальных валют", в частности, биткойна; пресс-релиз от 04.09.2017 «Об использовании частных "виртуальных валют" (криптовалют)»; доклад для общественных консультаций от 20.01.2022 «Криптовалюты: тренды, риски, меры»).

² Информационное письмо Банка России о рисках совершения операций с цифровыми валютами и рекомендациях финансовым организациям исключить предложение услуг, предусматривающих совершение таких операций от 29.02.2024 № ИИ-08-12/18.



заблокированных ресурсов — более 230 млн пользователей сети Интернет.

Кроме того, с 2022 года мы стали добавлять сведения о нелегальных компаниях (юридических лицах и индивидуальных предпринимателях) на платформу «Знай своего клиента», чтобы банки могли оперативно учитывать их при оценке риск-профиля своих клиентов и их контрагентов, а также для применения в отношении нелегальных поставщиков финансовых услуг противолегализационных мер. На текущий момент на платформу добавлены сведения о примерно 2300 субъектах — пирамидах, нелегальных кредиторах, нелегальных форекс-клубах и др.

Дополнительно в 2023 году было рекомендовано³ кредитным организациям в случае наличия оснований применять меры антиотмывочного законодательства вплоть до ограничения операций по счетам ко всем организациям из Списка компаний с выявленными признаками нелегальной деятельности, который публикуется на официальном сайте Банка России, и их посредникам. Это позволит сократить срок жизни финансовых пирамид, затруднит сбор средств нелегальными поставщиками финансовых услуг, снизит ущерб для граждан от незаконных схем.

Например, если рассматривать микрофинансовый рынок, то сейчас большим запросом со стороны клиентов пользуются онлайн-займы — 75% договоров займа с МФО по сравнению с 66% в 2022 году заключаются именно в сети Интернет. Соответственно, увеличилось число случаев, когда мошенники маскируются под заемщика для вывода из МФО денег в виде займов с последующим невозвратом. В таких схемах есть две пострадавшие стороны.

Во-первых, граждане, на которых оформлены мошеннические займы, — такие займы портят их кредитную историю, для исправления и урегулирования последствий часто требуется много ресурсов. Во-вторых, сами МФО — именно они несут убытки в виде выданных мошенникам займов, которые не возвращаются, и не менее важные репутационные риски. Объем подобных мошеннических атак достаточно велик, и с 2022 года он вырос. В 2022–2023 годах максимальный объем попыток мошенников получить заем только в одной крупной МФО составил: по числу операций — около 350–700 тыс. шт.; по объему займов — около 2–4 млрд рублей. Это достаточно высокая интенсивность и потенциальный размер ущерба для компании. Компанией было предотвращено более 98% таких операций. Но все же в ближайшее время микрофинансовым организациям нужно активнее улучшать процедуры идентификации и антифрод при выдаче онлайн-займов. Банк России активно коммуницирует с профсообществом по этим вопросам.

Для повышения безопасности потребителей и снижения рисков мошенничества при оформлении кредитов онлайн подготовлен закон⁴, повышающий финансовую ответственность банков за мошеннические операции. В частности, с июля 2024 года вводится двухдневный период «охлаждения», в течение которого банк не будет переводить деньги на подозрительный счет из базы данных регулятора.

За эти два дня человек может одуматься, разобраться, что имеет дело с мошенниками, и отказаться от перевода. Если банк совершит такой перевод до истечения периода «охлаждения», то обязан будет компенсировать клиенту потери. Кроме того, закон обязывает банки отключать доступ к дистанционному обслуживанию лицам, которые занимаются выводом и обналичиванием похищенных денег, если информация о совершенных ими противоправных действиях поступила от МВД России. Также граждане смогут обезопасить себя от ситуации, когда мошенники оформляют на их имя кредит, и добровольно отказаться от возможности заключать договоры кредита или займа. Соответствующий закон вступит в силу с 1 марта 2025 года — с этого момента можно будет оформить или отменить самозапрет на портале «Госуслуги». При этом в случае, если, несмотря на установленный запрет, кредитор заключит договор, он не сможет потребовать от заемщика исполнения обязательств по нему. Самозапрет можно будет отменить в любой момент, если человеку действительно потребовался кредит или заем.

Учитывая темпы роста дистанционного формата взаимодействия, его стремительное проникновение в повседневную жизнь потребителей финансовых услуг, а также интенсивную медиаповестку по вопросам криптоактивов и цифровых валют, противодействие недобросовестным практикам может переместиться почти полностью в онлайн-сегмент финансового рынка.

³ Информационное письмо Банка России о повышении внимания кредитных организаций к операциям с участием лиц, в деятельности которых имеются признаки осуществления нелегальной деятельности на финансовом рынке от 27.12.2023 № ИН-08-12/69.

⁴ Федеральный закон от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон “О кредитных историях” и Федеральный закон “О потребительском кредите (займе)”».

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СБОРЕ, ОБРАБОТКЕ И ОБОБЩЕНИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ И ИНЫХ ДАННЫХ, ИСПОЛЬЗУЕМЫХ В ПРОКУРОРСКОЙ ДЕЯТЕЛЬНОСТИ,

НА ПРИМЕРЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ
«ЭЛЕКТРОННЫЙ КАБИНЕТ ПРОКУРОРА»



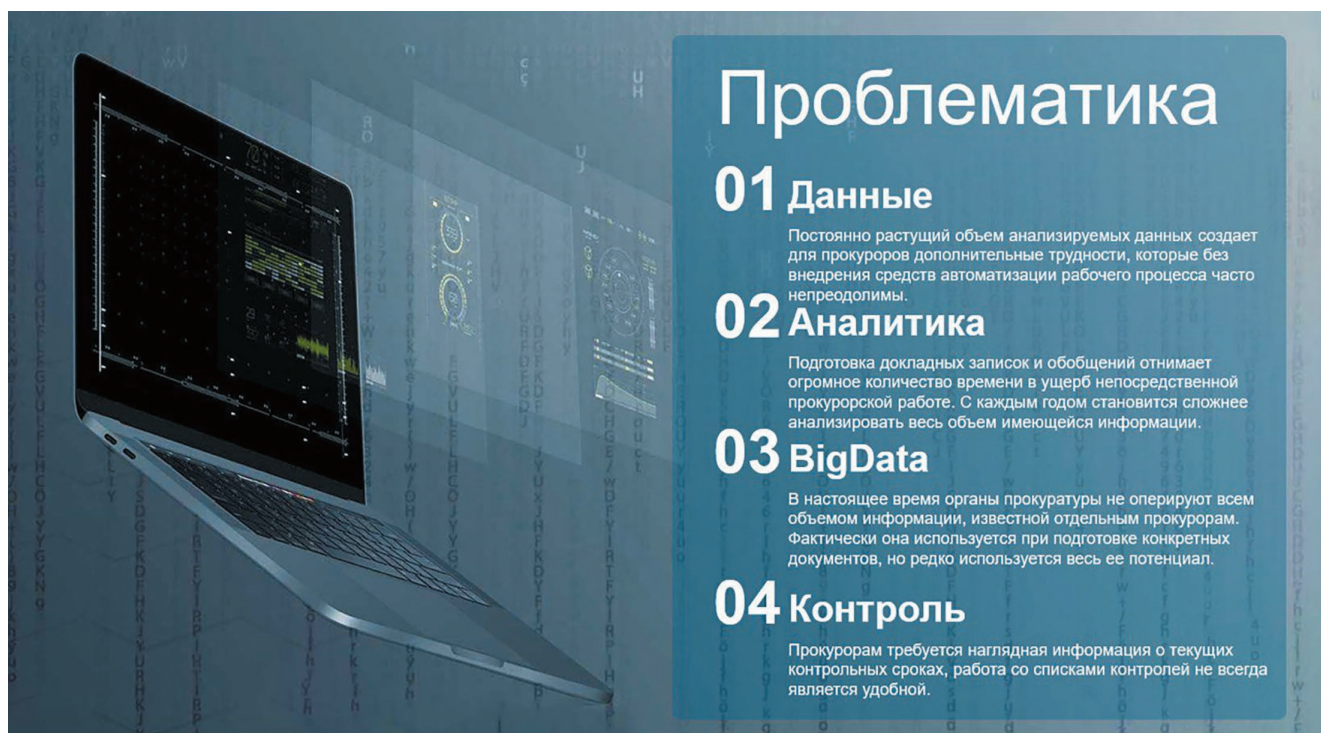
ОЛЕГ КИПКАЕВ,
начальник отдела по надзору
за исполнением законов в сфере
информационных технологий
и защиты информации
Генеральной прокуратуры
Российской Федерации

В целях уменьшения непроизводительных трудозатрат прокуроров, связанных со сбором и обработкой большого объема данных, путем использования в их деятельности современных цифровых технологий в Генеральной прокуратуре Российской Федерации ведется работа над проектом информационно-аналитической системы «Электронный кабинет прокурора» (ИАС «ЭКП»)

Необходимость разработки названного продукта обусловлена объективно назревшими потребностями в переформатировании традиционных способов организации прокурорской деятельности в условиях ускоряющейся цифровой трансформации общественных отношений, которая требует внедрения новых, более эффективных и оперативных инструментов для выполнения как аналитических задач, так и задач, обеспечиваемых средствами прокурорского надзора. Среди основ-

ных факторов, требующих инновационных программно-технических решений, выделяются следующие:

- 1) **данные** — постоянно растущий объем анализируемых данных создает для прокуроров дополнительные трудности, которые без внедрения средств автоматизации рабочего процесса часто непреодолимы;
- 2) **аналитика** — подготовка докладных записок и обобщений отнимает огромное количество времени в ущерб непосредственно прокурорской работе.



Проблематика

01 Данные

Постоянно растущий объем анализируемых данных создает для прокуроров дополнительные трудности, которые без внедрения средств автоматизации рабочего процесса часто непреодолимы.

02 Аналитика

Подготовка докладных записок и обобщений отнимает огромное количество времени в ущерб непосредственной прокурорской работе. С каждым годом становится сложнее анализировать весь объем имеющейся информации.

03 BigData

В настоящее время органы прокуратуры не оперируют всем объемом информации, известной отдельным прокурорам. Фактически она используется при подготовке конкретных документов, но редко используется весь ее потенциал.

04 Контроль

Прокурорам требуется наглядная информация о текущих контрольных сроках, работа со списками контролей не всегда является удобной.

Искусственный интеллект упрощение и стандартизация

Быстрая подготовка обобщений
Описание нарушений стандартизовано и всегда под рукой



Аналитика по конкретным нарушениям
При необходимости найти все факты реагирования на нарушения конкретного НПА по всей стране достаточно сформулировать запрос.



Для формирования базы не требуется работник
Планируется, что акты реагирования просто будут собираться в одной папке уполномоченным лицом, обработка будет автоматизированной.



Подготовка проектов тематических докладных записок по клику
В случае результативной работы по обработке отдельных документов и наполнении базы возможен переход к следующему этапу – обучению ИИ на генерацию аналитических документов.



С каждым годом становится сложнее анализировать весь объем имеющейся информации;

3) **большие данные** — органы прокуратуры не оперируют всем объемом информации, известной отдельным прокурорам. Фактически она используется при подготовке конкретных документов, но редко используется весь ее потенциал;

4) **контроль** — прокурорам требуется наглядная информация о текущих контрольных сроках,

работа со списками контролей не всегда является удобной.

Концепция продукта заключается в автоматизации программными средствами, включающими в перспективе технологии искусственного интеллекта, процессов сбора, обработки, накопления, обобщения и анализа информации о состоянии законности и правопорядка, о практике надзорной и иной деятельности органов прокуратуры.

Единицами первичных данных планируется использовать акты прокурорского реагирования, до-

кладные записки об исполнении поручений и иные документы, пригодные для обработки генеративными нейросетями, в том числе путем извлечения сущностных характеристик соответствующих текстовых файлов. Из загруженного в систему массива данных предполагается в автоматическом режиме формировать сводные информационно-аналитические справки по заданным параметрам с возможностью их ручной доработки.

Например, для оценки состояния надзора в сфере ЖКХ АИС «ЭКП»

сможет подобрать по заданным критериям все представления, протесты, иски и другие акты, в которых есть упоминания о нарушениях закона в указанной сфере, и выдать готовую аналитическую справку с примерами как по отдельному региону, так и стране в целом.

Вместе с тем при выполнении поставленных задач возникают некоторые вопросы, связанные с особенностями машинной обработки текстовой информации, которые требуют поиска принципиальных решений.

Структура и содержание актов реагирования зачастую кардинально отличаются в разных прокуратурах в зависимости от особенностей региональной практики, сложившегося на местах шаблонного стиля изложения информации, перенасыщения документов выписками из законов, в том числе прямо не относящихся к выявленным нарушениям.

Указанное является препятствием для интеллектуальной обработки данных актов с использованием информационных технологий на принципах машинного обучения, которые запрограммированы на работу со

структурированными данными, объединенными единой логикой изложения информации, и требует пересмотра требований к таким документам.

В перспективе использование ИАС «ЭКП» позволит подготавливать и акты прокурорского реагирования, структура которых будет единообразной во всех органах прокуратуры, с последующей их обработкой машинным путем и получением аналитических выкладок, в том числе прогностического характера.

Отдельные модули системы, которые оперируют структурированными данными, не требующими сложной обработки, запущены в пробную эксплуатацию и тестируются.

Фактически реализована функция суммирования цифровых показателей (в одно нажатие, с проверкой логического контроля), она использовалась при сборе таблиц по отдельным заданиям, что позволило на деле убедиться в реальном упрощении рутинной типовой работы и значительном сокращении ее сроков. В дальнейшем применение продвинутых электронных инструментов обработки сведений приведет к

гораздо более высокой оперативности информирования руководства Генеральной прокуратуры об актуальном состоянии и динамике надзорной и иной деятельности, особенно при отсутствии отчетных данных, что, помимо всего прочего, положительно отразится на качестве управленческих решений.

Также функционирует компонент ИАС — «Электронный календарь поручений», который предназначен не только для контроля за своевременностью исполнения поручений и мгновенного поиска их первоисточника, но и призван в дальнейшем стать официальным электронным реестром всех действующих заданий с признанием не подлежащими исполнению документов, в него не вошедших. Данная функция также преследует своей целью снижение организационной нагрузки и, как следствие, высвобождение рабочего ресурса для выполнения непосредственно надзорных задач, стоящих перед органами прокуратуры.

Календарь предоставляет возможности для его ведения во всех звеньях органов прокуратуры.

Первыми этот функционал начали осваивать в Курганской об-

Визуальный календарь



ласти. Работниками соответствующей прокуратуры использована возможность гиперссылок на документы, зарегистрированные в АИК «Надзор-WEB». Таким образом можно не только увидеть информацию о наступившем сроке исполнения, но и быстро получить доступ к самому документу, установившему его.

В отношении докладных записок по направлениям работы апробируется создание их электронного шаблона, структурированного согласно логико-тематическим блокам задания или поручения, наполнение которых (для придания необходимой лаконичности) ограничено количеством печатных знаков, заданы иные параметры заполнения типовой схемы в целях улучшения быстрого поиска информации, ее обработки.

Такой подход позволит:

- 1) обеспечить безопасное хранение, возможность использования аналитического функционала, в дальнейшем собранные данные можно применять для обучения искусственного интеллекта (информация сохраняется в базе данных);
- 2) сделать мгновенным поиск по собранным докладным запискам, повысить эффективность использования аккумулированных данных, а также их накопление (сквозной поиск);
- 3) сохранить историю переписки по аналитическому предмету, то есть при смене работника все докладные записки по направлению надзора будут доступны новому сотруднику (преимуществом аналитической работы);
- 4) агрегировать данные докладных записок по тематическим разделам согласно установленной структуре, что облегчит обработку информации в зависимости от объема аналитической задачи (упрощение обобщения докладных записок по заданным параметрам).

В ИАС «ЭКП» предусмотрены успешно эксплуатируемые специализированные модули, которые уже стали существенным подспорьем в прокурорской деятельности, в частности «Реестр интернет-ресурсов с противоправной информацией» (далее — Реестр, РИПИ).

Письмом первого заместителя Генерального прокурора Российской Федерации от 12.04.2023 «О повышении эффективности работы по подготовке заключений и административных исковых заявлений в целях блокировки в сети "Интернет" информации, распространяемой с нарушением закона» прокуроры ориентированы использовать указанный Реестр в целях сверки адресов интернет-ресурсов и исключения дублирования мер реагирования в отношении них.

До использования Реестра при подготовке заключений, направляемых в Генеральную прокуратуру Российской Федерации по интернет-ресурсам, содержащим предложения о приобретении поддельных документов, предоставляющих права или освобождающих от обязанностей, эффективность прокурорского реагирования составляла не более 15%. Это было обусловлено дублированием предлагаемых ими сайтов для включения в требование о принятии мер по ограничению доступа к информационным ресурсам.

К примеру, 10 прокуроров могли сообщить об одном и том же ресурсе: diplom.com. При этом в каждом субъекте затрачивалось время на проверку и подготовку необходимого пакета документов.

После начала использования РИПИ эффективность работы отдельных прокуроров на рассматриваемом участке повысилась до 50–70%. При условии использования соответствующего ресурса всеми прокурорами прогнозируется повышение названного показателя до 95%.

Немалую роль в улучшении качества надзорной деятельности в настоящее время играет реестр государственных контрактов, заключенных в рамках национального проекта «Цифровая экономика».

Этот реестр, размещенный в ИАС «ЭКП», позволяет прокурорам без дополнительных запросов получать сведения о заключенных на поднадзорной им территории государственных контрактах в рамках названного национального проекта. Источником информации является Росфинмониторинг, обновление данных происходит ежеквартально.

Сведения о возможностях упомянутого Реестра доведены до нижестоящих прокуроров в информационном письме первого заместителя генерального прокурора Российской Федерации от 31.07.2023 «Об активизации прокурорского надзора за исполнением законодательства при реализации национального проекта "Цифровая экономика"».

Таким образом, платформу ИАС «ЭКП» можно уже сейчас рассматривать как реально действующего электронного помощника для прокуроров всех уровней, а в перспективе доработка данного продукта с раскрытием всего его потенциала может кардинально поменять традиционные способы организации прокурорской деятельности, значительно сместив баланс трудозатрат с выполнения сугубо технических задач на непосредственно интеллектуальную обработку данных, а следовательно, повысить качество надзора и состояние обеспеченности прав и свобод граждан.



КРИПТОВАЛЮТА: В ПОИСКАХ РЕШЕНИЙ

68 ОЛЬГА ТИСЕН

Правовое регулирование оборота виртуальных активов и противодействия их использованию в целях ОД/ФТ в отдельных странах ЕАГ

73 ДМИТРИЙ МАЧИХИН

AML-расследования в Web-3 индустрии

77 ШОН МУНИР

Работа с цифровыми активами: криптовалюта, NFT и финансовая безопасность



ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА ВИРТУАЛЬНЫХ АКТИВОВ И ПРОТИВОДЕЙСТВИЯ ИХ ИСПОЛЬЗОВАНИЮ В ЦЕЛЯХ ОД/ФТ В ОТДЕЛЬНЫХ СТРАНАХ ЕАГ

За почти 15 лет существования технологии распределенного реестра отношения в этой сфере существенно трансформировались. Появились миксеры, тумблеры и анонимайзеры, позволяющие скрыть следы связи конкретного владельца с транзакциями, сформировалась развитая инфраструктура провайдеров услуг виртуальных активов (ПУВА¹), в том числе работающих в теневом секторе, а количество криптовалют многократно увеличилось



ОЛЬГА ТИСЕН,
начальник Юридического
управления Росфинмониторинга,
сопредседатель РГОП ЕАГ, д.ю.н.

Первым документом на международном уровне, посвященным тематике новых цифровых сущностей, предназначенных для расчетов, стал отчет Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) «Виртуальные валюты», выпущенный в июне 2014 года². В нем содержались ключевые определения, связанные с функционированием виртуальных активов, и установленные на тот момент производные риски. Здесь же был зафиксирован впоследствии многократно подтвердившийся тезис о том, что виртуальные валюты в руках преступников становятся новым мощным инструментом для перемещения и хранения денежных средств таким образом, что они оказываются вне досягаемости

правоохранительных и иных компетентных органов.

Через год, в июне 2015 года, ФАТФ выпустила Руководство по применению риск-ориентированного подхода в отношении виртуальных активов. В нем описываются основные способы минимизации рисков использования цифровых валют в целях отмывания доходов, полученных преступным путем, и финансирования терроризма.

В октябре 2018 года стандарты ФАТФ были распространены на финансовую деятельность, связанную с виртуальными активами. Рекомендации ФАТФ обновляются с 2021 года ежегодно. В 2020 году выпущен отчет ФАТФ о признаках легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма при обороте виртуальных активов,

¹ ПУВА — провайдеры услуг в сфере виртуальных активов — любое физическое или юридическое лицо, которое осуществляет в качестве предпринимательской деятельности один или более следующих видов операций для/или от имени другого физического или юридического лица: обмен между виртуальными активами и фиатными валютами; обмен между одной или более формами виртуальных активов; перевод виртуальных активов; хранение и/или администрирование виртуальных активов или инструментов, позволяющих осуществлять контроль над виртуальными активами; участие и предоставление финансовых услуг, связанных с предложением выпускающего лица и/или продаж виртуального актива // Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ, июнь 2014.

² Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ, июнь 2014 // www.fatf-gafi.org.

а также отчет ФАТФ для участвующих в Группе 20 министерств финансов и центральных банков стран по вопросу стейблкоинов³.

С принятием указанных документов сформировалась международно-правовая основа для установления в государствах режимов в отношении оборота ВА в целях противодействия угрозам безопасности, включающим в себя использование криптовалюты⁴ транснациональной организованной преступностью, в том числе в целях легализации (отмывания) преступных доходов и финансирования терроризма⁵.

**ОЧЕВИДНО, ЧТО
ВВЕДЕНИЕ ПРАВОВОГО
РЕГУЛИРОВАНИЯ
ДЕЯТЕЛЬНОСТИ ПУВА,
РАСПРОСТРАНЕНИЕ
НА НИХ ТРЕБОВАНИЙ
МЕЖДУНАРОДНЫХ
СТАНДАРТОВ ПОД/ФТ,
ЛИБО ПОЛНЫЙ ЗАПРЕТ
ВИРТУАЛЬНЫХ АКТИВОВ —
НЕИЗБЕЖНАЯ РЕАЛЬНОСТЬ
ДЛЯ ВСЕХ ГОСУДАРСТВ.**

Основные требования стандартов ФАТФ в отношении оборота виртуальных активов заключаются в следующем:

- государства должны выявлять, оценивать и снижать риски ОД/ФТ, возникающие в связи с операциями с виртуальными активами (далее — ВА);
- для целей применения стандартов ФАТФ ВА должны быть отнесены к имуществу, что влечет за собой их признание предметом преступлений, в том числе связанных с ОД/ФТ. ВА в статусе иму-

щества подлежат блокированию (замораживанию), аресту и конфискации;

- деятельность ПУВА, которые осуществляют обменные операции с ВА, перевод виртуальных активов, их хранение, должна контролироваться, включая регистрацию/лицензирование таких лиц и надзор за ними. На ПУВА должны быть возложены обязанности по идентификации клиентов, их бенефициарных владельцев, направлению в подразделение финансовой разведки сообщений о подозрительных операциях, хранению данных.

В Руководстве по применению риск-ориентированного подхода в отношении ВА и ПУВА, принятом ФАТФ в октябре 2021 года, разъяснено, что страны могут запретить или ограничить деятельность с ВА либо работу ПУВА, основываясь на оценке рисков и особенностях национального законодательства, а также следуя иным политическим целям, например таким, как защита потребителей, безопасность и стабильность, денежная политика⁶. В случае принятия решения о запрете или ограничении деятельности с ВА на территории страны, положения Рекомендации 15 ФАТФ в этой части неприменимы, но юрисдикции будут обязаны оценивать возникающие риски. В случае нарушения запрета на оборот ВА государства, принявшие такое решение, должны принимать соответствующие меры к нарушителю (пункты 108, 109 Руководства), а также выявлять физических и юридических лиц, осуществляющих деятельность в указанной сфере без регистрации и лицензии.

В Резолюции Совета Безопасности ООН 1617 указано на необходимость соблюдения стандартов ФАТФ и всеобъемлющих междуна-

родных стандартов, отраженных в Сорока рекомендациях Целевой группы по финансовым мероприятиям, касающихся отмывания денег, и Девяти специальных рекомендаций, касающихся финансирования терроризма.

В части подхода к имплементации 15-й Рекомендации ФАТФ выделяют 3 модели правового регулирования оборота виртуальных активов:

- 1) запрет оборота и использования виртуальных активов в стране в качестве средства платежа;
- 2) разрешительный подход — легализация оборота ВА на территории страны, в том числе в качестве средства платежа, создание рынка и соответствующей инфраструктуры;
- 3) регулирование оборота ВА при одновременном введении законодательных ограничений их использования и правовом регулировании деятельности ПУВА. Эта модель является самой распространенной в странах мира.

В большинстве стран уже действуют нормы, законодательно определяющие статус ВА в пределах юрисдикции: запрет/разрешение на их использование в качестве средства платежа, возможность владения и инвестирования и т. д. Однако законодательное отнесение ПУВА к субъектам ПОД/ФТ, позволяющее противодействовать использованию криптовалют преступниками, идет во многих государствах более замедленными темпами.

В странах ЕАГ применяются все три описанные модели. Так, в материковом Китае в 2017 году введен запрет на использование криптовалют; в Беларуси, Индии, Казахстане, Кыргызстане, Узбекистане ПУВА уже отнесены к субъектам ПОД/ФТ, в Российской Федерации к субъектам установлено правовое регулирование функциониру-

³ www.fatf-gafi.org.

⁴ Под криптовалютой в рамках статьи понимается децентрализованная конвертируемая виртуальная валюта. Понятия «криптовалюта», «виртуальные активы», «криптоактивы» используются в рамках статьи как тождественные.

⁵ Приложение к постановлению ПА ОДКБ от 05.12.2022 № 15-6.5.

⁶ www.fatf-gafi.org.

вания ПУЦА⁷, а в Таджикистане и Туркменистане идет процесс разработки таких норм.

РЕСПУБЛИКА БЕЛАРУСЬ

Правовой статус оборота ВА в *Республике Беларусь* введен еще в 2017 году Декретом Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики»⁸ (далее — Декрет). Документ предусматривает создание условий для внедрения в экономику республики блокчейна и иных технологий, основанных на принципах распределенности, децентрализации и безопасности совершаемых с их использованием операций.

Согласно приложению 1 к Декрету под криптовалютой понимается биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена.

Согласно законодательству Республики Беларусь, граждане страны вправе покупать и продавать криптовалюту на любых криптобиржах, в том числе международных. В свою очередь юридические лица могут работать только с резидентами Парка высоких технологий⁹. Индивидуальные предприниматели вправе осуществлять операции по приобретению, отчуждению криптовалюты будучи резидентами ПВТ (подпункт 2.2 Декрета).

Является незаконной и запрещается предпринимательская деятельность физических и юридических лиц, не являющихся резидентами ПВТ, по оказанию содействия на территории Республики Беларусь и (или) с использованием интернета иным лицам в совершении и (или) исполнении сделок (операций) с токенами (в том чис-



ле выступать стороной по таким сделкам (операциям) с использованием функционирующей в интернете информационной системы либо посредством предоставления права (разрешения) иным лицам использовать ее, а также по приобретению и (или) отчуждению, в том числе обмену токенов (подпункт 2.6 пункта 2 Декрета).

Деятельность ПУВА в стране регулируется Администрацией ПВТ, Национальным банком Республики Беларусь и Комитетом государственного контроля. Проведение проверок резидентов Парка высоких технологий не может осуществляться без предварительного согласования с государственным учреждением «Администрация Парка высоких технологий» (п. 4.6 Декрета).

Согласно законодательству, в Беларуси на территории ПВТ резидентам разрешены следующие виды предпринимательской деятельности, относящиеся согласно стандартам ФАТФ к ПУВА: криптобиржа, криптообменник, организатор ICO, майнинг-пул.

Все ПУВА, действующие на площадке ПВТ, отнесены к субъектам ПОД/ФТ и обязаны проводить процедуры, направленные на соблюдение требований в сфере отмывания денег.

РЕСПУБЛИКА КАЗАХСТАН

Правовое регулирование оборота виртуальных активов в *Республике Казахстан* введено Законом от 25.06.2020 № 347-VI ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий», согласно которому цифровые активы были признаны имуществом, но использовать их в качестве платежного средства на территории Казахстана запрещено.

Цифровые активы в законе о криптовалютах подразделяются на два вида: обеспеченные и не обеспеченные. Криптовалюты приравниваются к необеспеченным активам, их выпуск и оборот в Казахстане находятся под запретом, за исключением территории созданного в 2018 году Международного финансового центра «Астана» (МФЦА).

Согласно Закону Республики Казахстан от 18.11.2021 № 73-VII ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»,

⁷ ПУЦА — провайдер услуг цифровых активов.

⁸ <https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrya-2017-g-17716>.

⁹ Далее — ПВТ, Парк.

лица, осуществляющие деятельность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество, установлены в качестве субъектов финансового мониторинга. Для этих субъектов введены обязательства по уведомлению уполномоченного органа в сфере информатизации о начале и прекращении своей деятельности, что фиксируется в соответствующем государственном реестре.

Законом Республики Казахстан от 24.06.2021 № 53-VII ЗРК «О внесении изменений и дополнений в Кодекс

Республики Казахстан «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс) и Закон Республики Казахстан «О введении в действие Кодекса Республики Казахстан "О налогах и других обязательных платежах в бюджет" (Налоговый кодекс)» регламентированы вопросы налогообложения цифрового майнинга.

В целях развития индустрии цифровых активов 06.02.2023 года Президентом подписан Закон Республики Казахстан «О цифровых активах в Республике Казахстан» (далее — Закон), которым для цифровых активов введены государственный контроль, лицензи-

рование и администрирование, налогообложение.

Уполномоченным органом в части определения правового режима оборота цифровых активов является Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Согласно Закону о цифровых активах, на территории Республики Казахстан запрещаются выпуск и оборот необеспеченных цифровых активов, а также деятельность бирж цифровых активов по необеспеченным цифровым активам, за исключением территории МФЦА. В МФЦА регулирование провайдеров услуг цифровых активов, а также оборота цифровых активов осуществляется в регуляторной «песочнице».

Помимо оборота цифровых активов, актами МФЦА осуществляется регулирование широкого круга провайдеров услуг цифровых активов (ПУЦА), включая криптобиржи, брокеров, дилеров, касто-дианов, управляющих фондами и лиц, предоставляющих консультационные услуги.

В целях недопущения использования ПУЦА для целей отмыывания денег и финансирования терроризма ПУЦА обязаны обеспечить следующие ключевые системы контроля: «знай своего клиента» («know your customer») и «знай свою транзакцию» («know your transaction»). То есть ПУЦА проводят идентификацию и надлежащую проверку не только каждого клиента, но также и проверку его личного цифрового кошелька, историю транзакций на признаки нарушения требований законодательства о противодействии легализации (отмыыванию) доходов, полученных преступным путем, и финансированию терроризма.

Статьей 3 Закона Республики Казахстан «О противодействии легализации (отмыыванию) доходов, полученных преступным путем, и финансированию терроризма» лица, осуществляющие деятель-





ность по выпуску цифровых активов, организации торгов ими, а также предоставлению услуг по обмену цифровых активов на деньги, ценности и иное имущество, отнесены к субъектам финансового мониторинга. В приказе председателя Агентства финансового мониторинга Республики Казахстан «Об утверждении Правил представления субъектами финансового мониторинга сведений и информации об операциях, подлежащих финансовому мониторингу, и признаков определения подозрительной операции» установлены признаки определения подозрительной операции в сфере цифровых активов.

В Казахстане отдельное внимание уделено правовому регулированию деятельности майнинговых пулов, отнесенных стандартами ФАТФ к ПУВА¹⁰.

КЫРГЫЗСКАЯ РЕСПУБЛИКА

В Законе *Кыргызской Республики* от 21.01.2022 № 12 «О виртуальных активах» (вступил в силу 28.07.2022) определены основные понятия, относимые к регулируемой сфере, правовой статус виртуальных активов, требования к участникам оборота криптовалюты.

В Кыргызской Республике определены следующие субъекты, участвующие в обороте криптовалюты: поставщики услуг виртуальных активов, операторы торгов виртуальных активов, криптобиржи, майнинг-пул¹¹.

Согласно п. 19 ч. 1 ст. 5 Закона Кыргызской Республики от 06.08.2018 № 87 «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов»¹² (далее — Закон № 87) ПУВА отнесены к финансовым учреждениям, обязанным осуществлять надлежащую проверку клиентов, направлять в Государственную службу финансовой разведки при Министерстве финансов Кыргызской Республики сообщения о подозрительных операциях и выполнять иные обязанности в рамках внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Во исполнение статей 16, 18, 25, 28 Закона Кыргызской Республики «О виртуальных активах» принято постановление Кабинета Министров КР «О вопросах регулирования отношений, возникающих при обороте виртуальных активов» от 16.09.2022 № 514. Статьей 2 Закона

от 05.08.2022 № 81 «О внесении изменений в некоторые законодательные акты в сфере виртуальных активов» внесены изменения в Закон № 87. ПУВА отнесены к финансовым учреждениям, и все требования, установленные в Законе № 87 и касающиеся Рекомендаций 10–21 ФАТФ, распространяются на ПУВА.

Деятельность ПУВА в Кыргызстане подлежит лицензированию. Лицензии выдает Служба регулирования и надзора за финансовым рынком при Министерстве экономики и коммерции Кыргызстана. Поставщики услуг виртуальных активов должны быть исключительно юридическими лицами, зарегистрированными на территории страны.

Взаимодействие Государственной службы финансовой разведки Кыргызской Республики с операторами электронных платежных систем осуществляется в соответствии с Законом № 87 и Положением о порядке представления информации и документов в орган финансовой разведки Кыргызской Республики (утверждено постановлением Правительства Кыргызской Республики от 25.12.2018 № 606). Этим положением ПУВА должны руководствоваться при проведении реализации процедуры «знай своего клиента».

Спустя 15 лет после создания криптовалют очевидно, что пробелы правового регулирования их оборота создают дополнительные угрозы экономической безопасности и многократно повышают риски их использования для совершения преступлений.

Продолжение статьи о том, как регулируется оборот криптовалют в других странах СНГ и БРИКС, читайте в следующем выпуске журнала.

¹⁰ П. 5 ст. 11 Закона Республики Казахстан «О цифровых финансовых активах» // https://online.zakon.kz/m/document?doc_id=33689356.

¹¹ <http://cbd.minjust.gov.kg/act/view/ru>.

¹² <http://cbd.minjust.gov.kg/act/view/ru-ru/111822?ysclid=loiruxojbb75473943>.

AML-РАССЛЕДОВАНИЯ В WEB3-ИНДУСТРИИ

За последние 10 лет финансовый мир значительно трансформировался благодаря появлению криптовалют. Фактически, мы можем говорить о возникновении новой параллельной финансовой системы. И хотя речь, конечно, не идет о том, что 100% транзакций в этой системе носят противоправный характер (в реальности не более 0,5%), количество правонарушений крайне велико



▶ ДМИТРИЙ МАЧИХИН,
международный эксперт по
платежам и AML (ПОД/ФТ)
в сфере Web3, член Экспертного
совета рабочей группы
«По вопросу законодательного
регулирувания криптовалют»
Государственной Думы
Федерального Собрания
Российской Федерации

Речь идет, прежде всего, об отмытии денег (Anti-Money Laundering, далее — AML), финансировании терроризма и различных формах мошенничества, взломах и хищениях. Для борьбы с этими угрозами успешно создаются и внедряются технологические инструменты мониторинга, расследований и борьбы.

В данном материале мы рассмотрим сильные и слабые стороны существующих AML-решений на криптовалютном рынке, расскажем о различных методах идентификации владельцев крипто-адресов и оценим частотность использования виртуальных активов в преступных целях.

КАК И КОГДА AML НАПРЯМУЮ ЗАТРОНУЛ КРИПТОВАЛЮТЫ

На заре биткойна и некоторых других первых криптоактивов вообще никакого AML в данной сфере не существовало. Именно этот период обязан появлению анонимных даркнет-маркетплейсов, вроде Silk Road.

В качестве регулирующих норм использовались общие законодательные акты (административное,

уголовное, налоговое право и т. д.). При этом отслеживанием транзакций в сети и их проверкой вообще никто не занимался. В свою очередь легальные торговые площадки самостоятельно определяли необходимость идентификации своих клиентов через KYC (англ. Know Your Customer), применяя финансовое регулирование по аналогии.

Так, понимая остроту проблемы и рост популярности криптовалют, а также благодаря раскрытию и аресту основателей Silk Road в июне 2014 года Группа разработки финансовых мер по борьбе с отмытием денег (англ. FATF) впервые обозначила риски, связанные с криптовалютным рынком. Именно тогда FATF опубликовала отчет «Virtual Currencies: Key Definitions and Potential AML/CFT Risks», в котором указаны потенциальные риски отмытия денег через криптовалюты. Спустя пять лет, в 2019 году, FATF представила первые рекомендации, которые затронули не только площадки, осуществляющие оборот виртуальных активов, но и сами криптовалюты. В частности, были определены основные принципы AML-регулирования криптовалютного рынка и полномочия государственных органов в этой сфере.



ПРЕСТУПЛЕНИЯ В КРИПТЕ: КАКИЕ, КАК ЧАСТО ОСУЩЕСТВЛЯЮТСЯ И КАКОВА ЕЕ РОЛЬ

Обладающие потенциалом в области демократизации финансовых рынков криптовалюты стали использоваться криминальными кругами. Различные токены, включая и сам биткоин, часто используются для широкого спектра преступлений.

Так, криптовалюту используют для легализации доходов от преступной деятельности, мошенничества и вымогательства. Здесь злоумышленники чаще всего прибегают к стейблкоинам, лишенным риска волатильности и приравненным к стоимости доллара США, например Tether (USDT) или USD Coin (USDC).

Довольно часто злоумышленники прикрываются знаменитостями, чтобы получить доверие. В конце 2023 года неизвестные смогли украсть у жертв свыше \$160 000 на разных блокчейн-сетях, выдавая себя за американского предпринимателя через видеосервис YouTube.

Повышенная анонимность отдельных криптовалют делает их привлекательными для трансграничных переводов между преступниками. Стоит отметить, что международное сообщество проявляет внимание к вопросу регулирования подобных активов.

Согласно данным американских аналитиков, начиная с 2017 года криптовалюты чаще всего фигурируют в мошеннических схемах.

Криптовалюты также используются в финансировании терроризма. Несмотря на достаточно масштабные меры по пресечению подобной активности, известны отдельные случаи, когда приложенных усилий оказалось недостаточно.

КАК НАХОДЯТ «ГРЯЗНЫЕ» КРИПТОВАЛЮТЫ И ЧТО ПРОИСХОДИТ, ЕСЛИ ИЗВЕСТНЫ ТОЛЬКО АДРЕСА

Для выявления незаконной деятельности с использованием криптовалют применяются различные методы идентификации и анализа транзакций в блокчейне. При этом исход расследований зависит не только от того, какими методами

пользуется AML-провайдер, но и от действий самих киберзлоумышленников.

AML-провайдеры используют разные методы для идентификации «грязных» средств. Один из известных методов предполагает распыление (англ. dust attack) незначительного объема криптовалюты на таргетированные адреса с целью дальнейшего выявления личности владельца адреса.

Сотрудники аналитических фирм Chainalysis и CipherTrace ранее публично отвергли использование этих методов в своих практиках. Однако они признали, что отдельные блокчейн-аналитики прибегают к таким способам анализа.

Впрочем, одним только анализом блокчейн-данных дело не ограничивается. Крупные AML-провайдеры, как правило, обладают целыми штатами экспертов в области блокчейн-аналитики и криминалистики, которые выявляют криптовалютные адреса детерминистическим образом.

Так, в случае с криптовалютными сервисами аналитики определяют адреса для депозита и вывода криптовалют. Через них

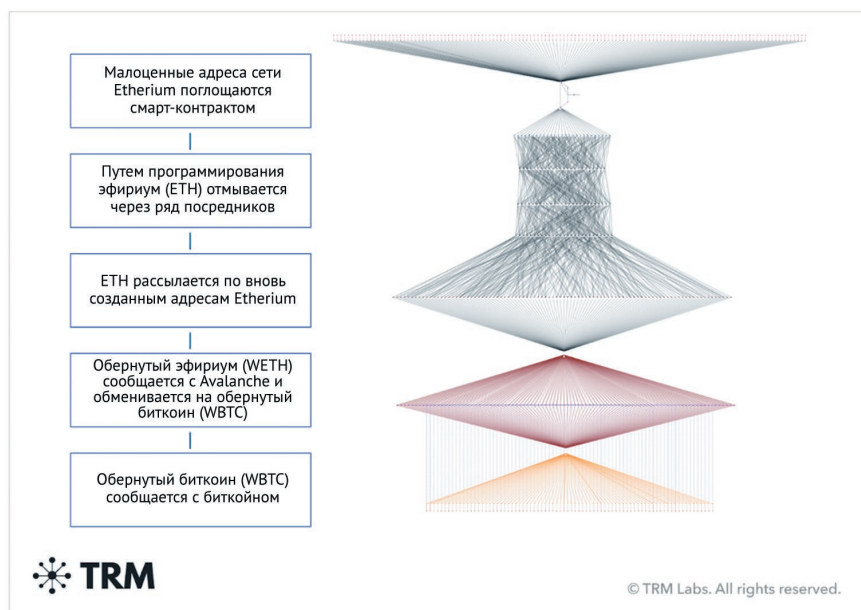
► Распределение объемов криптовалют, полученных на «грязные» адреса по категориям

Источник: Chainalysis

Совокупная стоимость криптовалюты, поступившей на адреса (кошельки) преступников, 2017–2022



► **Схема отмывания украденных ETH и конвертация их в другие токены с целью обмена на BTC**
 Источник: TRM Labs



в дальнейшем можно отследить перемещение виртуальных активов, а в некоторых случаях даже выявить личность владельца криптовалют.

Прибегают AML-провайдеры также к OSINT-аналитике. Как правило, это означает, что эксперты изучают данные, доступные в открытом доступе на площадках вроде YouTube, Telegram, X (бывш. Twitter), Reddit, форумах, даркнете и других подобных платформах.

Если известны только адреса кошельков, провайдеры AML могут использовать данные о прошлых транзакциях для выявления возможных контактов подозре-

ваемых с централизованными сервисами, которые зачастую верифицируют своих клиентов.

Некоторые AML-провайдеры сотрудничают с правоохранительными органами и криптовалютными биржами, что увеличивает возможности и скорость выявления злоумышленников.

Набирают популярность криптомиксеры и децентрализованные «бриджи», позволяющие усложнить трейсинг источника и конечного получателя. Печально известен миксер Tornado Cash, популярный среди нелегальных игроков крипторынка.

СЛАБЫЕ И СИЛЬНЫЕ СТОРОНЫ AML-ПРОВАЙДЕРОВ, КУДА НУЖНО РАЗВИВАТЬСЯ

Несмотря на постоянное совершенствование алгоритмов, AML-провайдеры по-прежнему сталкиваются с рядом проблем, например, с невозможностью получить ответную информацию со стороны криптовалютных бирж. Существенное различие требований к соблюдению нормативов в разных юрисдикциях значительно усложняет работу AML-провайдеров на международной арене.

Более того, каждый крупный AML-провайдер придерживается сугубо собственных, закрытых методов анализа данных и разметки адресов. С одной стороны, это повышает конкуренцию на рынке и помогает раскрытию преступлений. С другой стороны, отсутствие четких стандартов приводит к существенному различию качества выполняемых работ, а также к возможности манипулировать данными и разметкой.

Например, известен случай, когда централизованная биржа криптовалют публично признала, что ее пользователь занимался масштабным мошенничеством. Однако площадка при этом не стала блокировать своего клиента, сославшись на отсутствие запроса со стороны правоохранительных органов.



► **Идентификация криптовалютного адреса к сети биткойн-автоматов**
 Источник: Chainalysis

В 2021 году ФАТФ обратилась к группе AML-провайдеров с целью выяснить активность взаимодействия адресов напрямую с биржами и за их пределами. Разница в итоговых данных оказалась настолько большой, что ФАТФ пришлось признать невозможность формирования четких выводов на основе полученных результатов.



По мере развития единой базы требований и аттестации качества оказываемых услуг AML-провайдеры смогли бы в разы повысить эффективность своей работы и обеспечить общую безопасность криптовалютной среды.

При этом другой ключевой проблемой в области остается недостаточное регулирование. Множество юрисдикций имеют разные подходы к регулированию криптовалют, что создает проблемы для AML-провайдеров, работающих в различных регионах. Это также затрудняет международное сотрудничество в борьбе с финансовыми преступлениями.

Необходимо разработать согласованные международные стандарты AML-регулирования криптовалютного рынка. В ФАТФ, например, давно пытаются подвести международное регулирование под единые стандарты, однако до сих пор достичь этого не удалось.

Также следует отметить, что государственным органам стоит активнее идти на сотрудничество с AML-провайдерами, поскольку это не только сокращает время на обучение нового персонала, но и повышает качество проводимых мероприятий. Важно обучать специалистов в области AML, чтобы они могли эффективно противодействовать финансовым преступлениям в криптосфере. Программы повышения квалификации и

сертификационные курсы помогут специалистам развивать необходимые навыки и компетенции.

Отдельно хотелось бы выделить противоречие данных ряда AML-провайдеров друг другу, причем зачастую по политическим или санкционным признакам. Например, AML-провайдер в США может считать тот или иной кошелек санкционным, тогда как такой же провайдер в РФ может иметь обратные данные. В случае попадания активов с такого адреса на легальную централизованную биржу, могут возникнуть разночтения, вплоть до блокировки средств.

ВЫВОД

По итогам 2023 года объем «грязной» криптовалюты, полученной в результате неправомερных действий, снизился до 24,2 млрд долларов с 39,6 млрд долларов в 2022 году.

Цифра велика, однако меркнет на фоне правонарушений в традиционных финансовых рынках. Для решения преступлений в Web3-индустрии очевидно требуется комплексный подход.

При этом стоит помнить, что речь только о прямо размеченных «грязных адресах», а сколько криптовалютных транзакций находится в «серой» зоне, какое количество средств потенциа-

но является нарушением AML-политик банков и сколько активов сокрыты от налогообложения и идентификации, сложно представить, но цифра может оказаться в сотни раз выше.

Очевидно, что разработка одних только эффективных AML-механизмов проблему не решит. Необходимо международное сотрудничество и, что не менее важно, повышение компетенции в сфере AML для участников криптовалютной индустрии.

Тем не менее роль AML-провайдеров в борьбе с криптовалютными преступлениями трудно переоценить. Именно благодаря им криптовалютная индустрия не погрязла в регуляторных запретах.

Баланс между безопасностью и приватностью — ключевой элемент в эффективном регулировании. Меры AML-регулирования не должны ущемлять права пользователей, соблюдая при этом принципы приватности и безопасности данных.

Путь к безопасному будущему криптовалют тернист, но достижим. Совершенствование технологий, развитие международного сотрудничества и объединение усилий правительств, регуляторов, AML-провайдеров и криптовалютных компаний может создать безопасную и прозрачную основу для развития криптовалютной индустрии.



РАБОТА С ЦИФРОВЫМИ АКТИВАМИ: КРИПТОВАЛЮТА, NFT И ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

Цифровая революция, отмеченная появлением технологии блокчейна и криптовалюты, ознаменовала новую эру в финансовой индустрии, открыла новые возможности и бросила новые вызовы



ШОН МУНИР,
генеральный директор
и соучредитель компании
Coinweb.com (ОАЭ)

Крайне важно понимать двойственную природу цифровых активов. Обеспечивая развитие инноваций и расширение возможностей, в руках злоумышленников они также могут стать средством противоправной деятельности, в частности — финансирования терроризма.

После прочтения статьи вы получите представление о виртуальных активах и познакомитесь с практиками, которые помогут изменить работу вашей организации.

СОВРЕМЕННОЕ СОСТОЯНИЕ КРИПТОАКТИВОВ

Мы наблюдаем четвертый цикл развития криптовалюты. Хотя со стороны этот процесс кажется хаотичным, он упорядочен и связан с рыночной капитализацией, взаимодействием с разработчиками, стартапами и социальными медиа.

В 2024 году был одобрен биткоин ETF, то же самое ждет и Ethereum

ETF. При этом в мае 2024 года ожидается халвинг биткоина, что впоследствии положит начало резкому повышению цен на криптовалюты (период Буллран).

Если раньше DeFi, или децентрализованные финансы, практически не существовали, то сегодня они оцениваются в 100 млрд долларов. Этот путь был пройден за два года (2020–2022).

Стейблкоины, предназначенные для обеспечения стабильности, как доллар США или золото, получили значительное распространение в регионах с инфляцией и волатильностью валют (особенно в Африке, на Ближнем Востоке и в Юго-Восточной Азии).

В то же время рынок NFT переживает взрывной рост: в 2021 году объем транзакций достиг 44,2 млрд долларов по сравнению со 106 млн долларов в предыдущем году. Однако этот рынок не лишен проблем, включая вош-трейдинг и отмывание денег.

Капитализация глобального рынка криптовалют



ПРОТИВОДЕЙСТВИЕ ОТМЫВАНИЮ ДОХОДОВ И БОРЬБА С ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА

Криптовалюта, к которой часто относятся скептически, парадоксально стала первой отраслью, предлагающей жизнеспособное решение проблемы отмывания денег.

Прогресс во многом достигнут благодаря оперативной разработке нормативных актов при лидирующей роли ФАТФ, важнейшей международной организации по борьбе с отмыванием денег и финансированием терроризма.

Необходимо срочное принятие мер по треку противодействия отмыванию преступных доходов и финансированию терроризма (ПОД/ФТ). Преступники и террористы не ждут развития нормативного регулирования.

Частный сектор нуждается в регулировании

Интересно, что со стороны криптосектора очевиден запрос на регулирование. Это связано с

сетевым эффектом на финансовых рынках: организации предпочитают взаимодействовать с регулируемыми контрагентами, чтобы минимизировать риски.

Этот спрос на регулирование стал стимулом к развитию конкурентных регуляторных решений, позволяющих небольшим криптокомпаниям сотрудничать с традиционными игроками финансового рынка в целях получения ликвидности.

Несмотря на успехи, капитализация крипторынка остается довольно скромной, составляя 2 трлн долларов по сравнению с ежедневным объемом транзакций в долларах США в размере 2,6 трлн.

Сотрудничество частного сектора и регуляторов

Борьба с финансовыми преступлениями требует согласованных усилий по отслеживанию средств. Финансовым институтам отводится первостепенная роль в этой экосистеме. Им поручено анализировать действия клиентов, выявлять несоответствия и отслеживать транзакции.

Подозрительная активность докладывается подразделению финансовой разведки (ПФР), что подчеркивает совместные усилия частного сектора и регулирующих органов по выявлению и искоренению финансовых преступлений.

NFT — НОВЫЙ СПОСОБ ТОКЕНИЗАЦИИ АКТИВОВ

Невозмозгаемые токены (NFT) привели к революции нашего представления о цифровой собственности, преобразовав цифровые данные в уникальные активы на блокчейне.

Движение в этом направлении началось с CryptoPunks в 2017 году, коллекции из 10 000 уникальных пиксельных изображений. Она стала вдохновением к созданию стандарта ERC-721 — первоосновы современных NFT и криптохудожников.

NFT и преступления

Новые технологии влекут новые риски, и NFT — не исключение. Всплеск популярности NFT, особенно во время пандемии COVID-19, подчеркнул необходимость создания безопасных платформ и внедрения контроля со стороны регуляторов.

В результате пандемии и спада продаж предметов традиционного изобразительного искусства потоки инвестиций были перенаправлены в NFT: объем сделок вырос со 106 млн долларов в 2020 году до более чем 17 млрд долларов в 2021 году.

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА И ВИРТУАЛЬНЫЕ АКТИВЫ

Террористические организации используют криптовалюту. В частности, в 2020 году «Аль-Каида»¹

¹ Запрещенная в Российской Федерации террористическая организация.



собирала средства через социальные медиа. Благодаря действиям правоохранительных органов было изъято более 1 млн долларов.

Усилия по отслеживанию и выявлению таких транзакций в большинстве своем увенчались успехом, что позволило предотвратить легализацию средств через биржи.

NFT, распространяющие призывы к терроризму

6 сентября 2022 года Исламское государство (ИГ)* с помощью NFT распространило послание, восхваляющее теракт в Афганистане. Его авторами были Исламское государство в провинции Хорасан, ячейка ИГ в Афганистане.

Это стало первым случаем использования NFT в террористических целях. Ряд других NFT были созданы теми же акторами, чтобы изучить возможности обхода

правоохранителей и модерации контента NFT на различных платформах.

NFT и финансирование ультраправых

NFT «Редкий Пепе», изначально созданный как интернет-мем, стал использоваться ультраправыми группировками. Такой случай произошел в декабре 2020 года, когда более 500 тысяч долларов в биткоинах были пожертвованы одному из представителей крайнего правых.

При проверке его кошелька была выявлена операция по совершению платежа в целях пожертвования анонимному держателю коллекционной криптовалюты «Редкий Пепе» на основе биткоина.

Использование NFT «Редкий Пепе» подчеркивает потенциал NFT в финансировании экстремистской деятельности.

ВЫВОДЫ

Значимость описанных выше фактов заключается в возможности использования NFT для финансирования терроризма. Они показывают, что различные группировки, такие как Исламское государство, возможно, изучают варианты сбора средств и распространения сообщений с помощью новых технологий, включая NFT.

Использование NFT террористами для создания цепочки стоимости и финансирования не ново. Передача NFT «Лягушонок Пепе» и разработка IS-NEWS #01 казались неизбежными.

Хотя эти NFT не выставлялись на продажу, они остаются в цепочках блокчейна и распространяются по бесчисленным интернет-системам. Они практически неуязвимы перед мерами Министерства юстиции или других правоохранительных органов.

Так, они устойчивы к цензуре, насколько это возможно, что является серьезной проблемой в борьбе с экстремистским контентом.



Rare Pepe			
PEPEPARADO			
Выпущено 20 октября 2016 года		Дата последней сделки: 31 декабря 2021 года	
Последняя цена	Валюта	Владельцы	Сделки
0.08000000	XCP	472	145
Предложение	Сожжено	Выпущено	Делимая
4,100,109	1,899,891	6,000,000	No
Авторы	Формат		
+ CLAIM	JPG		
Open Orders		Trade History	

² Запрещенная в Российской Федерации террористическая организация.

О НЕОБХОДИМОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПРОВАЙДЕРОВ УСЛУГ ВИРТУАЛЬНЫХ АКТИВОВ В ЦЕЛЯХ ПОД/ФТ ВО ВСЕХ СТРАНАХ МИРА

В октябре 2018 года стандарты ФАТФ были распространены на финансовую деятельность, связанную с виртуальными активами. Рекомендации ФАТФ обновляются с 2021 года ежегодно. В 2020 году выпущен отчет ФАТФ о признаках легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма при обороте виртуальных активов, а также отчет ФАТФ для участвующих в Группе 20 министерств финансов и центральных банков стран по вопросу стейблкоинов



➤ СОФЬЯ РУДКОВИЧ,
студентка 1 курса МГУ имени М.В. Ломоносова, двукратный победитель Международной олимпиады по финансовой безопасности (2021 и 2022 гг.)

Однако до сих пор деятельность ПУВА не урегулирована во многих странах мира. Этот пробел делает использование виртуальных активов и ПУВА уязвимым для злоупотреблений¹, что влечет за собой препятствия ведению предварительного расследования преступлений, совершенных с использованием виртуальных активов (например, финансирование терроризма, легализация доходов, полученных преступным путем), и сложности при осуществлении ареста, блокировки и конфискации виртуальных активов, полученных преступным путем или предназначенных для финансирования терроризма.

Термин ПУВА раскрывается в Руководстве по применению риск-ориентированного подхода в от-

ношении виртуальных активов и ПУВА. Это любое физическое лицо или юридическое лицо, которое осуществляет на коммерческой основе один или более видов деятельности или операций для/или от имени другого физического лица и юридического лица:

- 1) обмен виртуальных активов на фиатную валюту и обратно;
- 2) обмен одной или нескольких форм виртуальных активов на другие виртуальные активы;
- 3) перевод виртуальных активов;
- 4) ответственное хранение и/или управление виртуальными активами или инструментами, позволяющими контролировать виртуальные активы;
- 5) участие в предоставлении и предоставлении связанных с предложением и/или продажей виртуальных активов эмитента².

¹ FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf>, p. 3.

² FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>, p. 109.

Согласно пункту 7 Резолюции Совета Безопасности ООН от 29 июля 2005 г. № 1617 Рекомендации ФАТФ являются обязательными для их соблюдения³. Однако в 2022 году ФАТФ пришла к выводу, что лишь малая часть государств-членов реализовала новые Рекомендации по отношению к ПУВА⁴.

В ОТНОШЕНИИ ВА И ПУВА ПРИМЕНЯЮТСЯ ПРЕЖДЕ ВСЕГО СТАНДАРТЫ ФАТФ, СВЯЗАННЫЕ С:

- применением риск-ориентированного подхода к деятельности и операциям, связанным с виртуальными активами и ПУВА;
- надзором или контролем за ПУВА в целях ПОД/ФТ;
- лицензированием или регистрацией;
- предупредительными мерами, в том числе в части надлежащей проверки клиентов, хранения записей и документов, а также направления сообщений о подозрительных операциях;
- применением санкций и других правоприменительных мер;
- международным сотрудничеством.

Неурегулированность функционирования ПУВА на практике не препятствует их работе, а лишь увеличивает долю теневого сектора экономики. Значительное количество бирж и обменников криптовалют действуют вне правового поля, не зарегистри-

рованы ни в одной юрисдикции, не идентифицируют владельцев криптоадресов, не осуществляют комплаенс-процедуры, не соблюдают какие-либо требования. Это создает возможность использовать криптовалюты для совершения преступлений, в том числе легализации преступного дохода и финансирования терроризма безнаказанно⁵.

Отсутствие регулирования правового статуса ПУВА существенно усугубляется в сфере уголовного процесса. Изъятие преступных доходов в форме криптовалюты осуществляется двумя способами:

- 1) в ходе проведения следственных действий или оперативно-разыскных мероприятий путем изъятия «холодных» (аппаратных) криптокошельков или получения приватного ключа владельца криптокошелька, который предоставляет доступ сотрудникам правоохранительных органов к преступным доходам;
- 2) путем взаимодействия с ПУВА.

Если в ходе следственных действий или оперативно-разыскных мероприятий не удалось изъять криптокошелек или приватный ключ, то единственным способом ареста или блокировки криптовалюты является направление правоохранительными органами в соответствующий ПУВА, которым пользовался подозреваемый/обвиняемый, обращения о предоставлении следующих данных: Ф.И.О., сведения о документе, подтверждающем личность, гражданство, адрес, фото пользователя, контактные данные, IP-адрес, сведения об использовании VPN, реальный IP-адрес при использовании программ анонимизации адресов, геолокация, сведения об

устройстве клиента, статистика, предпочтения, активность, номер счета получателя средств, дата и время его создания, статус обменной операции, сумма ввода и вывода⁶. Этот способ целесообразен только в том случае, если ПУВА легально осуществляет свою деятельность и производит верификацию своих пользователей согласно принципам KYC — Know Your Client, например, с обязательным предоставлением копии паспорта, фотографии с паспортом в руках при регистрации⁷.

Эти сведения нередко предоставляются провайдерами услуг в сфере виртуальных активов на основании национального законодательства. Однако на практике эта норма в отношении ПУВА действует лишь «на доверии»: ПУВА, находящиеся в юрисдикции иностранных государств, уклоняются и избегают предоставления сведений о клиентах. Несмотря на это, в некоторых странах, в которых правовое регулирование деятельности ПУВА находится на этапе формирования, имеется практика предоставления сведений ПУВА, зарегистрированных в других государствах⁸.

В связи с высокими рисками, которые влечет отсутствие регулирования правового статуса ПУВА, полагаю необходимым:

- 1) повсеместное отнесение ПУВА во всех странах мира к субъектам ПОД/ФТ, введение их регистрации и лицензирования;
- 2) установить пороговую сумму разовых операций, при превышении которой ПУВА обязаны проводить надлежащую проверку клиента, например, Руководство ФАТФ устанавливает 1000 долларов США/евро.

³ Резолюция Совета Безопасности ООН от 29 июля 2005 г. № 1617 (Принята в г. Нью-Йорке 29.07.2005 на 5244-ом заседании Совета Безопасности ООН) // СПС КонсультантПлюс.

⁴ FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, p. 7.

⁵ Тисен О.Н. Установление владельцев криптокошельков, обнаружение и изъятие приватных ключей при расследовании уголовных дел // Уголовный процесс. 2024. № 1. С. 78-83.

⁶ FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, p. 80.

⁷ Тисен О.Н. Методика выявления и расследования преступлений, совершенных с использованием криптовалют. Москва, 2023. С. 53.

⁸ Тисен О.Н. Отслеживание транзакций криптовалют для расследования преступлений // Уголовный процесс. 2024. № 2. С. 54-59, С. 59.

В руководстве ФАТФ 2021 года подчеркнута важность международного сотрудничества между надзорными органами с учетом трансграничного характера де-

ятельности и услуг ПУВА. Безусловно, в текущей ситуации, когда риски использования виртуальных активов в преступных целях лишь возрастают, государства

должны объединиться в борьбе с новыми вызовами и угрозами и не политизировать сферу антикриминального сотрудничества.

Я являюсь победителем первой и второй Международных олимпиад по финансовой безопасности. Об Олимпиаде я узнала в 9 классе из социальных сетей и сразу же загорелась желанием участвовать в ней. Еще с 8 класса я интересовалась правом и была участником сборной Москвы по праву. В целях подготовки к Олимпиаде я изучила стандарты ФАТФ и российское законодательство о ПОД/ФТ, видеоуроки по финансовой безопасности. Качественная подготовка позволила мне пройти в финал и стать победителем.



нансовой безопасности поразила меня, вдохновила на новые успехи и позволила определиться с будущей профессией. Больше всего

нам не только повысить уровень знаний, но и показать свои творческие способности, актерский талант и навыки коммуникации.

Навсегда запомнилась встреча с директором Росфинмониторинга Юрием Анатольевичем Чиханчиным — выдающимся человеком и профессионалом.

Меня восхищает и вдохновляет история борьбы нашего государства с финансовыми преступлениями. В 2001 году нашему государству был брошен вызов: включение в черный список ФАТФ. Благодаря совместным усилиям Российская Федерация спустя 20 лет становится государством, имеющим одну из самых эффективных систем борьбы с преступлениями, посягающими на финансовую безопасность.

В будущем я бы хотела связать свою профессиональную жизнь с финансовой безопасностью, быть ученым и практиком в этой области.



Организация финала Международной олимпиады по финансовой безопасности кардинально отличается от итогового тура других олимпиад, в том числе от Всероссийской олимпиады школьников, в которой я неоднократно побеждала в 2020–2022 гг.

Программа финала Международной олимпиады по фи-

нальной безопасности поразила меня, вдохновила на новые успехи и позволила определиться с будущей профессией. Больше всего

на Олимпиаде мне нравится программа финала. Заключительный этап проходит около недели, но на выполнение самих заданий отведено всего лишь два часа. Все остальное время было посвящено экскурсиям, развлекательным и обучающим мероприятиям, в ходе которых мы познакомились с теорией и практикой ПОД/ФТ. Методика обучающих мероприятий программы финала Олимпиады была незабываемой. Игровой уголовный процесс по мотивам сюжета советского фильма «Бриллиантовая рука», квест «Легализация доходов по мультфильмам и кино» стали важным событием для меня и моих друзей. Это позволило



НОВОСТИ АНТИОТМЫВОЧНОЙ СИСТЕМЫ

84 «Игры Будущего». Победители турнира «Кубок четырех континентов» посетили Казань

85 Состоялось первое заседание Совета БРИКС по противодействию отмыванию доходов и финансированию терроризма в расширенном составе

85 Вопросы финансовой безопасности обсудили на Всемирном фестивале молодежи

«ИГРЫ БУДУЩЕГО». ПОБЕДИТЕЛИ ТУРНИРА «КУБОК ЧЕТЫРЕХ КОНТИНЕНТОВ» ПОСЕТИЛИ КАЗАНЬ

Финалисты III Международной олимпиады по финансовой безопасности — ребята из России, Алжира, Ирана, Кубы, Кыргызстана, Таджикистана и Узбекистана — побывали в столице Татарстана на «Играх Будущего».

На финале Олимпиады молодые люди показали лучшие результаты в турнире по фиджитал-футболу, в Казани они познакомились с другими направлениями киберспорта.

На международные мультиспортивные соревнования «Игры Будущего» студентов пригласил заместитель Председателя Правительства Российской Федерации Дмитрий Чернышенко.

Кубинец Джордан Антонио Родригес, один из гостей и участник Олимпиады, познакомился с Россией заочно еще в детстве: его бабушка переехала на Кубу в молодости, но никогда не забывала о Родине. Молодой человек слушал истории о нашей стране, а в 2023 году приехал в «Сириус» на Международную олимпиаду по финансовой безопасности. Мы попросили Антонио поделиться мыслями о будущем международной финансовой безопасности:

«Людам и правительствам необходимо осознать ее важность в современном высокоглобализированном и технологичном мире: для защиты своих личных средств и для безопасности всей страны. Я мечтаю о глобальном сотрудничестве в области финансовой безопасности, где политические и экономические разногласия будут отброшены в сторону и объединены для иско-

ренения терроризма и таких вещей, как отмывание финансовых средств.

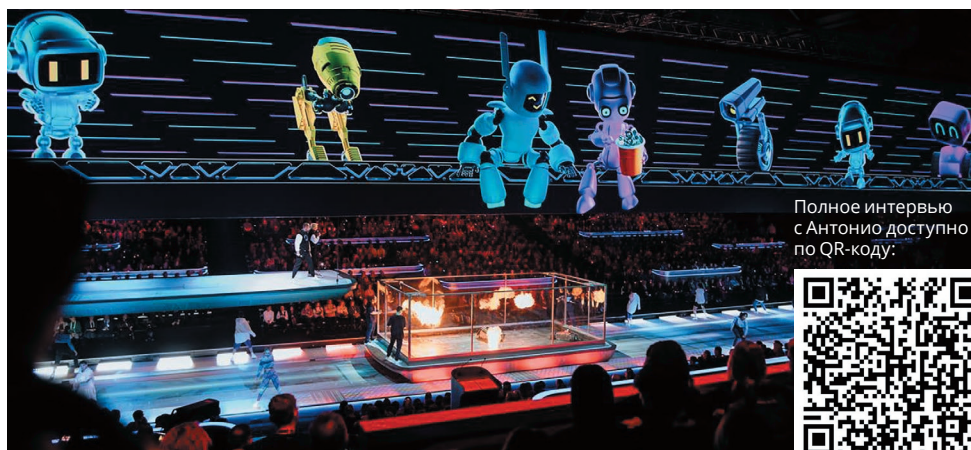
Двое из участников — Фатех Бусри из Алжира, Бахриддин Рустамов из Таджикистана — продолжили путешествие по России и посетили Всемирный фестиваль молодежи на федеральной территории «Сириус». Участвуя в насыщенной программе Фестиваля, ребята нашли время поделиться впечатлениями об «Играх Будущего» и Международной олимпиаде по финансовой безопасности.

«Я был капитаном интернациональной команды "Волки", победившей в матче по фиджитал-футболу на Олимпиаде по финансовой безопасности в прошлом году. Именно поэтому нас пригласили в Казань на "Игры Будущего", а теперь я нахожусь на Всемирном фестивале молодежи. Я хочу не только развивать свои знания в области финансовой безопасности, но и делиться ими. Сейчас я



активно готовлюсь к следующей Олимпиаде, очень хочу пройти в финал. Кроме того, я занимаюсь просветительской деятельностью в рамках Движения, стараюсь рассказать о проекте в своей стране», — поделился Бахриддин.

Среди самых ярких впечатлений Фатеха — встречи со знаменитыми политиками и спортсменами со всего мира: «Незабываемое впечатление об участии в "Играх Будущего" — моя встреча с Президентом Российской Федерации Владимиром Путиным на церемонии открытия, а также возможность смотреть на мероприятие с ложи почетных гостей с главами государств. Это было большой честью для меня и стало прекрасным воспоминанием. Я бы хотел поблагодарить всех вас за гостеприимство, конечно, я хочу снова посетить Россию».



Полное интервью с Антонио доступно по QR-коду:



СОСТОЯЛОСЬ ПЕРВОЕ ЗАСЕДАНИЕ СОВЕТА БРИКС ПО ПРОТИВОДЕЙСТВИЮ ОТМЫВАНИЮ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В РАСШИРЕННОМ СОСТАВЕ

В Росфинмониторинге в режиме видеоконференцсвязи состоялось первое в 2024 году заседание Совета БРИКС по ПОД/ФТ

Участники встречи обсудили вопросы совершенствования работы национальных антиотмывочных систем и дальнейшие совместные меры по обеспечению финансовой безопасности.

В рамках российского председательства в БРИКС представлены



инициативы, направленные на повышение уровня прозрачности финансовых систем, минимизацию рисков и угроз, укрепление государственно-частного партнерства, а также вовлечение молодежи в сферу финансовой безопасности.

В частности, интерес вызвали такие проекты, как Международный центр оценки рисков, сервис «Прозрачный блокчейн», Международная олимпиада по финансовой безопасности, Международный совет комплаенс.

Стороны выразили уверенность, что Совет БРИКС по ПОД/ФТ может внести весомый вклад в глобальную систему противодействия отмыванию доходов и финансированию терроризма, а также в реализацию Стратегии экономического партнерства БРИКС до 2025 года.

ВОПРОСЫ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ОБСУДИЛИ НА ВСЕМИРНОМ ФЕСТИВАЛЕ МОЛОДЕЖИ

В марте молодые люди со всего мира собрались на грандиозном событии в «Сириусе»

Всемирный фестиваль молодежи принял 20 тысяч российских и иностранных лидеров в сфере бизнеса, медиа, международного сотрудничества, культуры, науки, образования, волонтерства и благотворительности, спорта, различных сфер общественной жизни, а также подростков, представляющих различные детские организации и объединения.

Важной частью повестки Фестиваля стали и вопросы финансовой

безопасности. Эксперты из Росфинмониторинга, Международного учебно-методического центра финансового мониторинга и ПСБ представили стенд «Содружество» и провели ряд мероприятий для участников Фестиваля. Среди них более 50 финалистов Международной олимпиады по финансовой безопасности, а также молодые сотрудники финансовых разведок из разных стран.



Молодым людям рассказали, что такое Международное олимпиадное движение по финансовой безопасности и как стать его частью, как принять участие в Олимпиаде в этом году. На дискуссиях и деловых играх обсудили актуальные вопросы борьбы с финансовой преступностью, поделились опытом стран.



РЕДАКЦИОННЫЙ СОВЕТ



**Председатель
редакционного
совета**

Чиханчин Ю.А.



**Заместитель
председателя
редакционного
совета**

Овчинников В.В.



**Заместитель
председателя
редакционного
совета**

Негляд Г.Ю.



**Главный
редактор**

Рязанова И.С.

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА



Бобрышева Г.В.



Корнев И.А.



Крылов О.В.



Лисицын А.С.



Тетеруков С.А.



Петренко А.Г.



Андропова М.Ю.

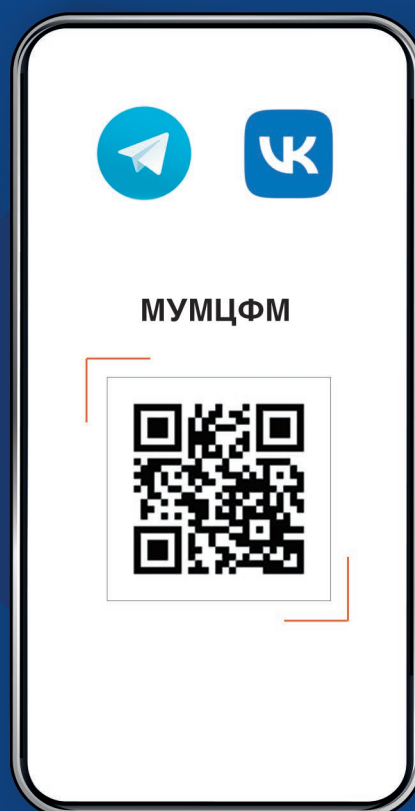
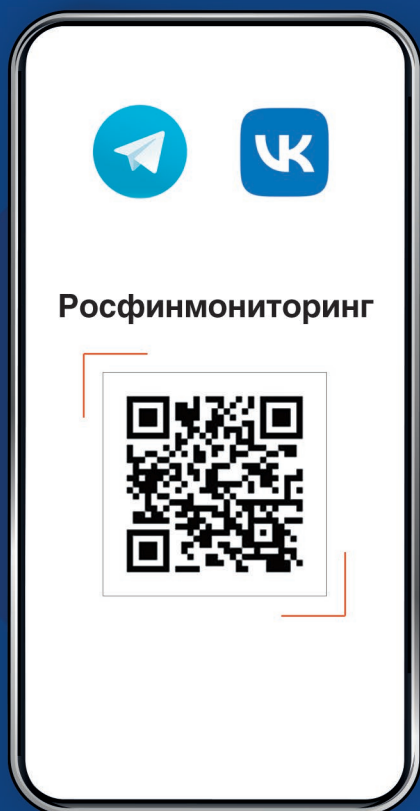


Гилета Е.С.



Шемякина М.С.

Росфинмониторинг и МУМЦФМ в Telegram и VKontakte



Издательство

Автономная некоммерческая организация
Международный учебно-методический центр финансового мониторинга
119017, Москва, Старомонетный переулок, д. 31, стр. 1.
E-mail: info@mumcfm.ru
Тираж 600 экземпляров.

Мнение редакции может не совпадать с позицией авторов.

МУМЦФМ
2024