ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

#46
ИЮНЬ/2025

Председатель Следственного комитета Российской Федерации

АЛЕКСАНДР БАСТРЫКИН:

«Технологии искусственного интеллекта открывают новую главу в эволюции киберпреступности и становятся фактором, влияющим на баланс сил между правоохранителями и преступниками»

ЮРИЙ ЧИХАНЧИН
Директор Росфинмониторинга,
председатель редакционного совета

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Этот номер журнала «Финансовая безопасность» посвящен мерам, принимаемым для защиты общества от противоправных деяний, совершаемых с использованием информационных технологий.

Цифровизация стала одним из ключевых направлений развития важнейших сфер общественной жизни, включая кредитно-финансовую. Невозможно представить современное общество без мобильной связи, электронных средств платежа, онлайн-банкинга, интернет-торговли. Но как у всякого прогресса, у стремительного развития цифровых технологий есть и оборотная сторона. Вместе с появлением высокотехнологичных сервисов и услуг возникают новые угрозы.

Регулярное обновление сценариев хищения денег, широкое использование в преступных схемах современных технологий требуют объединения усилий всех заинтересованных сторон – законодателей, правоохранительных органов, банковского сообщества и телеком-индустрии, некоммерческого сектора.

В этом году вступил в силу целый блок законов, предусматривающих меры по борьбе с телефонным и интернет-мошенничеством. Среди них – введение возможности установления гражданами самозапрета на заключение договоров потребительского кредитования и так называемого периода охлаждения при выдаче кредитов, создание единой информационной базы противодействия мошенническим действиям, запрет на передачу сим-карт третьим лицам, запуск профильной государственной информационной системы.

Киберпреступность охватила практически все страны и континенты. Зачастую преступления носят трансграничный характер. Меры противостояния международному криминалу вырабатываются в том числе на площадках региональных групп по типу ФАТФ. Так, на последней пленарной сессии Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма рассматривался целый комплекс вопросов борьбы с киберугрозами.

Однако, несмотря на позитивные изменения, телефонное и интернет-мошенничество остается одной из главных угроз финансовой безопасности граждан. Ведь как бы ни совершенствовались законы, какими бы изощренными ни становились защитные технологии, влияние человеческого фактора исключить невозможно. Поэтому крайне важной является просветительская деятельность, которая поможет человеку более осознано принимать финансовые решения и научит противостоять мошенничеству. Эта работа проводится при участии экспертного сообщества, представителей ведущих вузов страны, в том числе Международного сетевого института в сфере ПОД/ФТ.

Эти и многие другие темы, связанные с киберпреступностью, нашли отражение на страницах выпуска. Уверен, что мнение авторов будет интересно как специалистам, так и широкому кругу читателей.

СОДЕРЖАНИЕ

6 АЛЕКСАНДР БАСТРЫКИН:
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ОТКРЫВАЕТ НОВУЮ ГЛАВУ В ЭВОЛЮЦИИ КИБЕРПРЕСТУПНОСТИ

15 СУЛЕЙМАН АЛЬ-ДЖАБРИН:
МЕНАФАТФ: БОРЬБА С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ В ЦИФРОВУЮ ЭПОХУ

17 МЕЛАЙЕ ТИМОТИ ФЕМИ:
ПРЕСТУПЛЕНИЮ НЕ НУЖНА ВИЗА: ПОДХОД ЗАПАДНОЙ АФРИКИ К БОРЬБЕ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ

АЛЕКСАНДР БАСТРЫКИН:
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ОТКРЫВАЕТ НОВУЮ ГЛАВУ В ЭВОЛЮЦИИ КИБЕРПРЕСТУПНОСТИ

Новые технологии становятся оружием в руках злоумышленников и сегодня применяются при совершении практически любых видов преступлений, отмечает председатель Следственного комитета Российской Федерации Александр Бастрыкин. В интервью для журнала «Финансовая безопасность» Председатель СК России рассказал о работе по противодействию финансовым мошенничествам и методике расследования преступлений, связанных с дистанционными хищениями, использованием онлайн-сервисов и криптовалют.

АЛЕКСАНДР БАСТРЫКИН

Председатель Следственного комитета Российской Федерации, профессор, заслуженный юрист России, д. ю. н.

— Александр Иванович, финансовое мошенничество представляется одной из наиболее острых проблем, с которой граждане сталкиваются напрямую. С чем вы связываете такую активность преступников?

— Сегодня криминальная мысль легко приспосабливается ко всем происходящим в обществе изменениям. Особенно это касается сферы новейших достижений научно-технического прогресса и всеобщей цифровизации. Использование преступниками в мошеннических схемах новых технологий позволяет существенно расширить аудиторию потенциальных жертв. Организаторам, пособникам и исполнителям преступлений уже не обязательно находиться в той стране, где совершается противоправное деяние. Таким образом, преступность приобретает трансграничный характер. Расширяются способы выманивания у граждан денежных средств. Нередко в реализацию мошеннических схем вовлекаются граждане, которые не в полной мере осознают свою роль и степень ответственности за совершаемые действия.

Например, когда физические лица, так называемые дропы, за незначительное вознаграждение передают преступнику реквизиты своих платежных инструментов, которые используются ими для сокрытия следов хищения денежных средств и вывода активов за рубеж. Так, в этом году вынесен приговор индивидуальному предпринимателю, которая за денежное вознаграждение сбыла третьему лицу электронные средства платежа и электронные носители информации, предназначенные для неправомерного осуществления приема, выдачи и передачи денежных средств по указанным расчетным счетам.

Часто в качестве жертв мошенники выбирают пожилых людей и тех, кто находится в сложной жизненной ситуации. В результате преступных схем граждане попадают в глубокую долговую яму, а порой теряют последнее имущество.

Основные стадии финансовых мошенничеств совершаются дистанционно, а объектом преступления становятся безналичные денежные средства. Поэтому установление всей преступной цепочки вплоть до организатора — достаточно сложная задача, требующая проведения значительного количества следственных и оперативно-розыскных действий, изучения огромного массива документов, на что за-

«Особое внимание уделяется публикациям, в которых авторы приводят данные о причастности должностных лиц, а также об их попустительстве противоправной деятельности.

трачивается много времени и ресурсов. В свою очередь, эти же обстоятельства дают возможность преступникам скрыть следы преступления, вывести активы за рубеж и смешать их с другими деньгами.

В связи с этим все правоохранительные органы должны постоянно совершенствовать тактику и методику выявления и расследования таких преступлений.

— Какие комплексные меры защиты населения от этих угроз, по вашему мнению, нужно сейчас принять?

— Основными формами организации деятельности ведомства по противодействию финансовым мошенничествам являются оперативное и качественное расследование уголовных дел, организация доследственных проверок, установление в ходе предварительного следствия обстоятельств, способствовавших совершению преступлений, и внесение в порядке, предусмотренном ст. 158 УПК РФ, представлений о принятии мер по их устранению, контроль за их своевременным рассмотрением.

На постоянной основе в ведомстве проводится мониторинг средств массовой информации, материалов из интернета на предмет наличия сообщений о правонарушениях, влекущих уголовную ответственность. Особое внимание уделяется публикациям, в которых авторы приводят данные о причастности должностных лиц, а также об их попустительстве противоправной деятельности.

Стратегическое планирование работы в данной сфере, а также необходимость принятия дополнительных мер по совершенствованию нормативно-правового регулирования основано на результатах национальной оценки рисков, а также анализе особенностей экономической ситуации и криминогенной обстановки, складывающейся в стране.

К таковым отнесены, например, риски, связанные с нарастающей виртуализацией пользователей услугами банков и платежных систем, распространением деятельности нелегальных финансовых посредников, использованием приемов социальной инженерии, так как они способствуют возникновению новых криминальных инструментов для проведения незаконных финансовых операций.

— Могли бы вы привести примеры уголовных дел, которые расследуются в Следственном комитете? Какие особенности расследования таких преступлений стоит учитывать?

— Сегодня следственные органы уже разработали необходимую методику, выработали тактику, позволяющую расследовать сложные по механизму совершения

преступления, связанные с дистанционными хищениями, например, когда преступниками используются онлайн-сервисы обмена криптовалюты.

В качестве положительного примера расследования можно привести уголовное дело, расследованное в следственном управлении СК России по Республике Татарстан в отношении членов организованного преступного сообщества. Соучастники взаимодействовали с кол-центрами, находящимися в основном за пределами Российской Федерации. Злоумышленники обзванивали граждан, представлялись работниками различных служб и обманом убеждали оформить кредит и перенаправить свои средства на «безопасный счет». Деньги поступали как раз на банковские карты, предоставленные участникам преступной группы гражданами (дропперами) за денежное вознаграждение. Затем похищенные средства переводились путем транзакций в криптовалюте сообщникам за рубеж. Ущерб потерпевших составил более 30 млн рублей. Расследование уголовного дела в отношении 17 обвиняемых находится на завершающей стадии. Шесть человек объявлены в международный розыск.

Следует отметить, что отсутствие процессуального статуса криптовалют порождает определенные проблемы в правоприменении, однако в силу необходимости наложения ареста на виртуальные активы при расследовании преступлений должны использоваться наиболее эффективные механизмы, обеспечивающие сохранность арестованных активов.

Приведу еще один пример. Используя компьютерные программы для вмешательства в функционирование средств хранения компьютерной информации, а также фишинговый сайт фигурант похитил около 9 биткоинов потерпевшего, который ошибочно перешел по ссылке этого сайта. В последующем злоумышленник легализовал похищенные биткоины, конвертировав в фиатную валюту на сумму более 16 млн рублей и приобретя на вырученные деньги объекты недвижимости в Московской области. По результатам расследования следствием установлено имущество, приобретенное фигурантом за счет похищенных средств, на которое наложен арест (недвижимость, транспортные средства).

Еще один опасный фактор — это организованность деятельности преступных групп, связанных с финансовыми мошенничествами. Но и такие схемы тоже удается выявлять. Например, в Следственном комитете было расследовано уголовное дело в отношении организатора преступного сообщества и 13 его соучастников. Они проводили кассовые операции по расчетным счетам подконтрольных коммерческих организаций, не имевших лицензии на осуществление банковских операций. Кроме того, они обналичивали денежные средства с персональных банковских карт контролируемых ими лиц, зарегистрированных в качестве индивидуальных предпринимателей, но не осуществлявших коммерческую деятельность.

«Сегодня следственные органы уже разработали необходимую методику, выработали тактику, позволяющую расследовать сложные по механизму совершения преступления, связанные с дистанционными хищениями.

— Сегодня злоумышленники все чаще обращаются к новым технологиям для обмана граждан: используют ИИ и создают дипфейки, крадут данные с помощью вредоносных программ. Может ли государство использовать те же технологии для борьбы с преступниками?

— Действительно, новые технологии в руках злоумышленников являются самым настоящим оружием, и они применяются при совершении практически любых видов преступлений. Мы это видим по растущему из года в год количеству преступлений, совершенных указанным способом, и их разнонаправленности. В практике есть пример расследования уголовного дела по факту убийства двух лиц, организованного в сети Интернет.

Определенным ноу-хау преступников стали технологии искусственного интеллекта, который они все чаще используют в противоправных целях. Например, нейросети стали мощным инструментом, позволившим существенно повысить эффект от ранее известных видов киберпреступлений, а также породившим новые виды преступных деяний.

В связи с этим мы понимаем, что современные технологии искусственного интеллекта открывают новую главу в эволюции киберпреступности и, несомненно, становятся фактором, влияющим на баланс сил между правоохранителями и преступниками.

Поэтому, высоко оценивая возможности искусственного интеллекта при обработке больших объемов данных, в работе с цифровыми следами преступлений и в целом с электронной информацией, сотрудники нашего ведомства применяют целый комплекс существующих возможностей в этой сфере.

Например, ведется поиск и анализ цифровых следов и иной криминалистически значимой информации о расследуемых преступлениях в ИКТ-пространстве. Проводятся исследования в области криминалистической техники, предназначенной для поиска, фиксации и

«Качество ведомственного предварительного следствия находится на стабильно высоком уровне. Общий объем раскрытых и расследованных преступлений растет пропорционально повышению числа зарегистрированных деяний.

изъятия цифровых следов. Наши специалисты могут улучшать качество данных о следах преступлений, зафиксированных в цифровом формате. Разрабатываются системы поддержки принятия решений (построение поисковых портретов преступников и др.) и автоматизации технических операций в работе следователя (перевод устной речи в письменную).

— Какие сложности возникают в процессе расследования кибермошенничества и какие способы противостояния злоумышленникам уже показали свою эффективность?

— Оценка деятельности Следственного комитета на данном направлении позволяет отметить, что качество ведомственного предварительного следствия находится на стабильно высоком уровне. Общий объем раскрытых и расследованных преступлений растет пропорционально повышению числа зарегистрированных деяний.

Поэтому особых сложностей в расследовании киберпреступлений не отмечается. При этом количество уголовных дел, связанных с хищением денежных средств граждан, в общем количестве расследованных следователями ведомства деяний, связанных с использованием ИКТ, не является предопределяющим ввиду установленной подследственности.

Несмотря на это, есть ряд проблем, с которыми сталкиваются следователи ведомства при расследовании преступлений, совершаемых с использованием ИКТ. Это сложности во взаимодействии с операторами связи, зарубежными площадками — организаторами распространения информации и иными провайдерами интернет-услуг.

Вместе с тем принимаемые сегодня государством комплексные меры по регулированию деятельности таких поставщиков информации уже дают результаты. Следственный комитет, основываясь на складывающейся следственной практике, принимает активное участие наряду с иными федеральными органами власти в совершенствовании законодательства в сфере информационно-коммуникационных технологий.

— Как Следственный комитет взаимодействует с другими государственными органами в борьбе с финансовыми мошенничествами, в том числе с финразведкой?

— Между Следственным комитетом и другими правоохранительными структурами по данному направлению налажено эффективное сотрудничество. Межведомственное взаимодействие организовано как в рамках общих мероприятий, включая совместные совещания, заседания рабочих групп, семинары, так и по конкретным материалам проверок и уголовным делам.

Основными формами такой работы являются организация оперативного сопровождения расследования совершенных или подготавливаемых преступлений; создание межведомственных следственно-оперативных групп; осуществление в соответствии с поручениями следователей оперативно-розыскных мероприятий по конкретным уголовным делам; проведение совместных оперативных совещаний по вопросам планирования и проведения оперативно-розыскных мероприятий, следственных и иных процессуальных действий.

При расследовании преступлений в сфере экономики и коррупционных преступлений, а также

фактов легализации доходов, полученных преступным путем, важное значение имеет взаимодействие с органами Росфинмониторинга. В процессе нашей совместной работы обнаруживаются незаконные финансовые операции и многоступенчатые финансовые схемы, удается получить важную информацию для расследования сложных коррупционных преступлений, связанных в том числе с хищениями бюджетных средств.

— Учитывая всплеск использования новых технологий в преступных целях, принимаются ли меры для повышения квалификации следователей, занимающихся такими делами?

— Следователи — это первые лица, которые должны показывать пример своей грамотностью и компетентностью в этих делах и быть на два шага впереди преступников. Поэтому повышению квалификации наших сотрудников уделяется повышенное внимание.

Методика и рекомендации по профилактике преступлений, в том числе совершенных с использованием ИКТ, регулярно доводятся до следователей по результатам изучения смежных направлений в работе в рамках учебных занятий по профессионально-должностной подготовке.

В территориальных следственных органах ежемесячно проводятся стажировки следователей, в ходе которых уделяется особое внимание проблемным аспектам расследования преступлений обозначенной категории. К таким занятиям привлекаются и специалисты из других компетентных ведомств.

Представители Следственного комитета принимают участие в учебных курсах, организуемых ежеквартально по инициативе Центрального банка Российской Федерации для правоохранительных органов по вопросам противодействия преступлениям в кредитно-финансовой сфере с онлайн-подключением удаленных регионов.

В занятиях для следователей участие принимают также специалисты ФНС и Росфинмониторинга. Взаимодействие на данном направлении ориентировано на освещение актуальных вопросов деятельности в финансовой сфере.

Для повышения профессионального уровня сотрудников Следственного комитета ведомственными образовательными учреждениями внедряются новые подходы к организации процесса обучения. Созданы кафедры информационных технологий и организации расследования киберпреступлений, где реализуются соответствующие программы повышения квалификации.

Регулярно осуществляется обмен опытом и наилучшими практиками по расследованию преступлений, в том числе совершенных с использованием ИКТ, в формате прохождения тематических научно-практических мероприятий, стажировок, обучающих семинаров (курсов) сотрудниками следственных органов Следственного комитета и представителями правоохранительных органов иностранных государств.

— Телефонные мошенники говорят напрямую с жертвой, поэтому зачастую используют методы социальной инженерии для обмана и даже запугивания. Можно ли предостеречь население от психологических манипуляций и какие профилактические меры могут быть эффективны? Какую роль играют финансовая грамотность населения и информированность о схемах мошенничества в предотвращении этих преступлений?

— Если каждый гражданин будет осведомлен о возможностях финансовых организаций, предоставляемых ими услугах и способен отличить советы специалистов от действий мошенников, риски, что он станет жертвой преступления, минимальны. И к настоящему времени на государственном уровне разработан целый комплекс мер, при исключительном соблюдении которых наши граждане уже будут защищены и не должны попасть на удочку к мошенникам.

В Следственном комитете особое внимание уделяется профилактической работе с населением, повышению уровня правовой и финансовой грамотности граждан. В качестве механизмов реализации обозначенных мер во всех подразделениях ведомства используются различные способы и площадки распространения информации, привлекаются к участию иные заинтересованные ведомства, службы и организации, в том числе общественные. Кроме того, мы активно информируем общество через СМИ и соцмедиа о работе по противодействию обозначенным преступлениям.

В профилактических целях представители ведомства на постоянной основе посещают различного уровня образовательные и учебные учреждения, в которых организуются познавательные лекции, семинары, а также круглые столы и другие тематические мероприятия.

«На государственном уровне разработан целый комплекс мер, при исключительном соблюдении которых наши граждане уже будут защищены и не должны попасть на удочку к мошенникам.

ОЛЕГ КРЫЛОВ:

ТРАНСНАЦИОНАЛЬНЫЙ ХАРАКТЕР КИБЕРПРЕСТУПНОСТИ ДИКТУЕТ НЕОБХОДИМОСТЬ ПРОРАБОТКИ НОВЫХ ФОРМ МЕЖДУНАРОДНОЙ КООРДИНАЦИИ

В виртуальную среду переместилась основная масса различных преступных деяний в экономической сфере — лжеброкеры (практически все случаи), финансовые пирамиды (98%) и экономические мошенничества, а также нелегальная торговля запрещенными предметами и веществами, незаконный оборот наркотиков.

ОЛЕГ КРЫЛОВ
Первый заместитель директора Росфинмониторинга, ответственный секретарь Межведомственной рабочей группы по противодействию незаконным финансовым операциям

Изменения, обусловленные глобальной цифровизацией и развитием ИТ-технологий, затронули все сферы экономической, общественной и частной жизни граждан и стали причиной новых рисков в сфере финансовой безопасности. Это потребовало принятия соответствующих мер реагирования на государственном уровне.

Указом Президента России от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» предусмотрено создание системы эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (далее — ИКТ), и снижения ущерба от их совершения.

Вопросы повышения эффективности противодействия преступлениям, совершаемым с использованием ИКТ, в 2024 году рассматривались на оперативном совещании Совета Безопасности Российской Федерации (23 августа 2024 г.) и Координационном совещании руководителей правоохранительных органов Российской Федерации (10 октября 2024 г.).

Отмечалось, что указанные преступления с каждым годом занимают все более заметное место в структуре всех зарегистрированных противоправных деяний, а их удельный вес превышает 30%.

Подавляющее большинство противоправных посягательств рассматриваемой категории связано с кражами, мошенничеством, незаконным оборотом наркотиков и совершается с использованием сети Интернет, а также средств мобильной связи.

Важнейшим шагом стала разработка Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных

технологий (утверждена распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р), в том числе содержащей:

- назначение, функции, принципы создания и функционирования государственной системы;
- нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое и организационно-штатное обеспечение создания и функционирования государственной системы;
- критерии типизации и классификации основных видов правонарушений и преступлений, совершаемых с использованием ИКТ;
- основные направления совершенствования деятельности по выявлению, раскрытию, пресечению и предупреждению правонарушений и преступлений указанной категории;
- технологии, включая направления совершенствования мер административной и уголовной ответственности в зависимости от тяжести совершенных деяний;
- механизмы координации и организации межведомственного взаимодействия государственных органов, организаций и институтов гражданского общества на данном направлении.

Эффективное предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием ИКТ, в том числе легализации преступных доходов, финансирования терроризма, предусматривает активное участие Росфинмониторинга (далее — Служба). Ведомство обладает необходимыми возможностями, силами и средствами для проведения мониторинга рисков в кредитно-финансовой системе, прогнозирования возникновения угроз противоправных посягательств в информационном пространстве, своевременного обнаружения уязвимостей регуляторного и операционного характера, организации стабилизирующего воздействия на криминогенную обстановку.

Анализ поступающей в Службу информации и материалов финансовых расследований позволяет выделить следующие факторы и обстоятельства, оказывающие существенное влияние на общее состояние правопорядка в рассматриваемой сфере.

Недостатки нормативного регулирования такой новейшей сферы, как оборот криптовалют, и возникшей вокруг этого оборота высокотехнологической инфраструктуры. По сути, мы имеем дело с параллельной расчетной системой, первоначально предназначенной для виртуального сетевого пространства, на которую в отсутствие регуляторных норм можем оказывать весьма ограниченное влияние.

В противостоящей нам «профессиональной» среде остро проявляется ощущение вседозволенности, правового нигилизма, возможности осуществлять анонимную деятельность, не боясь никаких последствий. Это, в свою очередь, породило новые способы мошеннических действий и является одной из причин значительного роста в последние годы использования платежных инструментов (платежных реквизитов) третьих лиц.

47%

составила доля переводов с участием физических лиц в общем объеме подозрительных операций в 2024 году. С участием граждан Российской Федерации сумма таких операций выросла в 1,6 раза, с участием нерезидентов — в 3,5 раза.

Рост объемов операций с участием физических лиц связан с повышением доступности платежной инфраструктуры (P2P и P2C переводы), «выдавливанием» технических компаний из легальной экономики, в том числе в результате функционирования разработанной Банком России платформы «Знай своего клиента».

На этом фоне фиксируется и увеличение количества дропов, задействованных в различного рода расчетах и транзакциях, в том числе при использовании электронных средств платежей для проведения операций с онлайн-казино, криптообменниками, для реализации мошеннических схем и обналичивания. По сведениям нотариусов, наблюдается рост в 1,5 раза количества выданных доверенностей лицами с признаками дропов и объемов проведенных ими операций.

Распространенность противоправных посягательств на средства граждан (дистанционное мошенничество), высокие объемы преступных доходов, а также большой спрос на услуги по их легализации сформировали на территории России отдельный вид преступных групп – так называемых дроп-сервисов.

Администраторы данных теневых платформ, аккумулируя платежные инструменты (платежные реквизиты) третьих лиц, вовлекаемых в противоправную деятельность, предлагают полную инфраструктуру для отмывания преступных доходов, включая электронные средства платежа, услуги по разблокировке денежных средств в банках, обналичиванию, перевозке наличности, а также конвертации в криптовалюту.

В последнее время ряды дропов активно пополняются за счет несовершеннолетних и иностранцев. При этом результативность принимаемых компетентными органами профилактических мер снижает распространение контента, продвигающего практики недобросовестного финансового поведения, применение криминалом методов социальной инженерии и специальных технических средств, позволяющих преступникам сохранять свою анонимность.

Ситуация усугубляется тем, что современные технологии обеспечивают экстерриториальность деятельности, имеют место попытки уйти от ответственности в рамках применения национального права. При проведении финансовых расследований Службой было установлено более 400 криптобирж, обслуживавших наших граждан, и лишь несколько десятков из них — российские.

В виртуальную среду переместилась основная масса ряда преступных деяний в экономической сфере — лжеброкеры (практически все случаи), финансовые пирамиды (98%) и экономические мошенничества, а также нелегальная торговля запрещенными предметами и веществами, незаконный оборот наркотиков.

Таким образом, сама специфика подготовки и совершения ИКТ-преступлений ставит перед финансовой аналитикой основную задачу: деанонимизация участников подозрительных операций и установление цепочек их взаимодействия.

Транснациональный характер организованной киберпреступности диктует необходимость проработки новых форм международной координации и взаимодействия, создания особых институтов взаимной помощи с учетом практически мгновенного перемещения денежных средств в рамках юрисдикций многих стран.

Принимая во внимание подверженность финансовой сферы противоправным манипуляциям, в которые вовлекаются физические лица (в том числе несовершеннолетние и нерезиденты), вопросы повышения эффективности противодействия дропперству детально изучались на заседаниях Межведомственной рабочей группы по противодействию незаконным финансовым операциям (далее — МРГ) под председательством руководителя Администрации Президента Российской Федерации А.Э. Вайно, состоявшихся в 2023 и 2025 годах.

МРГ разработан комплекс мер по противодействию незаконным финансовым операциям, совершаемым с использованием дропов:

- введение уголовной ответственности за неправомерное предоставление другим лицам и использование в интересах других лиц банковских (платежных) карт и иных электронных средств платежа, а также их незаконное приобретение и использование лицами, не являющимися держателями таких электронных средств платежа;
- разработка и реализация механизма ограничения количества открываемых (выдаваемых) физическому лицу платежных карт;
- повышение эффективности мер противодействия кредитными организациями незаконным финансовым операциям, в том числе предоставление им права на отказ от заключения договора банковского счета (вклада) с клиентом — физическим лицом и расторжение указанного договора;
- централизация базы данных документов, удостоверяющих личность иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, а также установление доступа кредитных организаций к указанному централизованному ресурсу;
- введение запрета на заключение договоров на оказание банковских услуг, а также открытие счетов иностранным гражданам с использованием ими пластиковых ID-карт, удостоверяющих личность, за исключением национальных паспортов;
- создание единой базы данных электронных средств платежа и их идентификаторов (банковские карты, телефонные номера, счета), размещаемых в сети Интернет, социальных сетях и мессенджерах для проведения противоправных операций.

Подготовлен комплекс мер по совершенствованию системы профилактики безнадзорности и правонарушений несовершеннолетних, предусматривающих не только реализацию совместных мероприятий по выявлению, документированию и расследованию преступлений, связанных с вовлечением несовершеннолетних в теневые финансовые схемы, но и проведение на системной основе профилактической работы в отношении каждого несовершеннолетнего с привлечением Минпросвещения России, Минобрнауки России, Росмолодежи, профильных правительственных комиссий.

Полагаю, что дальнейшее практическое воплощение обозначенных инициатив позволит оперативно стабилизировать обстановку, создаст условия для успешной реализации межведомственных мероприятий по предупреждению, выявлению и пресечению преступлений, совершаемых с использованием ИКТ, а также существенно затруднит использование банковских карт, оформленных на подставных лиц.

БЕЗОПАСНОСТЬ БЕЗ ГРАНИЦ. МЕЖДУНАРОДНОЕ СООБЩЕСТВО В БОРЬБЕ С МОШЕННИЧЕСТВОМ

МЕНАФАТФ: БОРЬБА С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ В ЦИФРОВУЮ ЭПОХУ

MENAFATF
مينافاتف
GAFIMOAN

В эпоху высоких технологий финансовые преступления стали транснациональными, что требует от международного сообщества новых подходов и скоординированных действий.

На полях Пленарной сессии ЕАГ редакция журнала «Финансовая безопасность» побеседовала с **Сулейманом Аль-Джабрином,** исполнительным секретарем МЕНАФАТФ, о борьбе с финансовым мошенничеством в условиях глобальной цифровизации. Эксперт поделился своими впечатлениями от работы ЕАГ и рассказал о совместных инициативах, а также уязвимостях, которыми пользуются мошенники, и ключевой роли международного сотрудничества в противодействии этим угрозам.

— Каковы ваши впечатления от Пленарного заседания в Москве?

— ЕАГ всегда задает планку, и во время председательства Российской Федерации в ЕАГ мы снова видим улучшения. Продуктивное сотрудничество на площадке Евразийской группы, представляемые инициативы позволяют своевременно справляться с рисками, а именно со схемами отмывания денег и финансирования терроризма. Интересно наблюдать за техническими дискуссиями, направленными на предупреждение различных типов современных финансовых преступлений, например использования криптовалюты в противоправной деятельности, налоговых схем, незаконного оборота наркотиков и других. Я выражаю признательность стране-председателю и государствам – членам ЕАГ за работу и постоянное развитие.

— Совместный форум ЕАГ-МЕНАФАТФ был посвящен цифровым активам и новым технологиям в сфере финансовой безопасности. Какие угрозы представляют новые технологии для глобальной финансовой безопасности?

— Говоря о финансовой безопасности, следует отметить, что традиционные финансовые преступления уже стали трансграничными, а с процессами цифровизации они охватывают все больше стран и континентов. Это придает особую важность сотрудничеству на региональном и международном уровнях. Евразийский регион и Ближний Восток, находясь в непосредственной близости друг от друга, сталкиваются с различными аспектами финансовых преступлений. Подобные форумы необходимы для обмена опытом, потому что мы служим одной цели — предотвращению финансовых преступлений. Проведение такого форума крайне важно для того, чтобы учитывать текущие риски и их трансформацию. Мы надеемся, что это сотрудничество будет продолжено.

— В современном мире одной из самых опасных угроз, непосредственно затрагивающих общественность, являются мошенники и финансовые махинации. Какие виды мошенничества наиболее актуальны для региона МЕНА?

— Финансовое мошенничество — это один из самых быстро меняющихся рисков. Как только мы фиксируем одну схему, появляется новый способ мошенничества, например с применением мессенджеров или электронной почты. Преступники нацелены на наиболее уязвимых граждан — на тех, кто плохо ориентируется в технологиях, в частности, пожилых людей. Для них простой переход по ссылке может обернуться утечкой данных. Самый большой риск находится в наших руках — в наших телефонах, любых приложениях, системах обмена сообщениями, электронной почте. Даже нам, экспертам, следует с осторожностью относиться к этим рискам. Опять же, преступники очень быстро адаптируются, вот почему нам нужно не отставать и постоянно обучаться.

Кампании по повышению осведомленности обычно носят разовый характер, в то время как непрерывное обучение необходимо для того, чтобы люди осознавали быстро меняющийся характер угроз. Мошенники обычно используют новые технологии, постоянно изобретая новые способы манипулирования людьми. Поэтому государственные структуры должны идти в ногу с темпами развития новых технологий, брать их на вооружение для борьбы с финансовыми преступлениями, не допускать, чтобы люди теряли свои деньги, попадаясь на удочку злоумышленников. Государственные учреждения, использующие новые технологии, работают на двух фронтах: выявляют правонарушения и отслеживают инновации. Действия с обеих сторон жизненно необходимы для того, чтобы мы не давали преступникам возможности воспользоваться преимуществами новых технологий.

— Важно ли координировать усилия на международном уровне и адаптировать национальные стратегии к глобальной международной стратегии по борьбе с мошенничеством и финансовыми преступлениями?

— Несмотря на то, что важно понимать специфику страны и национальные риски, с которыми она сталкивается, современные финансовые преступления носят трансграничный характер. Государства должны взаимодействовать друг с другом, чтобы прогнозировать риски, быть в курсе их источников и вырабатывать меры реагирования. Готовность к коммуникации обеспечивает профилактику — как говорится, одной рукой узла не завяжешь. Знание источника риска и тех, кто ему подвержен, создает основу для эффективной борьбы с преступниками.

«Государственные учреждения, использующие новые технологии, работают на двух фронтах: выявляют правонарушения и отслеживают инновации. Действия с обеих сторон жизненно необходимы для того, чтобы мы не давали преступникам возможности воспользоваться преимуществами новых технологий.

ПРЕСТУПЛЕНИЮ НЕ НУЖНА ВИЗА: ПОДХОД ЗАПАДНОЙ АФРИКИ К БОРЬБЕ С ФИНАНСОВЫМ МОШЕННИЧЕСТВОМ

Развитие информационных технологий стирает границы между юрисдикциями. При этом каждый регион обладает определенными особенностями и сталкивается с уникальными вызовами.

Глава нигерийского офиса и исполняющий обязанности главы по коммуникациям и адвокации Межправительственной группы по борьбе с отмыванием денег в Западной Африке (ГИАБА) **Мелайе Тимоти Феми** рассказал редакции журнала «Финансовая безопасность» о региональной специфике, преимуществах международного сотрудничества, а также мерах Группы по просвещению населения. Именно просвещение, по мнению эксперта, способно предотвратить правонарушение, уберегая потенциальную жертву и предостерегая злоумышленников.

— Какие схемы финансового мошенничества наиболее распространены в юрисдикциях ГИАБА?

— ГИАБА работает в западной части Африки и объединяет 17 государств. В этих странах большинство финансовых преступлений, которые мы наблюдали, связаны с интернет-мошенничеством, преимущественно среди молодежи.

Такие аферы подразделяются на две категории. Первая классифицируется как мошенничество с авансовыми платежами, вторая известна как «романтическое мошенничество». Мошенничество с авансовыми платежами может быть связано с финансовыми

пирамидами, переводом грязных денег через чужой счет с целью отмывания. Мошенники убеждают людей под разными предлогами, в том числе предлагая определенный процент в качестве платы за контроль над счетами. Уязвимые и легко поддающиеся влиянию группы населения соглашаются участвовать в этом процессе. Несмотря на то, что большинство преступников просят перевести довольно небольшую сумму — от 100 до 500 долларов, — их жертвами становятся множество людей, в результате чего мошенники получают огромные суммы.

«Романтическое мошенничество» обычно подразумевает такую схему: молодые люди знакомятся с одинокими пожилыми женщинами, в ходе общения признаются им в любви и в определенный момент начинают просить у них деньги. Некоторые аферисты выманивают небольшие суммы у нескольких женщин, в то время как другие уговаривают перевести крупные суммы. Например, в нашей практике была женщина, которая перевела 300 тысяч долларов. Связь прекращается, как только преступники получают деньги.

— Как вы оцениваете проблему угроз кибербезопасности в контексте финансовых преступлений и схем мошенничества?

— Угрозы кибербезопасности не так распространены, как другие виды угроз, с которыми мы сталкивались. Однако в настоящее время есть риски похищения данных. Преступник получает контроль над данными организации и требует выкуп, но даже если вымогателю платят, происходят утечки. Кибератака может иметь разрушительные последствия. Например, безопасность данных финансовых учреждений очень важна, поэтому в случае взлома люди могут получать фальшивые инструкции по платежам, что может привести к серьезным нарушениям общей финансовой безопасности.

Угрозы кибербезопасности также усугубляют последствия традиционного мошенничества. И иногда это вопрос морали. Фактически преступник похищает личность и использует ее данные для доступа к информации на разных серверах. Таким образом, киберинструменты стимулируют деятельность мошенников.

Органы безопасности работают очень усердно, и им удается отслеживать, блокировать и задерживать большое количество тех, кто совершает подобные преступления.

— Важно ли использовать новые технологии в борьбе с преступниками?

— Действительно, технологии — это инструмент, который можно использовать во благо. Например, подразделения финансовой разведки в регионе внедряют искусственный интеллект для анализа данных, поскольку это дает определенную свободу действий: ИИ способен выполнять работу, которая обычно занимает 4 дня, за пару часов.

Новые технологии служат на пользу регулирующим органам. Например, искусственный интеллект может быть использован для отслеживания транзакций. Уже разработан ряд инструментов. В частности, goAML — это программное обеспечение для анализа отчетов о подозрительных транзакциях. Применение таких инструментов помогает упорядочить, классифицировать информацию и передавать ее в ПФР. Кроме того, правоохранительные органы используют искусственный интеллект для выслеживания, идентификации преступника, определения местоположения по IP-адресу, деактивации устройства.

Таким образом, технологии — это полезный инструмент для борьбы с преступниками, и их игнорирование может привести к тому, что компетентные органы проиграют в битве с незаконной деятельностью.

— Существует ли в рамках ГИАБА инициатива, направленная на борьбу с финансовым мошенничеством?

— В своей работе мы делаем акцент на профилактических мерах. Профилактика лучше лечения: если вы предотвращаете, вам не нужно будет лечить.

Одна из важнейших задач, которую необходимо решить, — это захватить внимание потенциальных преступников и будущих жертв до того, как они станут таковыми. Здесь важно вести просветительскую работу.

Представьте себе типичную финансовую пирамиду. Мошенники просят вложить 1 тысячу рублей, чтобы получить 3 тысячи рублей. Сам человек, его друзья, коллеги и родственники попадают в ловушку, и в итоге оказывается, что в нее вовлечено уже 10 тысяч человек. Что в итоге происходит? Все деньги пропали.

> **«Одна из важнейших задач, которую необходимо решить — это захватить внимание потенциальных преступников и будущих жертв до того, как они станут таковыми.**

Именно поэтому мы привлекаем внимание, обучаем, просвещаем молодых людей, повышаем их осведомленность, организуем программы для школьников, выпускников и реализуем неформальные программы для молодого поколения с целью убедиться, что они понимают закономерности, методы и тенденции.

В секретариате ГИАБА мы проводим работу по выявлению тенденций, методов и подходов, а также разработке контента для молодежи.

Осознание того, как изменяются тенденции, развиваются новые методы совершения преступлений, с одной стороны, не позволяет людям становиться жертвами. С другой стороны, преступники осознают негативные последствия участия в преступной деятельности. Мы пытаемся донести до них, что негативные последствия будут серьезнее, чем выгоды, которые они получат. В конечном счете они окажутся в тюрьме или даже в камере смертников. Это может повлиять на имидж их страны, общества, окружения. Наконец, деньги, которые они пытались украсть, будут возвращены в рамках процедуры возврата активов. Практика возврата активов позволяет разоблачить мотив преступления, уничтожить представление о потенциальной выгоде.

— Важно ли международное сотрудничество для борьбы с такого рода преступлениями?

— На практике международное сотрудничество чрезвычайно важно. Я бы даже сказал, что оно обязательно для достижения успеха в борьбе с преступностью. Преступник может фактически жить в Африке и пытаться обмануть кого-то, кто живет в России, и наоборот. Если мы не будем делиться информацией и разведданными, мы даем им шанс добиться своих корыстных целей. Сотрудничество на международной арене также важно для внедрения новых технологий — для совершения преступлений не требуются визы. Мошенничество с помощью телефонных звонков, ловушки в социальных сетях не зависят от границ государств. Мы должны попытаться создать среду, в которой мы сможем работать вместе без ограничений.

Я приведу практический пример. Однажды человек совершил преступление через финансовое учреждение в Африке, а затем деньги были переведены в другую африканскую страну. Однако, поскольку в этих странах уже существует так называемая взаимная правовая помощь, подразделение финансовой разведки в первой стране связалось с финансовым учреждением, чтобы остановить транзакции и наложить запрет на списание и перевод средств, чтобы предотвратить вывод денег через континенты. Благодаря взаимной правовой помощи с органами других юрисдикций властям удалось обнаружить преступника и деньги. Если бы страны не работали сообща, преступник бы скрылся.

Этот пример подчеркивает важность совместной работы и взаимодействия в создании более безопасного мира для всех нас. Когда в одной стране возникают проблемы, они возникают повсюду. Африканская пословица гласит: «Тот, кто бросит камень на рынке, попадет в своего родственника».

«Я особенно восхищен сотрудничеством на Пленарном заседании ЕАГ. Мы стали свидетелями партнерства между регионами, между разными региональными группами по типу ФАТФ, логистика и гостеприимство на этом мероприятии превосходные.

ФИКИЛЕ П. ЗИТА: ГЛОБАЛЬНАЯ ЗАДАЧА — ОБЕСПЕЧИТЬ СОТРУДНИЧЕСТВО МЕЖДУ СТРАНАМИ С УЧЕТОМ ИХ ПОТЕНЦИАЛА

Глобальная антиотмывочная система основана на правилах и принципах, единых для всех субъектов. При этом региональный контекст очень важен: все государства имеют свои особенности и свой потенциал, что требует разных подходов. В интервью на полях 42-й недели ЕАГ в Москве **Фикиле П. Зита,** исполнительный секретарь Группы по борьбе с отмыванием денег в Восточной и Южной Африке (ЕСААМЛГ), подчеркнула различия между странами Группы с точки зрения их уровня развития, ограниченности ресурсов и потенциала, а также региональных особенностей, учитывая, что большинство государств являются странами с низким потенциалом.

— Госпожа Зита, каковы ваши впечатления от Пленарной недели ЕАГ?

— Я узнала о многих идеях, которые мы можем применить в нашем регионе. Особенно интересен Форум парламентариев, потому что это новая область для нашей региональной группы по типу ФАТФ. Важно, чтобы мы привлекали парламентариев государств-членов, особенно в контексте следующего раунда оценки. Такой формат расширяет технические возможности парламентариев с целью лучшего понимания этих сложных проблем и путей их решения, и тогда процесс принятия законодательства становится проще.

Совместная инициатива ЕАГ и МЕНАФАТФ также впечатляет. ЕСААМЛГ могла бы присоединиться к сотрудничеству в рамках этого формата. Уверена, наши члены оценят возможность взаимодействия. Более того, сотрудничество между РГТФ необходимо для усиления обмена знаниями, в частности лучшими практиками и экспертизой в различных областях.

Преступления, связанные с ОД/ФТ, имеют трансграничный характер, выходя за рамки одной юрисдикции. Государствам следует учиться у передовых антиотмывочных систем, чтобы укреплять национальные режимы, внедрять современные меры и обеспечивать устойчивость финансовых структур.

— Что наиболее привлекло ваше внимание в ходе Пленарной недели?

— Процесс принятия решений. Он проходит быстрее из-за численности ЕАГ — ЕСААМЛГ имеет больший членский состав, объединяя 21 юрисдикцию. Роль Секретариата ЕАГ также достаточно велика, мы видим доверие к Секретариату и, следовательно, отличную организацию РГТФ.

«Государствам следует учиться у передовых антиотмывочных систем, чтобы укреплять национальные режимы, внедрять современные меры и обеспечивать устойчивость финансовых структур.

— В чем, на ваш взгляд, заключается важность сотрудничества между региональными группами по типу ФАТФ (РГТФ)?

— Сотрудничество между РГТФ и обмен опытом очень важны. Например, я возглавляю один из проектов ФАТФ в рамках Группы глобального сетевого сотрудничества (GNCG), который призван усилить влияние региональных групп в ФАТФ. Инициативы, способствующие совместной работе, помогут увеличить вес нашего голоса и внедрить наши инициативы в практику. Иногда стандарты сложно имплементировать в странах с низким потенциалом. В нашем регионе по-прежнему много государств с экономикой, основанной на наличности, со своими вызовами, в том числе ограниченностью ресурсов. Например, отчетность о подозрительных операциях будет отличаться от отчетности в странах с развитой экономикой и усовершенствованными финансовыми системами для различных учреждений. Странам, включенным в «серый» список, особенно трудно продемонстрировать свои улучшения. Например, в развитых странах с передовыми системами отчетность поступает из секторов с иной структурой. В ряде наших юрисдикций субъекты сектора установленных нефинансовых предприятий и профессий (DNFBP) или сектора недвижимости управляются как правило одним лицом — иногда это только вы и ваш портфель.

При таком сценарии они не могут позволить себе нанять комплаенс-специалистов, внедрить руководства, при этом несут такие же обязательства, как и любая крупная, хорошо структурированная организация, располагающая соответствующими сотрудниками.

В Восточной и Южной Африке ландшафт рисков довольно разнообразен. В одних странах терроризм, в других — финансирование терроризма, проблемы с платежными системами в результате внедрения мер по снижению рисков. Глобальная задача состоит в том, чтобы обеспечить сотрудничество между странами с разным уровнем развития.

В случае Российской Федерации — у вас есть учебно-методический центр, вы проводите курсы, которые полезны для государств — членов ЕАГ и других стран. Например, мы знаем, что некоторые из наших сотрудников посещали ваш центр, и мы ценим это.

— Что вы ожидаете от сотрудничества РГТФ в будущем?

— Я хочу, чтобы у нас были более тесные связи, чтобы мы могли выступать единым фронтом, так как нам не хватает участия в процессе принятия решений. Однако, если объединить все РГТФ, наш охват шире, чем сама ФАТФ. Вот почему нам необходимо продолжать укреплять связи между региональными группами, чтобы можно было обсуждать эти вопросы.

Первое совместное мероприятие двух региональных групп по типу ФАТФ:

ФОРУМ НАДЗОРНЫХ ОРГАНОВ И ЧАСТНОГО СЕКТОРА ПОД ЭГИДОЙ ЕАГ И МЕНАФАТФ ПРОШЕЛ В МОСКВЕ

В Москве прошел Совместный форум надзорных органов и частного сектора под эгидой Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) и Группы разработки финансовых мер борьбы с отмыванием денег на Ближнем Востоке и в Северной Африке (МЕНАФАТФ). Это первое совместное мероприятие двух региональных групп по типу ФАТФ.

▸ **Программа форума включила панельные дискуссии «Тренды будущего: глобальные вызовы и угрозы цифровизации», «Как узнать своего клиента в цифровом мире» и «Марафон или спринт: управление рисками будущего». На повестке дня вопросы противодействия киберпреступлениям и использованию виртуальных активов в преступных целях, развитие международного сотрудничества в цифровом мире, синергия антифрода и AML-систем, применение искусственного интеллекта и машинного обучения, социальная инженерия как фактор вовлечения в теневую деятельность, риск-ориентированный надзор, криптокомплаенс и другие темы.**

Тема Форума — «Управление рисками в эпоху новых технологий». Среди участников: руководители и специалисты надзорных органов, финансовых разведок, международных организаций и частного сектора из Алжира, Бахрейна, Беларуси, Египта, Индии, Казахстана, Катара, Китая, Кыргызстана, Ливии, России, ОАЭ, Саудовской Аравии, Таджикистана, Туркменистана, Узбекистана и Йемена. К работе подключились эксперты Контртеррористического комитета и Контртеррористического управления ООН, Нового банка развития.

На открытии Форума выступили председатель ЕАГ, директор Росфинмониторинга **Юрий Чиханчин,** вице-президент МЕНАФАТФ **Его Превосходительство Хамид Саиф Аль-Зааби,** исполнительный секретарь МЕНАФАТФ **Сулейман Аль-Джабрин** и исполнительный секретарь ЕАГ **Сергей Тетеруков.** Модератором Пленарной сессии стала заместитель директора Росфинмониторинга **Галина Бобрышева.**

Итоги Форума закреплены в совместных рекомендациях ЕАГ и МЕНАФАТФ. Мероприятие позволило представителям региональных групп по типу ФАТФ обменяться опытом и лучшими практиками надзорной деятельности. Участники подтвердили готовность к дальнейшему развитию партнерских отношений для минимизации рисков в антиотмывочной сфере и борьбы с финансовыми преступлениями.

Юрий Чиханчин поблагодарил коллег из МЕНАФАТФ за совместную работу и координацию общих усилий в подготовке Форума, отметив ключевую роль взаимодействия представителей региональных групп по типу ФАТФ в развитии национальных антиотмывочных систем, обмене знаниями и лучшими практиками в области государственно-частного партнерства.

«Преступники активно втягивают граждан в незаконную деятельность, используя такие возможности новых технологий, как скорость, анонимность и трансграничность. И порой граждане доверяют злоумышленникам больше, чем властям. Транснациональная преступность становится одной из важнейших угроз. Это требует ответных мер по вовлечению в межстрановой диалог молодежи, экспертов финансовых, научных и образовательных организаций для формирования ответственного поколения, способного защитить не только себя, но и общество от угроз финансовой безопасности», — сказал Юрий Чиханчин.

Галина Бобрышева подчеркнула роль финансовых организаций и лиц нефинансовых профессий в первичной оценке рисков. Как отметила замглавы ведомства, банки становятся ключевым звеном в совместной работе по минимизации рисков и, по сути, запускают всю цепочку финансового мониторинга.

«Надзорные органы, с одной стороны, создают регуляторную среду, а с другой — следят за соответствием установленным правилам. Мы понимаем, что общий результат невозможен без доверия между участниками антиотмывочной системы. Все дальнейшие этапы: финансовые расследования, уголовные преследования, возврат преступных активов во многом зависят от качества работы частного сектора», — сказала Галина Бобрышева.

Михаил Мамута, руководитель Службы по защите прав потребителей и обеспечению доступности финансовых услуг Банка России

Находясь под влиянием мошенников, использующих методы социальной инженерии, люди часто отказываются от помощи банка, который видит, что с человеком происходит что-то не то, и пытается остановить транзакции. Однако гражданин уверен, что в банке — мошенники, и он должен помочь органам правопорядка вывести их на чистую воду. Этот паттерн часто используют настоящие злоумышленники.

Дистанция между банком и человеком пока еще достаточно велика, и нужно, чтобы люди чувствовали, что банк — как можно ближе к ним. Что мы для этого делаем? Все крупные банки осенью должны будут внедрить кнопку: одна большая красная кнопка «нажми сюда, если ты столкнулся с мошенничеством или с подозрением на мошенничество». В разных банках сейчас эта система взаимодействия организована по-разному, а людям нужен, во-первых, простой путь, во-вторых, единообразный, и в-третьих, заметный, который будет сразу бросаться в глаза.

Также нужна постоянная просветительская работа не только со стороны государства, но и со стороны банков. Некоторые банки уделяют этому очень большое внимание: запускают различные тренажеры для людей, программы «защитим или вернем деньги», то есть стараются быть как можно ближе к человеку. Уровень доверия со стороны людей к этим банкам в целом более высокий.

Центральный банк старается максимально мотивировать кредитные организации к тому, чтобы такая работа велась на постоянной основе, в том числе усиливая требования к антифрод-мониторингу, вводя материальную и административную ответственность за нарушения. Это заставляет банки более внимательно относиться к поведению клиента, к его потребностям и к взаимодействию с ним.

Давид Султанходжаев, сотрудник отдела кибербезопасности Департамента информационной безопасности АКБ «Капиталбанк» (Республика Узбекистан)

Ландшафт угроз меняется очень быстро. Раньше мы руководствовались накопленным опытом в реагировании на те или иные вызовы, теперь же ситуация принципиально новая. Глобальная диджитализация, повсеместное внедрение искусственного интеллекта привели к возникновению рисков, с которыми раньше мы не сталкивались.

Банк аккумулирует огромное количество информации о клиенте: его персональные и банковские данные, движение средств по счетам и т. д. Каждая из систем банка, которых может быть в одной организации от 50 до 100, генерирует какие-то данные. Антифрод и другие системы по противодействию мошенничеству пытаются выявить подозрительные операции, попытки взлома аккаунта и т. д. Все это можно «скормить» искусственному интеллекту и моделям машинного обучения. Обучившись на этих моделях, ИИ будет не только видеть предыдущие кейсы, но и начнет предсказывать, какие виды кибератак и финансового мошенничества могут появиться.

Перспективным решением для предотвращения финансового мошенничества может стать глобальная интеграция, возможность подключить всех к единой антифрод-системе. Банки должны общаться между собой. Потому что бывает так, что человек оформляет кредит в одном банке, переводит деньги в другие, и это все трудно отследить. Если мы все это интегрируем, превратим в одну глобальную антифрод-систему, нам будет проще отследить транзакции.

Карим Элвардани, сотрудник отдела анализа и исследований финансовой разведки Египта

Искусственный интеллект делает жизнь людей проще, но в то же время предоставляет преступникам возможность создавать новые мошеннические схемы. Например, используя передовые технологии, злоумышленники могут полностью подделать личность в интернете, похитить средства граждан или отмыть криминальные доходы. Модели искусственного интеллекта и машинного обучения должны управляться и тщательно контролироваться.

Со своей стороны мы можем использовать искусственный интеллект для постоянного мониторинга и выявления случаев мошенничества и подозрительных транзакций. Однако это должно быть сделано с полным знанием используемой модели. Если мы можем предоставить системе предупреждающие знаки, сценарии и так далее, это поможет лучше и быстрее отслеживать подозрительные операции. Всякий раз, когда мы сталкиваемся с риском, — это возможность изучить новый сценарий и внедрить его в модель, используя машинное обучение, чтобы снизить его в будущем.

Другой актуальный аспект — это оборот криптовалюты и риски, связанные с ним. В Египте на законодательном уровне запрещены оборот и майнинг криптовалют. Мы находимся на пути к тому, чтобы начать разработку и введение соответствующих регламентирующих эту сферу правил и законов.

Криптовалюты — один из самых простых способов для преступников распоряжаться своими грязными доходами. Центральный банк Египта, являющийся надзорным органом, проводит значительную работу по выявлению таких транзакций, и в дальнейшем выявленные преступные доходы конфискуются.

Дмитрий Захаров, директор Департамента финансового мониторинга Комитета государственного контроля Республики Беларусь

Благодаря мероприятиям, которые проходят на полях Пленарной недели ЕАГ, мы обогащаемся новыми знаниями, новым опытом, который будет очень полезен в предстоящей оценке страны. Хотел бы отдельно обозначить проблему дропов — она транснациональная. Эту проблему нужно решать коренным образом — огромное количество людей страдает от манипуляций, которые проводят мошенники. Белоруссия так же, как и многие из собравшихся здесь стран, сталкивается с киберпреступностью, когда злоумышленники звонят гражданам в различных социальных сетях, вводят в заблуждение. В нашей стране примерно 20–25% всех преступлений, которые регистрируются ежегодно, связаны именно с кибермошенничеством. Эта форма сегодня агрессивна и на повестке — номер один. Мы должны разрабатывать механизмы борьбы с этим. Если мы объединим усилия всех структур, которые задействованы в этой работе, — финансовых разведок, правоохранительного блока, финансового и частного сектора, то мы победим эту проблему обязательно.

Михаил Пронин, вице-президент — директор Департамента финансового мониторинга Банка ПСБ

Преступность, не важно, связана она с кибермошенничеством или легализацией, стала более целостной и межстрановой. Поэтому необходимо взаимодействие. Крупные форумы, такие как надзорный, как раз для этого и проводятся: чтобы знакомиться, выстраивать контакты, вырабатывать совместные меры. Эффективно работают Совет комплаенс, он действует на базе Росфинмониторинга, а также Международный совет комплаенс.

Один из ключевых вопросов форума был посвящен тематике дропов, киберугроз. Сейчас у нас есть две зоны, действующие параллельно: это защита клиентов в рамках противодействия мошенничеству и выявление подозрительных клиентов, связанных с легализацией.

Расскажу на примере нашего банка. Несмотря на то, что это действительно два разных подразделения с разными функционалами, погрузившись в детали, мы поняли, что задача коллег в антифроде — защищать добропорядочного клиента, а задача в борьбе с легализацией — выявлять недобропорядочного клиента, который использует продукты и услуги в противоправных целях. То есть задачи совсем разные, но между ними часто бывают пересечения. Поэтому мы, не вторгаясь в зону работы другого подразделения, организовали взаимодействие и на регулярной основе обмениваемся результатами. У нас есть совместные примеры, когда с точки зрения автоматизации внутри систем друг друга мы выстраиваем свои аналитические сценарии.

Используя инструменты коллег и предоставляя им доступ к своим наработкам, мы можем лучше выполнять общую задачу. Поэтому нужно укреплять коммуникацию, тогда результаты будут более точными и общая эффективность повысится.

ПОД/ФТ в эпоху цифровых рисков:

АЛЖИР О ТОМ, КАК НОВЫЕ ТЕХНОЛОГИИ МЕНЯЮТ ЛАНДШАФТ УГРОЗ

Технологические инновации во многом облегчили жизнь современного человека — по обе стороны, как простого гражданина, так и преступника, теперь скрывающегося за ложным IP-адресом или украденной личностью. Борьба с такого рода угрозами возможна через диалог всех заинтересованных сторон, в том числе в рамках сотрудничества частного и государственного секторов. Тенденции схожи во всем мире, и осознание важности сплоченной борьбы разделяется международным сообществом. Глава подразделения финансовой разведки Алжира Мохаммед Саудия поделился взглядом североафриканской страны на эффективные диалоговые форматы и перспективы сотрудничества региональных групп в ПОД/ФТ на фоне появления цифровых рисков.

МОХАММЕД САУДИЯ
Глава подразделения финансовой разведки Алжирской Народной Демократической Республики

— Мистер Саудия, как быстро, по вашим наблюдениям, меняется ландшафт угроз с развитием финтеха и цифровых активов?

— Ландшафт угроз развивается в геометрической прогрессии с эволюцией финансовых технологий и цифровых активов. Действительно, инновации в этой сфере привели к беспрецедентному уровню удобства и доступности, но они также создали новые уязвимости с увеличением числа изощренных и целенаправленных атак. Киберпреступники используют новые технологии для кражи данных, угроз финансовым учреждениям и дестабилизации финансовых систем в целом. Чтобы справиться с этим вызовом, необходимо применять комплексный подход к кибербезопасности путем внедрения передовых мер, шифрования финансовых данных, многофакторной идентификации и непрерывного обучения сотрудников. Это способствует формированию культуры осведомленности о кибербезопасности, держит в курсе новых угроз.

— Как вы оцениваете перспективы сотрудничества между ЕАГ и МЕНАФАТФ?

— Инициатива ЕАГ пригласить членов МЕНАФАТФ впечатляет. На мой взгляд, перспективы сотрудничества между двумя региональными группами по типу ФАТФ многообещающие. Наши организации преследуют общие цели и сталкиваются с одинаковыми трудностями в процессе борьбы с отмыванием денег и финансированием терроризма. Перспек-

тивные меры сотрудничества направлены на достижение общей цели — укрепление финансовой безопасности. Обе организации могли бы работать вместе над повышением финансовой безопасности в регионе и делиться своим опытом и передовыми практиками в области ПОД/ФТ. Возможно также сотрудничать в сфере обучения и повышения осведомленности путем организации семинаров, практикумов для профессионалов финансового и нефинансового секторов о рисках ПОД/ФТ. Совместная работа по взаимной оценке и обучению оценщиков ориентирована на будущее, поскольку в итоге выявляются области для улучшения в следующем цикле оценки.

— Какие механизмы, по вашему мнению, должны быть усилены для улучшения обмена информацией между частным сектором и государственными органами?

— Для улучшения обмена информацией между частным и государственным секторами крайне важно укрепить и обезопасить механизмы обмена данными. Необходимы стандартизированные протоколы связи, которые облегчают обмен между частным и государственным секторами. Кроме того, важно разработать понятную нормативно-правовую базу, в которой четко определены правила и обязанности каждого участника. Возможно, стоит обязать частный сектор подписывать соглашения о конфиденциальности, чтобы предотвратить утечку данных, а также разработать механизмы проверки личности для обеспечения подлинности передаваемой информации. Говоря о технологиях шифрования, необходимо работать вместе, обеспечивать безопасность и прозрачность. Это, безусловно, будет способствовать укреплению национальной безопасности и предотвращению незаконной деятельности.

— Какие формы диалога между надзором и бизнесом вы считаете наиболее продуктивными в вопросах ПОД/ФТ?

— Одной из наиболее продуктивных форм диалога является проведение периодических и регулярных встреч между надзорными органами и компаниями для обсуждения последних тенденций и передовых практик в области ПОД/ФТ. Эффективный обмен информацией позволяет выявлять риски и потенциальные угрозы. Следует проводить обучение для компаний по новейшим нормативным актам и передовым методам обеспечения безопасности, что позволит следовать букве закона и бороться с отмыванием денег и финансированием терроризма.

«Следует проводить обучение для компаний по новейшим нормативным актам и передовым методам обеспечения безопасности, что позволит следовать букве закона и бороться с отмыванием денег и финансированием терроризма.

Необходимо внедрить эффективные механизмы отчетности для компаний, чтобы сообщать о подозрительной деятельности надзорным органам и обеспечить тесное государственно-частное сотрудничество для разработки инновационных решений в области ПОД/ФТ. Регулярная оценка рисков и угроз для бизнеса и надзорных органов также очень важна.

Совместные рабочие группы также являются продуктивной формой диалога для решения конкретных вопросов, связанных с ПОД/ФТ.

Цифровизация, доверие, риск-ориентированный подход и профилактика:

СПЕЦИАЛЬНАЯ СЕССИЯ СЧЕТНОЙ ПАЛАТЫ РФ ПРОШЛА В РАМКАХ KAZANFORUM

С 13 по 18 мая в г. Казани состоялся XVI Международный экономический форум «Россия – Исламский мир: KazanForum». Мероприятие посетили 8,5 тысяч гостей из 96 стран и 82 российских регионов. В рамках форума прошла Специальная сессия Счетной палаты Российской Федерации на тему «Государственный аудит на защите интересов государства и общества в современном мире», на которой традиционно обсуждаются актуальные вопросы развития государственного аудита.

Большой интерес к этой тематике на казанском форуме связан с серьезным укреплением экономических связей и ростом товарооборота между Россией и странами Организации исламского сотрудничества: за последние четыре года он увеличился на 44% и достиг отметки в 163 млрд долларов.

Модератором дискуссии выступила аудитор Счетной палаты Российской Федерации **Светлана Орлова.** Она подчеркнула, что государственный аудит является мостом между государственной властью и обществом, обеспечивая контроль за национальными стратегическими ресурсами и социальную справедливость.

«Предназначение института государственного аудита — это содействие эффективности госуправления, направленное, в первую очередь, на повышение качества жизни граждан наших стран. Обеспечивая подотчетность всех управленческих звеньев, высшие органы аудита способствуют развитию всестороннего диалога между обществом и властью, помогают повысить доверие общества к государству», — отметила Светлана Орлова.

В работе сессии приняли участие представители высших органов государственного контроля Азербайджана, Кыргызстана, Таджикистана, Объединенных Арабских Эмиратов, а также партнеры из других стран БРИКС. Со стороны Российской Федерации участвовали представители парламентов — Совета Федерации и Государственного Совета Республики Татарстан, Минэкономразвития России, Росфинмониторинга, Банка России, ПАО «Промсвязьбанк», Общероссийского движения детей и молодежи «Движение первых», Счетной палаты Татарстана. С приветственным словом на открытии сессии выступил Председатель Госсовета Республики Татарстан **Фарид Мухаметшин.**

Участники дискуссии обменялись мнениями о роли государственного финансового контроля в обеспечении устойчивого развития страны, укреплении культуры подотчетности госор-

ганов и эффективном управлении государственными ресурсами, а также обсудили основные тренды и перспективы развития государственного аудита в современном мире.

Первый заместитель председателя Комитета Совета Федерации по бюджету и финансовым рынкам **Сергей Рябухин** обозначил приоритеты внешнего государственного аудита. *«Среди них — мониторинг достижения скорректированных национальных целей в рамках нацпроектов, корректировка межбюджетных отношений в целях стимулирования регионального развития, контроль за государственными и муниципальными закупками и доработка законодательства в этой сфере, а также совершенствование законодательства с целью повышения эффективности формирования доходов и расходов»,* — сказал сенатор.

Одним из лейтмотивов беседы стала тема цифровизации. Выступающие отметили важность внедрения новых технологий в сферу контроля и надзора, в том числе возможности искусственного интеллекта.

«Мы живем в эпоху цифровой трансформации. Сегодня процесс цифровизации — необратим. Информатизация государственных органов — это глобальное современное направление, отвечающее национальным интересам. И Счетная палата поставила перед собой действительно амбициозные задачи в этом направлении. Мы утвердили программу цифровой трансформации Счетной палаты, создаем единую цифровую платформу государственного аудита, которая позволит перейти к риск-ориентированному подходу при 100 % охвате объектов контроля. Важно, что в создаваемый цифровой контур войдет блок по выявлению коррупционных рисков в финансово-бюджетной сфере», — сказала Светлана Орлова.

Главный аудитор Банка России **Валерий Горегляд** акцентировал внимание на преимуществах использования цифровых инструментов в контрольной деятельности.

«Автоматизация и роботизация аудиторских процедур позволяет не только высвободить большое количество времени, но и качественно изменить сущность аудита. Аудитор сегодня — это не просто контролер, который проверяет соответствие между первичными документами и их исполнением. Аудитор — это в первую очередь консультант и партнер, потому что простые операции делает компьютер. Это дает возможность аудитору работать на основе предиктивной аналитики, вырабатывать рекомендации, предупреждая не только правонарушения, но и неэффективность», — отметил выступающий.

Заместитель директора Росфинмониторинга **Галина Бобрышева** подчеркнула, что риски преступных посягательств в бюджетной сфере находятся в фокусе внимания финансовой разведки России. При этом развитие механизмов финансового мониторинга требует не только новейших технологических решений, но и формирования культуры финансовой безопасности и финансовой гигиены.

«Самое важное в системе противодействия отмыванию преступных доходов и финансированию терроризма — это доверие, партнерские отношения, которые мы выстроили и развиваем

с частным сектором. Это является основой антиотмывочной цепочки: информация, которая к нам поступает, должна быть основана на объективной оценке рисков со стороны финансовых организаций и других провайдеров. Для нас бюджетная сфера, фокус на бюджетные риски — приоритет номер один», — отметила Галина Бобрышева.

Замглавы Росфинмониторинга также обратила внимание на проблему вовлечения молодежи в незаконные финансовые схемы и рассказала о таком проекте, как Международная олимпиада по финансовой безопасности, которая уже в пятый раз собирает на своей площадке школьников и студентов с четырех континентов.

«Очень важно работать с молодым поколением. Мы понимаем, что это — не завтрашний день, это — сегодняшний день. Потому что, к сожалению, преступники уже сегодня эксплуатируют отсутствие навыков финансовой грамотности, финансовой безопасности и финансовой гигиены у детей. Не секрет, что основная масса тех, кто стоит на канале транзита, в простых операциях по обналичиванию средств, — это молодые люди, которые, не осознавая те риски, которые они на себя принимают, вовлекаются в подобные схемы», — сказала представитель Службы.

«Не секрет, что основная масса тех, кто стоит на канале транзита, в простых операциях по обналичиванию средств, — это молодые люди, которые, не осознавая те риски, которые они на себя принимают, вовлекаются в подобные схемы.

Председатель правления Общероссийского общественно-государственного движения детей и молодежи «Движение первых» **Татьяна Робина** обратилась к вопросу подготовки аудиторов будущего.

«Движение первых» объединяет не только детей, но и родителей, наставников, федеральные и региональные органы власти, детские и молодежные общественные организации, государственные корпорации и предпринимателей для того, чтобы вместе развивать единое воспитательное пространство, которое поможет каждому ребенку подготовить себя к самостоятельной взрослой жизни», — отметила она в ходе выступления.

Еще одним важным вектором развития системы госфинконтроля, о котором говорили практически все участники дискуссии, является профилактика и риск-ориентированный подход к проведению проверок. А от этого напрямую зависят такие важные факторы, как развитие культуры добросовестности объектов контроля и повышение доверия бизнеса к государству. Так, заместитель Председателя ПАО «Промсвязьбанк» **Владимир Катренко** отметил, что *«доверие к аудитору проявляется тогда, когда объект контроля не стесняется прийти к контролеру и задать ему вопрос».*

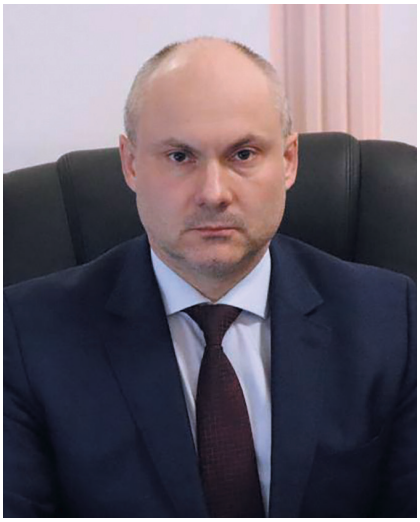
Подводя итог дискуссии, **Светлана Орлова** отметила, что вместе с государствами — партнерами мы сможем пройти очень важный и интересный путь цифровой трансформации в сфере государственного аудита. Риск-ориентированный контроль за бюджетами наших стран, которые являются сегодня социально ориентированными, позволяет не только повысить качество работы всех уровней власти, но самое главное — повысить качество жизни наших граждан.

«Уверена, что наша совместная работа послужит дальнейшему развитию партнерства на благо наших стран и народов!» — подытожила аудитор Счетной палаты.

НАЦИОНАЛЬНЫЙ КИБЕРФРОНТ: ЭФФЕКТИВНЫЕ РЕШЕНИЯ СТРАН НА БЛАГО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

СТАТИСТИКА И ДИНАМИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ФИНАНСОВОГО МОШЕННИЧЕСТВА: АНАЛИЗ И ТЕНДЕНЦИИ

Сегодня киберпреступность охватила все без исключения страны и стала мировой проблемой. В 2024 году Международной группой исследований под руководством Оксфордского университета (Великобритания) определены страны с самым высоким индексом киберпреступности, среди которых Украина, Китай, США, Нигерия, Румыния, Северная Корея, Великобритания, Бразилия, Индия.



ДАНИЛ ФИЛИППОВ
Заместитель начальника Следственного департамента МВД России, генерал-майор юстиции

Только в 2023 году Интерпол арестовал 3500 человек и 300 млн долларов в 34 странах. В США в 2022 году сумма похищенных денежных средств составила более 39,5 млрд долларов (или свыше 3 трлн рублей), в Китае только сумма возмещенных гражданам потерь составила 99,1 млрд юаней (1 трлн рублей).

Отличительной особенностью преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, является трансграничный характер. Это означает возможность их совершения из одной страны против граждан другой. Единственным условием является знание языка жертвы. Кол-центры по обману наших граждан работают из различных стран, в основном ранее входящих в состав союзного государства.

В настоящее время много сделано для противодействия этому виду преступной деятельности:

- в режиме реального времени организован информационный обмен между МВД России и Банком России;
- банкам предоставлена возможность использования двухдневного «периода охлаждения» по операциям в случае наличия признаков их совершения без согласия клиентов;
- предоставлена возможность установить самозапрет на оформление дистанционных кредитов.

Кроме того, МВД России разработаны два проекта федеральных законов:

- о введении уголовной ответственности лиц, передающих свои банковские карты третьим лицам, а также лиц, использующих такие банковские карты;
- о наделении следователя и дознавателя правом внесудебного приостановления на 10 суток операций по счетам, использовавшимся в преступной деятельности.

Указанные законопроекты приняты в первом чтении Государственной Думой Федерального Собрания Российской Федерации.

Кроме того, удалось исключить пропуск иностранного трафика с использованием подмены телефонных номеров, установлен лимит реализации сим-карт для граждан Российской Федерации и иностранных граждан, введена административная и уголовная ответственность компаний и их должностных лиц, допустивших утечку персональных данных.

Это позволило сократить прирост мошенничеств с 38,2% в 2023 году до 6,8% в 2024 году. И эта тенденция сохранилась в текущем году.

В прошлом году дистанционных мошенничеств за 4 месяца зарегистрировано 154 тысячи, а в этом году их 150 тысяч.

По результатам работы в 2024 году увеличилось на 2,1% количество мошенничеств, уголовные дела по которым направлены с обвинительным заключением в суд. Удалось достичь определенных положительных результатов в раскрытии дистанционных хищений, совершенных в составе организованных преступных групп и преступных сообществ. На 13,5% увеличилась сумма наложенного ареста по уголовным делам о дистанционных хищениях.

Однако принятых мер явно недостаточно, поскольку размер причиненного нашим гражданам ущерба продолжает расти, и в текущем году он уже больше на 30%. А в общей сложности за три года материальный ущерб от киберпреступлений составил более 485 млрд рублей.

Если говорить о трендах, то они зависят в том числе от общего противодействия мошенничеству. Злоумышленники используют любой инфоповод для обмана (от замены полисов медицинского страхования, страхового номера индивидуального лицевого счета до труб, приборов учета, сим-карт).

Когда банки стали активно блокировать банковские карты дропов, за деньгами к потерпевшим стали приходить курьеры, которые передают липовые документы, подтверждающие внесение денег на «безопасный» счет и свою принадлежность к государственным органам.

Как только банки приняли меры к «охлаждению» операций по счетам клиентов, мошенники стали убеждать жертву в том, что вот-вот придут сотрудники полиции, проведут обыск и заберут из дома все деньги и ценности в связи с информацией о причастности к финансированию ВСУ.

Сразу предлагают выход — все имеющиеся деньги внести на безопасный счет, сдать имущество в ломбард или передать курьерам.

Фактически это стало аналогом квартирной кражи, только собственник сам выносит свое имущество и передает курьеру. При этом в полицию, естественно, сразу никто не обращается, проходит время, и жертва забывает о том, как выглядел этот курьер, что усложняет его поиски и привлечение к ответственности.

Условно сценарии обмана, использующиеся мошенниками, можно объединить в шесть групп:

- Звонки от имени представителей правоохранительных органов и Банка России
- Звонки от представителей малых групп (Face boss)
- Взлом аккаунтов Госуслуг и мессенджеров (дальнейшая кража персональных данных, оформление микрозаймов, кредитов, рассылка сообщений о срочной материальной помощи в случае получения доступа к аккаунту в мессенджере)
- Фишинг (направление ссылок, переход на зеркальные сайты по оказанию услуг, продаже товаров)
- Рассылка файлов с программами удаленного доступа к управлению устройством (вредоносные программы для получения персональных данных, а также программы, позволяющие удаленно управлять телефоном, в том числе имеющимися на нем банковскими приложениями, и переводить денежные средства со счетов)
- Предложения инвестирования в несуществующие интернет-проекты для получения высоких доходов

Успех мошенника зависит от того, насколько полной информацией о своей жертве он обладает. Утекшие базы с персональными данными — главный источник для «развода», а в совокупности с возможностями технологии дипфейка это позволяет мошенникам разыгрывать самые правдоподобные сценарии и отбирать у граждан все их накопления.

21%

компаний, по данным открытых источников, пострадал от мошенничества с применением дипфейка. Наиболее уязвимым каналом использования дипфейков стали социальные сети. Самая серьезная угроза — подмена голоса руководителя. С развитием технологий 5G (скорость передачи данных) качество дипфейков будет только улучшаться.

Бытует мнение, что жертвы киберпреступлений — это люди пенсионного возраста. Но это далеко не так. В истекшем году от действий мошенников пострадали 344 тысячи человек, из них только 23,9% — пенсионеры.

На уловки мошенников чаще попадаются лица в возрасте от 25 до 44 лет. Это молодые, активные люди, пользующиеся современными достижениями информационного пространства, маркетплейсами, интернет-ресурсами, системами электронных расчетов. Они уверены в собственных знаниях, активно пользуются социальными сетями, в которых оставляют о себе личные сведения, что делает их уязвимыми для мошенников.

В ходе расследования уголовных дел мы полностью установили механику воздействия мошенников на своих жертв, начиная от особенностей работы человеческого мозга до применяемых методик воздействия и целей преступников.

Для чего мы это сделали? Чтобы разработать эффективные меры противодействия.

Поддаются этому воздействию люди с особенными личностными качествами, недостаточно осведомленные о работе банковского сектора и органов правоохраны. А также те, кто излишне уверены в себе и считают, что не поддадутся этому обману.

Находясь под таким воздействием, они не только отдают свои денежные средства, но и способны причинить вред себе и окружающим.

Существует психологическое определение этому состоянию — фасцинация, означающая такое действие сигнала, при котором ранее принятая информация полностью или частично стирается, создавая эффект повышения воздействия информации на поведение.

Нахождение жертв в таком состоянии подтверждается в ходе допросов как потерпевших, так и свидетелей (первый контакт с жертвой: менеджеры кредитных организаций, риелторы, нотариусы), которые характеризуют состояние в момент совершения преступления «как под гипнозом», «как в тумане».

Накопив эмпирический материал, мы разработали меры профилактики как для тех, кто уже попался на уловки, так и для тех, кто еще не стал жертвой.

Сценарии мошенников вызывают испуг у жертвы, который возникает из-за отсутствия необходимых для адекватной реакции знаний.

«В ходе расследования уголовных дел мы полностью установили механику воздействия мошенников на своих жертв, начиная от особенностей работы человеческого мозга до применяемых методик воздействия и целей преступников.

Поэтому никакие технологические и законодательные меры не помогут без системного и постоянного просвещения всех групп населения. Воспитывать критическое мышление и обучать цифровой гигиене необходимо начиная со школьного возраста.

Отражая атаки мошенников, мы стали участниками гибридной войны, в которой гражданами управляют с помощью эмоций не только для получения денежных средств, но и используют для нанесения вреда интересам государства в целом. Ее задача — «взлом личности» с помощью использования уязвимостей человеческого мозга, который рассматривается как поле битвы XXI века. Такая война имеет всеобщий охват — от отдельных людей до государств и транснациональных корпораций.

Поэтому такие преступления направлены на подрыв устоев государства и не могут быть в разряде традиционных, а возможность управления человеком выводит их на новый уровень с переводом в категорию особо опасных. Предлагаю обратить внимание на необходимость новых исследований в данной области.

РЕГУЛИРОВАНИЕ ФИНАНСОВОГО РЫНКА ДЛЯ ЗАЩИТЫ ОТ КИБЕРМОШЕННИЧЕСТВА: НОВЫЕ МЕРЫ И ИНИЦИАТИВЫ

Текущее состояние проблемы кибермошенничества свидетельствует о том, что назрела необходимость качественного изменения подходов к совершенствованию действующих инструментов защиты. Постоянное появление новых схем и сценариев для хищения денег, вовлечение граждан, в том числе молодежи, в дропперскую деятельность, рост объемов кредитного мошенничества — эти и другие вызовы требуют внедрения комплексных механизмов противодействия. Их эффективность напрямую зависит от способности действовать на опережение злоумышленников и учитывать риски социальной инженерии. Банк России разрабатывает и внедряет соответствующие подходы к борьбе с кибермошенничеством в финансовой сфере, решение этой задачи находится в фокусе пристального внимания регулятора.

ГЕРМАН ЗУБАРЕВ
Заместитель Председателя Банка России

Для объективной оценки объемов кибермошенничества Банк России ориентируется на отчетность финансовых организаций об операциях без добровольного согласия их клиентов. Банки составляют свою отчетность на основании обращений граждан, которые пострадали от действий злоумышленников. По имеющимся в Банке России данным, в 2024 году мошенники похитили 27,5 млрд рублей, что значительно превышает аналогичный показатель предыдущего года.

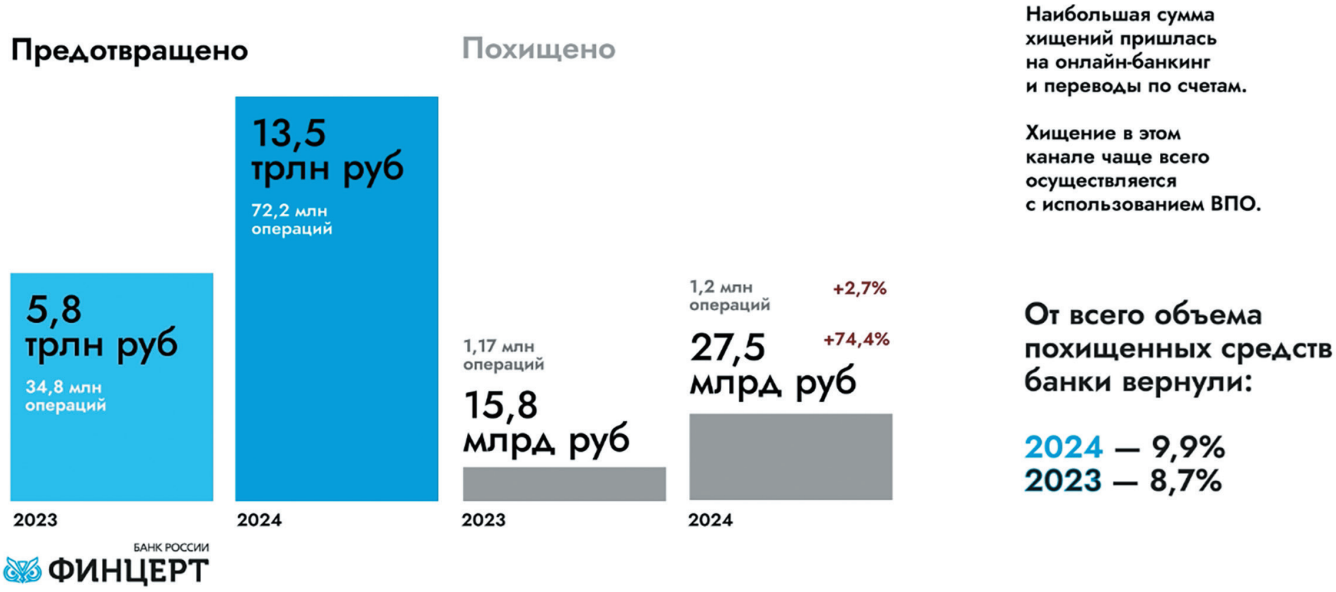
При этом потери могли бы быть еще больше, если бы не защитные системы банков. Они отразили более 72 млн попыток мошенников совершить хищение средств со счетов клиентов. Это позволило спасти от злоумышленников рекордную сумму — 13,5 трлн рублей[1]. Эффективность систем защиты от мошеннических списаний со счетов физических лиц у наиболее крупных кредитных организаций стабильно высокая и в прошлом году превысила 99,7%.

Повышению качества работы антифрод-систем банков способствовала системная работа Банка России по совершенствованию действующих норм.

Так, в 2024 году регулятор вдвое расширил перечень признаков мошеннических операций[2], которыми должны руководствоваться банки для предотвращения подозрительных переводов. В дополнение к ранее действующим признакам кредитные организации обязаны учитывать информацию, которую получают в рамках прямых договоров с опе-

[1] Ежегодные обзоры операций, совершенных без добровольного согласия клиентов финансовых организаций, опубликованы на официальном сайте Банка России (http://cbr.ru/analytics/ib/operations_survey/2024/).
[2] Приказ Банка России от 27.06.2024 № ОД-1027 «Об установлении признаков осуществления перевода денежных средств без добровольного согласия клиента и отмене приказа Банка России от 27.09.2018 № ОД-2525».

МОШЕННИЧЕСКИЕ ОПЕРАЦИИ: СТАТИСТИКА



раторами связи: о нехарактерной телефонной активности клиента перед переводом денег, о росте числа входящих смс-сообщений с новых номеров, в том числе в мессенджерах. Другие новые критерии — наличие информации о возбужденном уголовном деле в отношении получателя средств по фактам, связанным с совершением мошеннических операций, а также информация из внутренних перечней банков о совершении подозрительных переводов.

Кроме того, Банк России обязал крупные банки вносить в свои антифрод-системы реквизиты злоумышленников из базы данных Банка России «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента» (далее — база данных Банка России) в течение часа, остальные банки — в течение 3 часов с момента их получения[3].

База данных Банка России содержит большое количество параметров — уникальных идентификаторов, в том числе сведения о совершенных операциях, о плательщиках и получателях денежных средств (номер телефона, номер счета и карты, документа, удостоверяющего личность, ИНН и другие). Этими данными Банк России обменивается со всеми кредитными организациями для повышения качества их антифрод-процедур.

Не менее важно для повышения качества информационного обмена и, как следствие, работы антифрод-систем банков, чтобы как можно больше пострадавших от действий мошенников обращались с заявлениями в свои банки и информация о злоумышленниках быстрее поступала в базу данных Банка России. Поэтому регулятор обязал[4] крупные банки до 01.10.2025 доработать мобильные версии своих приложений, чтобы гражданин мог подать заявление о мошеннической операции без посещения банка и получить справку об этой операции для предоставления в полицию.

Кроме того, к этому времени банки должны будут обеспечить возможность приема и регистрации заявлений граждан о случаях за-

[3] Указание Банка России от 19.08.2024 № 6828-У «О порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных, о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, порядке запроса и получения Банком России у них информации о переводах денежных средств, связанных с переводами денежных средств без добровольного согласия клиента, в отношении которых от федерального органа исполнительной власти в сфере внутренних дел получены сведения о совершенных противоправных действиях в соответствии с частью 8 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе", а также о порядке реализации ими мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента».

[4] Положение Банка России от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (далее — Положение Банка России № 851-П).

числения наличных денег на счета злоумышленников под их воздействием с использованием токенизированных карт через банкоматы. При этом не важно, является пострадавший клиентом этого банка или нет.

Особое внимание в работе по противодействию кибермошенничеству Банк России уделяет борьбе с дропперством — деятельностью по выводу и обналичиванию похищенных денег.

В частности, налажена комплексная реализация принятых при участии Банка России законов[5], которые значительно усложнили деятельность злоумышленников. В соответствии с их положениями Банк России и МВД России осуществляют автоматизированный информационный обмен сведениями о мошеннических операциях практически в онлайн-режиме. Это значительно сокращает время получения информации, необходимой для расследования фактов мошенничества и уголовных дел. Кроме того, с 25.07.2024 банки обязаны блокировать электронные средства платежа (карты и онлайн-банкинг) дропам, если информация об их противоправной деятельности поступила от МВД России. С этого же периода все переводы на счета дропов, информация о которых содержится в базе данных Банка России, приостанавливаются на 2 дня.

Результаты мониторинга Банка России свидетельствуют об эффективности этих механизмов. Минимальное время ответа Банка России на запросы правоохранительных органов о мошеннических операциях составляет от 1 минуты. Ежемесячно в адрес регулятора поступает около 20 тысяч таких запросов. За прошлый год общее количество сведений о злоумышленниках, которые Банк России аккумулирует в своей базе данных о мошеннических операциях, увеличилось практически в 1,5 раза. Это значит, что в отношении все большего числа дропов применяются ограничительные меры, предусмотренные законодательством, в том числе блокировка дистанционного банковского обслуживания.

Крупные банки ежемесячно приостанавливают около 300 тысяч переводов на реквизиты из базы данных Банка России. Банки также блокируют карты и онлайн-банкинг всем лицам, в отношении которых от правоохранительных органов в Банк России поступили сведения о возможной причастности к хищениям денег. Только в 1-й день действия Закона одномоментно был заблокирован доступ к 30 тысячам электронных средств платежа злоумышленников. По счетам остальных лиц из базы данных Банка России фиксируется значительное снижение транзакционной активности. После того как реквизиты платежной карты мошенника попадают в базу, транзакционная активность по ним снижается в 40 раз. Таким образом, платежные карты и другие электронные средства платежа становятся одноразовым инструментом деятельности дропов.

Совершенствование действующих законодательных механизмов, которые создают барьеры для дропперской деятельности, продолжается[6]:

- разработан механизм противодействия мошеннической схеме, при реализации которой человека под влиянием обмана побуждают внести наличные деньги на счет злоумышленника с использованием токенизированной карты. Так, с 01.09.2025 банки должны будут вводить ограничения по внесению наличных денежных средств на вновь токенизированные карты на общую сумму более 50 тысяч рублей в течение первых 48 часов;
- с 01.09.2025 банки не смогут выдавать новые электронные средства платежа, включая банковские карты, лицам из базы данных Банка России;
- если в отношении таких лиц кредитной организацией не был установлен запрет на использование электронных средств платежа, то с 15.05.2025 сумма их переводов себе и другим людям не может превышать 100 тысяч рублей в месяц.

Кроме того, в Законе[7] закреплена обязанность кредитных организаций с 01.09.2025 ограничить выдачу наличных денег с использованием банкоматов на сумму более 100 тысяч рублей в месяц лицам, сведения о которых (в том числе об их электронных средствах платежа) находятся в базе данных Банка России.

Учитывая, что мошенники активно вовлекают в дропперскую деятельность подростков, которые зачастую не осознают ее противоправный характер, регулятор обязал[8] банки уведомлять родителей несовершеннолетнего клиента в возрасте от 14 до 18 лет о предоставлении ему карты или онлайн-банка, а также обо всех его операциях: покупках и переводах. Информирование и его способ прописываются в договоре с банком. Эта норма заработала с 29.03.2025.

[5] Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона “О банках и банковской деятельности” и статью 27 Федерального закона "О национальной платежной системе", Федеральный закон от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон “О национальной платежной системе”».
[6] Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».
[7] Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».
[8] Положение Банка России № 851-П.

В прошлом году Банк России зафиксировал рост объемов кредитного мошенничества: чтобы увеличить сумму хищений, злоумышленники убеждают человека оформить кредит и передать им заемные деньги. В крупных банках объем похищенных кредитных денег составил 37% в сравнении с общим объемом хищений (против 25% в 2023 году). Поэтому при участии регулятора был принят комплексный закон[9], который обязывает банки и микрофинансовые организации (далее — МФО) проводить антифрод-мероприятия при выдаче кредитов и займов.

Закон предусматривает:

- введение «периода охлаждения» между заключением договора потребительского кредита (займа) и моментом перечисления кредитных денег человеку. Продолжительность «периода охлаждения» составит 4 часа, если кредит или заем оформляется на сумму от 50 тысяч до 200 тысяч рублей, и 2 дня — для сумм, превышающих 200 тысяч рублей (с 01.09.2025);
- обязанность МФО зачислять деньги на счет, только если сведения о заемщике и получателе денег совпадают (при дистанционном оформлении займа), а также отказывать в выдаче займа, если информация о заемщике содержится в базе данных Банка России о мошеннических операциях (с 01.09.2025);
- ускорение обмена информацией между кредиторами и бюро кредитных историй (далее — БКИ). Так, БКИ будут обязаны принимать информацию, направляемую банками и МФО, и передавать ее им в онлайн-режиме (с 01.07.2026). В свою очередь банки и МФО будут получать информацию из БКИ, фиксировать факт ее получения, хранить и учитывать ее в своих антифрод-процедурах (с 31.12.2026).

При выдаче кредита или займа с нарушением антимошеннических норм и при наличии возбужденного уголовного дела по факту хищения денег банк или МФО не сможет требовать исполнения заемщиком обязательств, начислять проценты и передавать долг коллекторам (с 01.09.2025).

Кроме того, с 01.03.2025 каждый гражданин может добровольно через портал Госуслуг установить в своей кредитной истории запрет на заключение с ним договоров потребительского кредита или займа[10]. Не позднее 01.09.2025 эта услуга будет доступна и в многофункциональных центрах. Запрет может быть разным: по виду кредитора (банк или МФО) или по способу обращения за кредитом или займом (в офисе и дистанционно либо только дистанционно). Если самозапрет установлен, кредитор должен отказать в выдаче кредита или займа. Этот механизм востребован — за 2 месяца им воспользовались более 10 млн человек.

Таким образом, при участии Банка России проводится активная работа по совершенствованию механизмов противодействия кибермошенничеству в финансовом секторе. Но очевидно, что для наступления переломного момента в этой борьбе необходима консолидация усилий всех заинтересованных сторон. Поэтому крайне важно, что решение этой проблемы вынесено на общегосударственный уровень. Президент Российской Федерации 01.04.2025 утвердил перечень поручений[11], в которых определены главные направления противодействия кибермошенничеству.

С учетом этих поручений Банк России в ближайшей перспективе планирует сосредоточить свои усилия на следующих основных направлениях деятельности:

- ☑ эффективной реализации новых механизмов и инструментов, предусмотренных законодательством и нормативными актами Банка России и направленных на противодействие кредитному мошенничеству, дропперству, а также на повышение качества работы антифрод-систем банков
- ☑ создании экономических и организационных барьеров для деятельности дропов, в том числе ограничении количества и срока действия платежных карт, выдаваемых банками клиентам, а также выявлении цепочек вывода и обналичивания похищенных денег в автоматизированном режиме
- ☑ участии в организации системного обмена данными о кибермошенниках между правоохранительными органами, Банком России, кредитными организациями, операторами связи и другими участниками рынка

[9] Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».
[10] В соответствии с Федеральным законом от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон “О кредитных историях”» и Федеральный закон "О потребительском кредите (займе)"».
[11] Перечень поручений Президента Российской Федерации по итогам совещания с членами Правительства от 01.04.2025 № Пр-706.

ОСОБЕННОСТИ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ СФЕРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ситуация в экономике и финансовой сфере постоянно меняется. Мы являемся свидетелями таких изменений на микро- и макроуровнях, в масштабах государств и целых континентов.

МУХАРБИЙ УЛЬБАШЕВ

Сенатор Российской Федерации, первый заместитель председателя Комитета Совета Федерации по бюджету и финансовым рынкам, член Национального финансового совета

Для всех очевидно, что глобальным трендом финансовой сферы, который определяет ее развитие, является повсеместная цифровизация и широчайшее внедрение цифровых технологий. Наша страна по праву занимает здесь лидирующие позиции. Как отметил Президент Российской Федерации Владимир Владимирович Путин в ходе инвестиционного форума «Россия зовет», уровень цифровизации финансовых услуг в России превышает общемировой, что подтверждает высокую технологичность этой сферы отечественной экономики, ее устремленность в будущее, умение ставить большие цели и работать на опережение.

Оборотной стороной развития цифровых технологий является резкий рост числа киберугроз в отношении наших граждан и организаций. И на повестке дня остро стоят вопросы совершенствования форм и методов работы в области противодействия таким угрозам на всех уровнях.

Здесь у законодателей особая роль — сформировать тот нормативный базис, который позволял бы адекватно и своевременно реагировать на возникающие вызовы, а в идеале — быть на шаг или несколько шагов впереди злоумышленников.

Текущий год ознаменовался принятием и вступлением в силу целого блока таких базисных законов. Один из них касается введения возможности установления гражданами добровольного самозапрета на заключение договоров потребительского кредитования. Этот действенный защитный механизм оказался в высшей степени востребованным. Соответствующий сервис на портале Госуслуг заработал с 1 марта этого года, и по настоящее время оформлено уже более 10 млн самозапертов.

Два принятых в этом году закона непосредственно посвящены мерам противодействия кибермошенничеству. Первый разработан сенаторами Российской Федерации совместно с депутатами Государственной Думы. Им вводится в том числе так называемый период охлаждения при выдаче потребительских кредитов: на сумму от пятидесяти до двухсот тысяч — на четыре часа, свыше двухсот тысяч — на двое суток. Кроме того, теперь на токенизированные (виртуальные) карты банки не смогут зачислять больше 50 тысяч рублей в течение 48 часов с момента их выпуска. Сейчас злоумышленники активно используют для обмана людей цифровые карты.

Второй закон — это комплексный антимошеннический закон, разработанный и внесенный Правительством Российской Федерации. Законом, в частности, создается единая информационная база противодействия мошенническим действиям, устанавливается обязательная маркировка звонков от организаций на экране телефона, запрещаются звонки от имени госорганов и сотрудников банков через мессенджеры гражданам, предусматривается запрет на передачу сим-карт третьим лицам и вводится возможность установления гражданам самозапрета на их дистанционное оформление.

Особенностью этих законов являются четко проработанные с точки зрения юридической техники механизмы защиты наших граждан от противоправных действий третьих лиц. Именно такой подход позволит сделать законодательство действенным и эффективным.

В свою очередь, такая глубокая проработка создаваемых норм возможна только в результате взаимодействия органов законодательной и исполнительной ветвей власти на всех этапах нормотворчества. В работе над законопроектами принимают активное участие Банк России, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерство финансов Российской Федерации, Министерство внутренних дел Российской Федерации, Министерство экономического развития Российской Федерации и другие ведомства.

Особое место в этой сложившейся системе эффективного взаимодействия занимает наша совместная работа с Федеральной службой по финансовому мониторингу.

Совет Федерации благодарен директору Росфинмониторинга Юрию Анатольевичу Чиханчину, статс-секретарю — заместителю директора службы Герману Юрьевичу Негляду и всем ее сотрудникам за профессиональное участие в мероприятиях и обсуждениях, инициированных сенаторами Российской Федерации.

Так, в апреле текущего года в Совете Федерации был проведен круглый стол «Укрепление национальной и международной финансовой безопасности» при непосредственном участии Росфинмониторинга. По итогам состоявшегося обсуждения был подготовлен документ, содержащий конкретные предложения по совершенствованию законодательства и правоприменительной практики. В документе еще раз подчеркивается, что минимизировать риски национальной и международной финансовой безопасности возможно только совместными усилиями общества, государства, а также международного сообщества, применяя все доступные средства противодействия преступности, включая просветительскую работу.

В рамках дальнейшего совершенствования законодательства в сфере противодействия киберугрозам и финансовой безопасности граждан продолжается работа над вторым пакетом антифрод-законопроектов с учетом имеющихся наработок и правоприменительной практики. Особое внимание уделяется комплексу законодательных мер, направленных на пресечение деятельности дропперов. И здесь важно помнить, что под ударом мошенников находится подрастающее поколение. Статистика неумолима — подростки часто обманом, часто за небольшие деньги втягиваются в противоправную деятельность киберпреступников. Однако при разработке защитных мер мы неизбежно сталкиваемся с тем, что соответствующие нормы будут иметь ограничительную природу в чувствительной для граждан банковской сфере, например, касаться ограничения количества дебетовых карт в одних руках, предусматривать обязательное согласие родителей при открытии счета несовершеннолетними лицами с 14 до 18 лет и т. д. Представляется, что задача законодателей в данном случае — определить разумный баланс ограничительных мер и сохранения для граждан возможности реализации своих прав и законных интересов.

Для дальнейшего развития законодательного регулирования в сфере международной финансовой безопасности расширяется наше взаимодействие в рамках международных площадок. При этом совместная работа именно с парламентариями дружественных государств представляется особенно перспективной в целях гармонизации национального и международного законодательства. Так, на площадке Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) при поддержке Председателя Совета Федерации Федерального Собрания Российской Федерации Валентины Ивановны Матвиенко и директора Федеральной службы по финансовому мониторингу Юрия Анатольевича Чиханчина был создан Форум парламентариев государств — членов ЕАГ. Особенно лестно, что председателем Форума был избран представитель Российской Федерации, заместитель Председателя Совета Федерации Федерального Собрания Российской Федерации Николай Андреевич Журавлев.

Уже проведены четыре форума — в Душанбе в 2022 году, в Алматы в 2023 году, в Бишкеке в 2024 году и в Москве в 2025 году. По результатам форумов были приняты декларации, которые касаются важных практических аспектов взаимодействия участников на законодательном уровне и служат ориентиром для работы над совершенствованием внутреннего законодательства. Четвертый Форум парламентариев государств — членов ЕАГ в Москве в мае этого года прошел с участием значительного количества стран – членов ЕАГ и наблюдателей и стал серьезной площадкой для выработки решений и рекомендаций, которые обязательно будут учтены в законотворческой деятельности парламентариев.

Таким образом, в условиях развития информационных технологий в финансовой сфере и роста киберугроз вследствие этого перед законодателями стоит задача на постоянной основе, последовательно, скрупулезно, учитывая правоприменительную практику, работать над совершенствованием законодательства по противодействию этим угрозам, активно используя опыт межпарламентского взаимодействия.

БЕЛОРУССКИЙ ОПЫТ ВЗАИМОДЕЙСТВИЯ КОМПЕТЕНТНЫХ ОРГАНОВ

В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ И ПРЕСЕЧЕНИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ СКАМ-ГРУПП

Активное использование возможностей и результатов цифрового развития, сети Интернет, дистанционного банковского обслуживания, онлайн-услуг маркетплейсов и виртуальных игорных заведений обусловило в Республике Беларусь на протяжении последних лет рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе посредством фишинга.

АНДРЕЙ МОТОЛЬКО

Начальник главного управления цифрового развития предварительного следствия центрального аппарата Следственного комитета Республики Беларусь, полковник юстиции

Если в 2016 году количество хищений путем модификации компьютерной информации составляло 1844, то уже через пять лет в 2020 году количество таких преступлений увеличилось в 12 раз и достигло 23 587.

В ходе проводимых в Следственном комитете Республики Беларусь мероприятий и принимаемых мер по противодействию киберпреступности было установлено, что абсолютное большинство хищений с использованием ИКТ совершаются путем фишинга с применением поддельных интернет-ресурсов.

По результатам проведенной следственной и аналитической работы сотрудниками Следственного комитета Республики Беларусь были установлены три организованные преступные скам-группы[1], осуществлявшие хищение денежных средств посредством фишинга у пользователей белорусских торговых интернет-площадок.

Общее количество совершенных указанными скам-группами преступлений за последние три года превысило 20 тыс., а общий размер похищенных денежных средств составил более 2,5 млн долларов США.

В состав организованных преступных скам-групп на протяжении 2022–2024 годов в различные периоды входило в общей сложности более 2 тыс. участников, которые, как правило, не знали друг друга, общались посредством мессенджеров, дислоцировались в разных странах постсоветского пространства, ближнего и дальнего зарубежья.

В рамках расследуемого главным управлением цифрового развития предварительного следствия центрального аппарата Следственного комитета Республики Беларусь уголовного дела по преступлениям, предусмотренным статьей 212 Уголовного кодекса Республики Беларусь (хищение путем модификации компьютерной информации), следователями проведен комплекс мероприятий, по результатам которых удалось получить доступ к ин-

[1] Скамеры — интернет-мошенники, которые выманивают деньги или данные пользователя.

формационным ресурсам преступных скам-групп, детально изучить их структуру, механизм совершения фишинговых преступлений в отношении пользователей белорусских маркетплейсов, а также схему отмывания доходов, полученных преступным путем.

Схема хищения выглядела следующим образом. Преступник под предлогом приобретения размещенного потерпевшим на маркетплейсе товара предлагал оплатить товар и забрать его курьером, в этих целях отправлял потерпевшему специально сгенерированную ссылку на фишинговый интернет-ресурс, на котором потерпевший вводил реквизиты своей платежной банковской карточки, с которой в последующем похищались денежные средства.

Преступниками использовались следующие схемы отмывания похищенных денежных средств:

- путем перечисления денежных средств на расчетные счета подставных лиц (дропов) с последующим обналичиванием дропами денежных средств либо переводом за рубеж на банковские счета иностранных дропов (Российская Федерация, Казахстан и др.)
- путем совершения криптообменных операций и перевода похищенных фиатных денег в цифровые активы
- путем совершения ставок в онлайн-казино и участия в играх в виртуальных игорных заведениях с целью легализации похищенного под видом выигрыша

В целях принятия мер по пресечению предикатной преступной деятельности и противодействию отмыванию преступного дохода были осуществлены мероприятия по организации взаимодействия по следующим направлениям.

1. Организация должного взаимодействия с компетентными органами и заинтересованными организациями Республики Беларусь:

- подразделением финансовой разведки;
- субъектами оперативно-разыскной деятельности;
- торговыми интернет-площадками (маркетплейсами);
- интернет- и хостинг-провайдерами;
- банковскими учреждениями;
- операторами обмена криптовалюты и криптоплатформ;
- виртуальными игорными заведениями;

2. Организация международного сотрудничества с компетентными учреждениями иностранных государств:

- Федеральной службой по финансовому мониторингу (Российская Федерация);
- Агентством Республики Казахстан по финансовому мониторингу;
- Следственным департаментом МВД России;
- Управлением по организации борьбы с противоправным использованием ИКТ МВД России;
- Главным управлением криминалистики Следственного комитета Российской Федерации.

В первую очередь в ходе следствия был налажен канал оперативного онлайн-обмена информацией между следователями и специалистами белорусских маркетплейсов, которые, получив от следствия необходимую информацию и осуществив ряд технических мер, уже по истечении нескольких часов устраняли уязвимости, блокировали преступный инструмент и удаляли фейковые аккаунты преступников на торговых интернет-площадках.

Принимая во внимание, что основным способом хищения являлся фишинг, в ходе расследования уголовного дела был выработан алгоритм оперативного взаимодействия с белорусскими поставщиками интернет-услуг, в том числе операторами сотовой связи, по принятию мер, связанных с ограничением доступа в национальном сегменте сети Интернет к фишинговым интернет-ресурсам, используемым в преступной деятельности. Налажено взаимодействие с белорусскими и российскими компаниями, осуществляющими услуги по регистрации доменов в целях принятия мер по оперативной блокировке фишинговых веб-страниц, используемых преступниками для совершения хищений.

Учитывая, что в рамках отмывания и легализации похищенных скам-группами посредством фишинга денежных средств осуществлялось их перечисление на расчетные счета подставных лиц (дропов) с последующим обналичиванием либо переводом за рубеж на иностранные счета (Российская Федерация, Казахстан и др.), актуальным стал вопрос наличия возможности быстрого обмена информацией между банковскими учреждениями и следственными органами о подозрительных операциях по банковскому счету и возможности их оперативной блокировки.

В связи с этим при содействии Национального банка Республики Беларусь был разработан и внедрен алгоритм получения следователями из банковских учреждений информации, содержащей банковскую тайну, в электронном виде посредством Автоматизированной информационной системы представления банковской информации (АИС ПБИ), обеспечивший быстрое взаимодействие с банковскими учреждениями в электронном формате.

Кроме этого, с марта 2024 года с внедрением в Республике Беларусь Автоматизированной системы обработки инцидентов Национального банка Республики Беларусь (АСОИ) у правоохранительных органов Республики Беларусь появилась возможность оперативно блокировать движение денежных средств по используемым в преступной деятельности банковским счетам и тем самым препятствовать выводу похищенных денежных средств.

В ходе следствия было установлено, что значительная часть денежных средств, дистанционно похищаемых у жителей Беларуси участниками скам-групп из-за рубежа, отмывалась посредством обмена на цифровые активы. Скамеры использовали широкую вовлеченность белорусских граждан в криптовалютный обмен, переводя на счета указанных граждан похищенные фиатные деньги и получая взамен на свои криптокошельки криптовалюту. Было также установлено, что в качестве легализации преступного дохода под видом выигрыша использовались услуги онлайн-казино и других виртуальных игорных заведений.

В связи с этим был налажен постоянный обмен информацией с белорусским регулятором криптоиндустрии — Парком высоких технологий, операторами криптоплатформ и операторами обмена криптовалют, а также с белорусскими игорными заведениями.

По результатам взаимодействия с Департаментом финансового мониторинга Комитета государственного контроля Республики Беларусь в ходе предварительного следствия были получены криминалистически значимые сведения в отношении отдельных физических и юридических лиц, чьи банковские счета использовались при отмывании похищенных денежных средств.

В свою очередь, Следственным комитетом Республики Беларусь в адрес Департамента финансового мониторинга Комитета государственного контроля Республики Беларусь для последующего анализа и выработки мер противодействия были предоставлены полученные в ходе расследования сведения относительно схем легализации похищенных денежных средств с использованием криптообменных сервисов.

Из Федеральной службы по финансовому мониторингу (Российская Федерация) и Агентства Республики Казахстан по финансовому мониторингу получены сведения в отношении российских и казахских граждан, фигурирующих в цепочке перечислений похищенных денежных средств, а также при совершении криптообменных операций. При содействии Росфинмониторинга была получена криминалистически значимая информация по результатам анализа отдельных транзакций в блокчейне посредством использования российского сервиса мониторинга и анализа криптовалютных транзакций.

«Скамеры использовали широкую вовлеченность белорусских граждан в криптовалютный обмен, переводя на счета указанных граждан похищенные фиатные деньги и получая взамен на свои криптокошельки криптовалюту.

В рамках взаимодействия с Департаментом финансовой разведки Комитета государственного контроля Республики Беларусь и Главным управлением по противодействию киберпреступности МВД Республики Беларусь организовано оперативное сопровождение по уголовному делу и проведен комплекс необходимых оперативно-розыскных мероприятий по поручению следователей.

В ходе следствия было установлено, что от действий участников преступных скам-групп также пострадали граждане Российской Федерации, которые перешли на фишинговые веб-страницы, в результате чего с их карт-счетов были похищены денежные средства. В рамках международного сотрудничества Следственным департаментом МВД России предоставлены сведения в отношении потерпевших российских граждан, проведены с их участием следственные и процессуальные действия в рамках оказания международной правовой помощи.

При содействии Главного управления криминалистики Следственного комитета Российской Федерации в результате проведенных российскими коллегами криминалистической разведки методом OSINT и иных мероприятий по особой методике были получены важные для белорусского следствия сведения, позволившие впоследствии установить личности участников организованной преступной скам-группы и принять меры по их задержанию.

По результатам предварительного расследования по уголовному делу с учетом организации должного взаимодействия Следственного комитета Республики Беларусь с компетентными органами и заинтересованными организациями, эффективного международного сотрудничества были установлены личности 110 участников преступных скам-групп из числа граждан Республики Беларусь. Был также установлен организатор и «кодер» (основной разработчик преступного программного обеспечения) одной из преступных скам-групп — житель г. Минска, 2005 г. р.

С учетом собранных доказательств 39 лицам, включая трех руководителей, по расследуемому уголовному делу было предъявлено обвинение

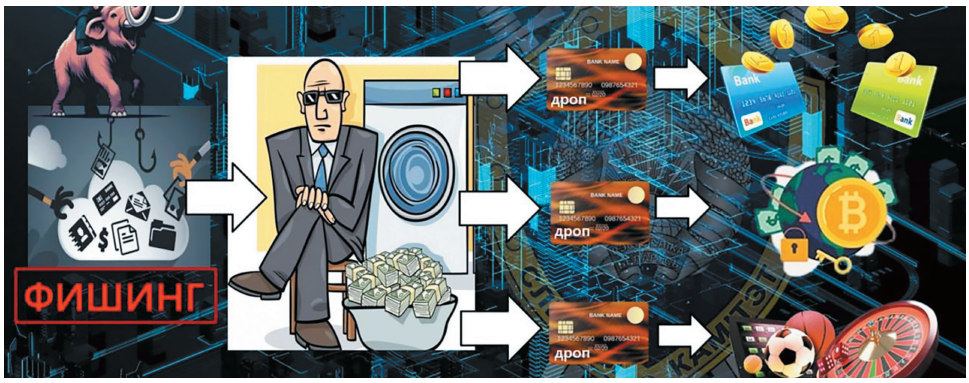
в совершении преступлений. В отношении 30 из них уголовные дела направлены в суд, где по результатам судебного разбирательства в отношении них вынесены обвинительные приговоры.

Необходимо отметить, что досудебное производство по уголовному делу до настоящего времени не окончено. В одном производстве соединено более 2 тыс. уголовных дел. Устанавливаются дополнительные факты преступной деятельности.

Кроме этого, во взаимодействии с Управлением по организации борьбы с противоправным использованием ИКТ МВД России проведен комплекс совместных мероприятий по установлению участников скам-групп из числа российских граждан. В результате проделанной работы на территории Российской Федерации установлено 10 исполнителей преступной деятельности и один руководитель организованной преступной скам-группы. В установленном порядке в МВД России направлены просьбы об оказании международной правовой помощи в части проведения обысков и иных следственных действий с участием указанных лиц.

Одновременно Следственным комитетом Республики Беларусь выделены из уголовного дела и направлены в МВД России для осуществления уголовного преследования материалы в отношении гражданина Российской Федерации, организатора одной из преступных скам-групп. По результатам проведенного следственным управлением УМВД России по г. Брянску расследования фигуранту предъявлено обвинение в совершении хищения денежных средств с банковского счета в составе организованной группы, уголовное дело передано в суд, которым виновный осужден к лишению свободы.

СХЕМА ОТМЫВАНИЯ ДОХОДОВ



В рамках принятия мер по предотвращению совершения преступлений в ходе предварительного следствия по уголовному делу были применены инновационные подходы. Так, в целях пресечения совершаемых хищений, получив доступ к преступным программным продуктам и подробно изучив механизм совершения преступных деяний, белорусские следователи с учетом имеющихся технических навыков и умений модифицировали разработанное скамерами программное обеспечение. В результате проделанной работы последние шесть цифр в реквизитах платежных банковских карт, получаемых участниками преступной скам-группы с фишинговых веб-страниц от потерпевших, стали автоматически рандомно меняться, что сделало невозможным дальнейшее хищение денежных средств по искаженным реквизитам.

В целом благодаря принятым мерам во взаимодействии с маркетплейсами, интернет- и хостинг-провайдерами, банковскими учреждениями, операторами криптоплатформ и виртуальных игорных заведений, в тесном международном сотрудничестве с подразделениями финансовой разведки и правоохранительными органами преступная деятельность трех организованных преступных скам-групп в отношении белорусских граждан была пресечена, а сами они, распавшись, прекратили свою деятельность.

Как результат, в Республике Беларусь удалось не только остановить тенденцию роста фишинговых преступлений, но и значительно снизить уровень данной преступности. Так, количество хищений путем модификации компьютерной информации снизилось с 23 587 в 2020 году до 6 307 преступлений в 2024 году.

В рамках принимаемых мер по повышению профессиональной подготовки следователей по результатам расследования с учетом наработанного опыта по материалам уголовного дела по фактам фишинга скам-группами совместно с Институтом Следственного комитета Республики Беларусь, следователями и сотрудниками указанного учреждения образования было подготовлено и издано в 2024 году учебное пособие «Особенности расследования интернет-мошенничеств, совершенных организованными скам-группами».

Кроме этого, основываясь на материалах уголовного дела и результатах следствия, в Институте Следственного комитета Республики Беларусь с 2023 года организованы учебные занятия для следователей по образовательной программе повышения квалификации «Особенности расследования киберпреступлений, совершенных организованной группой».

ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ КАК ИНСТРУМЕНТ ДОВЕРИЯ И БЕЗОПАСНОСТИ: ОПЫТ КАЗАХСТАНА

Современные финансовые и технологические сервисы развиваются в стремительном темпе, предлагая клиентам удобные и быстрые способы доступа к услугам. Однако рост цифровизации несет в себе и серьезные риски — в первую очередь связанные с мошенничеством. В ответ на это цифровая идентификация становится не просто инструментом верификации личности, но и важным элементом в системе противодействия финансовому мошенничеству.

МАКСАТ ШАГДАРОВ
Главный комплаенс-контролер АО «Altyn Bank» (ДБ China CITIC Bank Corporation Ltd)

Цифровая идентификация — это процесс установления и подтверждения личности клиента с использованием электронных средств, таких как биометрические данные, электронные подписи, технологии NFC, видеоидентификация и другие цифровые решения. В отличие от традиционной идентификации этот подход позволяет проводить процесс удаленно, быстро и, при должной защите, безопасно.

Международные стандарты (например, Рекомендации ФАТФ, Базельский комитет, директивы ЕС) допускают использование цифровой идентификации при соблюдении условий безопасности, достоверности и независимости механизмов верификации. Это находит отражение и в национальных нормативных актах.

Регуляторы подчеркивают необходимость оценки рисков при внедрении цифровых решений. Это включает:

- учет уровней риска клиентов (Risk-Based Approach);
- проверку на наличие в санкционных и террористических списках;
- проведение углубленной проверки (Enhanced Due Diligence) для высокорисковых клиентов — особенно важно для дистанционного обслуживания;
- хранение и прозрачный аудит данных идентификации и операций.

При этом цифровые технологии позволяют автоматизировать многие проверки, делая процедуры более эффективными и прозрачными.

Во многих странах, включая Казахстан, внедрение цифровой идентификации поддерживается на государственном уровне. Регуляторы разрабатывают стандарты и правовые рамки, обеспечивающие законность и безопасность таких решений. В частности:

- требования по удаленной идентификации в рамках законодательства о противодействии легализации доходов (AML/CFT);
- стандарты KYC (Know Your Customer) и eKYC;
- регламенты обработки персональных и биометрических данных.

Внедрение цифровой идентификации требует соблюдения принципов privacy by design, а также прозрачности в отношении клиентов.

В ближайшие годы ожидается также широкое внедрение:

- децентрализованных идентификаций на базе технологии blockchain (Self-Sovereign Identity);
- единых цифровых удостоверений (цифровой ID гражданина);
- интеграции с государственными и международными платформами для трансграничной идентификации.

Эти изменения сделают процессы еще более надежными и масштабируемыми, но при этом потребуют от организаций гибкости и адаптации под новые риски.

В Казахстане использование цифровой идентификации регулируется законодательством, а также обеспечивается подключением к соответствующим сервисам:

- Закон РК «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- требования к надлежащей проверке клиентов в случае дистанционного установления деловых отношений;
- интеграция с цифровыми госуслугами (например, ЭЦП, eGov Mobile, сервисы НАО «Государственная корпорация «Правительство для граждан»).

В условиях цифровой трансформации финансовой отрасли вопросы надежной идентификации клиентов и эффективной защиты от мошенничества приобретают первостепенное значение.

Цифровая трансформация открыла путь новым видам мошенничества, таким как:

- кража и подделка цифровых идентификаторов
- использование дипфейк – технологии для обхода видеоверификации
- социальная инженерия и фишинг, направленные на получение доступа к учетным данным
- создание поддельных аккаунтов и «мошеннических клиентов» для отмывания денег

Эти угрозы требуют от финансовых организаций внедрения многоуровневых механизмов идентификации, сочетающих удобство и высокий уровень надежности.

Эффективная защита возможна при комплексном подходе. Современные антифрод-системы все

чаще интегрируются с решениями цифровой идентификации.

АО «Altyn Bank» (ДБ China CITIC Bank Corporation Ltd), один из технологических лидеров банковского сектора Казахстана, демонстрирует системный подход к построению цифровой среды, в которой сочетаются удобство, безопасность и строгое соблюдение требований законодательства, включая меры по противодействию отмыванию доходов и финансированию терроризма (ПОД/ФТ), не создавая лишней нагрузки на клиента.

АО «Altyn Bank» активно внедряет электронную идентификацию клиентов (eKYC) — удаленную процедуру установления личности, основанную на современных технологиях. Клиенты могут пройти идентификацию онлайн через видеоверификацию, биометрические данные и проверку через государственные реестры.

Этот подход обеспечивает не только комфорт при подключении к банковским продуктам, но и высокий уровень достоверности и контроля. Все этапы идентификации фиксируются, шифруются и соответствуют требованиям регуляторов, включая Агентство РК по регулированию и развитию финансового рынка и Министерство цифрового развития и аэрокосмической промышленности.

Ключевые технологии, применяемые АО «Altyn Bank»:

- видеоидентификация с элементами антиспуфинга — осуществление видеофиксации клиента в приложении банка с использованием защиты от подделки изображений и видео, а также защиты от дипфейк - технологий
- биометрическая аутентификация — распознавание лица клиента при доступе к сервисам по фото- и видеоизображению
- интеграция с eGov и базами данных — мгновенная сверка подлинности документов с государственными базами данных физических лиц
- безбумажные процессы — цифровая подача заявлений и дистанционное открытие счетов
- сквозной анализ данных — сопоставление данных клиента с внешними источниками, государственными реестрами, черными списками
- AI-алгоритмы для оценки риска — прогнозирование мошенничества на основе машинного обучения и анализа больших данных

Для борьбы с цифровыми угрозами АО «Altyn Bank» внедрил многоуровневую антифрод-систему, способную в реальном времени отслеживать и предотвращать подозрительные действия.

Такая система позволяет не только реагировать на уже совершенные инциденты, но и работать на упреждение, создавая надежную экосистему для клиентов.

Таким образом, цифровая идентификация становится ключевым элементом не только в построении клиентского сервиса, но и в стратегиях информационной безопасности и противодействия мошенничеству. Инвестируя в современные технологии идентификации, финансовые организации не только соответствуют регуляторным требованиям, но и формируют доверие клиентов, укрепляют защиту данных и минимизируют финансовые риски.

Цифровая идентификация и интеллектуальные системы противодействия мошенничеству — неотъемлемая часть стратегии АО «Altyn Bank» по обеспечению доверия, прозрачности и безопасности. Использование передовых технологий позволяет эффективно противостоять современным вызовам и строить устойчивые цифровые отношения с клиентами.

«Цифровая идентификация и интеллектуальные системы противодействия мошенничеству — неотъемлемая часть стратегии АО «Altyn Bank» по обеспечению доверия, прозрачности и безопасности. Использование передовых технологий позволяет эффективно противостоять современным вызовам и строить устойчивые цифровые отношения с клиентами.

Сочетая высокие стандарты технологичности и требования законодательства, АО «Altyn Bank» подтверждает свою репутацию надежного и инновационного финансового института, ориентированного на интересы клиентов и защиту их цифровой личности.

Противодействие мошенничеству: ФИНАНСОВАЯ БЕЗОПАСНОСТЬ КАЖДОГО ГРАЖДАНИНА В ЦИФРОВУЮ ЭПОХУ

В эпоху цифровизации и глобальной трансформации финансовых рынков проблема защиты граждан от мошенничества становится приоритетом не только на международной арене, но и в каждой стране в отдельности.

АНДРЕЙ ПОЛЯКОВ
Главный инспектор Центра оценки рисков Департамента по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан

В Республике Узбекистан вопросы обеспечения финансовой безопасности населения выходят за рамки экономических задач и становятся частью национальной стратегии устойчивого развития.

В современных мошеннических схемах все чаще используются передовые технологии, искусственный интеллект и анонимные коммуникации, что требует комплексного и инновационного подхода к противодействию им.

СОВРЕМЕННЫЕ ФОРМЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ

Развитие цифровых платформ, онлайн-банкинга, криптоактивов и социальных сетей создало благоприятную среду для появления новых типов финансовых преступлений. Мошенники используют фишинг, социальную инженерию, поддельные инвестиционные платформы и кибервирусы для доступа к личным данным и средствам граждан.

Одним из ярких примеров являются схемы с использованием поддельных веб-сайтов государственных органов или банков, через которые злоумышленники получают доступ к реквизитам карт.

Кроме того, растет число случаев телефонного и мессенджер-мошенничества, когда граждане получают ложные сообщения от «представителей» банков или правоохранительных органов.

Мошенничество с инвестиционными приложениями приобрело массовый характер, подменяя легитимные финансовые услуги фейковыми копиями.

Борьба с такого рода преступлениями требует не только ужесточения ответственности, но и внедрения новых технологических методов предупреждения и раннего выявления рисков.

УЯЗВИМОСТИ ГРАЖДАН И ОРГАНИЗАЦИЙ

Наиболее уязвимыми перед лицом цифрового мошенничества остаются рядовые граждане, особенно пожилые люди, молодежь и лица с низким уровнем цифровой грамотности. Неосведомленность о базовых принципах кибербезопасности, доверчивость и недостаток критического мышления — это основные факторы риска.

Организации, в том числе государственные учреждения, также подвержены атакам, особенно если их системы защиты не обновлены либо в недостаточной мере внедрены системы информационной безопасности. Угрозы включают утечку персональных данных, вмешательство в электронный документооборот, компрометацию служебной переписки и финансовые потери.

ИНСТРУМЕНТЫ ПРОТИВОДЕЙСТВИЯ ФИНАНСОВОМУ МОШЕННИЧЕСТВУ

Современные методы борьбы с финансовыми преступлениями включают внедрение систем поведенческой аналитики, мониторинг транзакций в реальном времени, технологии машинного обучения для выявления подозрительных схем. Банковские и телекоммуникационные организации усиливают внутренние протоколы верификации клиентов, двухфакторную аутентификацию и антифрод-модули.

Государственные органы создают единые платформы для обмена информацией между банками, операторами связи и правоохранительными органами. Кроме того, развиваются базы данных, содержащие сведения о номерах телефонов и банковских счетах, используемых мошенниками, с возможностью блокировки в автоматическом режиме.

НАЦИОНАЛЬНЫЕ ИНИЦИАТИВЫ УЗБЕКИСТАНА: ИННОВАЦИОННЫЕ ПОДХОДЫ

Возрастание угроз требует принятия в приоритетном порядке мер защиты интересов физических и юридических лиц от таких преступлений, обеспечение целостности финансовой системы путем укрепления нормативно-правовой базы, правоприменительной практики, а также межведомственного сотрудничества.

Одним из ключевых направлений стало создание специализированных аналитических центров при государственных органах, занимающихся мониторингом и выявлением подозрительной активности в финансовом секторе. Кроме того, внедряются мобильные приложения и онлайн-сервисы, с помощью которых граждане могут оперативно сообщать о попытках мошенничества и проверять информацию о контрагентах.

Совместно с международными организациями реализуются проекты по адаптации глобальных методик к национальному контексту, включая риск-ориентированный подход и классификацию угроз.

Это позволяет не только модернизировать инфраструктуру, но и формировать профессиональные кадры в сфере финансовой и цифровой безопасности.

Принимая во внимание приоритетные направления в сфере защиты прав и законных интересов граждан, а также в целях дальнейшего усиления деятельности компетентных органов по борьбе с преступлениями, совершаемыми с использованием информационных технологий, в апреле 2025 года принят документ, направленный на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий.

Согласно данному документу:

- на уполномоченные государственные органы, а также на организации, банки, операторов платежных систем и платежные организации возложена строгая ответственность за принятие всех необходимых мер, направленных на предупреждение киберпреступлений и повышение киберкультуры населения
- внедряется система выявления признаков мошеннических схем или вызывающих подозрение случаев, направленных на привлечение денежных средств населения, путем ведения мониторинга осуществления транзакций физическими и юридическими лицами, а также оперативного оповещения правоохранительных органов о них
- образован Центр содействия цифровому расследованию и борьбе с киберпреступлениями в структуре Научно-исследовательского института цифровой криминалистики Правоохранительной академии
- внедряется платформа электронного обмена данными между МВД, Генеральной прокуратурой и Центральным банком в целях оперативной передачи данных и принятия неотложных мер по поступающим обращениям в сфере борьбы с киберпреступлениями

«Одним из ключевых направлений стало создание специализированных аналитических центров при государственных органах, занимающихся мониторингом и выявлением подозрительной активности в финансовом секторе.

Кроме того, в целях определения требований по обеспечению информационной и кибербезопасности платежных систем, операторов платежных систем и поставщиков платежных услуг, а также профилактики правонарушений, совершаемых посредством цифровых технологий, принято постановление Центрального банка «Об утверждении Положения о мерах по обеспечению информационной безопасности и кибербезопасности платежных систем операторов платежных систем и поставщиков платежных услуг и профилактики правонарушений, совершаемых посредством цифровых технологий» (рег. от 21.05.2024 № 3513).

ФИНАНСОВАЯ ГРАМОТНОСТЬ КАК ЛИНИЯ ОБОРОНЫ

Наряду с технологическими и правовыми инструментами важнейшим элементом защиты является повышение осведомленности граждан. Национальные кампании по финансовому просвещению, обучающие платформы, онлайн-курсы и школьные программы формируют культуру кибербезопасного поведения.

Информированные граждане способны самостоятельно отличать легитимные предложения от мошеннических, не раскрывать персональные данные и критически относятся к получаемым сообщениям. Только при наличии широкой общественной поддержки возможно формирование устойчивой системы финансовой безопасности.

ЗАКЛЮЧЕНИЕ

Противодействие мошенничеству — это задача, требующая слаженной работы государства, частного сектора и самих граждан. Цифровые угрозы быстро эволюционируют, и только постоянное обновление подходов, технологий и образовательных инициатив может обеспечить эффективную защиту. Республика Узбекистан уверенно движется в направлении построения современной системы финансовой безопасности, где интересы граждан находятся в центре внимания.

Только совместными усилиями можно противостоять новым вызовам и сохранить доверие общества к финансовым институтам в цифровом будущем.

ЦИФРОВОЕ ФИНАНСОВОЕ МОШЕННИЧЕСТВО НА КУБЕ: РЕАЛИИ И ВЫЗОВЫ

На Кубе, в стране, где цифровая трансформация развивается на фоне экономических и геополитических трудностей, финансовое мошенничество, связанное с новыми технологиями, стало острой проблемой. В статье рассматривается, как действуют на острове эти преступные практики, как они влияют на население и какие принимаются меры для борьбы с ними.

ФЕРНАНДО ЛУИС КАМЕХО ДЕ ЛА РОСА
Глава финансовой разведки Республики Куба

КОНТЕКСТ: ЦИФРОВИЗАЦИЯ ВО ВРЕМЕНА КРИЗИСА

В последние годы кубинская пресса, например Granma и Juventud Rebelde, освещает усилия государства по модернизации технологической инфраструктуры. С 2019 по 2023 год зафиксировано увеличение доступа к мобильному интернету на 320% — во многом благодаря кубинской телекоммуникационной компании ETECSA. Платформы Transfermóvil и EnZona продвигались как инструменты для укрепления национальной экономики и развития электронной коммерции. СМИ, включая Cubadebate, признали, что такая открытость несет риски: в 2022 году Центральный банк Кубы (Banco Central de Cuba; BCC) сообщил о 45-процентном росте числа заявлений о цифровом мошенничестве.

СЛУЧАИ, ОСВЕЩЕННЫЕ КУБИНСКИМИ СМИ

Фишинг и подмена государственных учреждений

• *Пример 1.* В октябре 2023 года газета Granma опубликовала предупреждение о поддельных смс-сообщениях, отправленных якобы от имени BCC, с запросами личных данных для «получения субсидий в СКВ». Пострадавшие сообщили об убытках в результате операций, проведенных через Transfermóvil.

• *Пример 2.* В 2022 году Cubadebate раскрыл деятельность сети в Facebook[1], предлагающей «мобильные пополнения за полцены» через вредоносные ссылки.

[1] Facebook принадлежит компании Meta, признанной экстремистской организацией и запрещенной в РФ.

Мошенничество с криптовалютами

Куба ввела нормативный пакет, включающий, в первую очередь, государственную политику в области использования виртуальных активов. Кроме того, заработала процедура подачи заявлений на получение лицензий для осуществления деятельности провайдеров услуг виртуальных активов (ПУВА), а также процедура по надзору, мониторингу и контролю за деятельностью тех ПУВА, которые получили лицензию Центрального банка Кубы для работы на внутреннем и внешнем рынках. В 2021 году Министерство юстиции в своем заявлении упомянуло случай с платформой CubaBit (нерегулируемой), которая исчезла с деньгами 200 пользователей после обещаний «прибыли для покупки жилья».

Финансовая разведка Кубы в тесной координации с компетентными органами успешно пресекла действия двух платформ, работавших по схеме финансовой пирамиды.

Это Trust Investing и ROI Academia, которые для обмана своих жертв использовали виртуальные активы. В первом случае было обеспечено эффективное международное взаимодействие с юридической поддержкой. Такое сотрудничество и помощь со стороны Главного управления финансовой разведки (DGIOF) позволили властям Бразилии инициировать уголовное преследование лидеров этой мошеннической платформы с обвинением в отмывании денег.

Мошенничество в сфере электронной торговли

- **Фальшивые интернет-магазины.** В 2023 году телевизионная программа Mesa Redonda обнародовала деятельность таких сайтов, как SuperMLC.com (в настоящее время не функционирует), продававших бытовую технику, которая никогда не доставлялась покупателям.
- **Мошенничество с предложениями трудоустройства.** В 2022 году Juventud Rebelde обнародовала случаи мошенничества, в которых от жертв требовали оплаты в долларах США за «оформление рабочих виз» в такие страны, как Россия и Никарагуа.

ОТВЕТНЫЕ МЕРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Действия правительства и официальных СМИ

1. Информационные кампании

- В 2023 году ETECSA запустила кампанию Navega Seguro («Безопасный поиск»), в рамках которой на телевидении транслировались ролики, обучающие распознаванию мошеннических электронных писем.
- BCC и DGIOF (подразделение финансовой разведки) опубликовали руководство «Защитите свои деньги в интернете» (доступно на официальном сайте), предупреждающее о несанкционированных денежных переводах.

2. Законодательная поддержка

- В 2021 году был обновлен Уголовный кодекс (Закон № 151): предусматривается наказание до 15 лет лишения свободы за киберпреступления.
- Указ-закон № 35/2021 (Политика в сфере кибербезопасности) регулирует деятельность цифровых платформ в стране.

3. Блокировка мошеннических платформ

- ETECSA заблокировала домены фишинговых сайтов, о которых сообщили пользователи, как подтвердил один из руководителей компании в интервью Cubadebate в апреле 2024 года.

Вызовы с точки зрения кубинских аналитиков

- Ограниченный доступ к средствам обеспечения безопасности. Куба пребывает в состоянии экономической, финансовой и торговой войны. За последние 11 лет при действующих администрациях США эта ситуация обострилась. Страна сталкивается с жесткими ограничениями в доступе к новым технологиям, в том числе к средствам кибербезопасности. В этом контексте и при дефиците ресурсов продвижение цифровизации и цифровой трансформации общества остается серьезным вызовом. Тем не менее политическая воля государства и реализация государственных программ позволили добиться значительного прогресса в данной области.

Пример:

- Санкции мешают Кубе приобрести передовое программное обеспечение для отслеживания криптовалют.
- Международные платформы, такие как PayPal или Stripe, недоступны, что вынуждает кубинцев использовать менее безопасные альтернативы.

МЕРЫ ПРЕДУПРЕЖДЕНИЯ, ПРЕДЛАГАЕМЫЕ МЕСТНЫМИ ЭКСПЕРТАМИ

Цифровое просвещение широких масс

- Центральный банк Кубы продвигает Национальную стратегию финансового образования (ENEF). Финансовые институты, Министерство образования и Министерство высшего образования, другие государственные органы и общественные организации объединили усилия для распространения финансовой культуры как элемента противодействия отмыванию денег и финансированию терроризма.
- С 2020 года DGIOF продвигает финансовую безопасность как составляющую национальной безопасности. Подписано Соглашение о сотрудничестве с Гаванским университетом по данному направлению. В рамках этих действий с целью снижения рисков мошенничества и других преступных проявлений поощряется культура электронной торговли, использование электронных платежных платформ, личная ответственность за защиту персональных и банковских данных.
- В учебные курсы таких вузов, как Университет информационных наук (UCI), включены программы по кибербезопасности.
- Молодежные компьютерные клубы (Joven Club de Computación) подключились к проведению семинаров в местных сообществах.

Технологии «Сделано на Кубе»

Разрабатываются приложения для безопасной аутентификации, такие как двухфакторная проверка (2FA) для платформы Transfermóvil, предложенная инженерами государственной компании DESOFT.

ЗАКЛЮЧЕНИЕ. ПУТЬ К ЦИФРОВОЙ УСТОЙЧИВОСТИ

Куба решает задачу защиты своего населения в условиях хрупкой цифровой экосистемы и экономического давления. Хотя власти приняли законодательные и образовательные меры, эксперты настаивают на необходимости следующих шагов:

- повышение прозрачности и безопасности при обработке пользовательских данных;
- инвестиции в расширение технических возможностей для расследования киберпреступлений;
- расширение прав граждан, предоставление им доступной и достоверной информации.

В 2023 году президент Мигель Диас-Канель заявил: *«Борьба с цифровым мошенничеством — это не только технологическая задача, это и борьба за доверие к нашему социальному проекту».*

«Финансовые институты, Министерство образования и Министерство высшего образования, другие государственные органы и общественные организации объединили усилия для распространения финансовой культуры как элемента противодействия отмыванию денег и финансированию терроризма.

ОПЕРАТОР СВЯЗИ В СИСТЕМЕ БОРЬБЫ С МОШЕННИЧЕСКИМИ ДЕЙСТВИЯМИ

Операторы связи постоянно совершенствуют методы обработки и защиты персональных данных клиентов, внедряют ролевые модели доступа к клиентским данным для тех работников, функционал которых связан с обслуживанием абонентов, а также применяют технические методы защиты информации.

МегаФон

БОРИС ИСАДЧЕНКО
Эксперт в области безопасности ПАО «МегаФон»

Одной из актуальных угроз сегодня является колоссальный рост количества преступлений, подпадающих под определение «телефонное мошенничество», реализуемых с использованием средств связи. Эту тенденцию иллюстрирует статистика МВД России[1]. Если в 2023 году было зарегистрировано почти 303 тыс. мошенничеств, проводимых с использованием средств связи, то в 2024 году это число увеличилось на 14,3% и составило 346 тыс. Размер ущерба от незаконной деятельности мошенников вырос на 36% и превысил 200 млрд рублей.

Наиболее подвержены телефонному мошенничеству граждане в возрасте от 25 до 44 лет, пользующиеся социальными сетями, мессенджерами, ресурсами по продаже товаров/услуг, поскольку при регистрации на интернет-ресурсах они вносят свои персональные данные. Кроме того, вся размещаемая о себе в социальных сетях информация является потенциально доступной для неопределенного круга лиц и может быть использована против человека.

Вторая категория, которая также страдает от действий злоумышленников, — это пенсионеры. Цифровые технологии усложняются с каждым годом, а люди пожилого возраста все больше становятся уязвимыми, поскольку иногда не в силах разобраться в нюансах обслуживания и овладеть новыми цифровыми навыками. В то же время злоумышленники постоянно адаптируются к новым технологиям и находятся в постоянном поиске новых способов воздействия.

Телефонное мошенничество выделяет три типовых этапа, встречающихся в большинстве изученных схем воздействия на жертву.

ЭТАП ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ

Характеризуется получением первичной информации о потенциальной жертве, подготовкой технических средств воздействия, с помощью которых будет проводиться контакт с потенциальной жертвой (оборудование для организации звонков через Wi-Fi, симкарты и т.д.), разработкой сценария воздействия на абонента, а также организацией схемы увода полученных денежных средств. Выбор сценария зачастую зависит от объема той информации, которая находится в распоряжении злоумышленников.

Всемирная сеть является хранилищем огромного массива информации. И при желании с использованием даркнета возможно найти интернет-ресурсы, которые торгуют «слитыми» базами данных компаний.

Абонентские номера потенциальных жертв могут выбираться также случайным образом из открытых источников либо методом перебора определенного пула абонентских номеров.

Для противодействия на данном этапе необходима как работа по изменению текущих нормативных

[1] https://tass.ru/proisshestviya/22978955.

актов, направленных на борьбу с распространением «слитых» в сеть клиентских баз данных, так и активная работа компаний по внедрению программ защиты информации с учетом вызовов реального времени.

В конце 2024 года принят нормативный акт[2] о борьбе с незаконными ресурсами, торгующими базами персональных данных во всемирной сети, ужесточающий ответственность за их использование. Была введена уголовная ответственность за незаконную обработку компьютерной информации, содержащей персональные данные, а также ужесточена ответственность за создание и поддержку информационных ресурсов, предназначенных для хранения, распространения незаконных баз данных, ужесточены меры ответственности к компаниям за нарушения при обработке персональных данных.

Кроме того, Роскомнадзором активно применяются меры по ограничению доступа к ресурсам, торгующим базами клиентских данных.

С точки зрения работы оператора связи постоянно совершенствуются методы обработки и защиты персональных данных клиентов, внедряются ролевые модели доступа к клиентским данным работникам компании, функционал которых связан с обслуживанием абонентов, применяются технические методы защиты информации. Кроме того, проводятся мероприятия по обучению персонала требованиям работы с персональными данными и информированию о мерах ответственности за неправомерный доступ к ним. Это далеко не полный перечень тех мероприятий, которые реализуются для снижения рисков распространения баз данных клиентов компании.

ЭТАП НЕПОСРЕДСТВЕННОГО КОНТАКТА МОШЕННИКОВ С ПОТЕНЦИАЛЬНЫМИ ЖЕРТВАМИ

Этот этап связан с воздействием на потенциальную жертву, получением недостающей информации, реализацией сценария завладения денежными средствами. Этап реализуется как с применением технических средств (включая использование технологий Wi-Fi или мобильной связи), так и методов психологического воздействия на абонента для формирования у него определенного поведения.

Цель звонка абоненту — получение необходимой информации для оформления через интернет-сервисы кредита, регистрации доступа к онлайн-банкингу, смены контактных данных личного кабинета Госуслуг и т.д. Все это позволяет получить доступ к денежным средствам потенциальной жертвы либо побудить ее добровольно перевести их на счета мошенников, в результате чего абонент утрачивает контроль над собственными сбережениями и переводит их на счета мошенников, электронные кошельки.

Для борьбы с прямыми звонками мошенников ведется активная работа по изменению законодательства в области связи, банковской деятельности.

Здесь стоит упомянуть развитие государственной информационной системы, внедряемой Главным радиочастотным центром (ГРЧЦ) — платформы «Антифрод», которая блокирует вызовы и сообщения с подменных номеров, подозрительных звонков еще до того, как мошенник сможет связаться с потенциальной жертвой.

Принятые недавно изменения в законодательство[3] запретили обслуживание клиентов компаний и госорганов через иностранные мессенджеры, ограничили передачу сим-карт третьим лицам, реализовали абоненту право запретить массовые телефонные вызовы и уведомления от банков и других организаций, интерес к которым у них отсутствует.

Помимо этого, операторами связи ведется собственная работа по оценке вызовов, абонентских номеров с алгоритмами и критериями подозрительных действий, которые основываются на анализе деятельности абонента, перечне оказываемых ему услуг, а также обратной связи от абонентов по факту контакта с определенными вызовами. Работа в этом направлении ведется на инструментальном уровне, создаются средства защиты абонентов от телефонного мошенничества на сети связи, а также предлагаются услуги для абонентов, которые предупреждают о потенциальном контакте с мошенниками.

Примером такой услуги выступает виртуальный секретарь Ева компании «МегаФон», который решает простые типизированные задачи обслуживания и позволяет определять спам и звонки от мошенников, применяя собственную систему оценки вызовов, выводя предупреждение о спам-звонке, либо указывает категорию абонента, к которой принадлежит номер, а также блокирует звонок, если имеется подозрение на мошеннический вызов.

На своем сайте компания размещает информацию[4] для профилактики телефонного мошенничества, услуг, которые направлены на борьбу с мошенничеством, и описывает действия на случай, если абонент стал жертвой телефонных мошенников.

---

[2] Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

[3] Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

[4] Как защититься от телефонных мошенников? | Защита от спам-звонков и SMS-спама от МегаФона Московский регион.

ЭТАП ЗАВЛАДЕНИЯ ДЕНЕЖНЫМИ СРЕДСТВАМИ И УНИЧТОЖЕНИЯ СЛЕДОВ ВОЗДЕЙСТВИЯ, ВКЛЮЧАЯ ВЫВОД МОШЕННИКАМИ В БЕЗОПАСНУЮ ЗОНУ ПОЛУЧЕННЫХ ДЕНЕГ, УНИЧТОЖЕНИЕ СЛЕДОВ КОНТАКТОВ С ЖЕРТВОЙ

По информации РБК[5], около 80% хищений денег сейчас происходит с помощью me2me-переводов[6] или через мобильные платежные системы (pay-сервисы) для бесконтактной оплаты, а также вовлечения в схемы дропперов[7] с последующим обналичиванием денежных средств.

И ведущая роль в противодействии такому поведению отводится мониторингу денежных переводов.

Законодательные требования нацелены на регулирование мониторинга по двум направлениям: анализ клиентских данных с совершенствованием процедуры подтверждения их достоверности и создание системы анализа потока операций клиентов на риски совершения противоправной деятельности.

Так, законодательно были введены ограничения[8]: использование до 20 абонентских номеров для граждан РФ и до 10 для иностранных граждан, скорректирован порядок проверки достоверности сведений об абоненте, которая теперь проводится до начала оказания услуг, внедрено право Росфинмониторинга вводить запрет на проведение операций на определенный срок.

Мониторинг операций абонентов строится на принципах риск-ориентированного подхода, заключающегося в контроле за операциями в зависимости от оценки клиентских рисков, исторического профиля их операций, а также итогов взаимодействия с ними. Такой подход позволяет более эффективно распределять ресурсы компании.

Большую роль здесь играют автоматизированные решения, изучающие операции клиентов, оценивающие их на соответствие критериям сомнительных и применяющие меры, направленные на реализацию требований по ПОД/ФТ и ФРОМУ.

Использование автоматизированных проверок позволяет вычленять из огромного потока те операции, которые необходимы для изучения. Профиль таких операций не только рекомендован в нормативных актах[9] как основа построения системы контроля необычных операций, но и дополнен при изучении операций абонентов, взаимодействия с ними.

Применение таких инструментов позволяет выстраивать систему оценки операций абонента на основании различных источников информации, сведений об историческом профиле и применять риск-ориентированный подход при работе с абонентом.

Работа по обеспечению финансовой безопасности абонентов должна носить системный характер и включать участие каждого элемента системы, начиная от государства, как регулятора общественных отношений, компаний, оказывающих финансовые услуги и услуги связи, и самих граждан, против которых направлены действия мошенников.

Все те нововведения, которые реализуются государством, те инициативы, которые воплощаются на практике операторами связи, не будут иметь должного эффекта, если на уровне абонентов не развивать критическое мышление и не формировать у них навыки защиты от мошеннических посягательств. Важно понимать, что методы воздействия мошенников на свои жертвы постоянно совершенствуются, в связи с чем требуется ведение постоянной работы по следующим направлениям:

- информирование о новых и распространенных схемах мошенничества и рекомендации по мерам противодействия. Для всех должно стать нормой знание о том, что сотрудники полиции, банков и других организаций никогда не запрашивают личные данные по телефону
- проведение обучающих программ и выпуск социальной рекламы, ориентированной на пожилых людей и детей, рассказывающих о том, как распознать признаки мошеннических звонков и что делать в таких случаях
- использование интернет-сервисов и продуктов виртуальных помощников с определителями номеров, которые предупреждают о мошенниках
- распространение поведенческих моделей при контактах с телефонным мошенничеством, включая прекращение вызова, запрет передачи информации о себе, дополнительные способы проверки полученной от мошенников информации, контроль своего эмоционального состояния и т. д.

[5] https://www.rbc.ru/rbcfreenews/66f41c049a79479d762f9171.
[6] Переводы между счетами одного клиента в разных банках.
[7] Дроппер (дроп) — это человек, чья банковская карта/счет используются для транзита или обналичивания похищенных денег.
[8] Федеральный закон от 08.08.2024 № 303-ФЗ «О внесении изменений в Федеральный закон "О связи" и отдельные законодательные акты Российской Федерации».
[9] Приказ Росфинмониторинга от 08.02.2022 № 18 «Об утверждении Особенностей представления в Федеральную службу по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ „О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма“».

ЗАЩИТА ОТ МОШЕННИКОВ: ОПЫТ РОССИЙСКОЙ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПАНИИ Т2

Т2 непрерывно наращивает усилия по защите клиентов от телефонного мошенничества. Компания последовательно развивает комплекс мер, направленных на сокращение количества жертв социальной инженерии. Для анализа подозрительной активности оператор применяет современные технологии обработки больших данных, включая собственные алгоритмы и математические модели. Так, за первый квартал 2025 года система защиты Т2 заблокировала 212,5 млн нежелательных звонков, включая рекламные и потенциально мошеннические.

Системы Т2 оценивают финансовую активность, информацию от правоохранительных органов, обращения клиентов и другие источники, чтобы заблокировать мошеннические операции до их совершения. Компания активно взаимодействует с банками и другими участниками рынка, обмениваясь данными о потенциальных рисках. Т2 передает партнерам данные по скорингу телефонного трафика, которые используются в банковских системах антифрода.

В апреле этого года Т2 первой внедрила меры, предусмотренные новым законом о борьбе с киберпреступлениями. Сообщения от Госуслуг и банка с кодом для входа в аккаунт стали приходить с задержкой — достаточной, чтобы сократить риски для клиента при атаке злоумышленников. Инициатива была направлена на самые уязвимые аудитории — клиентов старше 60 лет и молодых людей от 14 лет до 21 года.

> **«Системы Т2 оценивают финансовую активность, информацию от правоохранительных органов, обращения клиентов и другие источники, чтобы заблокировать мошеннические операции до их совершения.**

Помимо технологической борьбы с угрозами, Т2 развивает продуктовые решения, помогающие абонентам самостоятельно распознавать и предотвращать мошенничество. Например, оператор предлагает бесплатную услугу «Антиспам для звонков», которая работает не только для вызовов по мобильной сети, но и в мессенджерах — Telegram и WhatsApp. Благодаря ей пользователь получает информацию о звонящем даже в том случае, если его номер не сохранен в контактах.

Еще один инструмент безопасности — сервис проверки утечки персональных данных, реализованный Т2 совместно с ГК «Солар». Абонент может бесплатно проверить, попали ли его данные в открытый доступ, и своевременно принять меры — изменить пароли, защитить аккаунты и обратить внимание на подозрительные сервисы. С момента запуска услуги в августе 2024 года абоненты Т2 заказали более двух миллионов отчетов. А около 65% клиентов воспользовались сервисом более одного раза.

Не менее важным направлением остается информирование клиентов о мерах предосторожности и новых схемах телефонного мошенничества. Т2 регулярно обновляет материалы на своих информационных ресурсах, публикует рекомендации по распознаванию мошеннических схем и проводит просветительскую работу через все доступные каналы связи.

РОСФИНМОНИТОРИНГ НА ПМЭФ-2025: ПОДРОБНОСТИ В СПЕЦИАЛЬНОМ РЕПОРТАЖЕ

Представители Федеральной службы по финансовому мониторингу приняли участие в XXVIII Петербургском международном экономическом форуме.
В ходе сессий Форума обсуждались вопросы развития государственного аудита, противодействия теневой экономике, укрепления диалога между регуляторами и бизнесом, борьбы с телефонным мошенничеством и дропперством, обеспечения финансовой безопасности молодежи и многие другие темы. Рассказываем, как это было, в специальном материале.

ВЗГЛЯД В БУДУЩЕЕ ГОСУДАРСТВЕННОГО АУДИТА

Директор Федеральной службы по финансовому мониторингу Юрий Чиханчин выступил на деловой сессии «Взгляд в будущее государственного аудита: приоритеты развития», организованной Счетной палатой Российской Федерации в рамках Форума.

В мероприятии приняли участие: заместитель председателя Счетной палаты Галина Изотова, заместитель Председателя Совета Федерации Николай Журавлев, руководитель Федерального казначейства Роман Артюхин, губернатор Новосибирской области Андрей Травников, первый заместитель председателя правления ПАО «Сбербанк» Александр Ведяхин, представители органов государственного финансового контроля Республики Беларусь, Королевства Саудовская Аравия, Арабской Республики Египет, Королевства Бахрейн. Кроме того, спикером выступил директор Института системного программирования имени В.П. Иванникова Российской академии наук Арутюн Аветисян.

Модератор сессии — главный редактор медиагруппы «Россия сегодня» и телеканала RT Маргарита Симоньян.

В ходе дискуссии обсуждались различные аспекты совершенствования государственного аудита с учетом цифровизации и многоплановых рисков, в том числе связанных с активным использованием искусственного интеллекта.

Юрий Чиханчин поздравил руководство Счетной палаты с 30-летним юбилеем и отметил многолетнее продуктивное межведомственное сотрудничество. Переходя к теме сессии, глава ведомства подчеркнул, что в совместной работе органов госконтроля ключевую роль играет доверие, единое видение рисков и угроз, а также технологическая оптимизация процессов аудита.

«Сегодня доверие между контролирующими органами — это самый главный фактор для эффективной работы. С целью проверки компании нужно изучить миллионы документов и различных других источников. Человек вручную такую задачу не решит. Необходимо объединение ресурсной базы, внедрение программных продуктов, цифровых платформ. Это сэкономит трудозатраты и способствует более объективной оценке проверяемого субъекта. Например, наша Служба использует систему личного кабинета, который позволяет дистанционно взаимодействовать с поднадзорными субъектами. Инструмент продемонстрировал высокую эффективность», — сказал глава Росфинмониторинга.

Юрий Чиханчин подчеркнул, что аудитор сегодня и в будущем — это отраслевой специалист высокого уровня, который способен выстраивать эффективный диалог и с профессиональным сообществом системы контроля за финансами, и с контролируемыми объектами.

ПРИОРИТЕТ И ПОДДЕРЖКА — ЛЕГАЛЬНОМУ БИЗНЕСУ

Заместитель директора Росфинмониторинга Галина Бобрышева выступила на деловой сессии «МСП и нацпроекты: приоритет и поддержка — легальному бизнесу».

В дискуссии приняли участие заместитель Министра экономического развития Российской Федерации Денис Тюпышев, заместитель руководителя Федеральной налоговой службы Дмитрий Сатин, заместитель председателя правления ПАО «Сбербанк» Анатолий Попов, а также представители малого и среднего бизнеса. Модератором встречи выступила вице-президент Торгово-промышленной палаты Российской Федерации Елена Дыбова.

Участники обсудили вопросы противодействия теневой экономике, способы обеспечения справедливой конкуренции и конструктивного диалога между регулятором и бизнесом.

Галина Бобрышева рассказала о работе российской антиотмывочной системы по снижению объемов теневой экономики, в том числе о специфических инструментах оценки рисков в этой сфере. К индикаторам теневого рынка относятся и объемы подозрительных операций, сведения о которых поступают в Росфинмониторинг, и объемы операций, в проведении которых отказывают банки, и сегмент красной зоны платформы «Знай своего клиента», а также ряд других маркеров.

Замглавы Службы отметила, что инфраструктура теневого сектора в последние годы претерпевает изменения: если раньше ее в основном составляли фирмы-однодневки, то сейчас вовлекается все больше физических лиц, среди которых молодежь и представители мигрантской среды.

«Отказ в совершении подозрительных операций успешно работает как сдерживающая мера активности в теневом секторе. Только за 5 месяцев этого года кредитные организации отказали в проведении более 150 тысяч операций на общую сумму около 300 млрд рублей», — констатировала Галина Бобрышева.

В заключение представитель ведомства отметила большую роль антиотмывочной системы в формировании навыков финансовой безопасности и финансовой гигиены, а также неприятия теневой деятельности.

ТЕЛЕФОННЫЕ МОШЕННИКИ: СКОЛЬКО МОЖНО?

Статс-секретарь — заместитель директора Росфинмониторинга Герман Негляд принял участие в панельной сессии ПАО «Сбербанк» «Телефонные мошенники: сколько можно? Откровенный разговор с Ольгой Скабеевой».

Спикерами также выступили статс-секретарь — заместитель Министра внутренних дел Российской Федерации Игорь Зубов, председатель комитета Госдумы по информационной политике, информационным технологиям и связи Сергей Боярский, заместитель председателя правления ПАО «Сбербанк» Станислав Кузнецов, заместитель начальника следственного департамента МВД России Данил Филиппов.

В формате программы «60 минут» участники дискуссии обсудили меры по защите граждан от атак телефонных мошенников, актуальные угрозы, с которыми могут столкнуться пользователи цифровых сервисов, вопросы сотрудничества в сфере борьбы с киберпреступностью.

Герман Негляд в своем выступлении подчеркнул, что все чаще в перемещении похищенных денежных средств используется дропперская сеть, когда граждане за небольшое вознаграждение передают доступ к своим банковским картам другим, что позволяет на первом этапе обходить банковский контроль. Кроме того, отметил спикер, злоумышленники применяют и новые средства расчета, в том числе криптовалюту.

«Статус криптовалюты в настоящее время, к сожалению, до конца не урегулирован в нашей стране. Это тоже проблема, о которой нужно говорить. Криптообменники, которые действуют в нашей юрисдикции, должны выполнять такие же функции, как банки, то есть идентифицировать своих клиентов, оценивать операции по обмену криптовалюты на фиатную валюту на предмет подозрительности, отказывать в проведении определенных операций и взаимодействовать с органами государственной власти: финансовой разведкой, правоохранительными органами и другими», — сказал замглавы ведомства.

В качестве эффективной меры снижения риска финансового мошенничества выступающий отметил необходимость лишения преступников возможности пользоваться полученными незаконным путем средствами:

«Только личным наказанием, помещением в колонию мы не решим проблему. Нужно демотивировать преступников получать преступный доход, то есть оперативно блокировать эти средства, замораживать, изымать, конфисковывать. Наша главная задача — сделать так, чтобы преступный доход перестал быть привлекательным. Снизить мотивацию мошенников — вот что действительно работает».

Герман Негляд акцентировал внимание на важности дальнейшего внедрения новых технологий в деятельность органов государственной власти, банков, сотовых операторов для борьбы с финансовой преступностью, а также необходимости объединения усилий разных ведомств и организаций в реагировании на эти угрозы.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ МОЛОДЕЖИ

Статс-секретарь — заместитель директора Росфинмониторинга Герман Негляд и руководитель пресс-службы ведомства Ирина Рязанова приняли участие в пресс-брифинге «Финансовая безопасность молодежи: вызовы и решения в цифровую эпоху».

Спикеры обсудили вопросы противодействия киберугрозам, с которыми сталкивается молодежь, вовлечению молодых людей в дропперство и другие преступные схемы.

Герман Негляд отметил, что миграция преступности в цифровую сферу и использование злоумышленниками молодежи требуют адекватных мер реагирования на всех уровнях:

«Молодые люди становятся как соучастниками финансовых преступлений, так и их жертвами. В дропперские схемы, по данным российских банков, вовлечено около 2 млн человек, и более половины — это люди до 24 лет. В отношении молодых людей как активных пользователей интернета применяются технологии искусственного интеллекта — мошенничеству с использованием дипфейков сегодня подвержены граждане независимо от возраста».

Выступающий подчеркнул, что наряду с законодательными мерами по борьбе с киберпреступностью и использованием дропов нужна системная просветительская работа.

Так, Росфинмониторингом совместно с партнерами проводится Международная олимпиада по финансовой безопасности. Создано Международное движение по финансовой безопасности, которое объединяет школьников, студентов и экспертов из разных стран.

Ирина Рязанова отметила необходимость создания экосистемы контента, который бы формировал модель финансово безопасного поведения в молодежной среде.

Для этого необходима широкая вовлеченность заинтересованных ведомств, организаций, лидеров общественного мнения и молодежи, эффективное использование востребованных ресурсов.

«При создании такой экосистемы важно выстраивать модель «молодежь-молодежи», когда сами молодые люди транслируют смыслы финансовой безопасности среди своих сверстников, разговаривая с ними на одном языке. Так, сейчас формируется пул амбассадоров Международного движения по финансовой безопасности, который нацелен именно на это», — отметила представитель Росфинмониторинга.

Как подчеркнула Ирина Рязанова, эффективными инструментами взаимодействия со школьниками и студентами сегодня выступают интерактивные цифровые платформы.

Для трансляции актуального контента по финансовой безопасности создана платформа «Содружество», выступающая технологическим партнером тематической Олимпиады.

ИНВЕСТИЦИИ В ЗНАНИЯ. ПРОСВЕТИТЕЛЬСКИЕ ПРОЕКТЫ В СФЕРЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В ОБЛАСТИ ЧАСТНОГО ИНВЕСТИРОВАНИЯ

ЕВГЕНИЯ СИДОРЧУК
Начальник отдела развития финансовых рынков Департамента финансовой политики Минфина России

АНДРЕЙ ПОПУДРЕНКО
Главный специалист-эксперт отдела регулирования негосударственных пенсионных фондов Департамента финансовой политики Минфина России

Авторами статьи рассматривается проблематика мошенничества в области частного инвестирования. Популяризация финансовых инструментов провоцирует злоумышленников воспользоваться чужими успехами в выстраивании мошеннических схем на фондовом рынке. Ущерб, причиняемый мошенниками, наносится не только частным, но и публичным интересам. Одной из форм мошенничества в области частного инвестирования является лжеброкерство. В связи с этим принимаются меры различного характера с целью профилактики и снижения уровня мошенничества с частными инвестициями. Тем не менее основным способом профилактики является повышение уровня финансовой грамотности населения. Таким образом, одна из главных задач государства в области противодействия мошенничеству с частными инвестициями — разработка и внедрение программ, направленных на повышение уровня финансовой грамотности и просвещение населения страны.

В современном мире финансовая грамотность занимает особое место в системе знаний и навыков человека, позволяя принимать обдуманные финансовые решения и формировать собственный капитал. Под финансовой грамотностью принято понимать наличие навыков у населения или отдельного человека по подбору информации о банковских и страховых продуктах, способность учитывать финансовые поступления и контролировать де-

нежные расходы[1]. Безусловно, одной из важнейших составляющих финансовой грамотности является наличие определенных знаний, позволяющих защитить себя от действий мошенников. Специфика таких знаний достаточно широка, поскольку действия мошенников могут быть направлены на разные сферы жизни человека.

Популяризация финансовых инструментов является серьезным стимулом для роста частного инвестирования на отечественном фондовом рынке. Так, количество частных инвесторов только на Московской бирже, у которых есть брокерские счета за период 2024 года, составило 35,1 млн человек и более 64,3 млн счетов[2]. Вместе с положительной динамикой роста частных инвесторов увеличилось и число мошеннических действий с частными инвестициями.

9027

субъектов, имеющих признаки нелегальной деятельности, было выявлено Центральным банком Российской Федерации в 2024 году, а число нелегальных участников рынка ценных бумаг из общего числа составило 1 936[3]. Данная статистика отражает количество выявленных субъектов, осуществляющих нелегальную деятельность на рынке ценных бумаг, однако в действительности же количество данных субъектов может быть значительно больше.

Важно отметить, что следствием такого мошенничества является не только утрата гражданами денежных средств, перечисляемых мошенникам, но и подрыв доверия к отечественному фондовому рынку. Таким образом, мошенничество в области частного инвестирования наносит вред как частным, так и публичным интересам.

Одним из основных способов мошенничества в области частных инвестиций является так называемое лжеброкерство.

Лжеброкеры — это мошенники, представляющиеся потенциальным жертвам мошеннической схемы в качестве брокера и предлагающие свои «услуги» по сопровождению инвестиционной деятельности частного лица с гарантированной высокой прибылью.

Можно выделить три основных этапа мошенничества под видом брокера.

На первом этапе происходит утечка персональных данных пользователей, зарегистрированных на различных сайтах в информационно-телекоммуникационной сети «Интернет». Незаконно получив персональные данные пользователей, мошенники направляют на почту потенциальной жертвы мошеннической схемы многочисленные письма с недостоверной рекламой, в рамках которой предлагаются «услуги» лжеброкера по сопровождению инвестиционной деятельности. Основными аргументами лжеброкеров для обмана граждан являются «гарантированные» высокие доходы от инвестиционной деятельности, страхование суммы первоначального вложения на случай падения стоимости брокерского портфеля, возможность вывода вложенных денежных средств, а также сопровождение частного лица на всех этапах инвестиционной деятельности.

На втором этапе происходит непосредственный контакт мошенника с гражданином в результате ответа на рассылки. Используя методы социальной инженерии, мошенники вводят гражданина в заблуждение путем убеждения. Когда у клиента возникает желание вывести вложенные денежные средства, мошенники сообщают о невозможности проведения указанной операции под различными предлогами. Так, достаточно часто в качестве предлога не возвращать денежные средства гражданину мошенники ссылаются на то, что переводы или счета гражданина заблокированы по решению федеральных органов исполнительной власти или Центрального банка Российской Федерации. Ставку мошенники делают на то, что граждане, как правило, являются неосведомленными в части полномочий указанных органов. Дополнительно мошенники пытаются выманить у гражданина новые денежные средства, аргументируя это тем, что необходима оплата некой страховки или оплата за ежедневное размещение валюты на «европейской ячейке» для срочного платного вывода средств.

На третьем этапе для вывода средств мошенники предлагают найти и зарегистрировать поручителя, гарантируя, что это поможет обналичить денежные средства. Клиентам предлагается оставить электронное обращение на официальном сайте федеральных органов исполнительной власти с указанием данных поручителя, номера счета и суммы средств, которые необходимо ему пере-

[1] См.: Белехова Г. В. Финансовая грамотность населения // Актуальные вопросы экономических наук. 2012. № 26. URL: https://cyberleninka.ru/article/n/finansovaya-gramotnost-naseleniya-1.

[2] Число частных инвесторов на Московской бирже превысило 35 миллионов. URL: https://www.moex.com/n76900.

[3] Противодействие нелегальной деятельности на финансовом рынке. URL: https://www.cbr.ru/analytics/inside/2024_2/.

дать. В качестве мер давления мошенники рассылают клиентам поддельные письма федеральных органов исполнительной власти (на которых оставлено электронное обращение), угрожая блокировкой средств, взысканием долга или арестом имущества гражданина. По результату исчерпания доверия гражданина и получения определенной суммы денежных средств мошенники перестают выходить на связь.

Основной профилактикой для выявления и противодействия мошенническим схемам лжеброкеров для граждан является первоначальная проверка брокера на наличие законных оснований осуществления брокерской деятельности. Так, в соответствии с абзацем 2 части 1 статьи 3 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»[4] (далее — Закон о рынке ценных бумаг) брокер является профессиональным участником рынка ценных бумаг. В соответствии со статьей 39 Закона о рынке ценных бумаг брокерская деятельность осуществляется на основании специального разрешения (лицензии), выдача которого производится Банком России.

Кроме того, Банк России на своем официальном сайте публикует реестр брокеров, имеющих лицензию на осуществление брокерской деятельности. Таким образом, перед переводом лицу денежных средств необходимо удостовериться в том, что данное лицо является настоящим брокером, предварительно проверив его в реестре на официальном сайте Банка России.

Ситуация для граждан усложняется, когда мошенники действуют под видом настоящего зарегистрированного брокера или финансового аналитика. В этом случае гражданину наиболее сложно определить мошенника. Прежде всего необходимо удостовериться, что с гражданином вышел на связь настоящий брокер (например, уточнение информации о предложении по адресу почты или телефона с официального сайта брокера). Кроме того, необходимо отметить, что финансовые аналитики осуществляют свою деятельность без необходимости получения лицензии. Однако Банк России совместно с СРО «Национальная финансовая организация» создали Реестр финансовых аналитиков. Внесение информации о финансовом аналитике в указанный реестр осуществляется на добровольной основе, при этом для инвестора наличие информации об аналитике в реестре свидетельствует о том, что финансовый аналитик принял на себя обязательства следовать нормам этики и стандартам профессионального поведения, рекомендованным Банком России[5].

В части противодействия мошенничеству с частными инвестициями Министерство внутренних дел Российской Федерации (далее — МВД России) осуществляет проверочные мероприятия и возбуждение уголовных дел в отношении мошенников, представляющихся брокерами. Практика МВД России показывает, что такие дела, как правило, квалифицируются по статье 159 Уголовного кодекса Российской Федерации[6] (далее — УК РФ) «Мошенничество» или статье 158 УК РФ «Кража».

Ключевые механизмы по борьбе с мошенниками в области частных инвестиций осуществляются через публикацию материалов для информирования граждан о противодействии мошенникам, публикацию докладов в средствах массовой информации, на официальных ресурсах ведомств и так далее.

Например, Минфином России в информационно-коммуникационной сети «Интернет» разработан и опубликован раздел, информирующий граждан о том, как отличить брокера от мошенника[7]. Кроме того, на официальном сайте Банка России в разделе «Противодействие недобросовестным практикам» в подразделе «Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке» (далее — Список) можно ознакомиться со списком лиц, в деятельности которых Банком России выявлены признаки нелегальной деятельности на финансовом рынке. Отсутствие информации о лице в Списке не означает, что предлагаемые им услуги на финансовом рынке предоставляются законно[8].

Таким образом, ключевым способом противодействия мошенничеству с частными инвестициями является повышение уровня финансовой грамотности и осведомленности граждан о возможностях и рисках получения инвестиционного дохода на фондовом рынке.

[4] Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг». URL: https://base.garant.ru/10106464/?ysclid=mb9ifhn3vw854636840.

[5] Реестр финансовых аналитиков. URL: https://nfa.ru/services/analysts_register/?ysclid=mb0mbivzfz118936622.

[6] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. URL: https://base.garant.ru/10108000/?ysclid=mb9id2h3pi754536396.

[7] Осторожно, мошенники! URL: https://minfin.gov.ru/ru/ministry/info/warning/.

[8] Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке. URL: https://cbr.ru/inside/warning-list/.

ОБРАЗОВАТЕЛЬНЫЕ ПРОЕКТЫ ПО ПРОФИЛАКТИКЕ ДРОППЕРСТВА И МОШЕННИЧЕСТВА СРЕДИ СТУДЕНТОВ

УЧЕБНЫЙ ЦЕНТР ГОСУДАРСТВЕННОЙ СЛУЖБЫ ФИНАНСОВОЙ РАЗВЕДКИ ПРИ МИНИСТЕРСТВЕ ФИНАНСОВ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

В целях повышения осведомленности и выработки компетенций по определению подозрительных финансовых схем с 2024 года Учебный центр Государственной службы финансовой разведки при Министерстве финансов Кыргызской Республики активно ведет работу по внедрению компонента «Финансовая безопасность» в школьную программу.

ЛИРА ОМУРБЕКОВА
Директор Учебного центра Государственной службы финансовой разведки при Министерстве финансов Кыргызской Республики

Расширение охвата финансовыми продуктами, внедрение виртуальных активов в жизнь граждан, повышение доступности финансовых инструментов и, как следствие, рост количества случаев неправомерного использования платежных карт, электронных кошельков и широкое распространение криптовалюты ставят перед государством новую задачу — повышение осведомленности граждан о рисках вовлечения в незаконные схемы.

Согласно статистике, за 12 месяцев 2024 года в стране было зарегистрировано 1658 уголовных дел в сфере информационных технологий, куда включаются и мошеннические схемы. Из общего количества зарегистрированных дел раскрыто 796, что меньше 50% всех преступлений.

При этом в разрезе типологий мошеннических схем преобладающее количество преступлений связано с кражей данных платежных карт, электронных кошельков, данных доступа к банковским мобильным приложениям, мошенничеством посредством использования дропперов. Согласно данным правоохранительных органов, в схемы дропперов привлекаются студенты и учащиеся колледжей.

В новостных сводках не единожды были опубликованы пресс-релизы в отношении вовлечения несовершеннолетних лиц и студентов в схемы обналичивания средств или передачи средств через дропперов.

Так, в 2024 году правоохранительными органами было раскрыто преступление, в ходе которого студент одного из столичных вузов, забиравший денежные средства у потерпевших и пересылавший их на счета третьих лиц (т.е. лицо, выступавшее в качестве дроппера), был привлечен к ответственности.

Поэтому в целях повышения осведомленности и выработки компетенций по определению подозрительных финансовых схем с 2024 года Учебный центр Государственной службы финансовой разведки при Министерстве финансов Кыргызской Республики активно ведет работу по внедрению компонента «Финансовая безопасность» в школьную программу.

На сегодняшний день уровень понимания рисков вовлечения в схемы дропперов среди молодежи довольно низок, поэтому для комплексного охвата и повышения эффективности усилий в Кыргызстане разработаны учебные материалы государственного образовательного стандарта по теме дропперства.

Благодаря такому обучению молодежи в среднесрочной перспективе планируется как снижение случаев «разводных» дропперов, так и повышение компетенций населения в целом в части определения схем финансового мошенничества.

Однако проблема заключается не только в обучении молодежи. Перед государством на сегодняшний день стоит задача по информированию населения о возможных рисках вовлечения в незаконную деятельность, внедрении уголовной ответственности за дропперство путем просветительских инициатив и информирования всех граждан. Так, Национальный банк Кыргызской Республики, правоохранительные органы, финансовые институты и отраслевые ассоциации прикладывают усилия для освещения среди студентов последствий неправомерных деяний через информационные кампании, внедрение системы «охлаждения кредитов», проверку операций и многое другое.

> **Важным компонентом просвещения является** обучение навыкам и выработка компетенций в части определения подозрительности любых финансовых операций и сделок, понимание, когда вовлечение в какую-либо деятельность, особенно сферу «быстрого заработка» и «легких денег», несет в себе потенциальную ответственность за незаконные деяния.

В практике довольно часто встречаются случаи, когда подросткам или студентам предлагают за определенную оплату открыть компанию, платежный инструмент или получить статус индивидуального предпринимателя.

«Перед государством на сегодняшний день стоит задача по информированию населения о возможных рисках вовлечения в незаконную деятельность, внедрении уголовной ответственности за дропперство путем просветительских инициатив и информирования всех граждан.

Нашей общей задачей является обучение и разъяснение последствий этих действий так, чтобы молодое поколение понимало, где проходит тонкая грань дозволенного и незаконного. Можно ли переводить через свои электронные кошельки деньги, если тебя об этом попросил хорошо знакомый человек? А если вместо этого человека просьба исходит от лица, которое предлагает за определенную плату проводить через свои счета средства, происхождение и назначение которых неизвестно?

На сегодняшний день наша задача — обезопасить финансовую систему страны путем повышения знаний и информирования граждан. А студенты и в целом молодое поколение — будущее Кыргызстана — должны стоять в авангарде данного движения, рассказывать о возможных рисках своим близким и старшему поколению, а также понимать ответственность за свои действия.

Федеральный университет Рио-де-Жанейро:

ВКЛАД В БОРЬБУ С ФИНАНСОВОЙ ПРЕСТУПНОСТЬЮ

Финансовые преступления, которые затрагивают представителей всех социально-экономических групп, отличаются широким разнообразием: начиная с простого мошенничества, когда используется человеческое доверие, заканчивая сложными криминальными операциями, связанными с отмыванием денег и коррупцией. Эволюционирующий характер этих преступлений обусловил необходимость эффективной системы образования, которая не только обеспечит техническую грамотность, но и воспитает твердые этические и моральные ценности.

РОБЕРТО ДЕ АНДРАДЕ МЕДРОНЬО
Ректор Федерального университета Рио-де-Жанейро, профессор, к. н.

ФАБИО КРЫХТИН
Специальный координатор международных отношений с Российской Федерацией от Федерального университета Рио-де-Жанейро, профессор, к. н.

Федеральный университет Рио-де-Жанейро, крупнейший и старейший государственный вуз Бразилии, делает решительные шаги в деле укрепления финансовой безопасности. Ведущий вуз Бразилии продвигает принцип финансовой безопасности в стенах учебного заведения и на международной арене и позиционирует себя как лидер просвещения по этим вопросам.

УЧАСТИЕ В МЕЖДУНАРОДНЫХ ПРОЕКТАХ

Университет участвует в международных инициативах по укреплению финансовой безопасности с 2022 года, с момента присоединения к Международной олимпиаде по финансовой безопасности. Вуз сразу стал активным посредником в диалоге между бразильскими академическими кругами и профильными структурами, связывая регулирующие, оперативные и правоохранительные органы на разных уровнях.

В 2023 году университет вошел в состав Международного сетевого института в сфере ПОД/ФТ, деятельность которого направлена на развитие образования в области финансовой безопасности.

Профессор Фабио Крыхтин, один из основных активистов в области образования по финансовой безопасности: *«График Международной*

олимпиады позволяет формировать такую учебную среду, в которой студенты мотивированы получать знания и развивать их: регистрация — в начале учебного года, само состязание — во втором семестре».

МЕЖВУЗОВСКИЙ ДИАЛОГ

Федеральный университет Рио-де-Жанейро также активно развивает межвузовское сотрудничество: преподаватели и студенты участвуют в семинарах вместе с международными экспертами.

Ректор Роберто Медроньо: *«Мы постоянно получаем запросы от вузов, которые стремятся наладить партнерство в области образования по проблемам финансовой безопасности. Построение справедливого и многополярного мира предполагает взаимосвязь образования, законодательства, правового регулирования и развития технологий. Мы осознаем роль Федерального университета Рио-де-Жанейро в этом формирующемся мировом пространстве».*

В прошлом году совместно с Финансовым университетом при Правительстве Российской Федерации бразильский вуз провел онлайн-семинар, на котором специалисты и студенты представили современные стратегии борьбы с отмыванием денег. На семинаре выступил государственный прокурор Рио-де-Жанейро: доктор Фабио Корреа поделился некоторыми деталями своей работы по ликвидации преступных организаций в регионе.

Положительные результаты этих инициатив очевидны в достижениях как отдельных студентов, так и команд, получивших национальное и международное признание. Политехническая школа Федерального университета Рио-де-Жанейро вручила команде «Минерва» награду за блестящее выступление на Международной олимпиаде в Сочи в 2024 году.

В нынешнем году вопросы финансовой безопасности станут центральной темой Форума Лиги ректоров России, Бразилии и Белоруссии и Форума ректоров стран БРИКС+, которые состоятся на базе Федерального университета Рио-де-Жанейро. Предстоящие форумы — еще одно доказательство стремления вуза стать мировым центром подготовки специалистов в области финансовой безопасности и международного сотрудничества.

Об авторах

Роберто де Андраде Медроньо, ректор Федерального университета Рио-де-Жанейро, профессор, к. н.

Стремясь к интеграции образования, технологий и общества, профессор Медроньо выступает за устойчивое развитие, социальное равенство и финансовую безопасность — сферы, в которых Федеральный университет Рио-де-Жанейро достиг всемирного признания.

Фабио Крыхтин, специальный координатор международных отношений с Российской Федерацией от Федерального университета Рио-де-Жанейро, профессор, к. н.

Содействует межвузовскому партнерству с российскими университетами. Его научные интересы лежат в областях экологии, аэрокосмической отрасли, искусственного интеллекта, мировой экономики и геополитики.

Формирование финансовой культуры населения: ПРОЕКТЫ ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА УПРАВЛЕНИЯ

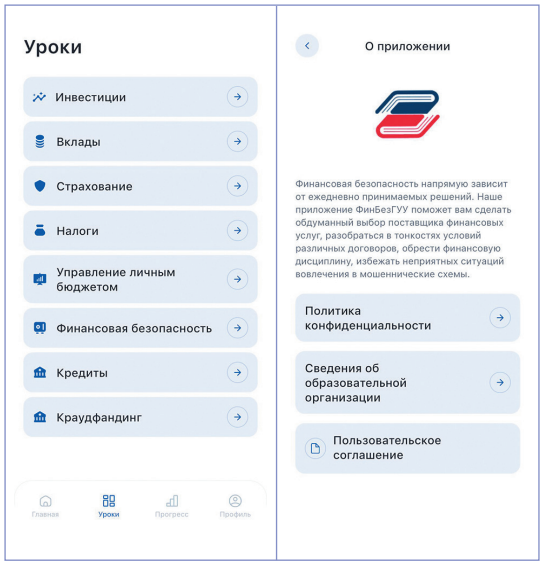
Сегодня, когда особенно остро встает вопрос противодействия финансовым преступлениям, важно формировать финансовую культуру у всех возрастных групп населения. Причем такая работа должна вестись планомерно с применением современных технологий. Участвуя в развитии Международного движения по финансовой безопасности, мы подошли к решению задачи комплексно, охватив несколько каналов связи с потенциальной аудиторией.

ВЛАДИМИР СТРОЕВ
Ректор Государственного университета управления, профессор, д.э.н.

Основной подход, который применяется в университете для широкого привлечения молодежи к решению проблем финансовой безопасности, — это применение проектных методов обучения. Начиная с первого курса студенты ГУУ объединяются в команды и разрабатывают собственные проекты, включающие в себя деловые игры по формированию финансовой культуры и финансово безопасного поведения, материалы для проведения открытых лекций и интересные кейсы.

Деловые игры, разработанные студентами, активно применяются не только во время занятий, но и для проведения профориентационных мероприятий для школьников. Студенты ежегодно проводят занятия со школьниками в виде деловых игр и финансовых квизов во время Фестиваля финансовой грамотности и предпринимательской культуры в Москве.

В 2022 году, используя подходы программной инженерии и объединив несколько проектных команд студентов, в ГУУ было разработано мобильное приложение ФинБезГУУ, которое теперь доступно в библиотеке приложений RuStore. Благодаря этому приложению можно в легкой и доступной форме не только изучить основные принципы финансово безопасного поведения и освоить базовые навыки, но также узнать о рисках и видах финансового мошенничества. Особенно важно, что весь контент разрабатывают сами студенты под руководством опытных педагогов. В данном случае студенты, применяя технологии программного обучения и решая задачу подготовки материалов, сами обучаются основам финансовой безопасности.



Практика работы с молодежью показала, что подростки и молодые люди склонны больше прислушиваться к информации, полученной от сверстников. Именно педагогическая технология «дети – детям», когда студенты старших курсов рассказывают ребятам младших курсов о проблемах финансовой безопасности, а те в свою очередь проводят лекции в школах, из которых недавно выпустились, стала еще одной основой организации движения по финансовой безопасности в стенах университета. Такой же подход с 2025 года мы стали применять и при проведении тематического урока по финансовой безопасности.

«Именно педагогическая технология «дети – детям», когда студенты старших курсов рассказывают ребятам младших курсов о проблемах финансовой безопасности, а те в свою очередь проводят лекции в школах, из которых недавно выпустились, стала еще одной основой организации движения по финансовой безопасности в стенах университета.

Кроме того, в текущем году студенты ГУУ провели пробные занятия с людьми пожилого возраста, которые все чаще страдают от действий мошенников[1]. Эксперимент получил хорошие отклики, и на следующий учебный год было принято решение продолжить эту практику, наладив взаимодействие с Центрами московского долголетия.

Расширяя охват потенциальной аудитории, студенты ГУУ решили снимать короткие видеоролики о потенциальных угрозах финансовой безопасности. Сценарий видеоролика выстроен таким образом, что диалог ведется от лица пострадавшего. После чего специалисты дают свои комментарии о том, что неверно сделал пострадавший, и предлагают способы избежать подобных ситуаций. Ролики размещаются на RUTUBE-канале университета и в его социальных сетях.

Комплексное развитие движения финансовой безопасности невозможно без междисциплинарного взаимодействия. Это взаимодействие заключается не только в привлечении к движению студентов, обучающихся по программам экономики и финансов, но и студентов других направлений. Государственный университет управления уделяет особое внимание перспективным направлениям решения задач обеспечения финансовой безопасности, формируя среду, в которой каждый студент и сотрудник университета сможет не только сам получить важные актуальные знания в этой области, но и грамотно и доступно донести их до своего окружения.

[1] Согласно данным Банка России, в 2024 году наблюдался рост числа граждан старше 65 лет, пострадавших от действий кибермошенников, в 2024 году 16,6% пострадавших — это пожилые люди.

ПРОФИЛАКТИКА ДРОППЕРСТВА И МОШЕННИЧЕСТВА СРЕДИ СТУДЕНТОВ РГЭУ (РИНХ)

Современное общество — это общество массовых коммуникаций и больших данных, где под влиянием технологий происходит трансформация социальной реальности и актуализируются риски манипулирования финансовым поведением населения.

ЕЛЕНА МАКАРЕНКО
Ректор РГЭУ (РИНХ), заместитель Председателя Общественной палаты Ростовской области, профессор, д. э. н.

ЮЛИЯ ЕВЛАХОВА
Заведующая кафедрой финансового мониторинга и финансовых рынков РГЭУ (РИНХ), профессор, д. э. н.

Функциональные возможности цифровых технологий создают новую платформу финансовой активности человека: поддержка принятия кредитных и инвестиционных решений, доступность финансовых продуктов и услуг и их персонификация благодаря обработке и анализу больших данных, новые виды инвестиционных активов и многое другое. С развитием технологий появляется возможность получить для исследования и анализа такую информацию, которая раньше была недоступна.

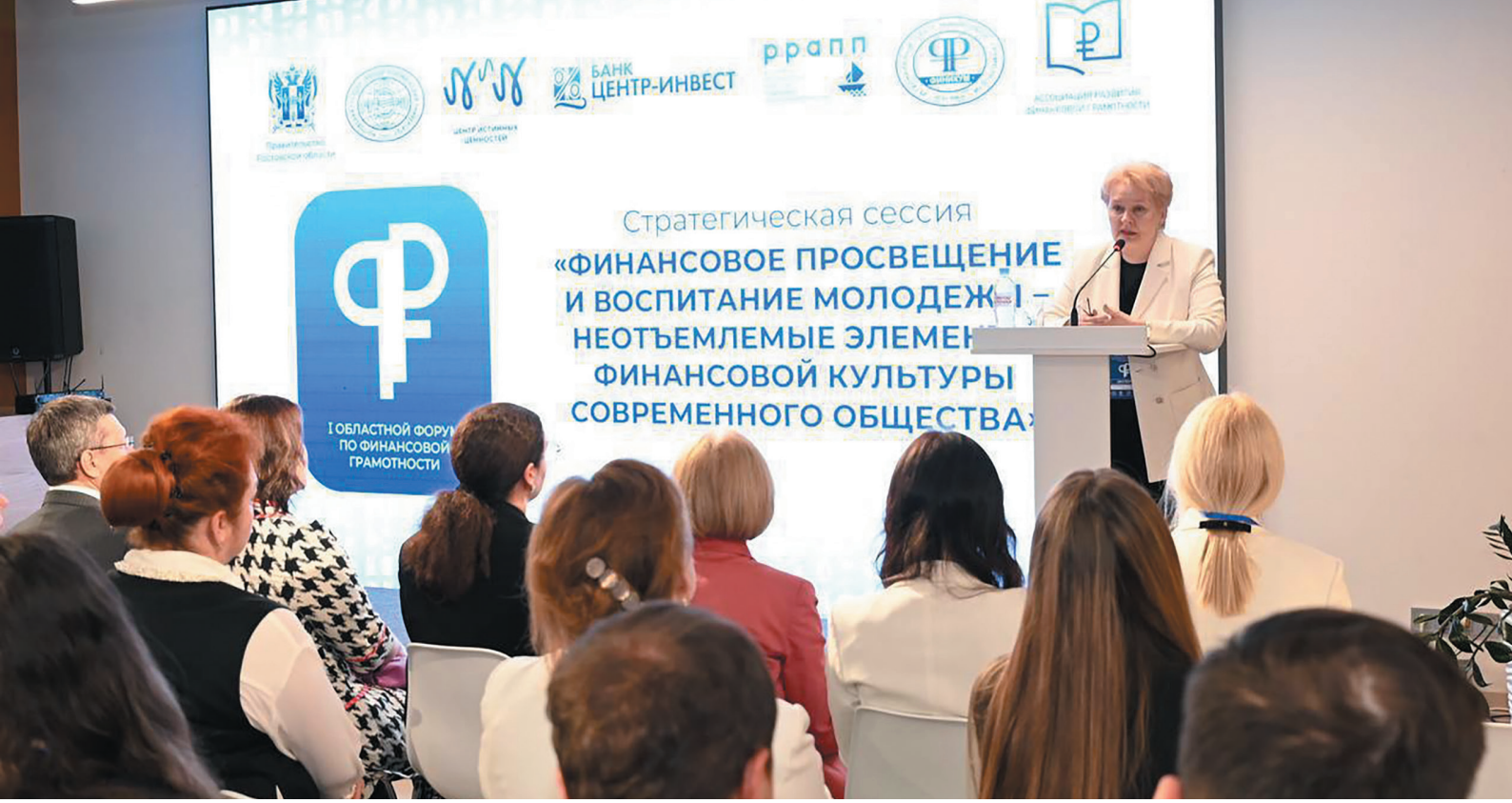
В то же время эта трансформация приводит к появлению новых видов финансовых мошенничеств, актуализации цифрогенных угроз финансовой стабильности.

В сегодняшних условиях цифровизации экономики, когда стоит задача расширения пользы от распространения цифровых инноваций с одновременным ограничением рисков от их использования, в Ростовском государственном экономическом университете (РИНХ) особое внимание уделяют профилактике вовлечения студентов в незаконные финансовые операции.

Образовательная деятельность по профилактике вовлечения студентов РГЭУ (РИНХ) в дропперство и мошенничество реализуется по двум ключевым направлениям:

- в рамках учебного процесса — при изучении дисциплин по противодействию коррупции и отмыванию преступных доходов, по типологиям сомнительных финансовых операций, по регулированию финансовых рынков
- вплетение профилактики дропперства и мошенничества во внеучебную активность: научно-исследовательскую, проектную, воспитательную работу

Уже более 10 лет РГЭУ (РИНХ) готовит специалистов для противодействия легализации доходов и финансированию терроризма в экономике Южного федерального округа по всей линейке образова-



тельных уровней: бакалавриат — магистратура — аспирантура. В программы дисциплин включены модули по характеристике сомнительных финансовых операций, а также по обучению навыкам и умениям противодействия им. Для обучения студентов в университете используются передовые образовательные технологии. Преподаватели РГЭУ (РИНХ) совместно с практиками из МРУ Росфинмониторинга по ЮФО разрабатывают учебники и учебные пособия. Например, учебник и практикум «Финансовая кибербезопасность», включающие в том числе задания по профилактике дропперства и мошенничества. В настоящее время преподаватели университета ведут работу над практическим пособием «Путеводитель по личной финансовой безопасности», сфокусированным на темах противодействия дропперству, телефонному, кредитному, криптовалютному мошенничеству, финансовым пирамидам.

Профилактика дропперства и мошенничества среди студентов университета осуществляется в том числе с использованием цифровых технологий на базе Междисциплинарной лаборатории финансовой разведки и компьютерной криминалистики. Эта высокотехнологичная научно-образовательная лаборатория, открытая в июне 2022 года, дает возможность интегрировать в образовательный процесс кейсы из реальной хозяйственной практики. В частности, в рамках курса по изучению типологий сомнительных финансовых операций студенты изучают кейсы «Финансовые пирамиды», учатся определять дропов среди участников финансово-хозяйственной деятельности, а также узнают о мерах ответственности физических и юридических лиц за участие в теневых схемах.

> **«В программы дисциплин включены модули по характеристике сомнительных финансовых операций, а также по обучению навыкам и умениям противодействия им.**

Существенную роль в профилактике дропперства и мошенничества в рамках учебного процесса играют мастер-классы и встречи с представителями субъектов российской системы ПОД/ФТ.

В 2025 году запущены семинары-практикумы по финансовой грамотности для трудовых коллективов «Осторожно, звонят» и для обучающихся образовательных организаций «Внимание, дроппер!» с участием представителей Главного управления МВД России по Ростовской области.

В рамках внеучебной активности вопросы профилактики дропперства и мошенничества среди студентов рассматриваются в университете при осуществлении научно-исследовательской и проектной деятельности.

Так, в апреле 2025 года в Центре истинных ценностей впервые прошел Областной форум по финансовой грамотности «К финансовой культуре через волонтерство, воспитание и просвещение». В течение двух дней площадки форума посетили более 1500 гостей.

Профилактика дропперства и мошенничества обсуждалась на различных площадках Форума. Одна из активных дискуссий развернулась в рамках форсайт-сессии «Личная финансовая безопасность в мире ИИ: вызовы времени», где действовали две команды: команда студентов и экспертов и команда ИИ. Каждая команда сформировала свой перечень потенциальных угроз финансовой безопасности со стороны ИИ. Примечательно, что обе команды сошлись во мнении об опасности использования ИИ как инструмента мошенников.

В ноябре 2024 года РГЭУ (РИНХ) провел II Международный научно-практический форум «Обеспечение финансового суверенитета на основе достижения финансовой безопасности и развития финансовых рынков». Одной из центральных тем, обсуждавшихся на Форуме, стало противодействие вовлечению молодежи в незаконные финансовые операции.

Проведение научно-образовательных форумов, затрагивающих тематику противодействия мошенничеству и дропперству, является отличным стимулом для студентов обратить внимание на эту проблему, изучить факты, условия, последствия как с практической, так и с исследовательской точки зрения. По итогам таких исследований студенты выступают с докладами, готовят научные статьи, участвуют в конкурсах.

Научно-исследовательская работа тесно сопряжена с просветительской деятельностью в части информирования молодежи об опасности дропперства. В апреле 2025 года студентами РГЭУ (РИНХ) был подготовлен просветительский видеоролик, показывающий последствия неверной модели поведения при встрече с мошенниками и, самое важное, формирующий правильные поведенческие установки.

Одним из наиболее эффективных для просвещения и пропаганды разумного финансового поведения становится видеоформат. Поэтому региональным Центром финансовой грамотности «Финикум», работающим на базе РГЭУ (РИНХ), весной 2025 года был организован конкурс видеороликов и публикаций в социальных сетях «Внимание, дроппер!» среди школьников в двух возрастных категориях (до 15 лет и старше).

Таким образом, профилактика дропперства и мошенничества среди студентов, а также противодействие их вовлечению в незаконные финансовые операции в Ростовском государственном экономическом университете (РИНХ) осуществляется в разных форматах с привлечением практических специалистов, инструментария искусственного интеллекта и социальных сетей.

НГУЭУ — ВУЗ С АКТИВНОЙ ПОЗИЦИЕЙ В ВОПРОСАХ ЗАЩИТЫ МОЛОДЕЖИ ОТ ВОВЛЕЧЕНИЯ В ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ

Финансовое мошенничество в современной России стало довольно распространенным явлением. Так, по данным Банка России, в 2024 году число субъектов с признаками нелегальной деятельности выросло почти в 1,6 раза, зафиксировано более 5 тысяч финансовых пирамид, почти 2 тысячи нелегальных профучастников рынка ценных бумаг и 1,5 тысячи черных кредиторов. Тенденцией в этой сфере становится то, что внимание мошенников все чаще обращается на молодое поколение с целью вовлечения его в противоправную деятельность.

ПАВЕЛ НОВГОРОДОВ
Ректор Новосибирского государственного университета экономики и управления, доцент, к.э.н.

СЕРГЕЙ АНОФРИКОВ
Заведующий кафедрой общественных финансов Новосибирского государственного университета экономики и управления, доцент, к.э.н.

НГУЭУ
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ

Как участник Международного сетевого института в сфере ПОД/ФТ НГУЭУ проявляет активную позицию в борьбе с данными негативными явлениями и осуществляет комплекс мер, направленных на нетерпимое отношение молодежи к финансовому мошенничеству. С самого зарождения Международной олимпиады по финансовой безопасности НГУЭУ выступает площадкой в СФО для проведения отборочного этапа, а также привлекает к участию в ней студентов, которые за все время проведения Олимпиады становились призерами и победителями.

Студенты — участники Олимпиады — формируют актив, реализующий ежегодно цикл встреч, посвященных вопросам финансовой безопасности. Со школьниками и обучающимися колледжей и вузов эти и другие студенты, присоединившиеся к Международному движению по финансовой безопасности, в текущем году проводили тематический урок «НЕдетские игры: 2.0. Дроп поневоле». Нужно отметить, что в НГУЭУ, с одной стороны, увеличивается количество студентов, вовлеченных в данную

волонтерскую деятельность, а с другой стороны, расширяется охват внешних слушателей из числа молодежи. Если за весь 2023/2024 учебный год в подобных встречах приняли участие более 1,5 тысяч школьников и студентов, то уже на конец апреля 2024/2025 учебного года их число превысило 2 тысячи человек.

Кроме того, работа НГУЭУ со школьниками в указанном направлении реализуется в рамках созданного на базе новосибирской Гимназии № 10 профильного класса по финансовой безопасности. Кроме уроков, связанных с тематикой ПОД/ФТ и проводимых преподавателями кафедры общественных финансов НГУЭУ, для ребят на регулярной основе организуются встречи с представителями Межрегионального управления Росфинмониторинга, студентами — участниками Олимпиады по финансовой безопасности, руководителями банков и других организаций финансового сектора.

Для обсуждения научных подходов и практических аспектов решения проблем финансовой безопасности государства и личности в НГУЭУ ежегодно проводится конференция, которая в 2025 году перешла в статус Международного форума.

Кроме того, НГУЭУ совместно с Новосибирским филиалом Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева проводит ряд мероприятий, в ходе которых организуются круглые столы и практические семинары, посвященные выявлению новых тенденций и схем совершения финансовых преступлений, а также и обмену опытом между исследователями и практиками.

Интересным инструментом решения прикладных задач является проект НГУЭУ «Интеллектуальная биржа: третья миссия университета». В рамках данного проекта студенты и преподаватели участвуют в разработке тем, актуальных для внешних заказчиков — органов власти и представителей бизнеса. В частности, по заказу МРУ Росфинмониторинга по СФО в 2024 году студенткой специальности «Экономическая безопасность» была разработана концепция и защищена выпускная квалификационная работа, посвященная рискам вовлеченности сделок по приобретению недвижимого имущества в отмывание доходов, полученных преступным путем, и финансирование терроризма, а в текущем году студенты готовят курсовые работы на тему «Вовлечение молодежи в финансовые преступления (дроппинг) как угроза экономической безопасности страны/личности».

В рамках проекта «Выпускная квалификационная работа как стартап» студенты НГУЭУ проводят исследования, направленные на решение проблем, связанных с кибербезопасностью. Например, в этом году студенты разработали веб-приложения, которые планируется использовать в целях повышения осведомленности и снижения риска вовлечения несовершеннолетних в киберпреступления.

Выражаем надежду, что прилагаемые НГУЭУ усилия, а также совместная работа участников Международного сетевого института в сфере ПОД/ФТ в рамках Международного движения по финансовой безопасности принесут положительные результаты в формировании негативного отношения молодежи к финансовым преступлениям.

ОБРАЗОВАТЕЛЬНЫЕ ПРОЕКТЫ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ В ТЮМЕНСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ

Сегодня, несмотря на стремление государственных институтов и общественности защитить население от мошенничества, граждане продолжают сталкиваться с фактами незаконных действий с финансовыми средствами. Нередки случаи дропперства, особенно среди молодежи.

ДМИТРИЙ СКИПИН
Заведующий кафедрой экономической безопасности, системного анализа и контроля ТюмГУ, доцент, к. э. н.

ДАРЬЯ ЛАЗУТИНА
Директор Финансово - экономического института ТюмГУ, проректор, доцент, к. э. н.

Студенты вузов активно пользуются услугами онлайн-сервисов, мобильными приложениями, в сети они встречаются с предложениями получения заработка, не требующего усилий и времени (например, по оказанию посреднических услуг, переводу и обналичиванию средств, которые они не всегда идентифицируют как нелегальные). Для предотвращения таких случаев вузам необходимо включать в образовательную и воспитательную работу проекты, направленные на повышение осведомленности студентов о рисках киберпреступлений, формирование у них критического мышления и способности к объективной оценке ситуации.

Тюменский государственный университет (ТюмГУ) активно внедряет образовательные и профилактические программы, чтобы защитить студентов от вовлечения в противоправную деятельность. В университете действует Управление молодежной политики и Координационный центр по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных и межконфессиональных конфликтов, противодействия идеологии терроризма и профилактике экстремизма. Одним из направлений деятельности этих структур является повышение правосознания и профилактика вовлечения молодежи в объединения деструктивной направленности.

▸ В ТюмГУ налажена систематическая просветительская работа по правовой ответственности за участие в мошеннических действиях.

- Центр информационных технологий регулярно делает рассылку предупреждений о новых схемах мошенников через корпоративные каналы
- Центр стратегических коммуникаций проводит информационные кампании, направленные на повышение финансовой грамотности студентов и сотрудников вуза
- Представители Управления по образовательной деятельности разъясняют последствия неправомерных действий

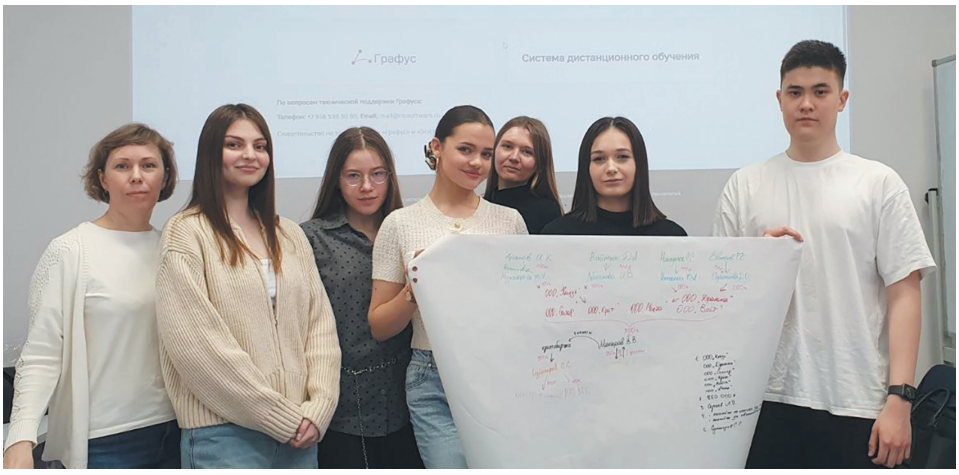
Организовано психолого-педагогическое сопровождение студентов на протяжении всего периода обучения. Действует консультативный центр психологической помощи, который осуществляет поддержку в том числе и в случаях угрозы вовлечения в мошеннические схемы, при необходимости в преодолении стресса и тревожности, а также в любой сложной ситуации. Внедренная в университете система индивидуальных траекторий и обучение по модели «2+2+2» в рамках стратегического проекта «Мультипарадигмальное образование» позволяют интегрировать в образовательные программы дисциплины, направленные на освоение знаний по финансовой грамотности, которая является залогом успеха в борьбе с мошенничеством.

В ряде образовательных программ в профессиональных блоках реализуются дисциплины, направленные на противодействие мошенническим схемам.

Работа по профилактике мошеннических действий финансового характера проводится как со студентами вуза, так и со школьниками. Ряд проектов, направленных на предотвращение участия молодежи в незаконных финансовых действиях, реализует кафедра экономической безопасности, системного анализа и контроля Финансово-экономического института. В них входят мастер-классы со школьниками, а также кейс-турнир по финансовой безопасности. В процессе мероприятий участники узнают о распространенных видах финансового мошенничества, учатся выявлять преступные схемы с помощью обучающей системы «Графус». Как участник Международного сетевого института в сфере ПОД/ФТ ТюмГУ регулярно выступает агентом по привлечению и подготовке школьников и студентов к участию в Международной олимпиаде по финансовой безопасности.

ТюмГУ системно организует научно-практические форумы, конференции, круглые столы, включающие вопросы цифровой безопасности и борьбы с мошенничеством. В качестве спикеров на мероприятия приглашаются представители вузов, правоохранительных органов, государственного сектора, бизнеса. Представители правоохранительных органов выступают как ключевые эксперты, обеспечивая практико-ориентированный подход к решению проблемы финансовых преступлений в студенческой среде. Банк России выступает как ключевой регулятор, обеспечивающий системную защиту от финансовых преступлений через регулирование, технологии и просвещение. Эксперты в области информационных технологий делятся опытом, представляют новые разработки, дают рекомендации по защите пользователей от цифровых угроз, что помогает формировать у студентов ответственность за действия в виртуальном пространстве.

Университет реализует комплексный подход в профилактике и борьбе с дропперством и мошенничеством, постоянно внедряются новые проекты и формы работы, направленные на обеспечение финансовой безопасности, растет число участников, задействованных в этой деятельности. Многоуровневая система профилактики и комплексные образовательные проекты ТюмГУ формируют у студентов культуру цифровой безопасности, превращая профилактику дропперства и мошенничества из набора правил в естественный образ мышления.



Международный диктант по финансовой безопасности:

ГЛОБАЛЬНЫЙ СРЕЗ КОМПЕТЕНЦИЙ И СТРАТЕГИЧЕСКИЙ ИНСТРУМЕНТ ПРЕВЕНТИВНЫХ МЕР

В 2024 году свыше 17 тысяч участников из 15 стран — школьников, студентов, учителей, преподавателей, экспертов и активных граждан — приняли участие в первом Международном диктанте по финансовой безопасности.

МАРИНА ШЕМЯКИНА
Руководитель Центра межолимпиадной подготовки школьников и студентов (ФИАН)

АЛЕКСАНДРА ВАЩЕНКО
Пресс-секретарь Центра межолимпиадной подготовки школьников и студентов (ФИАН)

Инициатива Росфинмониторинга, Центра межолимпиадной подготовки школьников и студентов ФИАН, Международного учебно-методического центра финансового мониторинга, Ассоциации развития финансовой грамотности и Санкт-Петербургского политехнического университета Петра Великого не только продемонстрировала значительный масштаб и широкую географию охвата, но и выявила высокий общественный интерес к области финансовой безопасности, включая критически важные вопросы противодействия отмыванию доходов и финансированию терроризма. Каковы ключевые итоги этого масштабного образовательного проекта, в чем его стратегическое значение как инструмента формирования культуры финансовой безопасности в обществе и почему экспертному сообществу стоит не только внимательно следить за его развитием, но и принять участие в новом цикле, запланированном на сентябрь – октябрь 2025 года?

ЗАЧЕМ ПИСАТЬ МЕЖДУНАРОДНЫЙ ДИКТАНТ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ?

Международный диктант по финансовой безопасности — это не просто проверка знаний, это эффективный инструмент просвещения, обучения и повышения осведомленности молодежи и людей разного возраста о проблемах в сфере финансовой безопасности, в том числе о финансовом мошенничестве. Он помогает формировать необходимые навыки и привычки, позволяющие лю-

дям защитить себя и свои финансы от потенциальных угроз стать жертвой и/или соучастником финансовых преступлений.

Диктант-2024 — это 20 интересных вопросов из предметной области: от истории возникновения финансовых пирамид до примеров финансового мошенничества с использованием криптовалют, дропперства и искусственного интеллекта.

Важным элементом методики проведения Диктанта является мгновенная обратная связь: к каждому вопросу прилагается подробный комментарий экспертов, объясняющий правильный ответ или оптимальный порядок действий. Это превращает Диктант в эффективный тренажер, который можно использовать для самостоятельного обучения. Тема Диктанта посвящена вопросам финансовой безопасности личности как основы финансовой безопасности государства. Она акцентирует внимание на том, что надежный фундамент национальной финансовой стабильности, за который отвечают специалисты в области ПОД/ФТ, формируется в том числе благодаря повышению финансовой грамотности и знаний в сфере финансовой безопасности каждого человека: от молодежи до людей старшего поколения, независимо от уровня образования, профессии и жизненного опыта.

КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ ДИКТАНТА-2024: ЧТО ПОКАЗЫВАЕТ СТАТИСТИКА?

Результаты первого Диктанта — это не просто цифры, а ценный срез общественного уровня знаний в области финансовой безопасности, позволяющий выявить как сильные стороны, так и зоны, требующие особого внимания со стороны государства и экспертного и образовательного сообщества:

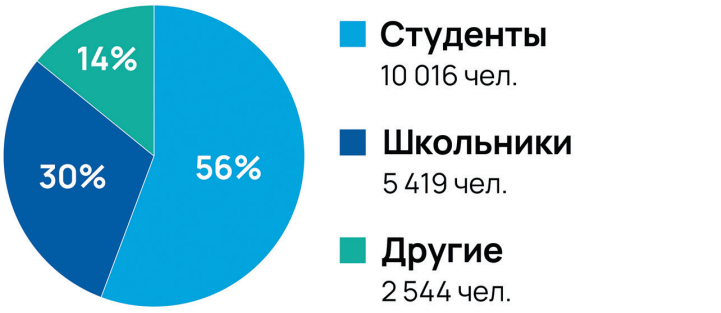
1. География и охват — свидетельство глобального интереса: участие 17 979 человек из 15 стран, включая страны ЕАГ и БРИКС, подчеркивает международный масштаб проекта и его востребованность среди разных аудиторий, что способствует укреплению межстранового сотрудничества в области финансовой грамотности и безопасности. Такой широкий охват показывает, что тема финансовой безопасности актуальна не только внутри страны, но и на международном уровне, объединяя участников разных возрастов и профессий для совместного повышения уровня знаний и обмена опытом.

2. Результативность — стимул для дальнейшего роста: около 45% участников (8183 человека) стали победителями, набрав 90 и более баллов из 100 возможных. Среднее число попыток для улучшения своего результата (в среднем 2,29 на 1 участника) свидетельствует о высокой вовлеченности и искреннем желании разобраться в материале, доказывая обучающий и мотивирующий характер Диктанта, что особенно важно при работе с молодежной аудиторией.

3. Форматы проведения — доступность для каждого: интеграция двух ключевых форматов проведения на онлайн-платформе (rosfindictant.ru) и в формате очного мероприятия (на финале IV Международной олимпиады по финансовой безопасности) способствовала максимальному привлечению участников различных категорий, обеспечило широкое географическое и демографическое покрытие.

4. «Точки роста» и необходимость фундаментальных знаний: анализ результатов Диктанта выявил, что наибольшие трудности у участников вызвал вопрос, связанный с определением базового понятия «финансовая безопасность»: лишь 62% респондентов дали правильный ответ с первой попытки. Полученные данные свидетель-

СТРУКТУРА УЧАСТНИКОВ МЕЖДУНАРОДНОГО ДИКТАНТА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ — 2024



«Проект успешно выполняет свою образовательную миссию, стимулируя рост финансовой грамотности и знаний в области финансовой безопасности среди широкой аудитории, создавая основу для развития подобных образовательных и просветительских инициатив в будущем.

ствуют о том, что интуитивное или поверхностное понимание проблематики финансовой безопасности не всегда подкреплено системными и четкими знаниями ее теоретических основ. Это обстоятельство актуально для всех целевых аудиторий Диктанта, независимо от уровня их подготовки. Следовательно, существует острая необходимость усиления фундаментальной образовательной и научной базы, что позволит повысить качество восприятия и применения знаний в области финансовой безопасности.

5. Сильные стороны — успех просветительской работы: в то же время вопрос о недопустимости предоставления удаленного доступа к устройствам «сотрудникам банка» оказался одним из самых легких (76% верных ответов). Это подтверждает, что целенаправленная просветительская работа способствует формированию у населения практических навыков и осознанного поведения, необходимого для защиты от финансовых рисков и угроз, противодействия распространенным мошенническим схемам.

Анализ этих данных показывает, что проект успешно выполняет свою образовательную миссию, стимулируя рост финансовой грамотности и знаний в области финансовой безопасности среди широкой аудитории, создавая основу для развития подобных образовательных и просветительских инициатив в будущем.

17 сентября - 1 октября 2024 г.

Всего попыток: **41170**
Всего участников: **17979**
Число попыток в среднем на 1 чел: **2,29**

Число стран: **15**

САМЫЙ СЛОЖНЫЙ ВОПРОС
1. Что такое финансовая безопасность?

62% опрошенных
ответили правильно (с первого раза)

СТРАТЕГИЧЕСКОЕ ЗНАЧЕНИЕ ДИКТАНТА-2025 ДЛЯ ФОРМИРОВАНИЯ БЕЗОПАСНОЙ ФИНАНСОВОЙ СРЕДЫ

Почему стоит рассматривать Международный диктант по финансовой безопасности не просто как еще одно очередное образовательное мероприятие, а как важный инструмент стратегического развития, который не только формирует компетенции в области финансовой безопасности у населения, но и создает основу для долгосрочной финансовой стабильности и безопасности государства в целом:

- **Масштабный инструмент повышения финансовой культуры:** Диктант охватывает аудиторию, до которой не всегда легко достучаться стандартными методами — от школьников до людей старшего поколения. Повышение их осведомленности снижает общую уязвимость населения перед финансовыми мошенниками.
- **Формирование превентивного мышления:** в процессе ответов на вопросы Диктанта участники учатся распознавать угрозы до того, как столкнутся с ними в реальной жизни. Это прямой вклад в профилактику и противодействие финансовых правонарушений.
- **Срез актуальных знаний для корректировки стратегий:** результаты Диктанта — это ценная обратная связь, показывающая, какие темы усвоены хорошо, а какие требуют дополнительного разъяснения. Представители научного и образовательного сообщества могут использовать эти данные для совершенствования своих образовательных программ и методик обучения, акцентируя внимание на наиболее проблемных вопросах, эксперты — при формировании публичных выступлений, государственные ведомства — в продвижении законодательных инициатив.
- **Популяризация профессий в сфере финансовой безопасности:** для молодежи участие в Диктанте может стать первым шагом к выбору профессии и/или формированию карьерной траектории в антиотмывочной системе, что важно для кадрового обеспечения отрасли.
- **Платформа для диалога и распространения лучших практик:** успешный международный формат способствует обмену опытом и адаптации передовых методик и технологий обучения в целях гармонизации и поддержания высоких стандартов образования в разных странах.

Таким образом, поддерживая и популяризируя Диктант, экспертное сообщество инвестирует в более грамотное и ответственное финансовое поведение граждан,

что, в свою очередь, укрепляет стабильность всей финансовой системы и снижает нагрузку на надзорные, правоохранительные и контролирующие органы.

СЛЕДУЮЩИЙ ЭТАП: 1 СЕНТЯБРЯ – 1 ОКТЯБРЯ 2025 ГОДА: НОВАЯ ВОЛНА ЗНАНИЙ!

Организаторы уже приступили к подготовке второго Международного диктанта по финансовой безопасности, старт которого намечен на 1 сентября 2025 года. Ожидается, что он станет еще более интересным, охватит новые актуальные темы.

Приглашаем школьников, студентов, представителей научного и образовательного сообщества, государственного и частного сектора принять участие в Международном диктанте по финансовой безопасности – 2025.

Международный диктант по финансовой безопасности представляет собой не просто инструмент оценки знаний, а драйвер трансформаций в общественном сознании. Он открывает уникальную возможность для каждого — от школьника до признанного эксперта — стать активным участником формирования устойчивой и защищенной финансовой среды. И чем шире будет его аудитория, тем ощутимее будет результат для всех нас.

Приглашаем заинтересованные ведомства и организации стать соорганизаторами Международного диктанта по финансовой безопасности – 2025!

Старт диктанта: 1 СЕНТЯБРЯ 2025 Г.

Актуальная информация и анонсы будут доступны на официальном сайте Диктанта (rosfindictant.ru) и официальных сайтах и телеграм-каналах партнеров.

rosfindictant.ru

РОЛЬ МЕЖДУНАРОДНОГО ДВИЖЕНИЯ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ И ЕГО ПОСЛОВ В ФИНАНСОВОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ:

КАК НЕ СТАТЬ СОУЧАСТНИКОМ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

В этой статье я хотел бы осветить важность привлечения внимания молодежи к вопросам финансовой безопасности и мер поддержки, которые Международное движение по финансовой безопасности оказывает студентам из разных стран.

МАССЕНГАР РОНГАР НГЕТОБАЙ

Посол Международного движения по финансовой безопасности

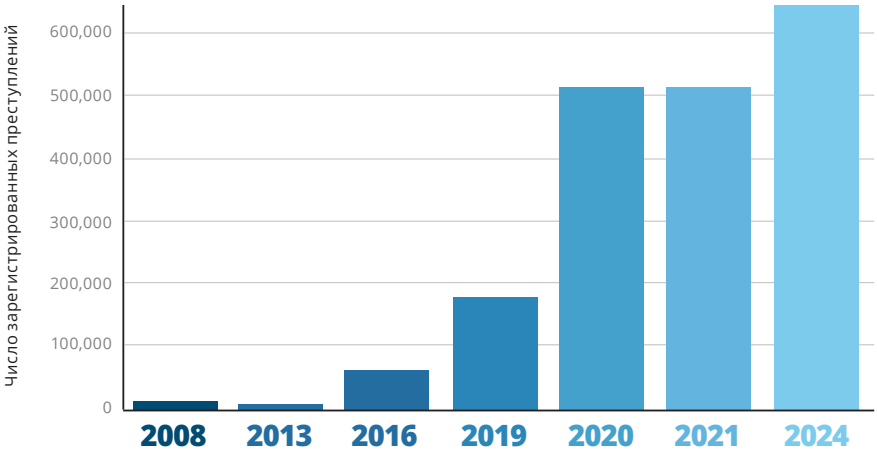
Современные технологии, предоставляя беспрецедентные возможности для развития бизнеса и коммуникации, одновременно порождают серьезные вызовы в сфере финансовой безопасности. Один из них связан с ростом киберпреступности: динамика зарегистрированных в России преступлений за период с 2008 по 2024 год позволяет увидеть, насколько быстро и масштабно меняется ландшафт цифровых угроз.

Так, в 2008–2013 годах число киберпреступлений оставалось относительно невысоким, порядка 11–14 тысяч случаев в год, однако уже к 2016 году их количество возросло почти в шесть раз, достигнув около 66 тысяч зарегистрированных инцидентов. Эта тенденция усилилась к 2019 году, когда за восемь месяцев было зафиксировано порядка 180 тысяч правонарушений.

В 2020–2022 годах цифровизация экономики и вынужденный переход многих сфер жизни в онлайн в условиях пандемии COVID-19 привели к более чем двукратному росту числа киберпреступлений — до 510 тысяч случаев. В 2024 году был побит очередной рекорд: за год зарегистрировано уже 640 тысяч преступлений, что на 25% превышает показатель 2022 года.

Такая динамика вызывает серьезное беспокойство, ведь каждый новый виток развития цифровых технологий открывает злоумышленникам дополнительные каналы для атак: фишинговые рассылки, мошенничество с банковскими кар-

ГИСТОГРАММА ЗАРЕГИСТРИРОВАННЫХ КИБЕРПРЕСТУПЛЕНИЙ В РОССИИ



Источник: составлено автором на основе данных МВД России и ФСБ России

тами, несанкционированный доступ к аккаунтам и корпоративным системам, кража данных и многое другое.

Чтобы молодые люди не стали жертвами финансового мошенничества, мы как послы Международного движения по финансовой безопасности, обращаем внимание на то, что тема финансовой безопасности касается каждого из нас. Для надежной защиты личных данных и финансовых активов необходимо:

- ответственно выбирать финансовые продукты: проверять их репутацию и избегать сомнительных предложений;
- развивать критическое мышление: осознанно использовать технологии и оценивать потенциальные угрозы;
- формировать финансовую грамотность с раннего возраста — это позволит новым поколениям принимать взвешенные решения и предотвращать кризисные ситуации.

Таким образом, финансовая грамотность и продуманное применение современных технологий — ключ к сохранению безопасности и стабильности в нашем быстро меняющемся мире.

Мы активно работаем над тем, чтобы Международное движение по финансовой безопасности находило последователей по всему миру. Как посол Движения я лично взаимодействую со студентами из разных стран Африки, Азии, Латинской Америки и других регионов.

Нашей целью является не только укрепление финансовой безопасности, но и создание глобального сообщества. Каждый участник Движения может внести свой вклад в формирование устойчивого финансового будущего. Только благодаря совместным усилиям, знаниям, ресурсам и опыту мы сможем противостоять быстрому росту киберпреступности и защитить финансовые интересы общества.

Нам необходимо не только реагировать на уже совершенные атаки, но и выстроить стратегию превентивной защиты, обеспечивающую финансовую безопасность в условиях постоянно меняющейся цифровой среды.

Для помощи студентам разработано мобильное приложение «Содружество», которое позволяет использовать все функции цифровой платформы со своего смартфона. После регистрации студенты получают доступ к материалам и учебным ресурсам: рабочим тетрадям, тестам и заданиям олимпиад прошлых лет, а также получают возможность присоединиться к дискуссиям и обменяться опытом, пройти тренировочные тесты для повышения своих навыков.

Международное движение по финансовой безопасности объединяет страны для борьбы с такими вызовами современности, как:

- отмывание денег, подрывающее экономические системы;
- киберпреступность, угрожающая безопасности транзакций;
- финансирование терроризма, разрушающее глобальную стабильность.

Многие иностранные студенты проявляют интерес к Международной олимпиаде по финансовой безопасности и стремятся присоединиться к нашему сообществу. Олимпиада — это не просто соревнование, это возможность:

- углубить знания в сфере финансовой безопасности;
- изучить лучшие практики и инновационные методы;
- стать частью международной сети единомышленников.

МЫ ПРИГЛАШАЕМ СТУДЕНТОВ И ШКОЛЬНИКОВ не только принять участие в Олимпиаде, но и стать активными членами нашего сообщества. Их идеи помогут создать мир, где финансовая стабильность доступна каждому.

НОВОСТИ АНТИОТМЫВОЧНОЙ СИСТЕМЫ

БРАЗИЛИА: СОСТОЯЛОСЬ ДЕСЯТОЕ ЗАСЕДАНИЕ РАБОЧЕЙ ГРУППЫ БРИКС ПО АНТИТЕРРОРУ (РГАТ)

В мероприятии приняли участие представители профильных министерств и ведомств Бразилии, Египта, Китая, Индии, Индонезии, Ирана, ОАЭ, России, Эфиопии, ЮАР и других стран.

Сотрудники Росфинмониторинга поделились с зарубежными коллегами опытом оказания технического содействия в сфере противодействия отмыванию преступных доходов и финансированию терроризма странам БРИКС, а также итогами первого этапа инициированного ранее российской стороной исследования по выявлению особенностей финансирования деятельности международных террористических организаций.

МОСКВА: РОССИЯ ПРИНЯЛА 42-Ю ПЛЕНАРНУЮ НЕДЕЛЮ ЕВРАЗИЙСКОЙ ГРУППЫ ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (ЕАГ)

Мероприятие объединило представителей финансовых разведок, профильных министерств и ведомств, частного сектора, экспертных и научных кругов более чем из 15 стран Евразийского региона, Ближнего Востока, Африки, Юго-Восточной Азии, а также международных организаций.

В течение недели прошли такие значимые события, как IV Форум парламентариев государств — членов ЕАГ, Совместный форум надзорных органов и частного сектора под эгидой ЕАГ и МЕНАФАТФ «Управление рисками в эпоху новых технологий», 22-е заседание Совета Международного сетевого института в сфере ПОД/ФТ, панельная дискуссия «Актуальные вопросы освещения темы финансовой безопасности в Евразийском регионе» и ряд других.

ВЕНА: В АВСТРИИ ПОД ЭГИДОЙ УПРАВЛЕНИЯ ООН ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ (УНП ООН) СОСТОЯЛАСЬ МЕЖПРАВИТЕЛЬСТВЕННАЯ ВСТРЕЧА ПО ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИИ О БЕНЕФИЦИАРНОМ ВЛАДЕНИИ В ЦЕЛЯХ УКРЕПЛЕНИЯ ВОЗВРАТА АКТИВОВ

В рамках Межправительственной встречи делегаты обменялись практиками по обеспечению прозрачности бенефициарной собственности, укрепления международного антикриминального сотрудничества и совершенствования механизмов возврата преступных активов.

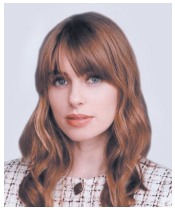
Представитель Росфинмониторинга выступил с докладом на тему правового регулирования обеспечения прозрачности бенефициарного владения юридических лиц и трастов в России.

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.

Гилета Е.С.

Корнев И.А.

Крылов О.В.

Лисицын А.С.

Петренко А.Г.

Тетеруков С.А.

Уваров И.А.

Шемякина М.С.

Росфинмониторинг и МУМЦФМ в Telegram и VKontakte

Издательство
Автономная некоммерческая организация
Международный учебно-методический центр финансового мониторинга
105064, г. Москва, Хомутовский тупик, 5А, стр. 1.
E-mail: info@mumcfm.ru
Тираж 600 экземпляров.

МУМЦФМ
2025