УДК 338.2
DOI: 10.52531/1682-1696-2025-25-2-47-53
EDN: IKNNAN
Научная статья

СОЦИАЛЬНЫЕ СЕТИ КАК ИНФОРМАЦИОННАЯ ОСНОВА ДЛЯ ДЕЯТЕЛЬНОСТИ ПО ОТМЫВАНИЮ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

А.Н. Столярова
АО «Институт региональных экономических исследований», Москва, Российская Федерация

В статье рассмотрены угрозы и риски использования социальных сетей и мессенджеров в целях ведения деятельности по отмыванию доходов, полученных преступным путем, и финансирования терроризма. Сформулированы и рассмотрены проблемы обеспечения безопасности социальных сетей и сформулированы рекомендации для сетевых пользователей по блокировке, локализации и снижению рисков вовлечения в противоправную деятельность, мошеннические схемы.

Ключевые слова: *социальные сети, мессенджеры, отмывание доходов, полученных преступным путем, финансирование терроризма, риски, угрозы*

Original article

SOCIAL NETWORKS AS AN INFORMATION BASIS FOR ACTIVITIES ON LAUNDERING PROCEEDS FROM CRIME AND FINANCING TERRORISM

A.N. Stolyarova
JSC "Institute of Regional Economic Research", Moscow, Russian Federation

The article examines the threats and risks of using social networks and instant messengers for the purpose of laundering criminal proceeds and financing terrorism. The problems of ensuring the security of social networks are formulated and examined, and recommendations for network users on blocking, localization and reducing the risks of involvement in illegal activities and fraudulent schemes are formulated.

Key words: *social networks, instant messengers, laundering criminal proceeds, financing terrorism, risks, threats*

ВВЕДЕНИЕ

Отмывание денег, полученных преступным путем, на сегодняшний день становится глобальным явлением и международной проблемой, поскольку оно имеет большое значение для эффективного функционирования практически всех форм транснациональной и организованной преступности, включая терроризм. Возникающие новые способы и методы отмывания денег в сфере теневой экономики [11] открывают широкие возможности для придания законного вида доходам, полученным преступным путем, без возможности быть раскрытыми правоохранительными органами, подразделениями финансовых разведок и другими уполномоченными органами, а также позволяют преступникам все более тщательно скрывать происхождение денежных средств и личность конечного бенефициарного владельца. Это представляет серьезную угрозу национальной и международной безопасности, а также имеет негативные последствия для общества и мировой экономики [8].

Технологический прогресс породил множество принципиально новых и инновационных разработок, которые в значительной степени изменили наш мир. Социальные сети тоже являются продуктом технологий. Использование социальных сетей в незаконных целях продолжает набирать обороты, подпитываясь увеличивающимся количеством пользователей, ростом потребления цифрового и информационного контента и отсутствием должного контроля как со стороны самих платформ, так и со стороны государства. Возможность доступа к общению с пользователями практически всего мира, анонимность, неурегулированность – все это способствует тому, что социальные сети и мессенджеры являются подходящим местом для незаконной деятельности. Неудивительно, что подавляющая часть онлайн-аудитории по всему миру регулярно посещает социальные сети. В настоящее

Поступила в редакцию 14.05.2025

время люди проводят все больше и больше времени в социальных сетях, а значит, финансовые и другие преступления с использованием каналов соцсетей также увеличиваются [1, 3, 5, 12]. В предлагаемой статье рассмотрены угрозы и риски использования социальных сетей и мессенджеров для отмывания доходов, полученных преступным путем, и финансирования терроризма. Сформулированы проблемы безопасности социальных сетей и рекомендации для пользователей по локализации и снижению рисков.

СОДЕРЖАНИЕ ИССЛЕДОВАНИЙ

Потенциальная роль соцсетей в схемах отмывания денег и финансирования терроризма привлекает все большее внимание. Одна из причин того, что социальные сети становятся привлекательными для преступных целей, заключается в том, что другие каналы в результате работы правоохранительных и финансовых органов стали практически перекрыты. Чем больше усиливался контроль в других областях, тем привлекательнее становились онлайн-платформы для отмывания денежных средств и финансирования терроризма. В России имеется не такая большая судебная практика по правонарушениям в данной сфере, поскольку значительное количество таких операций просто невозможно отследить. Также на данный момент очень мало научных исследований данной проблематики на русском языке, а как следствие, отсутствует законодательная база, позволяющая регулировать отрасль в области противодействия отмыванию (легализации) доходов, полученных незаконным путем, а также доходов, направляемых на финансирование терроризма (ПОД/ФТ).

Возможности данной сферы для отмывания денег и финансирования терроризма связаны со следующими причинами: социальные сети – это широкодоступный инструмент, позволяющий вовлекать в свою деятельность онлайн-аудиторию из разных уголков планеты; неурегулированность данной отрасли нормами права; возможность осуществлять управление процессами из любой точки мира, необходимо только наличие выхода в Интернет. Средства можно получать от лиц, непосвященных в истинные цели сбора средств, а не только от вовлеченных в финансирование терроризма; возможность сбора денежных средств, не привлекая при этом дополнительных специалистов; использование социально уязвимых людей в качестве «денежных мулов» для отмывания денег. Все эти причины – это потенциальные уязвимости отмывания денежных средств и финансирования терроризма, которые террористические группировки и преступники используют, чтобы замаскировать истинные источники происхождения преступных доходов, а также, чтобы запутывать «финансовые следы».

Социальные сети обладают рядом качеств, предоставляющим террористическим организациям возможности для манипулирования личностью. Манипулировать в социальных сетях можно целыми социальными группами, что позволяет использовать этих людей не только в качестве финансистов терроризма, но также для привлечения граждан в свои ряды. Развитие социальных сетей оказывает существенное влияние на финансовую и экономическую безопасность каждой страны в целом, поскольку их использование способствует возникновению рисков финансирования терроризма, причем в данном секторе может ожидаться рост финансовых преступлений.

Исходя из вышесказанного, существует большая вероятность, что социальные сети и мессенджеры – это «идеальное место» для легализации доходов, полученных преступным путем, и финансирования терроризма. В связи с этим исследование новых методов и способов отмывания денежных средств является очень важным и предопределяет актуальность и необходимость дальнейшего исследования данной проблемы.

В научной литературе выделяются следующие проблемы правового регулирования деятельности в социальных сетях.

– Теоретическая непроработанность многих вопросов, решение которых является необходимым для эффективного правового регулирования отношений в рамках интернет-сообществ. В работе Перчаткина С.А. и др. [9] отмечается, что «не определены надлежащим образом базовые правовые категории и понятия (например, «интернет-споры», «кибербезопасность» и т.д.); не установлен круг участников процесса управления и регулирования Интернета и их функции при распространении информации через информационно-коммуникационные сети; не определены правила установления места и времени совершения юридически значимых действий при использовании Интернета. В число наиболее сложных задач, связанных с обеспечением функционирования социальных сетей, входят определение пути правового влияния на формирование инфраструктуры информационно-коммуникационной сферы в рамках таких сетей, обеспечение интересов пользователей – потребителей информационной продукции и определение механизма правового регулирования реализации информационных прав в социальных сетях» [9].

– Социальные сети обладают специфическими свойствами, обусловливающими поведение пользователей (возможность оказывания взаимного влияния, подверженность информационным эпидемиям, подмена фактов субъективными, распространение дезинформации) и осложняющие правовое регулирование. В связи с этим, по мнению авторов работы Губанова Д.А. и др. [4], актуализируются задачи информационного управления социальными группами пользователей, создания конвенциональных поведенческих моделей, развития медиаграмотности населения.

– Соотношение информационного суверенитета и трансграничности сетей. В работе Polyakova T.A. и др. [10] обращается внимание на то, что «с каждым годом наблюдается стремительный рост как количества внутренних и внешних угроз, так и уровня их негативного воздействия на граждан, государство и общество. Эти угрозы носят трансграничный характер, что порождает новые вызовы для всей системы международной информационной безопасности и национального права». Поэтому необходимо усиление международного сотрудничества, имеющего цель создания единого правового пространства для социальных сетей.

– Сложность регулирования поведения виртуальной личности. Некоторые исследователи отмечают, что в ходе взаимоотношений в социальных сетях формируется виртуальная личность пользователя, часто не совпадающая с реальным субъектом отношений. Причины этому – пользователь выступает под вымышленным именем, обладает набором специальных характеристик. Главными правовыми проблемами контролирования поведения виртуальной личности, на взгляд специалистов, являются идентификация пользователя социальной сети и возможность привлечения его к юридической ответственности за совершение противоправных действий, совершаемых виртуальной личностью.

– Необходимость учета регулятивного потенциала информационных технологий. Проводя комплексный обзор форм взаимовлияния права и цифровых технологий, Р.В. Амелин отмечает возможность «конфликта между правом и ИТ» и приходит к выводу, что «те направления воздействия права на цифровые технологии, которые приводят к подобному конфликту, являются, наиболее деструктивными как для развития технологий, так и для самого права» [2]. Подобную опасность, по мнению специалиста, необходимо учитывать при правовом регулировании отношений в информационно-коммуникационном пространстве.

Таким образом, механизм противодействия распространению информации, нарушающей российское законодательство, должен включать в себя способы выявления противоправного контента: с помощью самоконтроля, осуществляемого владельцами соцсетей; реагирования на жалобы пользователей и мониторинга Роскомнадзора, по результатам которого владельцы соцсетей также обязаны удалять информацию, распространение которой запрещено российским законодательством.

Исследование в отношении использования социальных сетей и мессенджеров в целях ПОД/ФТ необходимо начать с рассмотрения понятий социальных сетей и мессенджеров, их развития, структуры и принципов работы. Затем следует проанализировать возможности, которые предоставляет данная сфера для отмывания денег и финансирования терроризма. Также определить понятие денежных мулов, особенности их использования для отмывания денег и финансирования терроризма в социальных сетях.

Террористические группы используют социальные сети, потому что инструменты социальных сетей дешевы и доступны, способствуют быстрому и широкому распространению сообщений и позволяют беспрепятственно общаться с аудиторией без фильтрации контента или «избирательности» основных новостных агентств. Кроме того, платформы социальных сетей позволяют террористическим группам взаимодействовать со своими единомышленниками. В то время как ранее террористические группы распространяли сообщения через посредников, платформы социальных сетей позволяют террористическим группам выпускать сообщения непосредственно своей целевой аудитории и общаться со своей аудиторией в режиме реального времени.

Социальные сети могут использоваться террористами как психологическое оружие для распространения дезинформации, сеющей страх, панику, для распространения запугивающих сообщений и угроз населению. Террористы имеют полный контроль над содержанием сообщений, размещаемых в электронных СМИ и социальных сетях, и это открывает для них большие возможности для сбора средств для финансирования своей деятельности, для вербовки и мобилизации новых членов, для установления связей и обмена информацией, для планирования и координации террористической деятельности.

Осуществляя мониторинг веб-сайтов в Интернете, террористические организации могут выявлять то, что интересует пользователей Интернета, и, соответственно, запрашивать выплату грантов или пожертвований для финансирования своих действий. Террористы используют соцсети для планирования и координации конкретных атак, в которых используют зашифрованные сообщения через чаты, карты, фотографии, знаки, технические особенности, скрытые в графических файлах и цифровых изображениях, а также различные стенографические инструменты.

Финансирование террористической деятельности также может осуществляться через Интернет и социальные сети. Многочисленные террористические группы добиваются прямых финансовых пожертвований от посетителей своих сайтов, а также от их членов и сторонников. Пожертвования могут быть не только денежные, это могут быть и какие-либо действия или предметы, которые террористические активисты могут найти полезными для основной деятельности (оружие, карты зданий и объектов, представляющих интерес, пуленепробиваемые жилеты и т.д.). Чтобы получить средства для финансирования террористической деятельности, члены террористических групп также очень часто стремятся совершить другие различные преступные действия, такие как злоупотребление или неправомерное использование различных

инструментов для электронной коммерции, дебетовых или кредитных карт, кража чужих личных данных, интернет-мошенничество и др.

Сегодня террористы обладают огромным количеством способов распространения своей идеологии. Среди них и семинары по вербовке лиц, и различные печатные брошюры, книги, статьи и т. д. [7]. Теперь в это число также входят социальные сети. Считанные секунды займет поиск интересующего нас человека, так как довольно часто социальные сети во время регистрации предлагают людям указывать о себе личную информацию: размещать фото и видео, указывать информацию о работе и образовании, семейном положении, а также хобби, интересы, любимые места для посещения, позволяют делиться личными мыслями, участвовать в опросах, по которым можно определить отношение человека к той или иной проблеме, и т.д. Поэтому так высок риск вербовки террористами, они уже заранее знают о нас всю нужную им информацию и могут использовать нас в своих целях. Одна из них – это как раз сбор денег на финансирование терроризма.

Риск в сфере ПОД/ФТ представляет собой вероятность нанесения ущерба финансовой системе страны путем осуществления финансовых операций с целью легализации доходов или финансирования терроризма. Через социальные сети любое юридическое или физическое лицо может быть вовлечено сознательно или без его ведома в противоправные действия, в том числе легализацию доходов, полученных преступным путем, и финансированием терроризма.

Предлагается регулирующим органам формировать списки групп и лиц, подпадающих под санкции. Эти списки включают следующую информацию о физических и юридических лицах: адреса электронной почты, IP-адреса и данные учетной записи в социальных сетях. Конечно, эта информация может быть относительно легко изменена физическими и юридическими лицами, подпадающими под санкции. Однако такие данные могут служить важными первичными индикаторами, которые могут использоваться для внутренних проверок и поисков, проводимых операторами платформ. В своей резолюции, касающейся борьбы с финансированием терроризма, Совет Безопасности ООН призвал государства-члены продолжать устанавливать эффективное партнерство с частным сектором, включая интернет-компании и компании социальных сетей, для устранения угрозы терроризма.

Учитывая глобальный охват ведущих социальных сетей, крайне важно, чтобы платформы принимали упреждающие меры для предотвращения неправомерного использования их услуг для финансирования терроризма. Техническая индустрия должна активно искать профили и аккаунты людей, финансирующих терроризм на своих платформах. Более того, корректировка стандартов сообщества этих платформ кажется важным первым шагом и давно назревшей мерой. Четко сформулированный запрет такой деятельности в стандартах сообщества важен для того, чтобы сосредоточить внутренние защитные системы платформ на этом типе нарушений. Это, в частности, относится к общественным стандартам краудфандинговых платформ, поскольку их услуги подвергаются особому риску неправомерного использования в качестве потенциального инструмента для сбора пожертвований для террористических групп и организаций.

Финансирование терроризма и отмывание денежных средств через эти платформы являются не только вопросом безопасности, а также вопросом мировой проблемы борьбы с организованной преступностью, которая находит все более изощренные способы для поддержания свой деятельности. Большинство других методов находится под пристальным вниманием правоохранительных органов, и поэтому для отмывания денег и финансирования терроризма преступники продолжают искать новые возможности.

Чтобы избежать нормативных мер, принятых для предотвращения отмывания денег, преступники стремятся использовать «денежных мулов» для осуществления незаконной деятельности от своего имени. Сети денежных мулов являются глобальной проблемой и используются для перемещения огромных сумм незаконных денег между счетами, способствуя целому ряду преступных и террористических действий. Денежный мул – это лицо, которое сознательно или неосознанно завербовано для действий от имени преступников в рамках схемы отмывания денег. Хотя исторически они использовались для перевода физических сумм наличных денег из одной точки в другую, в современном финансовом контексте они обычно подразумевают открытие банковских счетов и управление ими с целью облегчения внесения, перевода и вывода незаконных средств.

Преступники вербуют денежных мулов, предлагая получить неплохое денежное вознаграждение за работу, или используют для этого определенные рычаги давления или запугивания. После того, как денежные мулы набраны, им предлагается открыть банковские счета на свое имя, используя свои личные данные. Данная стратегия – возможность для преступников скрыть свою личность и источник своих незаконных средств, а также обойти CDD (Customer Due Diligence – надлежащая проверка клиентов).

В качестве альтернативы mule-счетам, открытым законными клиентами, преступники могут попытаться открыть mule-счет, используя синтетическую личность. В этом случае преступники могут использовать украденные личные профили реальных людей [6].

Как только денежный мул найден или учетная запись денежного мула была создана, преступники могут использовать его, чтобы начать переводить не-

законные деньги в законную финансовую систему. Процесс отмывания может протекать следующим образом: денежный мул открывает счет в банке; средства поступают на счет мула из криминального источника; преступники инструктируют денежного мула, как и куда следует перемещать деньги; мулы переводят незаконные средства на сторонний счет или снимают их наличными; деньги, переведенные со счета денежного мула, могут быть конвертированы в виртуальную валюту, такую как, например, Bitcoin, чтобы власти не могли отслеживать его происхождение.

В то время как преступники могут специально ориентироваться на уязвимых людей или лиц с криминальным прошлым для роли денежного мула, они могут также нанять законопослушных кандидатов без криминального прошлого, чтобы наверняка избежать проверки властей. Денежные мулы могут получить оплату непосредственно за их участие в схеме отмывания денег или могут сохранить некоторую сумму незаконных средств, из тех, что им переводили, для себя в качестве оплаты. Денежные мулы создают большую угрозу, а значит, банки и другие финансовые учреждения должны иметь представление, каким образом смурферы действуют в рамках данной схемы отмывания денег, и обеспечить функционирование программ ПОД / ФТ для выявления и предотвращения соответствующих методологий.

Каким образом финансовые учреждения могут обнаружить денежных мулов? Денежные мулы усложняют процесс выявления и устранения финансовых преступлений и поэтому создают значительную проблему в соблюдении требований ПОД/ФТ. Фирмы, которые не могут обнаружить преступников, использующих их услуги для отмывания денег, рискуют штрафами и значительным репутационным ущербом.

Финансовые учреждения должны убедиться, что их AML-программы (Anti-Money Laundering – это комплекс мер, направленных на предотвращение отмывания денег, финансирования терроризма и другой незаконной деятельности) могут обнаружить, когда их клиенты используются в качестве денежных мулов. Фирмы должны учитывать определенные так называемые «красные флаги» поведения или характеристики денежного мулинга как часть их борьбы с отмыванием денег. К ним относятся:

– модели транзакций: действия денежного мула могут стать очевидными только после серии транзакций, а не отдельного платежа. Мулы, скорее всего, будут участвовать в нескольких транзакциях, которые не соответствуют профилю риска их клиентов, не имеют очевидной цели или связаны с переводами средств в юрисдикции с более высоким риском. Для выявления подозрительных моделей транзакций финансовые учреждения должны постоянно осуществлять комплексный мониторинг, который учитывает не только характеристики самих транзакций, но также и второстепенную информацию, включающую получателей и пункты назначения;

– происхождение и назначение переводов: многие схемы отмывания денег включают переводы ценностей в страны с более высоким риском, которые имеют очень низкие оценки от международных наблюдателей. Соответственно, фирмы должны уделять особое внимание происхождению и назначению транзакций, связанных с потенциальными денежными мулами, отмечая участие юрисдикций со слабыми системами противодействия и контроля отмывания денег;

– подставные компании: преступники могут убедить денежных мулов создать подставные компании, чтобы скрыть бенефициарное владение другими объектами сети отмывания денег. Затем преступники могут использовать учетную запись фиктивной компании для перемещения незаконных денег, одновременно предотвращая попытки отслеживания AML со стороны банков и национальных властей. Подставные компании часто регистрируются в так называемых финансовых «убежищах», поэтому фирмы должны следовать по цепочке права собственности, чтобы установить бенефициарную собственность или, в качестве альтернативы, сообщать о подозрительных компаниях властям.

Рост использования социальных сетей и мессенджеров влечет за собой высокие риски мошенничества и отмывания денег, а также высокие риски финансирования терроризма. Отсутствие должного контроля за соцсетями способствует росту рисков ОД/ФТ, что в свою очередь оказывает негативное влияние на финансовую и экономическую безопасность каждой страны в целом. Появился и механизм защиты пользователей от незаконных блокировок в социальной сети: пользователь, в отношении информации которого приняты меры по ограничению доступа владельцем социальной сети, вправе обратиться с жалобой на это решение. Владелец обязан рассмотреть такую жалобу и направить ответ пользователю в течение 3 дней со дня ее поступления. В случае несогласия с ответом пользователь вправе обратиться с заявлением в Роскомнадзор об отмене мер по ограничению доступа к информации пользователя.

Можно выделить следующие рекомендации для пользователей по предотвращению рисков ОД/ФТ и других рисков:

– использовать уникальные и безопасные пароли. Под уникальностью подразумевается, что пароли не должны были использоваться ни в одной из ваших учетных записей, а также они не должны были использоваться кем-либо еще. Пользователи должны создать надежный и уникальный пароль для каждой учетной записи, а затем избегать повторного использования паролей на других учетных записях. Если это слишком затруднительно – можно использовать для этих целей менеджер паролей. Менеджеры паролей не только за-

поминают пароли пользователя от его имени, но и позволяют создавать надежные и уникальные пароли, а также сохранять их в безопасности;

– применять многофакторную аутентификацию. Проще говоря, многофакторная аутентификация – это акт применения дополнительной безопасности к учетным записям пользователя. В ситуациях, когда преступник пытается взломать учетную запись пользователя и пытается войти в систему от его имени, многофакторная аутентификация предотвращает такие попытки. Эта функция не позволит преступнику войти, если человек не окажется самим собой после аутентификации. Это может быть что угодно, от одноразового pin-кода, отправленного на адрес электронной почты или номер мобильного телефона, кода безопасности, секретного вопроса или чего-либо еще;

– проверять настройки безопасности своей учетной записи. Поскольку инциденты, связанные с кибербезопасностью, становятся обычным явлением, технологические гиганты постоянно обновляют свои настройки. Они продолжают внедрять новые функции, которые дают пользователю больше контроля над безопасностью его учетной записи. Однако такие обновления могут также изменить предыдущие настройки конфиденциальности. Поэтому необходимо взять за привычку периодически просматривать настройки конфиденциальности и безопасности своей учетной записи в социальных сетях;

– внимательность в отношении заявок в друзья. Необдуманное добавление слишком большого числа незнакомцев, несомненно, представляет угрозу безопасности. Сегодня социальные сети наводнены преступниками, замаскированными под невинных людей. Они часто выдают себя за других, создают безобидные профили, втираются в доверие и осуществляют свои преступные цели. Часто преступники также взламывают законные профили пользователей, которые они затем используют в противоправных действиях;

– проверка электронной почты. Пользователь получает оповещения по электронной почте всякий раз, когда кто-то пытается войти в его учетную запись без авторизации. В таком случае безопаснее сразу сменить пароль. Однако злоумышленники часто имитируют такие оповещения, чтобы украсть учетные записи в социальных сетях с помощью фишинговых писем – нельзя переходить по подозрительным ссылкам;

– быть аккуратнее с публикацией контента. Почти все, что публикуется в Интернете, может показаться неважным. Перед публикацией стоит подумать, связано ли это каким-либо образом с жизнью человека. Лучше ничего не публиковать, чем публиковать конфиденциальные материалы и рисковать своей безопасностью в социальных сетях;

– остерегаться фишинговых сообщений. Как и электронные письма, фишинговые атаки также осуществляются через личные сообщения в социальных сетях. Нельзя доверять ссылкам, полученным от незнакомца, даже если она кажется безобидной. В то же время в отношении друзей лучше также избегать переходов по ссылкам на игры или веб-сайты, если нет уверенности в них. Также не стоит доверять рекламе или предложениям с технической поддержкой, раздачей подарков или денежными призами;

– установка программного обеспечения для интернет-безопасности: некоторые угрозы, характер которых известен, могут быть легко обнаружены с помощью антивирусов. Такие угрозы, как кибергруминг, киберзапугивание, могут быть обнаружены в некоторой степени с помощью антивирусного программного обеспечения. Многие вредоносные ссылки могут быть переданы нашими друзьями неосознанно, что перенаправляет пользователя на какой-то фишинговый сайт. Антивирусное программное обеспечение должно регулярно обновляться из-за наличия множества вирусов, ежедневно создаваемых хакерами. Некоторые сайты социальных сетей также имеют свои собственные инструменты безопасности, которые могут использоваться пользователями для защиты от кибератак;

– сохранять бдительность. Это один из самых важных аспектов в отношении пользователей социальных сетей. Не стоит вестись на заманчивые предложения быстро поднять денег, скорее всего это незаконно, и пользователь может стать соучастником в схеме отмывания преступных доходов, даже не подозревая об этом, но неосведомленность в этом не освобождает от ответственности.

ЗАКЛЮЧЕНИЕ

Что касается общих рекомендаций, то к ним, прежде всего, относится совершенствование алгоритмов модерации контента социальных сетей, которые в настоящее время имеют недостатки, и их необходимо устранить. Это достаточно тонкий вопрос, поскольку при этом важно не нарушать конституционные права граждан (они же пользователи платформ социальных сетей). Совершенствование законодательства также является первоочередной мерой, поскольку в настоящий момент имеются пробелы в нормативно-правовых актах и не установлена ответственность для тех, кто вербует денежных мулов в социальных сетях для отмывания денег. Стоит увеличить количество работников в социальной сети, занимающихся рассмотрением жалоб, для более эффективного поиска и блокировки контента, нарушающего правила платформы социальной сети, а также нарушающего права граждан. Только сочетание разумного регулирования социальных сетей и мессенджеров со стороны государства и мер, принимаемых платформами социальных сетей, а также самими пользователями, приведет к эффективной борьбе с ОД/ФТ и иной незаконной деятельностью.

Литература

1. **Абидов Р.Р., Зумакулова З.А.** Противодействие экстремизму и терроризму в сети Интернет // Право и управление. 2024. № 6. С. 301–305.
2. **Амелин Р.В.** Право – цифровые технологии: основные направления-eas воздействия // Современное право, 2020. № 8. С. 50–56.
3. **Арипшев А.М. Экстремизм и терроризм в социальных сетях: проблемы обнаружения и противодействия** // Журнал прикладных исследований. 2022. Т. 1. № 9. С. 44–48.
4. **Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства.** М.: Физматлит, 2010. 228 с.
5. **Гурьянова К.В. Правовое регулирование противодействия терроризму и экстремизму в сети "Интернет"** // Вестник науки. 2024. Т. 1. № 10 (79). С. 132–137.
6. **Кондрат Е.Н. Международная финансовая безопасность в условиях глобализации Основные направления правоохранительного сотрудничества государств.** М.: Юстицинформ,2015. 592 с.
7. **Меркулов П.А. Распространение идеологии терроризма в молодежнои среде: современные реалии и направления противодействия** // Управленческое консультирование. 2019. № 5. URL: https:// cyberleninka.ru/article/ n/rasprostranenie- ideologii-terroriz
8. **Носова С.С., Норкина А.Н., Морозов Н.В.** Типологии финансовых махинаций: учебник. М.: КноРус, 2021. 474 с.
9. **Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В.** Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5. С. 14–24.
10. **Полякова Т.А., Минбалеев А.В., Наумов В.Б.** Форсайт-сессия «Информационная безопасность в XXI веке: вызовы и правовое регулирование». Труды Института государства и права РАН, 2018. Т. 13. № 5. С. 194–208.
11. **Столярова А.Н., Петросян Д.С., Леонова Ж.К.** Финансовый контроль как инструмент снижения угроз теневой экономики // Вестник РАЕН. 2021. Т. 21. № 3. С. 52–55.
12. **Столярова А.Н. и др.** Противодействие рискам легализации доходов, полученных преступным путем, и финансированию терроризма: виртуальные активы, социальные сети и мессенджеры. М.: Русайнс, 2024. 318 с.

References

1. **Abidov R.R., Zumakulova Z.A.** Counteracting extremism and terrorism on the Internet. *Pravo i upravleniye*. 2024;6:301–305. (In Russian).
2. **Amelin R.V.** Law – digital technologies: main directions of influence. *Sovremennoye pravo.* 2020;8:50–56.
3. **Aripshev A.M.** Extremism and terrorism in social networks: problems of detection and counteraction. *Zhurnal prikladnykh issledovaniy.* 2022;1;(9):44–48. (In Russian).
4. **Gubanov D.A., Novikov D.A., Chkhartishvili A.G.** Social networks: models of information influence, management and confrontation. Moscow: Fizmatlit, 2010:228. (In Russian).
5. **Guryanova K.V.** Legal regulation of counteraction to terrorism and extremism on the Internet. *Vestnik nauki.* 2024;1;10 (79):132–137. (In Russian).
6. **Kondrat E.N.** International financial security in the context of globalization. The main directions of law enforcement cooperation of states. Moscow: Yustitsinform, 2015:592. (In Russian).
7. **Merkulov P.A.** Spread of the ideology of terrorism among young people: modern realities and directions of counteraction. Management consulting. 2019;5. URL: https:// cyberleninka.ru/article/ n/rasprostranenie-ideologii-terroriz (In Russian).
8. **Nosova S.S., Norkina A.N., Morozov N.V.** Typologies of financial fraud: textbook. Moscow: Knorus, 2021:474. (In Russian).
9. **Perchatkina S.A., Cheremisinova M.E., Tsirin A.M., Tsirina M.A., Tsomartova F.V.** Social Internet networks: legal aspects. *Zhurnal rossiyskogo prava*. 2012;5:14–24. (In Russian).
10. **Polyakova T.A., Minbaleev A.V., Naumov V.B.** Foresight session "Information security in the 21st century: challenges and legal regulation". Proceedings of the Institute of State and Law of the Russian Academy of Sciences, 2018;13;5:194–208. (In Russian).
11. **Stolyarova A.N., Petrosyan D.S., Leonova Zh.K.** Financial control as a tool for reducing shadow economy threats. *Vestnik RAYEN*. 2021;21;3:52–55. (In Russian).
12. **Stolyarova A.N. et al.** Counteracting the risks of legalization of proceeds from crime and the financing of terrorism: virtual assets, social networks and instant messengers. Moscow: Rusains, 2024:318. (In Russian).

Столярова Алла Николаевна,
д.э.н., профессор, начальник отдела управления образовательных процессов АО «Институт региональных экономических исследований», профессор базовой кафедры торговой политики ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», профессор кафедры менеджмента и экономики ГОУ ВО МО «Государственный социально-гуманитарный университет»

119002, г. Москва, пер. Сивцев Вражек, д. 29/16, а/я 53, 119002 Moscow, Sivtsev Vrazhek lane, 29/16, P.O. Box 53, e-mail: : stolyarova2011@mail.ru