Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2023, Том 15, № s1 / 2023, Vol. 15, Iss. s1 https://esj.today/issue-s1-2023.html

URL статьи: https://esj.today/PDF/85FAVN123.pdf

Ссылка для цитирования этой статьи:
Гребенкина, С. А. Анализ международной практики цифрового взаимодействия в сфере противодействия отмыванию доходов и финансированию терроризма / С. А. Гребенкина // Вестник евразийской науки. — 2023. — Т. 15. — № s1. — URL: https://esj.today/PDF/85FAVN123.pdf

For citation:
Grebenkina S.A. Analysis of international practice of digital interaction in the field of anti-money laundering and terrorism financing. *The Eurasian Scientific Journal*. 2023; 15(s1): 85FAVN123. Available at: https://esj.today/PDF/85FAVN123.pdf. (In Russ., abstract in Eng.)

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета

УДК 338

Гребенкина Светлана Александровна
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Институт экономической политики и проблем экономической безопасности
Ведущий научный сотрудник
Кандидат экономических наук, доцент
E-mail: s.greb@list.ru
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=855670

Анализ международной практики цифрового взаимодействия в сфере противодействия отмыванию доходов и финансированию терроризма

Аннотация. Работа посвящена изучению зарубежного опыта цифрового межведомственного взаимодействия. Автором проведен анализ успешных практик внедрения искусственного интеллекта в вопросах противодействия отмыванию преступных доходов и финансированию терроризма. Раскрыты наиболее популярные высокотехнологичные инструменты и стратегии, применяемые регуляторами и финансовыми учреждениями как на национальном уровне, так и при межведомственном международном взаимодействии. Изучена зарубежная практика внедрения и основные элементы SupTech- и RegTech-стратегий, а также достигаемые с их помощью преимущества в области контрольно-надзорной деятельности, среди которых значимыми выступают: автоматизация и стандартизация бизнес-процессов в рамках осуществления надзорных требований, оптимизации сбора и обработки информации, сокращение временных и финансовых затрат, оперативность выявления признаков мошенничества и иные. Рассмотрен положительный опыт использования искусственного интеллекта на примере Великобритании, Сингапура, Японии, Китая, ряда европейских финансовых учреждений. Выделены основные проблемы использования передовых технологий поднадзорными субъектами и регуляторами при противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, выступающие барьером для масштабной цифровизации в данной сфере, а именно: сложности нормативно-правового регулирования и обеспечения должного уровня защиты информации, проблемы интерпретации результатов оценки, разная степень имплементации рекомендаций группы разработки финансовых мер борьбы с отмыванием денег, отличия в применяемых подходах к идентификации и иные. В заключительной части статьи автор утверждает, что для масштабного использования передовых технологий в рамках укрепления взаимодействия

между финансовыми учреждениями, международного сотрудничества с уполномоченными органами требуется решение несколько задач, указанных в статье.

Ключевые слова: международный опыт; противодействие отмыванию доходов и финансированию терроризма; искусственный интеллект; цифровое взаимодействие; передовые технологии; финансовая разведка; финансовые учреждения

Введение

Современные тенденции характеризуются масштабной цифровизацией во всех отраслях экономики, обеспечивая ее устойчивое и безопасное функционирование. Особую значимость передовые технологии играют в вопросах противодействия противоправной деятельности, позволяя ускорять анализ клиентов подотчетных субъектов, выявление незаконных операций, оперативно решать ключевые задачи и взаимодействовать с иностранными коллегами, тем самым результативнее соблюдать нормы в сфере действующего законодательства. Так, в последнее время группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) отдает приоритет цифровизации в области противодействия отмыванию преступных доходов и финансированию терроризма (далее ПОД/ФТ), отмечая среди основных преимуществ возможность обрабатывать большие объемы данных, строить модели поведения, выявлять общие закономерности, минимизировать комплаенс риски, обеспечивать надлежащее исполнение финансовыми учреждениями текущих требований, упрощать обмен данными между ними, а также между национальными и иностранными специальными ведомствами [6; 7]. Передовые страны уже успешно реализуют проекты цифрового межведомственного взаимодействия по вопросам ПОД/ФТ. В работе представлены зарубежные нововведения в этой области.

Цель работы — проанализировать особенности цифрового взаимодействия в сфере противодействия отмыванию доходов и финансированию терроризма.

Объект — противодействие отмыванию доходов и финансированию терроризма.

Предмет — цифровое взаимодействие в сфере противодействия отмыванию доходов и финансированию терроризма.

1. Методы и материалы

При написании научной публикации авторами использовались следующие методы: сравнительный, статистический, анализ научных исследований и статей, табличные и графические способы визуализации статистических данных.

Для достижения данной цели в работе были поставлены следующие задачи:

- рассмотреть основы направления и использования SAR;
- проанализировать международный опыт по противодействию отмыванию доходов;
- выделить основные инструменты, применяемые регуляторами в рамках SupTec;
- определить роль искусственного интеллекта в обеспечении финансовой и экономической безопасности.

Исследование основывается на теоретических и методологических положениях, разработанных отечественными авторами, в частности Лапиной С.Б. [1], Гаврюшенко А.П. [2; 3], Шараевым П.С. [4], Криштоповым С.В. [5] и другими.

Информационной базой исследования послужили Федеральные законы РФ, постановления и распоряжения Правительства РФ, нормативно-правовые документы, научные труды отечественных ученых, Интернет-ресурсы (официальные сайты) и зарубежные источники по тематике работы.

2. Результаты и обсуждения

Интересным представляется опыт Великобритании. В настоящее время одним из крупнейших информационных источников подразделения финансовой разведки (UKFIU) и правоохранительных органов является база данных отчетов о подозрительных операциях (далее SAR), направляемых от финансового сектора, а также полученных от иностранных коллег и правоохранительных органов Великобритании в отношении зарубежных запросов. Для отправки SAR используется безопасная бесплатная онлайн-система, которая обеспечивает мгновенное подтверждение и присвоение ссылочного номера (чего нет в ручных отчетах). При этом отчеты можно делать круглосуточно и без выходных. Ответственность за получение, анализ и осуществление финансовых расследований по материалам, представляемым через режим SAR, несет подразделение финансовой разведки Великобритании, которое ежегодно получает порядка 460 тыс. SAR в год. Данные отчеты хранятся в специальной защищенной центральной базе данных. После анализа наиболее важные SAR направляются в соответствующие организации для расследования (например, в Национальное подразделение по расследованию финансирования терроризма (NTFIU), подразделения профессиональных стандартов полиции и иные). Остальные предоставляются правоохранительным органам Великобритании по защищенному каналу. Быстрый поиск и обработка обеспечиваются путем поиска, по ключевым словам, и соответствующим кодам. При этом один и тот же SAR часто используется сразу несколькими пользователями для разных целей. Например, информация в SAR может информировать налоговую и таможенную службу о нарушениях налогообложения, местную полицию — о мошенничестве или краже, а правительственное учреждение — о проблеме или уязвимости какого-либо финансового продукта [6].

В целом основы направления и использования SAR можно представить в виде схемы, указанной на рисунке 1.

Рисунок 1. *Процесс информационного обмена при направлении SAR (составлено автором на основе [7])*

Стоит отметить, что не так давно в Великобритании также был реализован проект по IT-трансформации системы, в рамках которого предусмотрена замена инструмента поиска и анализа данных для правоохранительных органов (Arena) и онлайн портала, через который осуществляется доступ к SAR (Moneyweb), на единый интерфейс, обеспечивающий расширение спектра услуг по предоставлению аналитики и визуализации SAR. Проект направлен на усиление мер реагирования в области ПОД/ФТ, а также на улучшение результативности правоохранительной деятельности посредством преобразования существующего ИТ-пакета SAR в стабильное и расширенное программное обеспечение, внесения улучшений в его функциональные возможности для обеспечения дальнейшего использования в будущем. UKFIU в настоящее время предоставляет конечным пользователям SAR инструмент поиска и анализа, а также обучает тому, как лучше всего использовать SAR с его помощью. С целью дальнейшего расширения возможностей эксплуатации уполномоченными сотрудниками команда по IT-трансформации начала взаимодействовать с различными конечными пользователями, чтобы получить отзывы о том, как улучшить функциональные возможности системы [8]. Среди основных преимуществ реализуемого проекта отмечены:

- повышение удобства использования благодаря единому пользовательскому порталу, обеспечивающему «единый вход» во все правоохранительные системы и отражение текущих и будущих требований законодательства;
- повышение оперативности предоставления SAR правоохранительным органам;
- гибкость системы, возможность адаптировать под изменяющиеся условия.

Согласно статистическим данным, крупнейшим отправителем SAR в Великобритании выступает банковский сектор, на который приходится более 80 % сообщений [10]. Сохраняющейся динамике способствует постоянное появление новых высокотехнологичных продуктов, привлекающих внимание преступников и благоприятствующих появлению более сложных схем [8]. Наряду с этим, ряд британских банков функционируют полностью в цифровом формате, не имея физических отделений, что также расширяет возможности для осуществления противоправной деятельности со стороны злоумышленников. Для минимизации данного риска финансовые учреждения все чаще прибегают к инновационным методам для проведения проверки «Знай своего клиента» (KYC). Например, аутентификация владельцев счетов по видео используется некоторыми организациями в качестве альтернативы открытию счета в отделении, что также означает новые возможности финансовой разведки.

Положительным примером применения цифровых технологий в банковском секторе в рамках ПОД/ФТ также является опыт Нидерландов. В 2019 году крупнейшие голландские банки ABN Amro, ING и Rabobank для повышения эффективности идентификации корпоративных клиентов запустили проект по реализации платформы обмена результатами надлежащей проверки клиентов (далее НПК) при поддержке со стороны национальных регулирующих органов. Согласно проекту, сотрудники служб внутреннего контроля данных банков получили право обмениваться данными о бенефициарных владельцах клиентов-юридических лиц. Важным моментом является получение согласия таких клиентов. Похожий проект был также запущен скандинавскими кредитными учреждениями Danske Bank (Дания), DNB (Норвегия), Handelsbanken (Швеция), Nordea и SEB [9].

В последние годы большую популярность набирает использование передовых технологий для повышения эффективности контрольно-надзорной деятельности в целях ПОД/ФТ: Regulatory Technology (далее RegTech) и Supervisory Technology (далее SupTech). RegTech применяется в основном при мониторинге и выявлении мошеннических манипуляций, процессах идентификации клиентов, оценке и управлении рисками в целях отмывания

преступных доходов и финансирования терроризма (далее ОД/ФТ). Преимуществами технологии выступают: автоматизация и стандартизация бизнес-процессов в рамках осуществления надзорных требований, сокращение финансовых затрат, минимизация комплаенс рисков, оперативность выявления признаков мошенничества. В свою очередь, использование SupTech — стратегии обуславливает повышение качества аналитических данных за счет оптимизации сбора и обработки информации, оперативность выявления и минимизации рисков, сокращение временных затрат. Применяются преимущественно для совершенствования процессов предоставления регуляторной отчетности, оптимизации работы с большими объемами данных, выявления противоправной деятельности ОД/ФТ. Согласно результатам проведенных исследований, многие регуляторы уже имеют или переходят к реализации SupTech, более трети респондентов выступают за внедрение RegTech-стратегии в области соблюдения действующего законодательства и стандартов ПОД/ФТ [10].

Стоит отметить, что на текущий день регуляторы используют в своей деятельности около двухсот SupTech-решений с применением искусственного интеллекта. Анализ международной практики показывает, что для различных областей могут использоваться различные технологии в рамках той или иной стратегии. Ниже на рисунке 2 представлены инструменты, применяемые регуляторами в рамках SupTec.

Рисунок 2. *Используемые технологии в рамках стратегии SupTec для регуляторной деятельности [10]*

В качестве положительного опыта использования SupTec можно отметить выявление мошеннических манипуляций в Сингапуре. Денежно-кредитное управление Сингапура (MAS) с 2018 года для данных целей использует машинное обучение. Системой анализируются данные о выявленных предыдущих противоправных деяниях на финансовом рынке, за счет чего определяются схожие повторяющиеся подозрительные события. Выявленные системой случаи направляются сотрудникам для дальнейшего анализа. Согласно статистическим данным, система способна корректно определить факты мошеннических действий в 98 % случаев. Действующие алгоритмы построены на смоделированных разнообразных схемах возможных рыночных манипуляций [11].

Для выявления мошеннических действий в целях ПОД/ФТ поднадзорными субъектами все чаще встречается использование технологий RegTech. Приоритет на сегодняшний день отдается машинному обучению, однако для разных целей могут использоваться и другие технологии. Ниже на рисунке 3 представлены инструменты, используемые регуляторами и поднадзорными субъектами в рамках RegTech.

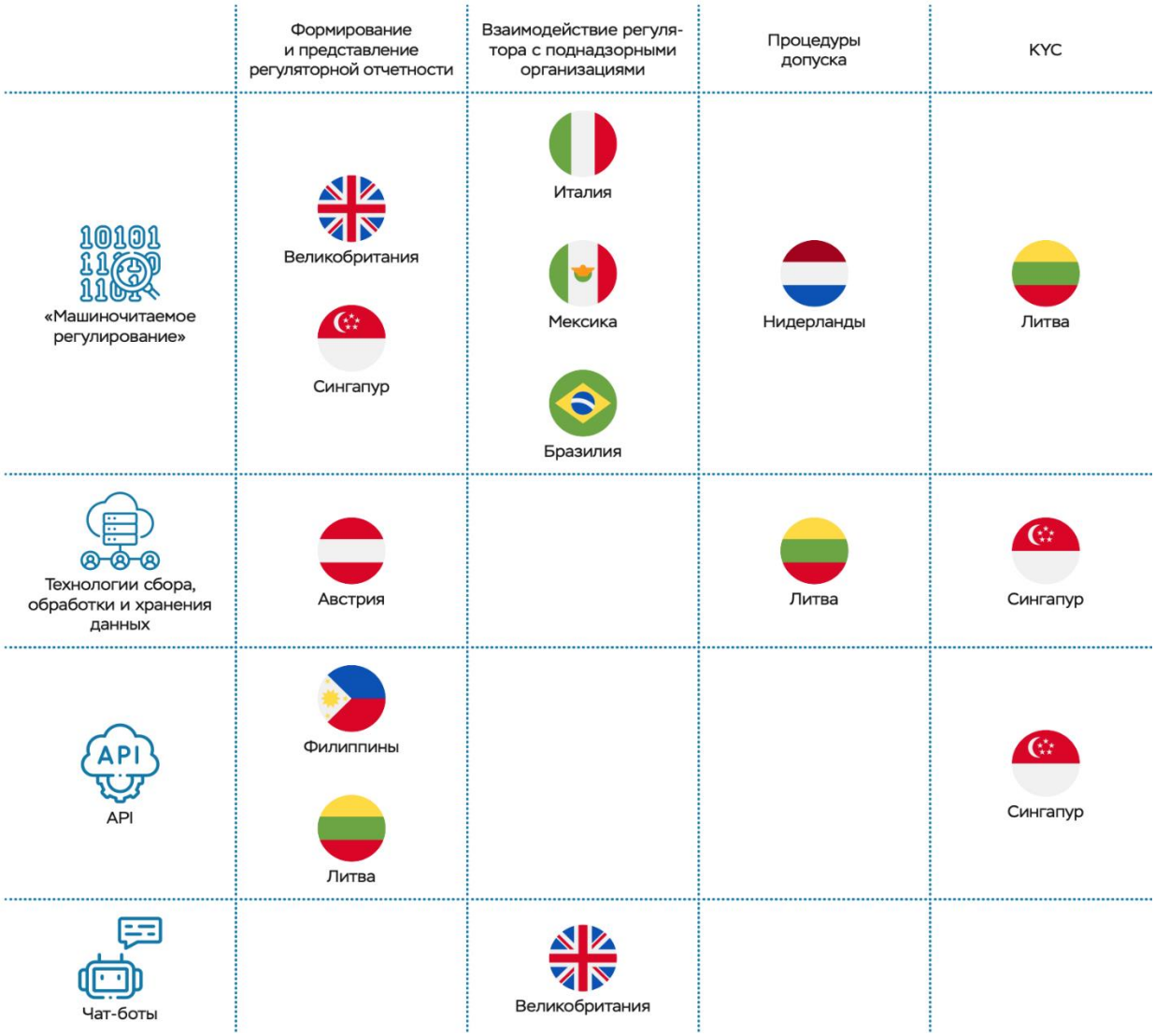

Рисунок 3. *Используемые технологии в рамках стратегии RegTech для регуляторной деятельности [11]*

Примером использования RegTech является развитие платформы KYC («Знай своего клиента») в Сингапуре для проведения проверки клиентов банковской сферы. Изначально предполагалась возможность обмена данными о клиентах-юридических лицах между финансовыми учреждениями. Однако, в силу высоких издержек, позже реализация данного проекта была приостановлена. Вместе с тем в настоящее время успешно функционирует платформа API Exchange — APIX, на базе которой финансовые и финтех организации имеют возможность интегрировать и проводить тестирования своих цифровых решений посредством облачной архитектуры. Недавно также Банком Англии и Управлением по финансовому регулированию и надзору Великобритании (Financial Conduct Authority, FCA) был успешно реализован проект «Цифровая регуляторная отчетность», направленный на оптимизацию процесса представления отчетности поднадзорными субъектами — финансовыми организациями [12].

Уникальный проект с использованием искусственного интеллекта (далее ИИ) в рамках ПОД/ФТ был реализован в Японии при участии нескольких финансовых учреждений и Агентства финансовых услуг, предполагающий объединение ИИ с инструкциями поднадзорных субъектов из каждого набора данных по финансовым операциям, создавая единую модель оценки, помогающей специалисту сделать суждение о наличии мошеннических действий. Это возможно благодаря автоматическому расчету вероятности для мониторинга той или иной операции и проверки на наличие в составе санкционных списков. Примечательно, что сами данные не передаются за пределы финансового учреждения и не систематизируются. В основе платформы заложена интеграция моделей ИИ на основе уже изученных данных поднадзорных финансовых организаций и настройка модели ИИ, которая проанализировала данные одного учреждения для проведения анализа другого. Данный процесс непрерывный, что благоприятствует в дальнейшем повышению точности модели ИИ.

ИИ также используется в Китае. В настоящее время проводится тестирование платформы по обмену рисков отмывания преступных доходов (далее ОД) между несколькими финансовыми организациями. В основе нововведений лежит использование блокчейна, цифровой идентификации и передовых технологий усиления конфиденциальности. Проект реализуется при инициативе и контроле Бюро по противодействию отмыванию денег Народного банка Китая. Среди преимуществ отмечается возможность поднадзорным субъектам шифровать информацию о клиентах, отнесенных к высокому риску, а далее уже загружать на блокчейн-платформу. При поступающем запросе о клиенте от какого-либо финансового учреждения происходит сопоставление и поиск с помощью блокчейн через защищенную вычислительную базу. Положительный результат может быть получен в случае, если ранее данные о таком клиенте были загружены другой организацией. Когда данные по клиенту, включая риски ОД, будут извлечены, система возвращает информацию обратно в базу в зашифрованном виде. Далее финансовое учреждение, которое направило запрос, получает сообщение об отнесении клиента другим учреждением к высокорискованным, и ей уже будут адресованы запросы со стороны иных финансовых организаций. Таким образом, исключается фактический обмен данными о клиентах [13]. Применение ИИ находит свое отражение и в противодействии предикатным преступлениям ОД/ФТ. Так, с 2012 года была запущена антикоррупционная система Zero Trust, основанная на построении сложных многоярусных схем социальных отношений и выявлении отклонений поведения чиновников. За 7 лет система позволила выявить более 8500 коррупционеров среди госслужащих. В 2019 году появилась информация о закрытии проекта. Однако ИИ используется и в настоящее время в судебной практике Китая. Стоит также отметить значимую роль Электронной справочной системы, применяемой для получения китайскими правоохранительными органами срочной информации у финансовых учреждений в рамках ПОД/ФТ. К системе в настоящий момент присоединилось около 60 % кредитных организаций. Она позволяет напрямую в оперативном

порядке наводить справки в кредитных учреждениях для применения целевых финансовых санкций в условиях возрастающего количества мошеннических манипуляций [14].

Несмотря на то, что многие зарубежные регуляторы в своей практике широко используют ИИ, все же стоит отметить некоторые проблемы межведомственного цифрового взаимодействия в сфере ПОД/ФТ как на национальном, так и на международном уровне. В первую очередь, это касается вопроса обеспечения конфиденциальности данных, нормативным регулированием защиты персональных данных, в частности соблюдения границ прав и свобод гражданина. Передавая информацию другим финансовым учреждениям в рамках ОД/ФТ, могут быть раскрыты данные, позволяющие составить суждение о материальном состоянии лица, его социальном положении и иные сведения. На национальном уровне во многих государствах данные вопросы регулируются нормами права о банковской тайне и защите персональных данных, что обуславливает дополнительные препятствия в силу необходимости получения согласия от клиента на передачу сведений другим финансовым учреждениям. Более того, существует риск утечки данных при информационном обмене, что предполагает обязательность процедуры шифрования данных, обуславливая дополнительные затраты и ответственность сторон. При международном цифровом взаимодействии возникает также проблема обеспечения равной надлежащей защиты данных, а это не всегда достижимо в силу разницы правовых режимов и возможностей государств. Помимо этого, при использовании ИИ с зарубежными коллегами могут возникнуть трудности с интерпретацией аналитических данных, их применимостью на фоне разных подходов учреждений к идентификации клиентов, степени имплементации требований по ПОД/ФТ. Существенным недостатком можно отметить разный уровень международного взаимодействия и согласованности действий межведомственных органов.

Выводы

Таким образом, цифровизация в сфере ПОД/ФТ выступает несомненным преимуществом в достижении стратегических целей. Применение отдельных высокотехнологичных инструментов на национальном уровне в ряде государств уже дает свои положительные результаты в сокращении временных затрат, минимизации рисков ОД/ФТ, упрощения предоставления регуляторной отчетности, возможности обработки больших объемом данных и т. д. Однако для масштабного использования передовых технологий в рамках укрепления взаимодействия между финансовыми учреждениями, международного сотрудничества с уполномоченными органами требуется решение несколько задач, среди которых вопросы нормативно-правового регулирования, обеспечение должного уровня защиты информации путем кодирования или возможного обезличивания информации, унификации применяемых моделей оценки, достижения максимальной имплементации требований ПОД/ФТ.

ЛИТЕРАТУРА

1. Лапина С.Б., Куцык В.П. Совершенствование способов противодействия легализации (отмыванию) доходов, полученных преступным путем, в условиях развития рынка цифровых финансовых активов // Современные проблемы обеспечения экономической безопасности хозяйствующего субъекта. — 2021. — С. 102–107.
2. Гаврюшенко А.П. Цифровая оффшоризация глобальной экономики: проблемы анализа и противодействия // Проблемы российской экономики на современном этапе. — 2021. — С. 29–35.

3. Гаврюшенко А.П. Международное взаимодействие в сфере противодействия теневым цифровым финансовым потокам // Научное обозрение: теория и практика. — 2020. — Т. 10. — № 5. — С. 764–775.
4. Шараев П.С. Противодействие отмыванию (легализации) денежных средств в условиях цифровой трансформации (финансово-правовой аспект) // Юридический вестник Самарского университета. — 2022. — Т. 8. — № 3. — С. 94–100.
5. Криштопов С.В. Противодействие финансированию экстремизма посредством передачи цифровой валюты, цифровых финансовых активов и цифровых прав // Военное право. — 2021. — № 2. — С. 267–272.
6. Гашенко И.В., Зима Ю.С., Оробинская И.В. Обеспечение налоговой безопасности государства в сфере противодействия современным вызовам и угрозам // Учет и статистика. — 2022. — № 2(66). — С. 71–80.
7. Курышева Н.С. Использование цифровых финансовых технологий как фактор в расследовании преступлений // Вызовы времени и ведущие мировые научные центры: сборник статей Международной научно-практической конференции (02 февраля 2022 г., г. Иркутск) / В 2 ч. Ч. 1. — 2022. — С. 163.
8. Бастрыкин А.И. Расследование легализации доходов, полученных преступным путем, и финансирования терроризма: практика Следственного комитета России // Вестник Санкт-Петербургского университета. Право. — 2021. — Т. 12. — № 3. — С. 493–501.
9. Понаморенко В.Е. Актуальные аспекты правового регулирования цифровых активов в странах ЕАЭС/ЕАГ в свете финансовой безопасности региона // Развитие российской экономики и ее финансовая безопасность в условиях современных вызовов и угроз. — 2020. — С. 41–48.
10. Прасолов В.И., Фешина С.С. Влияние цифровой трансформации на процессы выявления легализации доходов, полученных преступным путем // Экономика: вчера, сегодня, завтра. — 2020. — Т. 10. — № 8-1. — С. 130–145.
11. Ястребов О.А., Аксенова М.А. Влияние искусственного интеллекта на административно-правовой режим противодействия легализации доходов, полученных преступным путем и финансированию терроризма: вопросы права // Правовая политика и правовая жизнь. — 2022. — № 3. — С. 84–109.
12. Сурнина К.С., Подкаминная Н.С. Цифровизация экономики России: возникающие проблемы системы противодействия незаконным финансовым операциям // Актуальные проблемы и перспективы развития экономики. — 2019. — С. 309–310.
13. Захарченко Е.С. К вопросу о необходимости активизации государственного регулирования системы противодействия отмыванию доходов, полученных преступным путем, финансировании терроризма в условиях перехода к цифровой экономике // Особенности государственного регулирования внешнеэкономической деятельности в современных условиях. — 2020. — С. 143–149.
14. Батюкова В.Е., Асылбаев Н.А. Особенности взаимодействия органов финансового мониторинга с правоохранительными органами в отношении отмывания преступных доходов на примере Кыргызской республики // Журнал зарубежного законодательства и сравнительного правоведения. — 2021. — Т. 17. — № 6. — С. 29–37.

Grebenkina Svetlana Alexandrovna
Financial University under the Government of the Russian Federation, Moscow, Russia
Institute for Economic Policy and Problems Economic Security
E-mail: s.greb@list.ru
RSCI: https://www.elibrary.ru/author_profile.asp?id=855670

Analysis of international practice of digital interaction in the field of anti-money laundering and terrorism financing

Abstract. The work is devoted to the study of foreign experience of digital interdepartmental interaction. The author analyzed the successful practices of introducing artificial intelligence in matters of combating money laundering and the financing of terrorism. The most popular high-tech tools and strategies used by regulators and financial institutions both at the national level and in interdepartmental international cooperation are disclosed. The foreign practice of implementation and the main elements of SupTech- and RegTech-strategies, as well as the advantages achieved with their help in the field of control and supervision activities, among which the most significant are: automation and standardization of business processes in the framework of the implementation of supervisory requirements, optimization of the collection and processing of information, reduction of time and financial costs, efficiency in detecting signs of fraud and others. The positive experience of using artificial intelligence is considered on the example of Great Britain, Singapore, Japan, China, a number of European financial institutions. The main problems of using advanced technologies by supervised entities and regulators in countering the legalization (laundering) of proceeds from crime and the financing of terrorism, which act as a barrier to large-scale digitalization in this area, are identified, namely: the complexity of legal regulation and ensuring an adequate level of information protection, problems of interpreting the results of the assessment, varying degrees of implementation of the recommendations of the Financial Action Task Force on Money Laundering, differences in the approaches to identification and others. In the final part of the article, the author argues that for the large-scale use of advanced technologies in the framework of strengthening interaction between financial institutions, international cooperation with authorized bodies, it is necessary to solve several problems indicated in the article.

Keywords: international experience; countering money laundering and terrorist financing; artificial intelligence; digital interaction; advanced technologies; financial intelligence; financial institutions