Академия управления МВД России

Т. В. Пинкевич, Е. С. Смольянинов

МЕЖДУНАРОДНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Учебно-практическое пособие

Москва • 2021

УДК 343.9.01
ББК 67.51
П 32

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *Дмитренко А. П.,* профессор кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, профессор; *Степанов М.В.,* начальник кафедры уголовного и уголовно-исполнительного права Нижегородской академии МВД России, кандидат юридических наук, доцент.

П 32

Международный опыт противодействия преступной деятельности с использованием криптовалюты: учебно-практическое пособие / Т.В. Пинкевич, Е.С. Смольянинов – Москва : Академия управления МВД России, 2021. – 108 с.

ISBN 978–5–907187–60–3

Учебно-практическое пособие включает материалы по правовым основам международного сотрудничества в сфере предупреждения преступлений, совершаемых с использованием криптовалюты. Представлен анализ деятельности международных органов и организаций, принимающих активное участие в предупреждении преступлений с использованием криптовалюты. Особое внимание уделено уточнению функций, задач, выявлению роли в предупреждении преступной деятельности с использованием криптовалюты таких международных организаций, как Интерпол, Европол и ФАТФ.

Учебно-практическое пособие рекомендовано слушателям, проходящим обучение по направлениям подготовки 38.04.02 – Менеджмент, 38.04.03 – Управление персоналом, 38.04.04 – Государственное и муниципальное управление, 40.07.01 – Юриспруденция при изучении учебных дисциплин, таких как «Организация противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий», «Цифровая криминология» «Уголовная политика», научным и практическим сотрудникам правоохранительных органов, профессорско-преподавательскому составу и адъюнктам.

УДК 343.9.01
ББК 67.51

ISBN 978–5–907187–60–3

Авторский коллектив:

Пинкевич Татьяна Валентиновна, доктор юридических наук, профессор – предисловие, главы 1–4, заключение, список рекомендованной литературы;

Смольянинов Евгений Серафимович, доктор юридических наук, доцент – глава 5.

Список сокращений

БПЛА – беспилотные летательные аппараты.

ВЭФ – Всемирный Экономический Форум.

ДМС – Дирекция по международному сотрудничеству.

Евроюст – Агентство Европейского союза, взаимодействующее с судебными органами.

ЕКПП – Европейский комитет по проблемам преступности.

ЕС – Европейский Союз.

ИИ – Искусственный интеллект.

МВФ – Международный валютный фонд ООН.

ООН – Организация Объединенных Наций.

СНГ – Содружество Независимых Государств.

УНП ООН – Управление ООН по наркотикам и преступности.

ФБР США – Федеральное Бюро Расследований Соединенных Штатов Америки.

ФАТФ – Группа разработки финансовых мер борьбы с «отмыванием» денег.

ФЗ РФ – Федеральный закон Российской Федерации.

ЭКОСОС – Экономический и социальный совет ООН.

ЮНЕСКО – Организация Объединенных Наций по вопросам образования, науки и культуры.

ЮНИСЕФ – Международный детский фонд ООН.

ЮНОПС – Управление по обслуживанию проектов ООН.

ECPA – Европейская премия по предупреждению преступности.

EUCPN – Европейская сеть по предупреждению преступности.

DLT – распределенная бухгалтерская книга.

IOTA – криптовалюта с открытым исходным кодом.

NASDAQ – Служба автоматизированных котировок Национальной ассоциации дилеров по ценным бумагам.

SCIP – Международная организация конкурентной разведки.

WEF – Всемирный Экономический Форум.

Содержание

Предисловие

Применение цифровых технологий в современном мире способствовало активному развитию виртуальных экономических отношений, в том числе и электронной коммерции, которая в настоящее время стала неотъемлемой и весьма значительной частью национальной экономики каждого государства. Вместе с развитием электронных платежных сервисов и цифровых технологий, а также использованием электронных и виртуальных валют, не только увеличилось количество преступных проявлений, но произошло и изменение преступности в целом, появились новые ее виды, а также новые предметы, способы и средства совершения преступлений.

Результаты, полученные в ходе проведенного комплексного исследования преступности, свидетельствуют о том, что количественные и качественные показатели зарегистрированных преступлений, совершаемых с использованием криптовалюты, свидетельствуют о высоком уровне распространения деяний, проводимых как в отношении криптовалюты, так и с ее использованием[1]. В этой связи исследование опыта развития правовых основ международного сотрудничества в сфере противодействия преступной деятельности с использованием криптовалют, определение роли международных органов и организаций и рассмотрение проблем правового регулирования криптовалюты сегодня могут быть очень востребованы, поскольку она не имеет правового статуса; неподконтрольна национальным органам власти; не обеспечена ликвидными активами и какими-либо гарантиями государственного либо частного капитала, подвержена существенным курсовым колебаниям, в т. ч. спекулятивного характера; осуществление операций на «виртуальных биржах» несет высокий риск потери стоимости криптовалют; может конкурировать с национальными фиатными валютами и привести к их ослаблению.

Основная цель учебно-практического пособия – ввести, прежде всего, магистрантов, адъюнктов и соискателей Академии управления МВД России, в сферу криминологических проблем, решаемых

[1] *Пинкевич Т.В.* Преступность с использованием криптографических кодов и ее влияние на криминологическую безопасность России // Проблемы экономики и юридической практики. Москва, 2019 № 3. С. 88–91; *Пинкевич Т.В.* Некоторые проблемы создания механизма противодействия преступлениям, совершаемым с использованием виртуальной валюты и инвестиционных платформ // Сб. статей IV Всероссийской науч.-практ. конференции «Уголовно-правовое воздействие и его роль в предупреждении преступности» (30 сентября – 1 октября 2019 г.). Саратов: Изд-во Саратовской государственной юридической академии, 2019 г. С. 285–289.

международным сообществом, расширить круг криминологических знаний профессорско-преподавательского состава, а также практических работников системы МВД России, интересующихся проблемами противодействия преступной деятельности с использованием криптовалюты.

Учебно-практическое пособие включает материалы по правовым основам международного сотрудничества в сфере предупреждения преступлений, совершаемых с использованием криптовалюты, деятельности международных органов и организаций, принимающих активное участие в предупреждении названных преступлений, уточняющие их функции и задачи. Особое внимание уделено роли таких международных организаций, как Интерпол, Европол, а также ФАТФ в предупреждении преступной деятельности с использованием криптовалюты.

В то же время, следует обратить внимание на момент, который позволяет уяснить, прежде всего, проблемы понятийного аппарата криптовалюты. В международных документах, научных изданиях при характеристике криптовалюты используется разнообразный понятийный аппарат: «виртуальная валюта», «виртуальные активы», «криптовалюта», «электронная валюта», «имущество», «виртуальные деньги», «цифровой актив», «цифровой финансовый актив» и т. д. Такой разброс понятий свидетельствует только о том, что до настоящего времени на законодательном и доктринальном уровне понятие криптовалюты и вопросы ее правового регулирования не определены.

Так, например, Европейский центральный банк рассматривает криптовалюту как нерегулируемые цифровые деньги, выпускаемые и контролируемые их разработчиками, которые используются и принимаются среди членов определенного виртуального сообщества[1].

В Докладе (2014 г.) «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ» дано понятие криптовалюты как средства «выражения стоимости, представленное в цифровом формате и выступающее в качестве средства обмена, либо расчетной денежной единицы, либо средства хранения стоимости и при этом не подпадающее под понятие законного платежного средства, т. е. не являющееся официально действующим законным средством платежа при расчетах с кредиторами»[2].

---

[1] Регулирование криптовалют в Евросоюзе. URL: https://crypto-fox.ru/faq/regulirovanie-kriptovalyut-v-evrosoyuze (дата обращения: 20.03.2020).

[2] Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 20.03.2020).

Позже, в отчете «Рекомендации ФАТФ (FATF) по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг в сфере виртуальных активов (VASP)» рассматривается криптовалюта как виртуальный актив *(virtual asset),* а именно, как «цифровое выражение ценности, которое может цифровым образом обращаться или переводиться и может быть использовано для целей осуществления платежей или инвестиций. Виртуальные активы не включают в себя цифровое выражение фиатных валют, ценных бумаг и других финансовых активов, регулируемых иными Рекомендациями ФАТФ»[1]. В названном отчете также приводится мнение США, согласно которого «цифровые финансовые активы» *(digital financial assets)* или просто «цифровые активы» *(digital assets)* являются всеобъемлющим термином, который относится к целому ряду видов деятельности в экосистеме цифровых финансовых услуг, включая финансовую деятельность с участием цифровых валют – как национальных цифровых валют, так и цифровых, которые не выпускаются и не гарантируются национальным правительством, таких как цифровые формы конвертируемых виртуальных валют, как биткойн, а также цифровых ценных бумаг, товаров или их производных»[2].

При этом в зарубежных изданиях *цифровую (виртуальную) валюту классифицируют на четыре вида:*

1) мобильная фиатная валюта (используемая при проведении банковских платежей);

2) валюта корпоративного значения (вознаграждения за лояльность, например, скидки для клиентов, выражаемые в баллах, кредитах и т. п.);

3) валюта виртуальных миров (внутриигровая валюта);

4) децентрализованная валюта (прежде всего биткоин, альткойны и иные виды криптовалют, являющихся альтернативой централизованной банковской валюте)[3].

Итак, цифровая валюта как инструмент цифрового права может функционировать в цифровой форме в качестве средства выраже-

---

[1] Отчет. Рекомендации ФАТФ (FATF) по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг в сфере виртуальных активов (VASP). URL: https://mgimo.ru/upload/2020/02/rekomendacii-fatf-fatf-po-regulirovaniyu-oborota-virtualnyh-aktivov-i-deyatelnosti-provajderov-uslug-v-sfere-virtualnyh-aktivov.pdf (дата обращения: 20.03.2020).

[2] *Там же.*

[3] Aaron Smith Future of Money: Classifying Virtual Currency Systems. URL: http://bigthink.com/hybrid-reality/future-of-money-classifying-virtual-currency-systems (дата обращения: 20.03.2020).

ния стоимости, обмена, платежа, хранения[1]. Она функционирует в двух видах:

1) электронные деньги, являясь цифровым средством, используются для электронного перевода фиатной валюты и обладают статусом законного платежного средства;

2) виртуальная валюта (криптовалюта) представляет собой разновидность цифровой валюты, защищенной криптографическим кодом, не имеет централизованного эмитента[2] вещественной формы, а существует лишь в виде записей пользователей системы блокчейна[3], но доступна для майнинга[4] любым желающим при помощи имеющихся у него компьютерных мощностей[5].

В тексте учебно-практического пособия мы будем указывать криптовалюту (криптовалюты) без ссылки на ее виртуальность, т. к. виртуальная валюта может быть нескольких видов.

Авторы настоящего издания будут весьма признательны читателям за их замечания и пожелания, направленные на дальнейшее улучшение содержания представленного учебно-практического пособия.

---

[1] Виртуальные валюты: ключевые определения и потенциальные риски в сфере ПОД/ФТ. Отчет ФАТФ. Июнь 2014. С. 6.

[2] Эмитент – юридическое лицо, исполнительный орган государственной власти, орган местного самоуправления, которые несут от своего имени или от имени публично-правового образования обязательства перед владельцами ценных бумаг по осуществлению прав, закрепленных этими ценными бумагами.

[3] Блокчейн – это база данных, распределенная среди большого числа участвующих в сети узлов, которые обеспечивают безопасность системы.

[4] Майнинг (от англ. *mining* – добыча полезных ископаемых) – деятельность по созданию новых структур (обычно речь идет о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ.

[5] *Демидов О.* Связанные одним блокчейном: обзор международного опыта регулирования криптовалют: Индекс безопасности. № 2 (113). Т. 21. С. 43–58.

Глава 1. Правовая основа международного сотрудничества в сфере предупреждения цифровой преступности

Международное сотрудничество в сфере предупреждения преступности прошло длительный путь и является важным направлением уголовной политики, которая разрабатывается и реализуется на глобальном, региональном и национальном уровнях, и осуществляется на основании международных соглашений (конвенционная форма) и в рамках международных органов и организаций (институционная форма). Основой такого сотрудничества выступают международные и национальные многосторонние Конвенции и региональные соглашения. При этом государства стремятся к объединению усилий в противодействии наиболее опасным преступлениям. С этой целью координируется уголовная политика, проводится мониторинг криминальной ситуации, разрабатываются рекомендации, что «ведет к формированию особой группы норм международного публичного права – международно-правовых основ борьбы с преступностью или международного права борьбы с преступностью»[1].

К основным направлениям международного сотрудничества государств в сфере противодействия преступности следует отнести:

– договорно-правовую координацию противодействия преступлениям;

– научно-информационное обеспечение усилий международного сообщества;

– оказание профессионально-технической помощи государствам;

– экстрадицию и оказание правовой помощи по уголовным делам.

Началом международного сотрудничества принято считать середину XIX ст. Традиционно считается, что состоявшийся в 1872 г. в Лондоне Первый международный тюремный конгресс «оказался поворотным пунктом в международных встречах не столько потому, что заседания были заранее тщательно подготовлены ведущими теоретиками и практиками более чем из 20 суверенных государств, сколько потому, что это была первая международная конференция,

[1] *Уткин В.А.* Международное право борьбы с преступностью: учеб. пособие. Москва: ЮСТИЦИЯ, 2019. С. 8.

которая собрала вместе представителей правительств, а также ученых и администраторов судебно-исправительной системы»[1].

С этого момента Конгрессы ООН закладывают международно-правовые основы борьбы с преступностью. Их «можно характеризовать как принятые на международном уровне нормы, принципы и рекомендации в области специального предупреждения преступлений, деятельности системы уголовной юстиции, межгосударственного сотрудничества в борьбе с преступностью....»[2].

За годы существования ООН создан обширный свод стандартов и норм в области предупреждения преступности и уголовного правосудия, которые имеют криминологическое значение. К таковым, например, можно отнести: Конвенцию против транснациональной организованной преступности и три дополняющих ее протокола (Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее; Протокол против незаконного ввоза мигрантов по суше, морю и воздуху и Протокол против незаконного изготовления и оборота огнестрельного оружия и пр.), Конвенцию против коррупции, минимальные стандартные правила обращения с заключенными; Кодекс поведения должностных лиц по поддержанию правопорядка, меры борьбы против коррупции; Международный кодекс поведения государственных должностных лиц, основные принципы применения силы и огнестрельного оружия должностными лицами по поддержанию правопорядка; Декларацию основных принципов правосудия для жертв преступлений и злоупотребления; Основные принципы, касающиеся независимости судебных органов; Основные принципы, касающиеся роли адвокатов; Программу по контролю над наркотиками и др. Многие из них носят рекомендательный характер и не являются юридически обязательными для государств-участниц, хотя и оказывают существенное влияние на развитие законодательства государств в сфере предупреждения преступности и уголовной юстиции.

С 1872 по 2015 гг. Конгрессы проводились каждые пять лет, ими принимались решения, касающиеся предупреждения различных видов преступности. Одним из значимых, согласно проведенного исследования, следует считать XI Конгресс, состоявшийся в Бангкоке (2005 г.), в ходе которого была принята декларация

---

[1] *Alper B. S., Boren J. F. with a Forew by Clifford W.* Crime: International Agenda. Concern and Action in the Prevention of Crime and Treatment of Offenders, 1946–1972. United Nations. Toronto – London, 1972. P. 24

[2] *Уткин В.А.* Международное право борьбы с преступностью. Томск: Изд-во НТЛ, 2017. С. 10

«Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия». При проведении этого мероприятия государства-участники подтвердили решимость продолжать международное сотрудничество в противодействии преступности, в т. ч. киберпреступности, легализации (отмыванию) преступных доходов, терроризму, незаконному обороту культурных ценностей и др. Впервые на уровне Конгресса обращено внимание на предупреждение киберпреступности. Однако решений, связанных с предупреждением преступности в сфере цифровых технологий, незаконному обороту криптовалюты на уровне ООН в этот период времени не уделялось из-за отсутствия предмета обсуждения.

XII Конгресс ООН по предупреждению преступности и уголовному правосудию (12–19 апреля 2010 г.), который состоялся в г. Сальвадоре в Бразилии, с учетом выработанных выводов и рекомендаций[1], одобренных Генеральной Ассамблеей в ее резолюции 62/1734, открыл возможность для обсуждения проблем, связанных с расследованием этих преступлений и противодействием киберпреступности (ее транснациональный характер, сложность определения и подсчета количества совершенных преступлений и убытков от них, и пр.), а также с новыми международными мерами по противодействию киберпреступности и транснациональной организованной преступности. Решающее значение в выявлении и расследовании этих преступлений, по мнению организаторов, имеют «своевременность и эффективность взаимодействия между государственными органами разных стран, поскольку следы киберпреступлений во многих случаях уничтожаются автоматически через короткий промежуток времени»[2].

Позже всесторонне исследуются проблемы киберпреступности. Так, в 2013 г. Управление по наркотикам и преступности ООН представило проект исследований в этой сфере. В нем было представлено международно-правовое определение киберпреступности, очерчен круг деяний, являющихся таковыми, дана характеристика киберпреступника. Особое место отведено роли организованных преступных групп.

---

[1] Доклад совещания Межправительственной группы экспертов по рассмотрению уроков, извлеченных из опыта Конгресса ООН по предупреждению преступности и уголовному правосудию. Бангкок. 2006. 15–18 августа. URL: https://undocs.org/ru/A/CONF.213/9 (дата обращения: 21.03.2020).

[2] XII Конгресс ООН по предупреждению преступности и уголовному правосудию. Сальвадор. Бразилия. 12–19 апреля 2010 года. URL: https://undocs.org/ru/A/CONF.213/9 (дата обращения: 21.03.2020).

Генеральный секретарь ООН в своем докладе «Предупреждение, защита и международное сотрудничество в области борьбы с использованием новых информационных технологий для надругательства над детьми и (или) их эксплуатации» (2014 г.) дает оценку влияния новых информационно-телекоммуникационных технологий на ситуацию с насилием над детьми и их эксплуатацией[1].

Вместе с тем появились суждения, согласно которым одни авторы утверждали, что имеющиеся международные акты устарели, не продуктивны и не способствуют совершенствованию уголовного законодательства зарубежных стран, направленного на охрану цифровых технологий[2]. По мнению других, международно-правовые акты по обеспечению безопасности цифровых технологий до настоящего времени не утверждены, и иностранным государствам постоянно приходится подстраивать свое законодательство к вновь возникающим внешним и внутренним факторам[3]. В то же время, материалы отчета Ассоциации финансовых профессионалов за 2017 г. свидетельствуют о том, что Управление по обслуживанию проектов ООН исследует пакет решений для международных платежей Ripple. Вопрос о реагировании и наличие нового финансового инструмента (криптовалюты) стал все чаще беспокоить международное сообщество и ООН.

В ходе Азиатско-тихоокеанского регионального совещания по подготовке к XIV Конгрессу ООН по предупреждению преступности и уголовному правосудию (Бангкок, 22–24 января 2019 г.)[4] обсуждались вопросы подготовки XIV Конгресса ООН, на котором планируется рассмотреть вопросы международного сотрудничества и технической помощи в предупреждении всех форм преступности и борьбе с ними, в т. ч. с терроризмом во всех его формах и проявлениях; новыми и появляющимися формами деяний; современными тенденциями в области преступности, в частности, использование современных цифровых технологий как средства совершения преступлений и инструмента борьбы с ними.

---

[1] *Овчинский В. С.* Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. Москва: Норма, 2017. С. 34.

[2] *Тропина Т. Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86–95.

[3] *Овчинский В. С.* Криминология цифрового мира: учебник. Москва: Норма: ИНФРА-М, 2018. С. 11.

[4] Азиатско-тихоокеанское региональное совещание по подготовке к четырнадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Бангкок, 22–24 января 2019 года. URL: https://undocs.org/pdf?symbol=ru/A/CONF.234/RPM.1/L.2 (дата обращения: 22.03.2020).

В январе 2019 г. Департамент по экономическим и социальным вопросам ООН опубликовал доклад, посвященный обзору мирового экономического и социального положения в 2018 г., где был сделан вывод о том, что криптовалюты и блокчейн являются важной частью мировой финансовой системы, которые могут избавить мир от необходимости доверять централизованным институтам, сократить число бюрократических процедур, создать инновационные бизнес-модели и существенно повысить эффективность управления, изучить возможность использования технологии блокчейн для борьбы с такими явлениями, как преступность, коррупция, и особо выделяется борьба с торговлей детьми[1]. Здесь же раскрываются преимущества криптотехнологий, блокчейна и распределенной бухгалтерской книги, а криптовалюта рассматривается как «новый рубеж в области цифровых финансов»[2].

В мае этого же года Управление по обслуживанию проектов ООН (ЮНОПС) объявило о своем сотрудничестве с IOTA, чтобы «изучить, как инновационная технология IOTA на базе распределенного реестра с открытым исходным кодом для управления данными, может повысить эффективность операций ЮНОПС». В октябре ЮНИСЕФ (фонд организации, помогающий обездоленным детям по всему миру) начал принимать пожертвования в такой криптовалюте, как биткоин и эфириум.

В связи с вышеизложенным, ООН, специально для международной программы «Цели устойчивого развития», призванной решить такие глобальные проблемы, как бедность, неравенство, климатические изменения, ухудшение состояния окружающей среды и т. д., открывает фонд для финансирования цифровыми токенами, с целью привлечения нескольких сотен миллионов долларов и размещения их как в фиатном, так и в цифровом формате на блокчейне. Фонд стал первой структурой в составе программы ООН, которая может принимать и работать со всеми видами криптовалютных и цифровых активов. Известно, что фондом управляет децентрализованная платформа кредитования *Celsius Network,*

---

[1] Доклад ООН: криптовалюты и блокчейн – это «важная часть глобальной финансовой системы». URL: http://cryptoconsulting.info/ru/doklad-oon-kriptovalyutyi-i-blokcheyn-eto-vazhnaya-chast-globalnoy-finansovoy-sistemyi (дата обращения: 27.05.2020).

[2] ООН: блокчейн и криптовалюты – новый рубеж в бизнесе и госуправлении. URL: https://roskomsvoboda.org/44455/ (дата обращения: 27.05.2020 г.); Обзор мирового экономического и социального положения, 2018 год: передовые технологии в интересах устойчивого развития. URL: https://www.un.org/development/desa/dpad/publication/обзор-мирового-экономического-и-соци (дата обращения: 02.05.2020).

а проект запустил поставщик финансовых услуг *Fifth Element*. В рамках этой программы французское подразделение Международного детского фонда ООН (ЮНИСЕФ) объявило о том, что начнет принимать пожертвования в девяти криптовалютах: *Bitcoin, Bitcoin Cash, Ethereum, Litecoin, XRP, EOS, Monero, Dash* и *Stellar*. Более того, ЮНИСЕФ уже применяет вычислительные мощности компьютеров для сбора пожертвований с помощью майнинга криптовалюты Monero.

В то же время исследование международного опыта и развития зарубежного законодательства в сфере противодействия преступной деятельности с использованием криптовалюты и рассмотрение проблем ее правового регулирования сегодня свидетельствуют о том, что в этот период еще не принято никаких правовых решений, регулирующих использование криптовалюты. При этом масштабы ее распространения растут.

Что же касается в целом регулирования цифровых технологий, то предпринимались попытки правового регулирования на международном региональном уровне. Лидерами здесь можно назвать США и страны Европейского союза. Тем не менее такая технология, как Большие данные *(Big Data),* в настоящее время не получила нормативно-правового определения ни в одной из юрисдикций мира. Основное направление в их урегулировании сводится к защите персональной информации. Аналогичная ситуация складывается и в отношении системы распределенного реестра (блокчейна). Стремление создать правовую основу использования искусственного интеллекта и иных цифровых технологий пока не увенчалась успехом. Что же касается квантовых технологий, то международное законодательство здесь только формируется. В ряде стран, например, в США Конгрессом утвержден проект развития квантовых технологий, создана Национальная квантовая лаборатория в Китае, в Европе получила развитие программа «Квантовый Флагман». На международном уровне особое внимание уделяется регулированию квантовых вычислений, направленных на борьбу с преступностью; коммуникаций, связанных с криптографической защитой информации, использующей для передачи ключей индивидуальные квантовые частицы; квантовых сенсоров, с помощью которых возможно обеспечение обороны и безопасности государства[1].

Ряд стран уже информировали международное сообщество об использовании технологий блокчейн и криптовалюты. Так, пре-

[1] России нужен 51 миллиард на вторую квантовую революцию. URL: https://cnews.ru/news/top/2019-08-25_rossii_nuzhen_51_milliard_na (дата обращения: 02.12.2019).

мьер-министр Мальты Джозеф Мускат посвятил свое выступление на заседании Генеральной Ассамблее ООН и теме криптовалют и блокчейн-технологиям. В своем докладе глава правительства раскрыл перспективы и представил цифры экономических достижений, которые принесли плоды криптолиберализации национального законодательства, поскольку здесь официально разрешен выпуск токенов на ICO и уравнены в правах цифровые и фиатные валюты. Более того, привлечена биржа Binance, чьи $200 млн квартальной прибыли превысили показатели крупнейшего оператора рыночных торгов традиционными активами NASDAQ. Мальта получила практически мгновенный эффект от принятия законов, регулирующих цифровые активы, что особенно важно для бедных государств, лишенных традиционных источников доходов в виде полезных ископаемых. На примере интеграции блокчейн-технологий в госуправление, Мальта показала, как этот процесс может снизить коррупционные риски и эффективно управлять различными сферами, начиная от здравоохранения, заканчивая утилизацией отходов.

Из выступления начальника отдела по борьбе с киберпреступностью и отмыванием денег Управления ООН по борьбе с распространением наркотиков и преступностью Нила Уолша (от 30 августа 2019 г.) стали известны способы использования криптовалюты в преступных целях и причины, по которым важно научиться отслеживать подобные транзакции. По его мнению, криптовалюты мешают борьбе с финансированием терроризма, легализации (отмыванию) преступных доходов и киберпреступностью, за счет анонимности биткоин и альткоинов, поскольку они обеспечены новым уровнем секретности, помогающим преступникам. В свою очередь правоохранительным структурам сложно противостоять этим вызовам[1].

По данным исследования, которое было проведено ООН, ежегодно сумма легализованных (отмываемых) в мире денежных средств, полученных в результате совершения различного рода преступлений, составляет от 2 до 5 % мирового ВВП, или в денежном выражении – от 800 млрд до 2 трлн долл. США[2].

Однако базовых документов на международном уровне, положенным в основу формирования нормативно-правовых актов, направленных на противодействие преступной деятельности с использованием криптовалют, пока не было принято.

---

[1] *Теткин М.* Нил Уолш, ООН: криптовалюты помогают террористам. URL: https://www.rbc.ru/crypto/news/5d68caa79a79472991ab5e9c (дата обращения: 15.03.2020).

[2] Money-Laundering and Globalization. URL: http://www.unodc.ogr/unodc/en/money-laundering/globalization.html (дата обращения: 15.03.2020).

В январе 2020 г. Генеральный секретарь ООН Антониу Гутерриш заявил о том, что организация должна использовать блокчейн и технологию распределенной бухгалтерской книги (DLT), и порекомендовал включить технологию блокчейна в число основных технологий, используемых ООН. По его мнению, наступила цифровая эпоха, в ходе которой ООН могла бы лучше выполнять поставленные задачи с помощью использования новых технологий, таких как блокчейн, что ускорило бы достижение целей в области устойчивого развития[1]. Он также сообщил о том, что уже ведется работа со Всемирной сетью идентификации для изучения записей идентификаторов на блокчейне для противодействия торговле детьми. Более того, в отчете о мировой экономике ООН называет криптовалюты «новой границей» в цифровых финансах[2].

С момента запуска инициативы по цифровому сотрудничеству технология блокчейна повсеместно внедрялась в программы ООН. Недавно организация запустила блокчейн-инструмент, который помогает предотвращать эксплуатацию труда мигрантов в Гонконге. Помимо этого, ООН занимается разработкой решений с использованием системы блокчейн, способных обеспечить устойчивое развитие городских поселений в Афганистане.

В то же время в своей деятельности ООН обращает внимание и на недобросовестных участников крипторынков. Так, например, она обвиняет Северную Корею в том, что та занимается легализацией (отмыванием) преступных доходов, которая осуществляется через блокчейн-компанию «Marine China», находящуюся в Гонконге. По заявлениям специальной комиссии ООН, проводившей свое расследование и анализирующей деятельность компании Marine China, известно, что Северная Корея, вопреки санкциям, продолжила работу по развитию своего судоходства, но поскольку санкции не давали возможности государству полноценно использовать свою логистическую сферу, то компания «Marine China» проводила транзакции посредством виртуальных валют. В результате осуществлена легализация (отмывание) преступных доходов в больших объемах,

---

[1] Генеральный секретарь ООН Антониу Гутерриш (António Guterres) уверен, что возглавляемая им организация должна применять технологию блокчейна. URL: https://coinspot.io/technology/oon-kriptovalyuty-otkryvayut-novye-gorizonty-v-cifrovyh-finansah (дата обращения: 15.03.2020).

[2] Глава Организации Объединенных Наций рекламирует технологию блокчейна как важнейший компонент эпохи цифровых технологий. URL: https://cryptonews.one/blockchain/glava-organizacii-obedinennykh-nacijj-reklamiruet-tekhnologiju-blokchejjna-kak-vazhnejjshijj-komponent-ehpokhi-cifrovykh-tekhnologijj (дата обращения: 02.02.2020).

что причинило огромные убытки другим участникам конфликта[1]. Более того, по данным конфиденциального досье, криптовалюта, которая накоплена Северной Кореей, была в большей своей части получена преступным путем (хищение в результате кибератак и криптовалютных хаков). Именно она создает фундамент для совершенствования своих ядерных и ракетных программ[2].

И несмотря на то, что проблемы в противодействии преступности данного вида существуют, до последнего времени не было проведено ни одного Конгресса, посвященного противодействию преступности в сфере цифровых технологий, и не рассматривались проблемы противодействия преступлениям, совершаемым с использованием криптовалюты. Также не приняты базовые документы на международном уровне, которые могли бы быть положены в основу формирования нормативно-правовых актов, направленных на противодействие преступной деятельности с использованием цифровых технологий и криптовалюты.

Исследование опыта развития международных правовых основ и зарубежного законодательства в сфере противодействия преступной деятельности с использованием криптовалют и рассмотрение проблем ее правового регулирования сегодня могут быть востребованы, т. к. стремительное развитие инновационных технологий и беспрецедентный прогресс распространения цифровых технологий (искусственный интеллект и робототехника, информатика, технологии распределительного реестра и пр.) могут быть использованы для совершения преступлений. В рамках работы XIV Конгресса ООН по предупреждению преступности и уголовному правосудию, который должен был состояться 20–27 апреля 2020 г. в Японии (г. Киото), ООН запланировала рассмотрение ряда вопросов. Так, в соответствии с п. 3 ст. 27 проекта Конвенции об организованной преступности, предусмотрено, что «государства должны стремиться к укреплению сотрудничества с целью противодействия транснациональной организованной преступности, которая при осуществлении преступной деятельности активно использует современные технологии»[3]. Что же касается национального уровня, все больше

---

[1] ООН обвиняет Северную Корею в обмывании денег через криптовалюты. URL: https://crypto-news.space/kriptovalyuty/oon-obvinyaet-severnuyu-koreyu-v-obmyvanii-deneg-cherez-kriptovalyuty (дата обращения: 02.02.2020).

[2] Северная Корея накапливает криптовалюту для оружейных программ. URL: https://neovesting.com/security/оон-северная-корея-накапливает-крипт/2019/08/06 (дата обращения: 20.02.2020).

[3] Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Киото, Япония, 20–27 апреля 2020 г. (ПРОЕКТ). URL: https://undocs.org/ru/A/RES/69/313 (дата обращения 20.06.2020).

внимания уделяется правовым мерам и укреплению потенциала, наряду со стратегическим планированием, что может также включать, в соответствующих случаях, партнерские отношения между государственным и частным сектором.

В этой связи для ООН интересными являются шесть направлений, по которым сегодня должно укрепляться международное сотрудничество и которые тесно взаимосвязаны между собой, но они должны быть объединены и с таким явлением как терроризм, в т. ч. и его финансированием. К таковым авторы проекта предлагают отнести использование криптовалюты в преступных целях, незаконный оборот наркотиков, огнестрельного оружия с использованием цифровых технологий, а также связь современных информационных технологий с торговлей людьми, надругательствами над детьми и их эксплуатацией и роль технологий в расследовании дел, связанных с незаконным ввозом мигрантов.

В материалах проекта семинара-практикума «Современные тенденции в области преступности, последние изменения и новые решения в частности использования современных технологий как средства совершения преступлений и инструмента борьбы с преступностью» представлено понятие криптовалют как «конвертируемые, действующие между равноправными субъектами, децентрализованные сетевые цифровые валюты, в т. ч. биткоин и эфириум, использующие методы криптографии для регулирования генерации денежных единиц и проверки перевода средств, обращение которых осуществляется независимо от центрального банка. Обеспеченная ими высокая степень анонимности в сочетании с низким уровнем обнаружения позволяет избежать многих рисков, связанных с операциями по легализации (отмыванию) преступных доходов и финансированию терроризма, что таким образом создает благоприятные условия для совершения этих преступлений в виртуальной среде. Кроме того, криптовалюты могут облегчить совершение других преступлений, таких как вымогательство и мошенничество[1].

С учетом высокого влияния криптовалюты на преступность, которое будет сохраняться, рекомендуется следующее:

– компетентным органам принимать адекватные меры по урегулированию оборота криптовалюты, с учетом законного применения технологии блокчейн, включая использование криптовалют в качестве средства сохранения сбережений и способа оплаты законных товаров и услуг, и укреплять международное сотрудничество;

[1] *Там же.*

– государствам рассмотреть возможности разработки межведомственных стратегий, включая меры регулирования, директивные инициативы по предупреждению преступлений, совершаемых с использованием криптовалюты.

Особое внимание следует уделять подготовке специалистов правоохранительных органов с целью решения проблем и повышения потенциала для успешного и эффективного расследования и судебного преследования по таким уголовным делам.

По мнению ООН, предложенные меры будут способствовать выполнению, насколько это возможно в виртуальной среде, задач сокращения масштабов незаконных финансовых потоков, связанных с различными формами преступности, включая транснациональную организованную преступность.

Помимо создания правовой базы, международные организации готовы взять на себя ответственность по подготовке методических рекомендаций. Так, например, руководство Глобальной программы по киберпреступности Управления ООН по наркотикам и преступности (УПН ООН) совместно с представителями Глобальной программы против отмывания денег УНП ООН объединили усилия и на средства стран-доноров разработали интерактивный курс обучения по расследованию преступлений с использованием в своих целях криптовалюты – биткоин и эфириум. Данные рекомендации содержат информацию о природе работы криптовалют, способах и средствах слежения за криптовалютами, механизме ведения расследований и анализе транзакций с ними. Этими методическими рекомендациями могут воспользоваться все желающие, они есть в общем доступе и открыты не только для экспертов стран-членов УНП ООН. При этом следует помнить, что данные Рекомендации распространяются на страны, входящие в состав организации. Этот курс предназначен для подготовки специалистов в области расследования такого вида преступлений в различных регионах. Цель подготовки – повышение уровня квалификации сотрудников правоохранительных органов, прокуроров и судей с целью более глубокого понимания сущности криптовалюты, путей ее отслеживания при проведении финансовых расследований, поиска ресурсов для получения дополнительной информации и взаимодействия в изучении материалов международных судебных дел.

Надо признать, что УНП ООН принимает активное участие в налаживании партнерских отношений с субъектами секторов регулятивных *(RegTech)* и финансовых технологий *(FinTech)* и сотрудничает с отраслевыми лидерами в области криптовалют, такими как *Chainalysis Inc.,* для оказания помощи сотрудникам правоохрани-

тельных органов и аналитикам в отслеживании незаконных финансовых потоков.

В то же время следует учитывать и тот факт, что, несмотря на существование массы технических лазеек для технологии, лежащей в основе использования криптовалюты в преступных целях, между тем, некоторые аспекты технологии «блокчейн» открывают потенциально интересные возможности для следователей и могут быть полезным инструментом правоприменения, в т. ч. в выявлении подозрительных транзакций и использовании этого программного обеспечения для сбора доказательств.

Большая роль УНП ООН отведена организации конференций и практических семинаров. Проведение таких международных семинаров способствует диалогу и обмену мнениями технического характера относительно вышеуказанных шести тематических областей, представляющих интерес. Кроме того, этот семинар-практикум рассчитан на то, чтобы дополнить, при необходимости, те элементы обсуждения, которые касаются более широкого применения информационно-коммуникационных технологий террористами, в т. ч. для радикализации и вербовки молодых людей. Также обращено внимание на роль социальных сетей и современных коммуникационных технологий в более широком аспекте общественного участия и вклада в укрепление мер в области предупреждения преступности и уголовного правосудия.

Такие семинары позволяют обсудить и лучше понять различные методы, которые используются при совершении преступлений с применением цифровых технологий, и типы таких преступлений; изучить способы, с помощью которых система уголовного правосудия и правоохранительные органы могут более эффективно предупреждать и выявлять такие преступления, а также бороться с ними как на национальном, так и на международном уровне.

При этом семинары также позволяют изучить успешную практику и проблемы, в связи с современными требованиями, в отношении использования специальных методов расследования и сбора электронных доказательств в случае преступлений, совершаемых с применением цифровых технологий, и в связи с приемлемостью таких доказательств в суде; провести обзор действующих национальных нормативных стандартов и способствовать дальнейшему обсуждению возможного изменения законодательства, если таковое уместно, для удовлетворения новых потребностей и решения новых проблем; выявить примеры передовой практики и опыта в области успешного расследования и уголовного преследования в отношении преступлений, связанных с использованием названных технологий, с уделением особого внимания использованию технических нов-

шеств в качестве инструментов борьбы с такими преступлениями; обсудить появляющиеся тенденции и направления будущей деятельности в области использования цифровых технологий в борьбе с преступностью; оценить последствия использования этих технологий в борьбе с преступностью в области прав человека и пути надлежащего решения соответствующих проблем; способствовать диалогу относительно потребностей в профессиональной подготовке в области уголовного правосудия и правоприменения в целях более эффективного использования цифровых технологий в борьбе с преступностью, а также роли УНП ООН, с тем чтобы более адекватно ответить на эти потребности; обменяться информацией и опытом в отношении существующих пробелов и проблем в области международного сотрудничества, связанных с электронными доказательствами; оценить результаты партнерских отношений между государственным и частным сектором в деле предупреждения рассматриваемых преступлений и/или эффективной борьбы с ними.

В п. 167 Проекта материалов семинара-практикума № 4 «Современные тенденции в области преступности, последние изменения и новые решения, в частности использования современных технологий как средства совершения преступлений и инструмента борьбы с преступностью» XIV Конгресса ООН по предупреждению преступности и уголовному правосудию указывается на важность рассмотрения государствами возможности «разработки междисциплинарных стратегий (включая меры регулирования, директивные инициативы по предупреждению и подготовку сотрудников компетентных органов) с целью решения проблем и повышения потенциала для успешного и эффективного расследования и судебного преследования в соответствующих делах»[1].

Таким образом, можно констатировать, что имеющаяся правовая база в сфере киберпространства и противодействия преступности в сфере цифровых технологий в полной мере не отвечает современным реалиям и требует консолидации мирового сообщества к принятию единых правил игры как в повседневном их применении, так и в противодействии преступлениям, совершаемым с их использованием. При этом следует отметить, что на международном уровне предпринят ряд шагов, направленных на разработку правовых основ международного сотрудничества в сфере предупреждения цифровой преступности.

[1] Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию Киото, Япония, 20–27 апреля 2020 г.: https://undocs.org/ru/A/RES/69/313 (дата обращения: 20.06.2020).

Контрольные вопросы

1. Определите роль ООН в создании правовых основ предупреждения цифровой преступности.
2. Назовите основные направления международного сотрудничества государств в сфере предупреждения цифровой преступности.
3. Что является основой международного сотрудничества в сфере предупреждения цифровой преступности?
4. Назовите правовые основы международного сотрудничества в сфере предупреждения цифровой преступности.

Глава 2. Международные органы и организации в предупреждении преступной деятельности с использованием криптовалюты

В международном сотрудничестве в сфере противодействия преступности так или иначе участвуют все главные и вспомогательные органы, а также ряд специализированных[1] и неспециализированных[2] органов и организаций ООН. Все они активно включились в работу по противодействию новым вызовам преступности.

В настоящее время анонимность проводимых криптовалютных платежей вызывает озабоченность мирового сообщества. Финансовые, налоговые, судебные, правоохранительные и иные государственные органы, а также негосударственные или общественные организации не могут повлиять на транзакции участников названной платежной системы (отменить, заблокировать, оспорить или принудительно их совершить без доступа к приватному ключу владельца). Это вызывает проблемы у правоприменителей, связанные с идентификацией лиц, причастных к противоправной деятельности. В связи с этим Международный валютный фонд (МВФ), несмотря на то, что предусматривается применение в современной экономике криптовалюты как финансового актива и ее внедрение центральными банками в национальную экономику наравне с национальной и иностранной валютами, обратился к международному сообществу и призвал к глобальной координации регулирования криптовалют,

---

[1] Генеральная Ассамблея, Совет Безопасности, Секретариат, Экономический и Социальный Совет, Управление ООН по наркотикам и преступности, Комиссия по предупреждению преступности и уголовному правосудию, Международный суд, Комиссия ООН по правам человека, Комитет по ликвидации расовой дискриминации, Комитет по ликвидации дискриминации в отношении женщин, Комитет против пыток, Комитет по защите прав всех трудящихся и членов их семей, и др., а также структурные органы, созданные при Совете Безопасности ООН: Комитет по санкциям против «Аль-Каиды» и «Талибана», Контртеррористический комитет (КТК), Комитет 1540, и др.

[2] Международная морская организация (ИМО), Международное агентство по атомной энергии (МАГАТЭ), Международная организация труда (МОТ), Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), Международная организация гражданской авиации (ИКАО), Дирекция по международному сотрудничеству (ДМС), Международное общество социальной защиты (МОСЗ), а также неправительственные организации, имеющие консультативный статус при ООН: Международная ассоциация уголовного права, Международное криминологическое общество, Международное общество социальной защиты, Международный уголовный и пенитенциарный фонд, а также Международная организация по миграции (МОМ), Международная федерация обществ Красного креста и Красного полумесяца, Международная амнистия, Международная социологическая ассоциация и др.

поскольку рост цен, их волантильность рассматриваются организацией как серьезные риски для инвесторов. По этой причине, считают представители МВФ, нельзя легкомысленно относиться к вопросам правового регулирования криптовалют, т. к. масштабные изменения, которые будут происходить в финансовых системах всех государств, могут быть ощутимы. Поэтому необходимо международное регулирование и соответствующий надзор за оборотом криптовалют. При этом подчеркивается, что криптовалюты могут использоваться для легализации (отмывания) преступных доходов, финансирования терроризма, уклонения от налогов и мошенничества[1].

Более того, по инициативе МВФ, совместно со Всемирным банком, создана учебная монета или «квазикриптовалюта» на собственном блокчейне с ограниченным доступом в учебных целях. Поскольку технология распределительного реестра (блокчейн) стремительно совершенствуется, а с ней развиваются и различные виды криптовалют, необходимо изучение информации о них, механизме их применения, способах использования в преступных целях[2]. Основная цель применения «квазикриптовалюты» – оценка того уровня финансовой безопасности для частных лиц, который они могут предоставить, с одной стороны, а с другой, определение возможности гипотетической расплаты ею за товары и услуги. При этом будет уделено внимание сделкам, которые осуществляют физические лица ежедневно в незначительном объеме[3].

В июле 2019 г. МВФ опубликовал на официальном сайте отчет о результатах исследования криптовалют и признал важность их развития, и подтвердил мнение руководителя самого крупного по активным балансовым операциям банка США – *"JP Morgan"* – Джейми Даймона о том, что «криптовалюты уже являются конкурентами банков, а кредитные организации делают шаги, чтобы не отставать в этом рыночном соревновании за клиентов финансовых услуг»[4]. Вместе с тем предлагается упрочить свои позиции

---

[1] Глава МВФ: регулирование операций с криптовалютами неизбежно. URL: https://incrussia.ru/news/glava-mvf-regulirovanie-operatsij-s-kriptovalyutami-neizbezhno (дата обращения: 20.06.20).

[2] МВФ и Всемирный банк выпустили собственную криптовалюту. URL: https://ru.ihodl.com/topnews/2019-04-15/mvf-i-vsemirnyj-bank-vypustili-sobstvennuyu-kriptovalyutu (дата обращения: 22.02.2020).

[3] МВФ и Всемирный банк обучат сотрудников работе с криптовалютами через Learning Coin. URL: https://decenter.org/ru/mvf-i-vsemirnyi-bank-learning-coin (дата обращения: 20.06.2020).

[4] МВФ признает факт важности криптовалюты в мировой финансовой системе. URL: https://mining-cryptocurrency.ru/mvf-kriptovalyuty-v-mirovoj-finansovoj-sisteme (дата обращения: 20.06.2020).

и в глобальном финансовом мире центральные банки должны активно сами выступать эмитентами криптовалют, но МВФ высказывает предостережение об инвестициях в цифровые активы, т. к. это связано с большими финансовыми рисками.

Помимо создания законодательной базы, международные организации готовы взять на себя ответственность по подготовке методических рекомендаций и проведения исследований в этой области. Так, Европейский центральный банк стал одним из первых, кто подготовил и опубликовал доклад о криптовалютах, в котором дал их понятие и определил схемы их использования[1]. В течение нескольких лет он предупреждал об опасности криптовалют, и в 2015 г., после взлома *Mt.Gox,* который привел к потере более 350 млн долл. в биткоинах, Европейский центробанк подготовил очередной отчет, в котором изложил свою позицию относительно криптовалюты, и в т. ч. сделал вывод о том, что криптовалюта как «виртуальная валюта — это цифровое представление стоимости, не выпущенное центральным банком или кредитным учреждением, которое в некоторых случаях может использоваться в качестве альтернативы деньгам»[2] и может выполнять функцию средства обмена или единицы учета, но не средства сбережения.

Позже принимаются решения о внесении изменения в законодательства в сфере противодействия терроризму и экстремизму, а также их финансированию, легализации (отмыванию) преступных доходов и пр.

Европейский Союз (далее – ЕС) проводит активную работу в сфере противодействия преступности. С 1995 г. начинают действовать специализированные организации, такие как: Европейская полицейская организация, Европейская организация правосудия, Европейское бюро по борьбе с мошенничеством, Европейская сеть по предупреждению преступности и др., – они составляют организационную основу в области противодействия преступности, которое постепенно превратилось в одно из приоритетных направлений деятельности ЕС и достигается посредством:

1) сотрудничества полицейских сил, таможенных и других компетентных органов государств-членов как непосредственно, так и в рамках Европола;

2) сотрудничества между судебными и другими компетентными органами государств-членов;

---

[1] Регулирование криптовалют в Евросоюзе. URL: https://crypto-fox.ru/faq/regulirovanie-kriptovalyut-v-evrosoyuze (дата обращения: 20.06.2020).

[2] *Там же.*

3) сближения норм уголовного законодательства государств-членов ЕС.

Каждое из созданных подразделений ЕС принимает активное участие в противодействии преступности, в т. ч. и с использованием криптовалют. На международном уровне также активно обсуждаются проблемы, связанные с использованием системы распределенного реестра (блокчейна) и выделяются следующие основные направления:

– законное определение применения и использования блокчейн-систем. В настоящее время для более детального урегулирования 22 государства ЕС подписали Декларацию о создании Европейского партнерства в сфере блокчейн-технологий в целях развития блокчейн-инфраструктуры[1];

– законодательное и нормативное регулирование криптовалют;

– законное определение применения и использования смарт-контрактов[2]. Так, в ряде стран урегулированы отношения, связанные с заключением смарт-контрактов (США, Великобритания)[3], где они признаются программой, которая активируется происходящими событиями и действует в распределенном децентрализованном многопользовательском воспроизводимом реестре, может управлять и передавать в нем активы[4]. ЕС принял Директиву (ЕС) 2018/843 Европейского парламента и Совета об изменении ряда Директив[5], дополнив их рекомендациями о требовании от электронных платформ, обеспечивающих трансфер криптовалют и провайдеров электронных кошельков, принимать исчерпывающие меры по идентификации своих клиентов[6].

---

[1] Декларация о сотрудничестве в рамках европейского партнерства в сфере блокчейн-технологий: принята в г. Брюсселе 10 апреля 2018 г. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=57270#03891223908118764 (дата обращения: 02.12.2019).

[2] *Болотаева О.С.* Основные направления правового регулирования систем распределенного реестра в условиях формирования цифровой экономики // Серия «Вестник СВФУ». 2017. № 4 (08). С. 68–75.

[3] В Российской Федерации смарт-контракт получил законодательное определение в ГК РФ. См.: О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: федер. закон от 18 марта 2019 г. № 34-ФЗ. URL: http://www.consultant.ru/news/2 (дата обращения: 15.07.2019).

[4] *Лукоянов Н.В.* Правовые аспекты заключения, изменения и прекращения смарт-контрактов // Юридические исследования. 2018. № 11. С. 28–35. См.: XIII Программа правовой реформы (Thirteenth Program of Law Reform. Law Com №. 377).

[5] Директивы ЕС 2015/849 и 2009/138/ЕС, и 2013/36/ЕС13 о предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма // СПС «Консультант Плюс».

[6] *Ализаде В.А.* Оборот криптовалюты в Европейском союзе: на пороге правового регулирования // Библиотека криминалиста. Научный журнал. 2018. № 2 (37). С. 316–327.

Наряду с конвенционными механизмами в Совете Европы созданы специализированные структуры[1], в функции которых входит предотвращение и устранение отдельных видов преступлений. Так, например, «Группа Помпиду» принимала непосредственное участие в разработке международно-правовых документов, в т. ч. Европейской конвенции об отмывании, выявлении, изъятии и конфискации доходов, добытых преступным путем (1990 г.). В 1999 г. Россия присоединилась к данному соглашению и реализует в рамках деятельности «Группы Помпиду» около 300 программ, проектов и мероприятий[2].

В мае 2001 г. Совет Европейского союза основал Европейскую сеть по предупреждению преступности (EUCPN)[3], задачами которой являются изучение практики в области предупреждения преступности, оценка и распространение информации, собранной в странах-членах; содействие сотрудничеству и содействие в установлении новых контактов между странами в Сети; участие в разработке местных и международных стратегий предупреждения преступности. Одними из основных задач Сети являются: организация ежегодной конференции по передовым методам предупреждения преступности; организация ежегодного конкурса Европейской премии по предупреждению преступности (ECPA) на лучший европейский проект по предупреждению преступности[4].

В 2002 г. ЕС Рамочным решением 2002/584/ЛНА вводит Европейский ордер на арест, который выдается на основании судебного решения государством-участником в целях задержания и передачи другому государству-члену ЕС разыскиваемого лица для осуществления уголовного преследования либо для исполнения наказания или меры безопасности, связанных с лишением свободы (ст. 1

---

[1] Многопрофильная координационная структура «Группа Помпиду», Европейская Комиссия, Европейский центр контроля по исследованию наркотических средств и проблем наркомании (ЕВРОПОЛ); специализированные учреждения ООН (Управление по контролю над наркотиками и предотвращением преступности, Международный комитет по контролю над наркотиками, Всемирная организация здравоохранения, Международная организация труда (ЮНЕСКО), а также специализированные международные организации (ИНТЕРПОЛ, Всемирная таможенная организация) и международные неправительственные организации.

[2] *Кузнецов И.* Сотрудничество государств в борьбе с наркоманией в рамках Совета Европы. URL: http://www.observer.materik.ru/observer/N10_2007/044_052.pdf (дата обращения: 02.05.2020).

[3] Council Decision 2009/902/JHA of 30 November 2009 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA. URL: http://eur-lex.europa.eu (дата обращения: 02.05.2020).

[4] The European Crime Prevention Network (EUCPN). URL: http://www.rikoksentorjunta.fi (дата обращения: 12.06.2020).

Рамочного решения[1]). Целью Европейского ордера выступает упрощение механизма выдачи лиц, совершивших особо тяжкие преступления на территории государств-членов ЕС.

Необходимо также отметить, что в связи с транснационализацией преступности в сфере цифровых технологий, Советом Европы были приняты: Конвенция о преступности в сфере компьютерной информации[2], соответствующая Резолюция[3] и Декларация, направленные на построение безопасного информационного общества[4].

Из перечисленных выше международно-правовых документов в первом определяется уголовно-правовая политика мирового сообщества, нацеленная на защиту общества от преступлений в сфере цифровых технологий, путем подготовки нормативно-правовых актов и укрепления сотрудничества международного сообщества в указанной сфере. В данном документе участникам мирового сообщества рекомендовано предпринимать необходимые организационно-правовые мероприятия, направленные на борьбу с цифровыми преступлениями и предусмотреть в своем законодательстве конкретные составы преступлений в сфере цифровых технологий.

Российская Федерация указанный международно-правовой документ не подписала, т. к. в нем имеются положения, способные подорвать суверенитет и безопасность нашей страны. Так, в частности, правоохранительные органы государств-участников, в необходимых случаях, не получая разрешения другого государства-участника, имеют право получать доступ к хранящимся на его территории конфиденциальным киберданным[5].

---

[1] Рамочное решение Совета от 13 июня 2002 г. «О европейском ордере на арест и процедурах передачи лиц между государствами-членами» (2002/584/JAI). URL: http://eulaw.edu.ru/documents/legislation/law_defence/euro_order.htm#_ftnref1 (дата обращения: 12.06.2020).

[2] Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 (с изм. от 28 января 2003 г.). // СПС «КонсультантПлюс» (дата обращения: 18.11.2019).

[3] Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 января 1999 г. URL: https://www.ifap.ru/ofdocs/un/5753.pdf (дата обращения: 20.11.2019).

[4] Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», Женева, 2003. URL: https://online.zakon.kz/Document/?doc_id=30170561#pos=7;129 (дата обращения: 20.11.2019).

[5] О признании утратившим силу распоряжения Президента РФ от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»: распоряжение Президента РФ от 22 марта 2008 г. № 144-рп. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=417185#05091896676102123 (дата обращения: 18.11.2019).

В 2017 г. Европарламент принял резолюцию[1] для Еврокомиссии, предложив признать официальный статус машин с искусственным интеллектом, принимающих самостоятельные решения, с возможностью возложения на них ответственности за причиненный ущерб.

Законотворческие инициативы как в США, так и в ЕС пока не имеют на практике четкой методологической основы и представляют собой скорее «сборник предложений» по регламентации без формулирования принципов выбора средств правовой защиты[2].

В январе 2020 г. вступила в силу пятая директива ЕС по борьбе с легализацией (отмыванием) преступных доходов, которая ужесточила требования к транзакциям, проводимым с использованием криптовалюты через криптобиржи или цифровые платформы. Криптовалютные платформы теперь обязаны проводить аудит клиента *(customer due diligence, CDD)* и предоставлять:

а) информацию о подозрительных транзакциях *(suspicious activity reports, SAR);*

б) финансовую информацию, адреса владельцев криптокошельков с целью их идентификации;

в) криптовалютные биржи, провайдеры криптокошельков и поставщики услуг по хранению данных обязаны зарегистрироваться у местного регулятора, представлять отчеты о подозрительной деятельности и выполнять правовой аудит клиента.

Эти меры позволят в будущем повысить доверие к криптовалютному рынку со стороны традиционных финансовых институтов и привлечь институциональных инвесторов к стремительно развивающемуся рынку, а также снизить уровень преступности и анонимности криптодержателей.

И несмотря на то, что правовой статус криптовалюты не определен, она как разновидность виртуальной цифровой валюты приобрела высокую популярность и в ряде таких стран мира, как Великобритания, Япония, Швейцария, Швеция, Германия и др., *«стала не только полноценным платежным средством, но и выступает инвестиционным активом»*[3].

---

[1] Резолюция Европарламента от 16 февраля 2017 г. 2015/2013(INL) P8_TA-PROV(2017)0051, включает текст Хартии робототехники. URL: http://robopravo.ru/riezoliutsiia_ies (дата обращения: 28.11.2019).

[2] *Филипова И.А.* Правовое регулирование искусственного интеллекта: регулирование в России, иностранные исследования и практика // Государство и право. 2018. № 9. С. 79–88.

[3] *Пинкевич Т. В., Нестеренко А. В.* Проблемы обеспечения безопасности цифровых технологий в Российской Федерации // Вестник Костромского государственного университета. 2019. Т. 25. № 4. С. 163.

Кроме того, в мае 2018 г. группа регуляторов ценных бумаг Канады и США объявила о запуске программы «международного преследования» криптовалютных мошенников, ее целью является международное противодействие мошенникам в индустрии криптовалют. Данная программа получила одобрение Комиссии по ценным бумагам и биржам.

3 июля 2018 г. ознаменовалось тем, что было объявлено о создании альянса пяти стран – *Joint Chiefs of Global Tax Enforcement (J5)* – Международный альянс J5 по борьбе с серьезными международными преступлениями. Его особенность заключается в том, что это оперативное сотрудничество между пятью странами (Австралия, Канада, Нидерланды, Великобритания и США), состоит в организации деятельности, направленной на борьбу с транснациональными финансовыми преступлениями, в т. ч. с использованием виртуальных валют (криптовалют). В рамках альянса J5 предполагается «партнерство между Австралийской комиссией по уголовным расследованиям (ACIC) и Налоговой службой Австралии (ATO), Канадским налоговым агентством (CRA), Fiscale Inlichtingen-Opsporingsdienst (FIOD) в Нидерландах, Королевской налоговой и таможенной службой Великобритании (HMRC) и Налоговой службой США (IRS)»[1]. Целью создания Международного альянса J5 является:

– укрепление правопорядка путем обмена информацией и ресурсами;

– развитие международного сотрудничества по борьбе с легализацией (отмыванием) преступных доходов и финансовыми преступлениями, а также преступлениями, совершаемыми с использованием криптовалют;

– повышение эффективности работы организации по экономическому сотрудничеству и развитию с применением новых подходов и проведение совместных расследований;

– совместная разработка и выработка новых подходов к расследованию преступлений и подготовке совместных операций;

– обнаружение и устранение международных преступных схем и инструментов, способствующих совершению преступлений, совершаемых с использованием криптовалют;

– повышение уровня обмена информацией, пилотными программами;

[1] Пять стран начинают совместную борьбу с финансовыми преступлениями с участием криптовалют. URL: https://bits.media/pyat-stran-nachinayut-sovmestnuyu-borbu-s-finansovymi-prestupleniyami-s-uchastiem-kriptovalyut (дата обращения: 25.02.2020).

– совместные криминальные расследования[1].

Директор Канадского налогового агентства Йоханн Шарбоно (Johanne Charbonneau) относительно вышеперечисленных целей отметил: «Наши коллективные усилия и опыт будут использоваться для совместной идентификации и раскрытия все более сложных и глобальных схем и механизмов, которые облегчают осуществление финансового мошенничества»[2].

Государства-члены G20 также заявляли о необходимости международной дискуссии о новой цифровой индустрии.

Краткий анализ деятельности в сфере предупреждения преступности с использованием криптовалюты международных органов и организаций позволил прийти к выводу о том, что в этом направлении существуют проблемы правового характера, поскольку еще нет сложившегося понимания сущности цифровых технологий и криптовалют, отсутствуют методические рекомендации по расследованию этих преступлений, нет законодательного определения криптовалют на региональном уровне.

Большую роль в предупреждении преступной деятельности с использованием криптовалюты играют и такие организации, как Интерпол, Европол и ФАТФ, цели, задачи и функции которых в противодействии преступности с использованием криптовалюты будут рассмотрены в последующих материалах данного учебно-практического пособия.

Контрольные вопросы

1. Назовите международные органы, участвующие в предупреждении преступной деятельности с использованием криптовалюты.
2. Определите роль Международного валютного фонда в предупреждении преступной деятельности с использованием криптовалюты.
3. Дайте характеристику пятой директивы ЕС по борьбе с отмыванием денег (2020г.).
4. Назовите цели создания Международного альянса J5.

---

[1] Международный альянс J5 будет бороться с «криптовалютной угрозой» в сфере отмывания денег и уклонения от налогов. URL: https://news.myseldon.com/ru/news/index/191224059; США возглавили международный альянс силовиков по борьбе с отмыванием денег https://hashtelegraph.com/ssha-vozglavili-mezhdunarodnyj-aljans-cilovikov-po-borbe-s-otmyvaniem-deneg (дата обращения: 25.02.2020).

[2] Пять стран начинают совместную борьбу с финансовыми преступлениями с участием криптовалют. URL: https://bits.media/pyat-stran-nachinayut-sovmestnuyu-borbu-s-finansovymi-prestupleniyami-s-uchastiem-kriptovalyut (дата обращения: 25.02.2020).

Глава 3. Роль международных организаций уголовной юстиции (Интерпола) и Европейской полицейской организации (Европола) в предупреждении преступной деятельности с использованием криптовалюты

Особое место в деятельности по противодействию преступлениям, совершаемым с использованием криптовалюты занимает международная комиссия уголовной полиции, созданная в Вене в 1923 г. (с 1956 г. – межправительственная организация Интерпол)[1]. Она играет координирующую роль в противодействии преступности и в настоящее время объединяет более 190 государств (включая Россию). В настоящее время Интерпол является международным специализированным и информационным центром, который осуществляет борьбу с преступностью. С этой целью он стремится поддерживать контакты с национальными и международными органами; готовит обзоры и рекомендации для правоприменительной практики, в т. ч. по расследованию преступлений; активно участвует в разработке проектов международных договоров о борьбе с отдельными видами преступлений; оказывает помощь по пресечению готовящихся или совершенных преступлений; развивает международное сотрудничество, вносит существенный вклад в укрепление международного правопорядка[2], сотрудничает с ООН и другими международными организациями в области противодействия преступности.

Высшим органом Интерпола является Генеральная ассамблея, сессии которой проходят ежегодно. Интерпол как международная организация в странах-участницах имеет свои структурные подразделения (филиалы) – национальные центральные бюро (НЦБ). В их функции входит обмен информацией между правоохранительными и иными государственными органами, осуществляющими борьбу с преступностью, правоохранительными органами иностранных государств-членов Интерпола и Генеральным секретариатом Интерпола[3].

---

[1] Устав Международной организации уголовной полиции (ИНТЕРПОЛ) (вступил в силу 13 июня 1956 г., с изменениями по состоянию на 1 января 1986 г.) // Национальное центральное бюро Интерпола в Российской Федерации. Москва, 1994. С. 17–30.

[2] Site of the Council of Europe. URL: https://search.coe.int (дата обращение: 05.01.2020).

[3] Структурные подразделения (филиалы) НЦБ Интерпола действуют, в т. ч., и в субъектах Российской Федерации.

Он осуществляет информационное обеспечение международного розыска, в рамках которого использует международные извещения (циркуляры, уведомления) Интерпола. Особая роль в его деятельности отведена подготовке Специальных извещений (INTERPOL United Nations Special Notices)[1]. В данном случае речь идет о принятии международным сообществом мер по противодействию террористической угрозе со стороны «Аль-Каиды» и «Талибана», а также их сообщников.

Также Интерполом проводится работа по сбору и обработке информации о преступлениях, способах их совершения, особенностях раскрытия и расследования, а также о лицах их совершивших. Информация всех стран-участниц Интерпола поступает в Интерпол и используется для формирования и ведения криминалистических учетов[2].

Большое значение в деятельности Интерпола отведено и информационному обеспечению международного сотрудничества в противодействии отдельным видам преступлений, в их числе: легализация (отмывание) преступных доходов, финансирование терроризма, организованная преступная деятельность, преступления, посягающие на экономические и социальные основы жизнедеятельности общества, в т. ч. в финансовой сфере, и другие, совершаемые с использованием криптовалюты. Для установления местонахождения лиц, участвующих в преступной деятельности, Интерполом используется разработанная Генеральным секретариатом специальная система международного обмена информацией. Его роль в координации этой деятельности значительно возросла, поскольку Интерпол, обладая уникальными инструментами и механизмами, методами и практикой противодействия терроризму во всех его формах и проявлениях, (киберпреступности и др.), способствует организации содействия государствам-членам, международным организациям, проводит значительную работу по распространению опыта противодействия с этим явлением.

Принятые документы конвенционного характера свидетельствуют о том, что роль Интерпола в противодействии преступлениям международного характера, имеющим транснациональный

---

[1] См. Резолюцию Совета Безопасности ООН, принятую Советом Безопасности на его 5244-м заседании 29 июля 2005 г. URL: https://undocs.org/ru/S/RES/1617(2005) (дата обращения: 02.06.2020).

[2] Современные криминалистические учеты – это информационные системы сведений об объектах, представляющих для правоохранительных органов особый интерес. Такие сведения являются эффективным средством, используемым при раскрытии и расследовании преступлений, розыске и задержания лиц, совершивших их.

характер, высока. Эта организация поддерживает контакты со всеми международными органами и организациями, с которыми необходимо взаимодействовать в связи с противодействием преступности.

Интерпол предпринимает значительные усилия для противодействия преступности в киберпространстве, применяя новые методы и способы работы, поскольку преступники используют в настоящее время самые новые цифровые технологии, стойкую криптографию, позволяющую им уйти от уголовной ответственности. Осложняется работа еще и тем, что зачастую они используют теневой бизнес, в т. ч. используют такие цифровые площадки, как Даркнет, TOP, Гидра и др. Поэтому Интерпол объявил об ужесточении деятельности по противодействию преступности с противоправным использованием криптовалюты в Даркнете, поскольку она является площадкой для хакеров всех типов, мошенников и лиц, осуществляющих незаконный оборот оружия, наркотиков и т. п. В этом сегменте Всемирной паутины даже продавались персональные данные пользователей криптовалютных бирж[1]. В ходе работы по пресечению преступной деятельности в названной сфере им было заключено партнерское соглашение с южнокорейским стартапом S2W Lab, что позволило, с использованием разработанной ими системы мониторинга активности пользователей Даркнета (которая дает возможность анализировать данные и может выявлять источники подозрительных транзакций, в т. ч. с криптовалютами), расширить информацию о преступной деятельности для ее пресечения в так называемом «теневом интернете».

В апреле 2015 г. представители Интерпола объявили о разработке криптовалюты в образовательных целях, что позволило изучить методы, тактику и процедуры криминального использования криптовалют. Проведение таких исследований и создание учебной криптовалюты, по мнению Мадана Мохан Оберой, директора по кибер-инновациям и аутрич-работе в Глобальном комплексе инноваций Интерпола *(IGCI)* в Сингапуре, необходимо для повышения эффективности противодействия преступной деятельности с использованием криптовалюты[2].

Особенность таких разработок, исследование и выявление новых киберугроз, как утверждает исполнительный директор

---

[1] Интерпол усилит борьбу с криминальным использованием криптовалюты в дарквебе. URL: https://novator.io/blokchejn/interpol-usilit-borbu-s-kriminalnym-ispolzovaniem-kriptovalyuty-v-darkvebe (дата обращения: 02.06.2020).

[2] Интерпол создает собственную криптовалюту. URL: https://ru.secnews.gr/92170/Интерпол-создает-собственную-криптовалюту (дата обращения: 02.06.2020).

IGCI Нобору Накатани, являются одними из ключевых целей создания Глобального комплекса инноваций Интерпола, достижение которых позволит этой организации распространять полученные результаты среди общественности и правоохранительных органов, а также взаимодействовать в области кибербезопасности для поиска новых решений в борьбе с этими видами преступлений[1].

Большое значение Интерпол уделяет подготовке сотрудников к работе в новых цифровых условиях. С этой целью организуются тренинги по обучению сотрудников Интерпола, непосредственно участвующих в розыске преступности и отслеживающих незаконное использование криптовалюты. Так, например, в 2015 г. подразделение *Interpol Global Complex for Innovation (IGCI)* организовало пятидневный тренинг. В ходе обучения сотрудников была эмитирована учебная криптовалюта и запущен тренировочный магазин наркотиков по образцу *Silk Road*. Задачей тренинга являлось обнаружение места размещения подпольного магазина и блокировка его работы, что позволило агентам одновременно разобраться в организации технической инфраструктуры сети *Tor,* изучить инструменты, необходимые для работы[2].

Глава Интерпола, Мэн Хунвэй, выступая на международном конгрессе заявил, что Интерпол разработал стратегию борьбы с киберпреступлениями, однако имеющиеся методы борьбы с ними пока не дают должного эффекта, поскольку виртуальный мир преступлений имеет трансграничный и стремительно нарастающий характер, что не позволяет своевременно отреагировать на возникающие киберугрозы. Это дает возможность добытым преступным путем средствам быть легализованными в течение нескольких часов[3].

По его мнению, в противодействии преступности в сфере цифровой экономики важным является, во-первых, создание электронной платформы для предотвращения киберпреступлений, в котором должны принять участие самые вероятные жертвы хакерских атак – национальные банки, и, во-вторых, сотрудничество и взаимодействие со специалистами IT-технологий, провайдерами соответствующих услуг, и все те компании, которые связаны с цифровой

---

[1] *Там же.*

[2] Интерпол создал учебную криптовалюту и магазин наркотиков для тренировки агентов. URL: https://xakep.ru/2015/09/04/interpol-crypto (дата обращения: 02.06.2020).

[3] *Давыдов Д.* Интерпол придумал, как бороться с киберпреступностью. URL: https://teknoblog.ru/2018/07/06/90797 (дата обращения: 02.06.2020).

экономикой. Это позволит полицейским ведомствам каждой страны укрепить связи со своими коллегами[1].

В этих целях открываются учебные заведения, такие как: Антинаркотический тренировочный Центр, Глобальный учебный центр и Антикоррупционная Академия Интерпола.

Еще одним полицейским ведомством, но на европейским уровне является Европол, который был образован в 1995 г., а в полном объеме начал функционировать с 1 июля 1999 г.[2] Его целью является:

– развитие и координация деятельности между компетентными органами государств в сфере противодействия преступности;

– повышение эффективности сотрудничества компетентных органов государств-членов в предотвращении транснациональной организованной преступности;

– противодействие международному терроризму;

– противодействие иным «тяжким форм преступности» международного характера (всего 24 категории преступных деяний).

В рамках своей деятельности Европол осуществляет обмен информацией, которую предварительно систематизирует и изучает, – для конкретных операций, в которых порой участвует сам, готовит оперативный анализ. Проводит большую работу по получению от государств-членов ЕС и других государств информации о совершенных преступлениях, изучает, обобщает практики и на основе этих данных готовит обобщения и методические рекомендации по противодействию преступности. Более того, ежегодно Европол представляет стратегические доклады; оказывает экспертную и техническую поддержку в проведении расследований и операций на территории ЕС под надзором и ответственностью государств-членов[3].

В 1993 г. в России, по решению Совета глав правительств стран СНГ, создано Бюро по координации борьбы с отдельными видами преступлений и организованной преступностью, которое взаимодействует с Европолом и Интерполом. Информационные данные этого банка используются в т. ч. и правоохранительными органами государств-участников СНГ[4]. В рамках СНГ осуществляются

---

[1] Там же.

[2] О создании Европейского полицейского ведомства (Европол): решение ЕС от 6 апреля 2009 г. № 2009/371/ПВД. URL: http://docs.pravo.ru/document/view/24869591 (дата обращения: 22.05.2020).

[3] *Там же.*

[4] Общая информация (сотрудничество в сфере борьбы с преступностью и незаконным оборотом наркотических средств в СНГ). URL: http://www.cis.minsk.by/page.php?id=18780 (дата обращения: 22.05.2020).

совместные оперативно-профилактические мероприятия и специальные операции по розыску преступников, противодействию незаконному обороту наркотиков, оружия, боеприпасов, взрывчатых веществ, нелегальной миграции, по пресечению контрабанды сырьевых ресурсов и культурных ценностей, деятельности международных преступных группировок на транспорте и т. д.

В 2003 г. между РФ и Европолом подписано Соглашение о сотрудничестве[1], и в 2004 г. приказом МВД России в структуре Национального центрального бюро Интерпола при МВД России создан Российский национальный контактный пункт по взаимодействию с Европолом (РНКП), целью которого является обмен информацией между компетентными органами (МВД, ФСБ, ФТС, Росфинмониторинг) и Европолом, выработка мер, направленных на усовершенствование механизма этого сотрудничества[2].

Начиная с 2014 г., ежегодно Европол представляет доклад «Оценка угрозы со стороны организованной интернет-преступности», который пополняется новой информацией о киберпреступности. При этом доклад содержит не только информацию об использовании криптовалют организованной преступностью, но рассматриваются ее инструменты для обеспечения преступности «глубокого» интернета, в т. ч. и сексуальной эксплуатации детей, анонимность услуг которых обеспечивается такими цифровыми платформами, как *Tor*. Это свидетельствует о том, что правоохранительные органы не всегда могут отследить крупные сделки, совершаемые с использованием криптовалют, поскольку транзакции обеспечены высокой анонимностью, что способствует росту таких преступлений.

Так, например, в аналитическом докладе 2015 г. было уделено внимание деятельности нелегальных крипторынков, годовой оборот которых превышал более чем 20 млн долл. Сделан вывод, что правонарушители в своей преступной деятельности пользуются цифровыми площадками, биржи которых не зарегистрированы или имеют слабую систему идентификации пользователей, а также используют онлайн-гэмблинг либо специальные сервисы, позволяющие пользователям легализовать криптовалюту, добытую преступным путем за сравнительно небольшую плату.

---

[1] Соглашение о сотрудничестве между Российской Федерацией и Европейской полицейской организацией (заключено в г. Риме 6 ноября 2003 г.) // СПС «КонсультантПлюс».

[2] *Быкова Е.В.* Проблемы и перспективы сотрудничества Российской Федерации с международными организациями в сфере уголовного судопроизводства // Международное уголовное право и международная юстиция. 2016. № 5. С. 3–6.

При этом авторы доклада приходят к выводу о необходимости принятия закона на уровне Евросоюза об адекватных мерах регулирования криптовалюты, определения отношений между операторами цифровых валют, правоохранительными органами и банковской системой[1].

В ходе анализа современного состояния преступности Европол пришел к выводу о том, что существует реальная угроза массового незаконного использования криптовалют в преступных целях, что требует особого подхода и особых знаний в выявлении использования криптовалют в преступных целях. Так, например, криптовалюта в последнее время стала особенно популярной среди торговцев людьми. В частности, преступникам помогает анонимность, которая обеспечивается криптовалютой, что значительно усложняет процесс отслеживания транзакций и поиска подозреваемых.

Однако в большинстве случаев противоправное использование криптовалют связывают преимущественно с легализацией (отмыванием) преступных доходов, что послужило основанием создания в 2016 г. по инициативе Европейской комиссии на базе Европола специальной рабочей группы, которая непосредственно занимается борьбой с легализацией (отмыванием) преступных доходов с использованием криптовалют. В новую структуру вошли представители Интерпола и Базельского института управления *(Basel Institute on Governance)*. Задачами данной группы является сбор, анализ и обмен неоперативной информацией относительно использования цифровых валют в качестве инструмента легализации (отмывания) преступных доходов, а также следственные действия и изъятие криминальных доходов, хранящихся в цифровой форме. В обязанности этой группы также входит организация и проведение ежегодных семинаров для представителей правоохранительных структур, а также создание сети экспертов и практических специалистов в области криптовалют[2].

Подтверждением необходимости создания данной группы является рост преступной деятельности с использованием криптовалюты. Примером может служить схема незаконного оборота наркотиков, которая была раскрыта Европолом в 2018 г.: действуя через финскую биржу, по этой схеме было легализовано более 8 млн евро

---

[1] Европол анализирует Bitcoin-преступления в новом докладе. URL: https://bits.media/evropol-analiziruet-bitcoin-prestupleniya-v-novom-doklade (дата обращения: 22.05.2020).

[2] Асмаков А. Европол и Интерпол объединили усилия в борьбе с отмыванием денег через криптовалюты. URL: https://forklog.com/evropol-i-interpol-obedinili-usiliya-v-borbe-s-otmyvaniem-deneg-cherez-kriptovalyuty (дата обращения: 22.05.2020).

путем приобретения криптовалюты. Согласно сообщению, опубликованному 8 апреля 2018 г., представители Европола арестовали 11 человек за легализацию (отмывание) преступных доходов из Испании в Колумбию при помощи криптовалюты и кредитных карт. Правоохранительные органы Испании, Финляндии и США общими усилиями осуществили арест подозреваемых. Согласно заявлению, была расследована деятельность 137 чел., а подозреваемые использовали в общей сложности 174 банковских счета.

Европол поддерживал расследование с 2018 г. и содействовал обмену информацией между участвующими странами. Оперативная целевая группа этой организации взаимодействовала со следователями из Бельгии, Франции и Израиля, оказывая аналитическую и техническую поддержку и направляя экспертов на место для перекрестной проверки оперативной информации с базами данных Европола и, таким образом, предоставляя следователям вещественные доказательства[1].

Преступной организации удалось создать сложную систему, обещающую большие прибыли от инвестиций в биткойн, золото и алмазы. Подозреваемые предлагали свои финансовые услуги на онлайн-платформах. Преступная сеть также создавала фиктивные компании в рамках своей схемы легализации (отмывания) преступных доходов.

Кроме того, по сообщению издания Business Insider со ссылкой на Европол, европейский криминалитет в этот же период использовал криптовалюту с целью легализации преступных доходов на сумму $5,5 млрд. Также следует отметить, что в 2017 г. эта сумма составляла от 3 до 4 млрд фунтов стерлингов, которые рассматривались как криминальные, но были легализованы тоже с использованием криптовалюты в Европе.

Вместе с тем увеличилось количество преступлений против собственности, а именно, мошенничества с криптовалютами и их инвестированием. Таким ярким примером стало преступление, расследованное в 2019 г. Французская национальная жандармерия *(Gendarmerie Nationale)* в сотрудничестве с бельгийской федеральной судебной полицией *(Police Judiciaire Fédérale)* и израильской полицией, при поддержке Европола и Евроюста, разоблачили крупную сеть инвестиционных мошенников. Преступная группа занималась легализацией (отмыванием) преступных доходов и мошенничеством

[1] Fake Investors Busted in Belgium and France. URL: https://www.europol.europa.eu/newsroom/news/fake-investors-busted-in-belgium-and-france (дата обращения: 23.05.2020).

с бинарными инвестициями. Пострадало около 90 жителей Бельгии и Франции, а совокупный ущерб составил 6 миллионов евро.

Одним из проектов Европола является консультативная группа *SOCTA (Serious and Organized Crime Threat Assessment),* в состав которой входят государства-члены ЕС, агентства ЕС, Европейская комиссия и Генеральный секретариат Совета. Ее задача заключается в подготовке и одобрении методологии, и определении требований к сбору оперативных данных, их анализу, определению основных криминологических рисков и угроз, составлению отчетов по итогам исследований, а также в подготовке предложений по приоритетным направлениям. Особое внимание *SOCTA* уделяется организованной преступной деятельности. Представители организованной преступности «внедряют и интегрируют новые технологии в свой *modus operandi* или создают совершенно новые бизнес-модели вокруг них. Использование новых технологий организованными преступными группировками (далее – ОПГ) оказывает влияние на преступную деятельность по всему спектру серьезной и организованной преступности. В первую очередь это относится к цифровому криминалу, широко использующему масштабирование онлайн-торговли и повсеместное распространение зашифрованных каналов связи»[1]. Ими активно применяется криптовалюта, поскольку скоростная обработка транзакций и распространение эффективных средств анонимности оказывают большую помощь организованной преступности в легализации (отмывании) преступных доходов.

Европолом в деятельности по противодействию транснациональной организованной преступности активно применяется система раннего обнаружения ОПГ с использованием методов вычислительного сканирования и разведывательных систем – *ePOOLICE*. Благодаря ей создается эффективная общеевропейская система «средового сканирования для предупреждения готовящихся к преступлениям действующих и возникающих ОПГ»[2]. Уже создана «система сплошного мониторинга, включающая сбор информации из интернета, социальных сетей, из каналов части мессенджеров, информации о финансовых транзакциях, биллинговая информации, видеопотоков и т. п.»[3] Информация включает и такие данные как текстовой и видео-контент, финансовые данные и пр., что позво-

[1] *Ларина Е. С., Овчинский В.С.* Искусственный интеллект. Большие данные. Преступность. Москва: Книжный мир, 2018.

[2] *Там же.*

[3] *Там же.*

ляет анализировать полученные данные всесторонне и своевременно реагировать на вызовы транснационального криминала.

В настоящее время особым приоритетом работы Интерпола является противодействие киберпреступности, связанной с атаками на информационные системы, особенно на те, которые следуют бизнес-модели «преступление как услуга» и работают в качестве стимуляторов для онлайн-преступности.

Второе направление – это борьба с сексуальным насилием над детьми и сексуальной эксплуатацией детей, включая производство и распространение материалов о жестоком обращении с детьми.

Третьим направлением деятельности выступает противодействие мошенничеству и подделке безналичных платежных средств, в т. ч. крупномасштабное мошенничество с платежными картами (особенно мошенничество с поддельными банковскими картами), преступления, совершаемые с использованием криптовалюты.

Причина выбора этих направлений определена тем, что преступность в виртуальной среде становится все более агрессивной и конфронтационной. Это можно наблюдать в различных формах киберпреступности, включая цифровые преступления, утечку данных и сексуальное вымогательство. Мишенью для преступников в названной сфере являются не только финансовые данные, но и любые данные, позволяющие их использовать в преступных целях. Число и частота нарушений указанных данных растут, а это, в свою очередь, приводит к увеличению числа случаев мошенничества и вымогательства. Сам диапазон возможностей, которые пытаются использовать киберпреступники, впечатляет. Эти преступления включают в себя:

– использование ботнетов-сетей устройств, зараженных вредоносными программами без ведома их пользователей – для передачи вирусов, которые незаконно получают дистанционное управление устройствами, похищают пароли и отключают антивирусную защиту;

– создание «задних дверей» на скомпрометированных устройствах, позволяющих похищать деньги и данные;

– создание удаленного доступа к устройствам для создания ботнетов;

– создание онлайн-форумов для торговли хакерским опытом;

– пуленепробиваемый хостинг и создание контр-антивирусных сервисов;

– легализация традиционных и виртуальных валют;

– совершение онлайн-мошенничества, например, через платежные онлайн-системы, кардинг и социальную инженерию;

– различные формы сексуальной эксплуатации детей в интернете, включая распространение в интернете материалов о сексуаль-

ном насилии над детьми и прямую трансляцию сексуального насилия над ними;

– интернет-хостинг операций, связанных с продажей оружия, фальшивых паспортов, поддельных и клонированных кредитных карт, наркотиков и хакерских услуг.

Представители ведомства заявили, что Европол «будет продолжать координировать действия между государствами-членами ЕС и за его пределами в стремлении эффективно реагировать на эту растущую угрозу».

С этой целью в средине 2018 г. названная организация подготовила и провела конференцию по борьбе с легализацией (отмыванием) преступных доходов и другими преступлениями, которые совершаются с использованием криптовалюты. Помимо представителей различных служб и ведомств и представителей европейских властей, в конференции приняли участие 16 бирж, компании по обработке платежей и поставщики цифровых кошельков. В ходе конференции обсуждались вопросы, касающиеся возможности отслеживания маршрута криптовалют и методов идентификации участников транзакций, способов скрытия источников фондов, т. н. монетоприемников, некоторых криптопроектов, использование которых осуществляется для обеспечения секретности транзакций.

Одной из целей работы конференции является снижение преступности с использованием криптовалют и улучшение работы правоохранительных органов. Выступая в прениях, Генеральный директор *Bitpanda* Эрик Демут заявил о том, что уже есть обзор всех транзакций, совершенных на платформе, поэтому все, кто пытается заниматься легализацией (отмыванием) денег с помощью биткойна, опоздали на 3 года. В свою очередь Европол продемонстрировал, что он способен бороться с легализацией (отмыванием) преступных доходов и незаконной деятельностью без использования базы данных подозрительных адресов.

Представители Интерпола подтвердили данное направление работы своими кардинальными предложениями, а именно, подразделение Интерпола в Сингапуре, занимающееся расследованием преступлений в сфере высоких технологий *(Interpol Global Complex for Innovation, IGCI),* объявило о планах создания и развития собственной криптовалюты, что позволит оказать помощь своим сотрудникам в определении сущности криптовалюты и способов ее использования в противодействии киберпреступлениям.

Интерпол и Европол проводят и совместные семинары, позволяющие объединить усилия по противодействию преступной деятельности с использованием криптовалюты. Так, в начале 2018 г.

в Базеле и Швейцарии был проведен двухдневный семинар, организованный совместно с Базельским институтом по вопросам управления, в котором приняло участие более чем 60 финансовых следователей. Его целью стало согласование мер по снижению криминальной активности в сфере легализации преступных доходов, финансирования терроризма, незаконного оборота наркотиков с использованием криптовалюты. В результате было принято решение о следующем:

– о повышении качества и объема информации посредством использования таких каналов, как Европол, Интерпол, *Egmont Group и FIU.net* в области легализации преступных доходов, финансирования терроризма, незаконного оборота наркотиков с использованием криптовалюты;

– о регулировании криптобирж и провайдеров криптокошельков в рамках законов о противодействии легализации (отмыванию) преступных доходов и финансированию терроризма;

– о четком определении концепции противодействия названным преступлениям и закреплении таких понятий, как «криптовалюта», «провайдер криптокошелька» и их «шифровальщиков» в правовых рамках ЕС;

– о принятии мер по противодействию обороту цифровых валют, которые делают транзакции анонимными и усложняют работу правоохранительных органов по выявлению и отслеживанию подозрительных транзакций[1].

Итогом проведенного семинара стало официальное заявление Европола о росте использования криптовалют в криминальных целях, в связи с чем необходимо продолжать согласованные действия стран-членов ЕС и за его пределами, чтобы дать эффективный отпор нарастающей угрозе[2].

Уже в 2020 г. Интерпол подготовил и опубликовал доклад о преступности в сфере интеллектуальной собственности, который раскрывает особенности деятельности организованной преступности в этой сфере. Это обусловлено тем, что распространение контрафактных товаров нарушает права граждан, а посягательства на интеллектуальную собственность причиняют вред экономике в целом и компаниям, владельцам интеллектуальной собственности, и могут нанести ущерб здоровью и благополучию потребителей.

---

[1] *Новикова О.* Европол и Интерпол повысят меры по борьбе с отмыванием денег через криптовалюты. URL: https://zen.yandex.ru/media/freedmanclub/evropol-i-interpol-povysiat-mery-po-borbe-s-otmyvaniem-deneg-cherez-kriptovaliuty-5a70fc4b3dceb766bcd8fbc1 (дата обращения: 24.05.2020).

[2] *Там же.*

Тематические исследования, представленные в настоящем докладе, иллюстрируют, как широкий спектр различных преступлений в области интеллектуальной собственности, включая незаконный оборот оружия и наркотиков, экономические и финансовые преступления, а также различные виды мошенничества, легализацию (отмывание) преступных доходов, фармацевтические преступления, производство и распространение контрафактной продукции, принудительный труд, коррупцию с использованием криптовалюты.

Представители криминального мира быстро приспосабливаются к меняющейся ситуации. Так, например, при развитии пандемии COVID-19 они моментально отреагировали на складывающуюся ситуацию и уже на начальном ее периоде с использованием цифровых ресурсов для массового психологического воздействия на население, путем вброса фейковых новостей о надвигающейся эпидемии, расширили свои преступные границы и теневой рынок. На первоначальном этапе они не только способствовали созданию дефицита необходимых для населения товаров первой необходимости в условиях пандемии (маски для лица, одноразовые латексные перчатки антисептические и дезинфицирующие средства и фармацевтические препараты), но и быстрыми темпами наладили реализацию этих товаров по завышенным ценам, чем многократно увеличили свои преступные доходы. Стремительно меняется преступность в сфере распределения и использования бюджетных средств в области финансирования. Чтобы эффективно предотвращать и пресекать совершение названных преступлений, правоохранительные органы должны регулярно отслеживать подозрительные транзакции с целью изъятия преступных доходов.

Рост организованной преступности в сфере экономики и финансов, а также число обращений со стороны государств-членов ЕС с просьбой об оперативной поддержке способствовали созданию в штаб-квартире Европола Европейского центра по борьбе с финансовыми и экономическими преступлениями (EFECC), который будет укомплектован 65 международными экспертами и аналитиками. Центр расширит оперативную поддержку, оказываемую государствам-членам ЕС и органам ЕС в области борьбы с финансовыми и экономическими преступлениями с целью содействия финансовым расследованиям[1].

[1] Он создан по образцу аналогичных инициатив, таких как: Европейский центр по борьбе с киберпреступностью (EC3), Европейский Контртеррористический центр (ECTC), Европейский центр по незаконному ввозу мигрантов (EMSC) и Европейский центр по борьбе с серьезными организованными преступлениями (ESOCC), размещен-

Принятое решение обосновано тем, что экономические и финансовые преступления представляют собой чрезвычайно сложную и значительную угрозу, ежегодно затрагивающую миллионы отдельных граждан ЕС и тысячи компаний в ЕС. Кроме того, легализация (отмывание) преступных доходов и финансовые преступления укрепляют организованную преступность, без них преступники не смогли бы использовать незаконные доходы, которые они генерируют с помощью преступной деятельности, осуществляемой в ЕС. Согласно предыдущим отчетам Европола, 98,9 % предполагаемой преступной прибыли не конфискуется и остается в распоряжении преступников.

Легализация (отмывание) преступных доходов организованной преступностью способствует наращиванию ее финансовых активов, которые путем использования преступных схем «вливаются» в легальную экономику. Возможность проследить движение финансовых активов позволяет раскрыть преступные схемы и сети, а также выявить деятельность мул[1], которые переводят незаконно полученные денежные средства между счетами, часто в разных странах, от имени третьих лиц. По мнению представителей Европола, денежные мулы могут привлекаться к уголовной ответственности, в зависимости от их роли в преступной цепочке, за мошенничество или легализацию (отмывание) преступных доходов.

Расследование, проведенное в 2016 г. при поддержке Европола, Евроюста (Eurojust) и других организаций, показало, что более 90 % операций, проведенных денежными мулами, связаны с киберпреступностью. Незаконно полученные деньги часто поступают от фишинга, вредоносных атак, мошенничества с платежными картами и с онлайн-покупками/электронной коммерцией, и др. Так, в течение недели Европейский центр по борьбе с киберпреступностью Европола *(EC3)* и совместная целевая группа по борьбе с киберпреступностью *(J-CAT),* вместе с Евроюст *(Eurojust)* и Европейской банковской Федерацией *(EBF)* оказывали оперативную и аналитическую поддержку соответствующим органам власти. Эта операция привела к идентификации почти 700 денежных мулов по всей Европе. Полиция допросила 198 подозреваемых и произвела 81 арест.

ный в Европоле. URL: https://www.europol.europa.eu/newsroom/news/europol-launches-european-financial-and-economic-crime-centre (дата обращения: 24.05.2020).

[1] Денежные мулы – это люди, которые, зачастую сами того не зная, были завербованы в качестве посредников по отмыванию денег для преступников и преступных организаций.

При поддержке более 70 банков властям удалось выявить более 900 жертв этих денежных мулов или преступников, с которыми они работают. В этой связи Европол опубликовал плакат и листовку, доступные на шести языках, с советами о том, как избежать превращения в денежного мула[1].

Эта операция была частью европейского проекта Money Mule Action (EMMA), пилотного проекта, проводимого в рамках оперативного плана действий EMPACT по борьбе с киберпреступностью и мошенничеством с платежными картами. Она позволила сделать вывод, согласно которого, помимо организованных преступных групп, легализацией (отмыванием) преступных доходов занимаются профессионалы, оказывающие эти слуги от имени других лиц.

Масштабы легализации (отмывания) преступных доходов трудно оценить, но они считаются значительными. По оценкам Управления ООН по наркотикам и преступности (УНП ООН), ежегодно отмывается от 2 до 5 % мирового ВВП. Это от 715 млрд до 1,87 трлн евро ежегодно[2].

В предупреждении преступной деятельности с использованием криптовалюты Интерпол и Европол играют заметную роль. Это не только подготовка методических рекомендаций, проведение конференций и обучающих семинаров, но и серьезная помощь в раскрытии и расследовании тяжких преступлений в экономической сфере, в т. ч. легализации (отмывании) преступных доходов, в финансировании терроризма, торговле людьми, незаконном обороте оружия и наркотиков и др., осуществление мониторинга преступной деятельности с использованием криптовалюты, расширение сотрудничества международными организациями правоохранительной направленности и пр.

В то же время следует отметить, что предупредительная деятельность в сфере незаконного оборота криптовалюты усложняется из-за неопределенности сущности криптовалюты. В настоящее время нет базовых документов на международном уровне, положенных в основу формирования нормативно-правовых актов, направленных на противодействие преступной деятельности с использованием криптовалюты.

Существующая правовая база в сфере киберпространства и противодействия преступности в полной мере не отвечает современ-

---

[1] Money Muling. URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling (дата обращения: 24.05.2020).

[2] *Там же.*

ным требованиям и нуждается в консолидации мирового сообщества к принятию единых правил игры как в повседневном использовании криптовалюты, так и в противодействии преступлениям, с ее криминальным оборотом.

Контрольные вопросы

1. Место Интерпола в деятельности по противодействию преступлениям, совершаемым с использованием криптовалюты.
2. Назовите основные направления Интерпола в деятельности по противодействию преступлениям, совершаемым с использованием криптовалюты.
3. Определите роль Европола в предупреждении преступной деятельности с использованием криптовалюты.
4. С какими проблемами сталкивается Интерпол и Европол при осуществлении предупреждения преступной деятельности с использованием криптовалюты?

Глава 4. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) и ее роль в предупреждении преступной деятельности с использованием криптовалюты

Особую озабоченность у международного сообщества вызывает легализация (отмывание) преступных доходов и финансирование терроризма, о чем уже упоминалось в тексте настоящей работы. При этом уровень латентности таких преступлений высок, поскольку еще недостаточно разработаны стандарты противодействия этим явлениям и отсутствуют методические рекомендации по их пресечению, раскрытию, расследованию и предупреждению.

Данная деятельность на международном уровне проводится наряду с другими органами и организациями Группой разработки финансовых мер по борьбе с отмыванием денег – ФАТФ *(Financial Action Task Force – FATF)*. Это межправительственная организация, которая учреждена в июле 1989 г. Европейской комиссией в ходе Парижской встречи G7. Позже ее мандат расширился, – в октябре 2001 г. в ее деятельность включаются и проблемы противодействия финансированию терроризма, а с февраля 2012 г. – проблемы предотвращения финансирования распространения оружия массового уничтожения. Она охватывает более 190 государств и территорий. Членами ФАТФ являются 38 стран и два международных объединения, в ее работе принимают участие 26 наблюдателей, 9 региональных групп, созданных по типу ФАТФ. Она не только разрабатывает Международные стандарты (Рекомендации ФАТФ) по противодействию легализации (отмыванию) преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения, которые должны быть имплементированы в национальные законодательства (их уже более 40), но и проводит взаимные оценки национальных систем по борьбе с указанными преступлениями[1].

Более того, проводится серьезная работа:

– по осуществлению мониторинга за исполнением рекомендованных стандартов;

– по исследованию рисков, трендов и типологий легализации (отмывания) преступных доходов и финансирования терроризма с разработкой методологий борьбы с этими видами преступлений.

[1] Российская Федерация является членом ФАТФ с 2003 г.

ФАТФ стремится расширить сотрудничество с профильными международными организациями и тесно сотрудничает с ООН, опираясь на ее международную практику, Советом Европы, Всемирным банком, Европейским банком реконструкции и развития, Международным валютным фондом, Интерполом, Европолом, Советом по таможенному сотрудничеству и другими международными организациями, а также с международным профессиональным объединением подразделений финансовой разведки (ПФР) – Группой «Эгмонт»[1], и др.

В последние годы активизировалась работа по противодействию легализации (отмывания) преступных доходов и финансированию терроризма, т. к. не только возросло количество этих преступлений во всем мире, но и появились новые инструменты, с использованием которых осуществляется легализация. В этой связи только за 2013–2014 гг. ею подготовлены руководства по применению риск-ориентированного подхода в отношении предоплаченных карт, мобильных платежей и систем платежей через Интернет, в т. ч. и с использованием криптовалют[2].

Прежде всего речь идет об использовании в качестве средства совершения преступления криптовалют. Так, например, в представленном международному сообществу Докладе (2014 г.) «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ» дано понятие криптовалюты и представлена краткая характеристика криптовалют, определены их основные виды, риски, расширен перечень проблем, с которыми могут столкнутся государства-участники, а также даны рекомендации по принятию решений в национальных законодательствах о ее регулировании и правовом положении[3]. Что же касается правового регулирования криптовалют, то авторы рекомендаций принятие решения о запрете оборота криптовалют в той или иной стране либо принятие ее как финансовой единицы отдают на решение финансовых органов стран-участниц.

---

[1] Совместный доклад ФАТФ и Группы Эгмонт «Сокрытие информации о бенефициарных собственниках», июль 2018 г. URL: https://cbr.ru/Content/Document/File/48583/FATF-Egmont-Concealment-beneficial-ownership.pdf (дата обращения: 18.06.2020).

[2] Руководство по применению риск-ориентированного подхода: предоплаченные карты, мобильные платежи и онлайн платежи // ФАТФ. URL: http://www.eurasiangroup.org/files/FATF_docs/Rukovodstvo_FATF_po_primeneniyu_riskorientirovannogo_podhoda_dlya_predoplachennyh_kart_mobilnyh_platezhej_i_onlajn_platezhej_2013.pdf (дата обращения: 24.07.2020); Виртуальные валюты: ключевые определения и потенциальные риски в сфере ПОД/ФТ // ФАТФ. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 18.07.2020).

[3] *Там же.*

При этом было указано, что центры (обеспечивающие возможность доступа к регулируемой финансовой системе), в которых осуществляются операции с конвертируемой[1] криптовалютой, подлежат контролю в области противодействия легализации (отмыванию) преступных доходов и финансирования терроризма. Более того, на национальном уровне странам-участницам предлагается обеспечить «строгий контроль за подозрительными финансовыми операциями с банковскими счетами финансовых учреждений, деятельностью провайдеров, предоставляющих услуги в сфере оборота виртуальных активов, равно как и неотвратимую ответственность за уклонение от осуществления такого контроля. Это должно касаться и проверки клиентов, хранения данных, взаимоотношений с банками-корреспондентами, порядка осуществления услуг перевода денег и ценностей, применения новых технологий и т. д.»[2]

Государствам-участникам также предлагалось осуществлять следующее:

– контроль за деятельностью центров, проводящих операции с конвертируемой виртуальной валютой (обменные пункты и криптобиржи), и выявление степени финансовых рисков их деятельности;

– мониторинг деятельности этих организаций и введение дополнительных условий их существования на рынке криптоиндустрии, а именно:

а) применение имеющихся законных форм и методов противодействия легализации (отмыванию) средств, добытых преступным путем, финансированию экстремизма и терроризма;

б) ведение системы регистрации (лицензирования) субъектов, оказывающих услуги по обмену конвертируемой криптовалюты на фиатные валюты, и наоборот;

---

[1] В нашем случае «конвертируемая» виртуальная валюта никакого отношения не имеет к официальной конвертируемости, а только указывает на ее фактическую конвертируемость (например, по причине наличия соответствующего рынка) и является таковой до тех пор, пока некоторые частные участники предлагают с ней сделки, а другие принимают их, обладает эквивалентной стоимостью в реальной валюте и может обмениваться на реальную валюту и обратно. Такая «конвертируемость» никоим образом не гарантирована законодательством. Примерами конвертируемой виртуальной валюты являются: *Bitcoin* (Биткоин) и другие виды криптовалют: *E-Gold; Liberty Reserve; Second Life Linden Dollars* (в игре «Second Life») и *WebMoney* (ВебМани). См. подробно: *Пинкевич Т.В.* Преступность с использованием криптографических кодов и ее влияние на криминологическую безопасность России // Проблемы экономики и юридической практики. Москва, 2019. № 3. С. 89.

[2] Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / пер. с англ. Москва: МУМЦФМ, 2012.

в) подготовку и внесение предложений по определению форм и методов выявления подозрительных операций (транзакций) и возложения обязанности по осуществлению сбора информации о клиентах (политика «знай своего клиента»), субъектах, оказывающих услуги по обмену конвертируемых криптовалют, криптобирж и других видов организаций, связанных с названными валютами, пересекающимися с регулируемой финансовой системой;

г) идентификацию клиента посредством подтверждения идентификационных данных, полученных от клиента (например, документ, удостоверяющий личность) и совпадающих с информацией из сторонних баз данных или иных надежных источников; выявления IP-адреса клиента; поиска информации, подтверждающей деятельность клиента в части соответствия характеру проводимых им операций. В этих целях использование интерфейсов прикладного программирования, обеспечивающего получение информации о личности клиентов или позволяющего ограничивать объемы и скорость осуществления операций или ставить различные условия, которые должны быть выполнены прежде, чем криптовалюта может быть отправлена получателю; независимые системы цифровой идентификации личности; создание отраслевых ассоциаций.

В этот же период ФАТФ издает Методологию[1] для проведения оценки соответствия систем противодействия легализации (отмыванию) преступных доходов и финансированию терроризма в новой редакции Рекомендаций ФАТФ от 2012 г., в которой подтверждается риск-ориентированный подход и изложены все этапы оценки национальных систем противодействия названным явлениям, а также дает оценку эффективности. В то же время одним из ее недостатков является «отсутствие анализа затрат и выгод системы ПОД/ФТ в качестве этапа оценки, который позволил бы оценить задействованный ресурсный потенциал юрисдикции и выявить наилучшие практики имплементации стандартов ФАТФ с учетом ресурсной базы юрисдикции, которая, безусловно, будет разниться от юрисдикции к юрисдикции. Тем не менее, в обновленной Методологии закреплены критерии технического соответствия и эффективности национальных систем ПОД/ФТ. Оценка технического соответствия касается, главным образом, основных структурных элементов

[1] Methodology for Assessing Technical Compliance with the FATF. Recommendations and the Effectiveness of AML/CFT Systems // FATF. Paris, 2013. URL: http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%20 2013.pdf (дата обращения: 25.03.2013).

системы ПОД/ФТ: правовой и институциональной системы страны, полномочий и процедур компетентных органов»[1].

Вторым недостатком, как нам видится, следует считать «отсутствие явных количественных данных, которые могли бы служить солидным основанием для утверждения эффективности систем ПОД/ФТ. Их разработка представляет самостоятельную методологическую задачу»[2].

В ходе Консультативного форума ФАТФ с представителями частного сектора, который проходил 25–26 марта 2014 г. в Брюсселе, было выделено несколько направлений риска использования криптовалют[3].

На проблемы идентификации личности за последние годы ФАТФ неоднократно обращала внимание. Так, например, ею подготовлено Руководство «О цифровой идентификации личности», которое с 6 марта 2020 г. было направлено во все страны-участницы[4]. Основанием этого явился факт ежегодного роста цифровых платежей (в среднем – на 12,7 %) и прогноз количества транзакций, которые за 2020 г. может достичь 726 млрд, а к 2022 г, по оценкам экспертов, 60 % мирового ВВП будет оцифровано.

С ростом числа цифровых финансовых операций, по мнению ФАТФ, требуется более глубокое понимание того, как отдельные лица могут выявляться и проверяться в мире цифровых финансовых услуг. Технологии цифровой идентификации (ID) быстро развиваются, что приводит к появлению различных цифровых систем идентификации. В этой связи было подготовлено Руководство, предназначенное для оказания помощи правительствам в урегулировании этого вопроса, а также для уточнения относительно того, как цифровые идентификационные системы могут использоваться для проведения определенных элементов должной осмотрительности клиентов в соответствии с Рекомендацией 10 ФАТФ. Более того, в Разделе II кратко излагаются основные характеристики цифровых систем идентификации, а в приложении дается их под-

---

[1] Methodology for Assessing Technical Compliance with the FATF. Recommendations and the Effectiveness of AML/CFT Systems // FATF. Paris, 2013. URL: http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf (дата обращения: 25.03.2013); *Мелкумян К.С.* Эффективность деятельности Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в противодействии финансированию терроризма: дис. ... канд. полит. наук. 2019. С. 213–214.

[2] *Мелкумян К.С.* Указ. соч.

[3] *Достов В.Л.* Консультации ФАТФ с частным сектором: диалог продолжается // Финансовая безопасность. 2014. № 5. С. 48–50.

[4] О цифровой идентификации личности: руководство от 6 марта 2020 г. URL: www.fatf-gafi.org (дата обращения: 02.06.2020).

робные разъяснения. Раздел III Руководства содержит требование идентифицировать и проверять личность клиентов с использованием «надежных, независимых» исходных документов, данных или информации (Рекомендация 10 (а)). Это означает, что система цифрового удостоверения личности, используемая для проведения надлежащей проверки клиента, опирается на технологию, адекватное управление, процессы и процедуры, обеспечивающие надлежащий уровень уверенности в том, что система дает точные результаты. Руководство разъясняет, что наличная идентификация клиентов и транзакции, которые полагаются на надежные, независимые цифровые идентификационные системы с соответствующими мерами по снижению риска, могут представлять стандартный уровень риска или могут быть менее рискованными. Такие требования ФАТФ выдвигает к финансовым учреждениям, актив-провайдерам виртуальным платформ, установленным нефинансовым организациям и профессиям, и пр.

В то же время, учитывая, что виртуальная валюта и связанные с ней финансовые услуги обладают потенциалом для стимулирования финансовых инноваций и повышения эффективности, и расширения доступа к финансовым услугам, а с одной стороны, с другой – они дают возможность использовать ее в преступных целях, в т. ч. легализовывать (отмывать) преступные доходы и финансировать террористическую деятельность, в 2015 г. ФАТФ было подготовлено Руководство по применению риск-ориентированного подхода к виртуальным валютам[1]. Его рекомендации заключаются в том, чтобы все страны приняли скоординированные меры по предотвращению использования виртуальных активов в преступных и террористических целях.

Рекомендации ФАТФ устанавливают всеобъемлющие требования по борьбе с легализацией (отмыванием) преступных доходов и финансированием терроризма, которые применяются ко всем формам финансовой деятельности, включая и те, которые используют виртуальные валюты. Однако правительства и частный сектор обратились с просьбой о разъяснении того, к каким именно видам деятельности применяются стандарты ФАТФ в этом контексте. Подход, основанный на учете рисков, требует от юрисдикций выявления рисков легализации (отмывания) преступных доходов и финансирования терроризма и принятия соответствующих мер

[1] Руководство «О риск-ориентированном подходе в секторе виртуальных активов и провайдерах услуг в сфере виртуальных активов», июнь 2019 г. URL: https://mumcfm.ru/biblioteka/mezdunarodnye-dokumenty/fatf (дата обращения: 12.06.2020).

по снижению этих рисков. Это включает в себя выявление и смягчение рисков незаконного финансирования, связанных с новыми продуктами или деловой практикой, а также другие виды деятельности, прямо не упомянутые в рекомендациях ФАТФ. А поскольку возникла необходимость в уточнении ряда вопросов, в т. ч. и эффективного глобального, основанного на учете рисков реагирования на риски легализации (отмывания) преступных доходов и финансирования терроризма, связанных с финансовой деятельностью и оборотом виртуальной валюты (криптовалюты), ФАТФ приняла изменения к рекомендациям, которые разъясняют, как эти рекомендации применяются в случае финансовой деятельности, связанной с виртуальными активами[1].

Благодаря деятельности ФАТФ, была принята Декларация «Большой двадцатки» (G20) «Создание консенсуса для честного и устойчивого развития», которая стала результатом работы 13-й встречи представителей государств, входящих в «Большую двадцатку», прошедшей с 30 ноября по 1 декабря 2018 г. в Буэнос-Айресе (Аргентина). Она включала к рассмотрению такие вопросы, как регулирование рынков виртуальной валюты (криптовалют) в контексте «открытой и устойчивой финансовой системы», которая «важна для поддержания устойчивого роста»[2].

Признавая значимость индустрии виртуальных валют, члены G20 отметили, что работа в этой сфере будет включать меры по борьбе с легализацией (отмыванием) преступных доходов и финансированием терроризма в соответствии со стандартами межправительственной организации ФАТФ. Кроме того, в той же части Декларации участники G20 продемонстрировали позитивное отношение к небанковским финансовым институтам, указав на потенциальные преимущества технологии в финансовом секторе при условии, что создатели технологических инноваций управляют связанными рисками. Более того, они согласились с тем, что ФАТФ должна иметь свои стандарты для криптовалютных рынков в странах-членах, которые они обязуются внедрять применительно к криптоактивам, ожидается пересмотр данных стандартов, а также они призывают ФАТФ способствовать их глобальному внедрению. Между тем многие из участников «Большой двадцатки» поддержа-

[1] Регулирование виртуальных активов. URL: https://cbr.ru/counteraction_m_ter/international/fatf/doc_fatf (дата обращения 12.03.2020).

[2] Итоги Саммита G20: криптовалюты важны для глобальной экономики, но необходимо регулирование и налогообложение. URL: https://btcinfor.com/mine/itogi-sammita-g20-kriptovaluty-vajny-dlia-globalnoi-ekonomiki-no-neobhodimo-regylirovanie-i-nalogooblojenie.html (дата обращения 12.03.2020).

ли мнение о необходимости дальнейшего изучения криптовалюты, без которого не стоит делать конкретных шагов в сфере ее регулирования, а некоторые страны, включая Бразилию, заявили, что вообще не будут следовать рекомендациям G20[1].

ФАТФ в июне 2018 г. приступила к корректировке руководящих указаний и Стандартов, которые были подготовлены ею ранее с целью определения необходимости их изменения не только в связи с ростом использования криптовалют и иных виртуальных активов, но и определения рисков, которые они несут. Эта работа была проведена организацией при сотрудничестве как с частным сектором, учитывая технологическую сложность использования криптовалют, так и государственным сектором, в т. ч. включая следственные органы, принимая во внимание необходимость выработки соответствующих инструментов для расследования уголовных дел, связанных с использованием криптовалют[2]. Также в этот период ФАТФ при участии частных субъектов работает над проектом пояснительной записки к Рекомендации 15 для уточнения применения стандартов ФАТФ к действиям или операциям, связанным с виртуальными активами. И в ходе подготовки поправок к названной Рекомендации, ФАТФ, осознавая преимущества использования криптовалют в мировой финансовой системе, стремилась выработать подход, гарантирующий невозможность легализации (отмывания) преступных доходов и финансирования терроризма, а также избежать ненужные барьеры для их законного использования. Следует признать, что ФАТФ не ограничилась анализом только рисков использования криптовалют, а стала изучать более широкий круг последствий внедрения новых технологий в финансовую систему для противодействия. В то же время, «учитывая возрастающий интерес бизнес-структур и НПО к новым платежным инструментам, в т. ч. криптовалютам, увеличивающуюся их долю в мировой экономике, а также усиливающийся контроль за традиционными финансовыми институтами, риски их использования в неправомерных целях будут увеличиваться»[3].

В октябре 2018 г. ФАТФ обновила свои стандарты, чтобы уточнить их применение к виртуальным активам и поставщикам услуг виртуальных активов, внеся поправки в Рекомендацию 15. Кроме

---

[1] *Там же.*

[2] FATF Report to G20 Finance Ministers and Central Bank Governors. P. 3–4. URL: https://cbr.ru/content/document/file/84542/g20-april-2019.pdf (дата обращения 14.03.2020).

[3] *Мелкумян К.С.* Эффективность деятельности Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в противодействии финансированию терроризма: дис. ... канд. полит. наук. 2019. С. 161.

этого, были даны два новых определения: «виртуальный актив», под которым следует понимать обозначения цифровых представлений стоимости, которые в цифровом формате могут быть переданы и реализованы, а также могут быть использованы для инвестиционных целей или в качестве платежного средства, охватывая как конвертируемые, так и неконвертируемые, централизованные и децентрализованные формы, а также первоначальные предложения монет. Но здесь следует заметить, что данное понятие включает в купе не только криптовалюты, но и электронные деньги, потому что криптовалюта, как и виртуальная валюта, является конвертируемой и децентрализованной, и второй момент, на который обращено внимание – это «поставщик услуг виртуальных активов».

Это вызвало одобрение со стороны международного сообщества, в т. ч. и Совет Безопасности ООН, который не только поддержал усилия ФАТФ по решению проблемы регулирования и надзора за деятельностью и поставщиками услуг в области виртуальных активов, но и предложил свое видение решения проблем, включив их в резолюцию Резолюция 2462 (2019) на его 8496-м заседании 28 марта 2019 г.[1], которые были восприняты ФАТФ и сегодня воплощаются в жизнь. Следует отметить, что с этого момента начинается активная деятельность этой организации по противодействию преступной деятельности с использованием криптовалюты.

12 апреля 2019 г. был продлен мандат ФАТФ, который подтверждает ее роль в руководстве по противодействию легализации (отмыванию) преступных доходов, финансированию терроризма и распространению оружия массового уничтожения. Подтверждение мандата в канун 30-й годовщины ФАТФ отражает тот факт, что названные преступления угрожают целостности финансовой системы и устойчивой политической ситуации[2]. Благодаря новой Декларации и продлению мандата, на ФАТФ возлагается обязанность продолжать руководить решительными, скоординированными и эффективными глобальными действиями по противодействию злоупотреблениям финансовой системой со стороны преступников и террористов и укреплять свой потенциал реагирования на эти угрозы, с которыми сталкиваются все страны-участницы.

Это дает ФАТФ и региональным органам типа ФАТФ возможность участия в международных форумах, в т. ч. в рамках G7/G20

[1] Резолюция 2462 (2019): принята Советом Безопасности на его 8496-м заседании 28 марта 2019 г.: http://www.fedsfm.ru/content/files/documents/international/2019/s_res_2462(2019)_r.pdf (дата обращения: 02.06.2020).

[2] Новый, бессрочный мандат ФАТФ: http://www.fedsfm.ru/content/files/bulleten38_ru_print.pdf (дата обращения:14.05.2020).

и органов ООН, а также на поддержку деятельности ФАТФ и ее реагирования на текущие и возникающие угрозы и возможности.

В середине 2019 г. ФАТФ вносит поправки в Рекомендацию 15, согласно которым устанавливаются дополнительные требования, касающиеся базовых обязательств по применению риск-ориентированного подхода в отношении новых технологий.

ФАТФ предлагает помимо выявления и проведения оценки рисков легализации (отмывания) преступных доходов и финансирования терроризма, связанных с разработкой новых продуктов и новой деловой практики, включать перспективные механизмы распространения и использования новых или развивающихся технологий. В этой связи необходимо, чтобы финансовые учреждения стран-участниц, получившие лицензию или осуществляющие деятельность в их юрисдикции, «приняли соответствующие меры для управления и снижения рисков до запуска новых продуктов, для внедрения новой деловой практики или использования новых или развивающихся технологий. При этом требования, касающиеся новых технологий, должны распространяться на платЕжные продукты и услуги на основе виртуальной валюты»[1].

Здесь же указывается на необходимость повышения эффективного регулирования, контроля и мониторинга деятельности провайдеров (поставщиков) услуг в сфере оборота виртуальных активов и финансовой деятельности с их использованием. Для этого предлагается лицензировать деятельность поставщиков услуг виртуальных активов, а лица, занимающиеся такой деятельностью, должны быть зарегистрированы[2]. Помимо этого, страны-участницы должны обязать провайдеров данных услуг самостоятельно оценивать и снижать риски распространения названных преступлений, и осуществлять полный комплекс превентивных мер в соответствии с рекомендациями ФАТФ, включая должную осмотрительность клиентов, ведение учета, отчетности о подозрительных сделках и проверку всех сделок на предмет соблюдения целевых финансовых санкций, – среди прочих мер, как и другие субъекты, подпадающие под регулирование противодействия таким деяниям. Это включает в себя координацию с соответствующими органами для обеспечения совместимости тре-

[1] Виртуальные валюты. Руководство по применению риск-ориентированного подхода. Июль 2015 г. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (дата обращения: 28.03.2020).

[2] Публичное заявление о виртуальных активах и связанных с ними провайдерах. URL: http://www.fedsfm.ru/content/files/bulleten38_ru_print.pdf (дата обращения: 12.06.2020).

бований предупредительного воздействия с правилами защиты данных и конфиденциальности и аналогичными положениями.

Предпринятые меры и предложения организации, основанные на анализе совершаемых преступлений, явились обоснованием создания комплекса специальных рекомендаций для правоохранительных органов по расследованию преступлений, при совершении которых виртуальные валюты выступают средством их совершения, в т. ч. перемещения преступных активов в иностранные юрисдикции, легализации (отмывания) преступных доходов и финансирования терроризма. Более того, здесь же высказаны требования к странам, которые должны соблюдать соответствующие рекомендации ФАТФ по предотвращению неправомерного использования виртуальных активов.

Кроме того, установлены обязательные меры, имеющие отношение как к странам, так и к поставщикам услуг виртуальных активов (а также к другим обязанным субъектам, которые занимаются или предоставляют продукты и услуги таких активов), которые требуют создать более равные условия для всех участников экосистемы виртуальных валют. Эти обязательства требуют от стран оценивать и смягчать свои риски, связанные с деятельностью виртуальных актив[1].

В планах ФАТФ в свете стремительного развития ряда финансовых функций, выполняемых виртуальными активами, предлагалось в июне 2020 г. рассмотреть вопрос о выполнении странами и поставщиками услуг требований, применимых к этим активам и поставщикам услуг виртуальных активов, и уделить особое внимание мониторингу деятельности поставщиков услуг таких активов и их прогрессу в разработке технологических решений для безопасного представления информации об отправителе/бенефициаре между поставщиками при осуществлении передачи средств и оценке необходимости дальнейшего обновления для обеспечения того, чтобы стандарты ФАТФ оставались актуальными и эффективными.

На этом фоне ФАТФ создало контактную группу контроля за качеством соблюдения стандартов ФАТФ и более эффективной защиты международной финансовой системы от злоупотреблений. Эти изменения в деятельности ФАТФ были поддержаны и одобрены на встрече G20 в Фукуоке. В свою очередь ФАТФ продолжила свою деятельность по обеспечению эффективного регулирования и надзора за использованием новых технологий, в т. ч. в контексте виртуальных активов, в целях снижения связанных с этим рисков легализации (отмывания) преступных доходов и финансирования терроризма и поддержки ответственных инноваций в секторе финансовых услуг.

[1] *Там же.*

Кроме того, в рамках этой проблемы в ноябре 2019 г. опубликован проект Рекомендаций по развертыванию систем цифровой идентификации[1], которые направлены на анализ особенностей работы криптовалютных и блокчейн-компаний, с целью обеспечения соблюдения правил борьбы с легализацией (отмыванием) преступных доходов и противодействия финансированию терроризма.

При этом для решения возникающих проблем безопасности, т. к. процесс финансовых транзакций все больше уходит в цифровую сферу, ФАТФ предложила ряд ключевых вопросов к рассмотрению, которые следует согласовать с заинтересованными сторонами. К таковым она относит конкретные риски, которые цифровая идентификация может представлять для обеспечения соблюдения законов о легализации (отмыванию) преступных доходов и противодействия финансированию терроризма; вопросы о том, «как технология может способствовать расширению доступа к финансовым услугам, как система может помочь в мониторинге транзакций, а также потенциальное влияние на выполнение требований FATF по ведению учета»[2]. Здесь же раскрываются особенности технологии распределенного реестра, который, по мнению разработчиков, должен выступать в качестве инструмента, способного помочь росту сетей цифровой идентификации.

Между тем ФАТФ предлагает государствам-участникам на национальном уроне принять «руководящие принципы или нормативные акты, позволяющие надлежащим образом использовать независимые системы цифровой идентификации организациями, определенными для целей AML/CFT». Помимо названных принципов и нормативных документов, регулируемым учреждениям, например, криптовалютным биржам, предлагается «использовать информированный подход с учетом оценки рисков в случае развертывания систем цифровой идентификации для надлежащей проверки клиентов»[3].

К концу первой половины 2020 г. этот проект был дополнен рядом рекомендаций и уже опубликован в новой редакции. Так, были включены, например, положения, обязывающие операторов криптовалютных сервисов (в первую очередь, криптовалютных бирж) передавать информацию о клиентах при совершении ими переводов не только в фиатных валютах, но и в криптовалютных

---

[1] FATF опубликовала рекомендации по развертыванию систем цифровой идентификации. URL: https://bits.media/fatf-opublikovala-rekomendatsii-po-razvertyvaniyu-sistem-tsifrovoy-identifikatsii (дата обращения: 27.05.2020).

[2] *Там же*.

[3] Применение риск-ориентированного подхода для банковского сектора: Руководство ФАТФ. URL: https://eurasiangroup.org/files/FATF_docs/Rukovodstvo_FATF_ROP_v_bankovskom_sektore.pdf (дата обращения: 28.05.2020).

транзакциях. Такое решение ФАТФ при принятии этих рекомендаций «регуляторами стран, в которых зарегистрированы крупнейшие биржи криптовалют, сильно встряхнет рынок и осложнит работу как биржам, так и трейдерам»[1].

В своем заявлении о COVID-19 и мерах по борьбе с незаконным финансированием президент ФАТФ Сянмин Лю призвал правительства сотрудничать с финансовыми учреждениями и другими предприятиями с целью снижения рисков легализации (отмывания) доходов, добытых преступным путем. И, поддерживая и поощряя активное внедрение и использование современных цифровых систем, обращает внимание на безопасность глобальной платежной системы и указывает на проблемы риска финансовых преступлений. В то же время он призывает соблюдать бдительность, поскольку преступники стали активно использовать пандемию COVID-19 для совершения преступлений (мошенничество, незаконный оборот фальсифицированных лекарств, инсайдерская торговля, эксплуатация людей и др.).

В этой связи предложено продолжать обмениваться информацией о способах совершения преступлений, а также помнить о том, что преступники будут стремиться использовать пробелы и недостатки в национальных системах борьбы с названной преступностью.

На пленарной сессии ФАТФ, которая состоялась 8–24 июня 2020 г. было уделено внимание снижению рисков легализации (отмывания) преступных доходов и финансирования терроризма с использованием виртуальных активов, в т. ч. и «стейблкоинами», под которыми следует понимать криптовалюту с фиксированным обменным курсом, которая не подвержена волатильности, подобно стоимости традиционных криптовалют. Данное свойство обеспечивается за счет привязки курса стейблкоинов к стабильным активам, например, фиатным валютам (доллару США, евро) или физическим активам (нефти, золоту и др.). Стейблкоин может рассматриваться как виртуальный или как традиционный финансовый актив.

Ключевое отличие стейблкоинов от «стандартных» виртуальных активов заключается в том, что они обладают «потенциалом повсеместного распространения ввиду их большей привлекательности (более высокая стабильность, безопасность операций и простота использования по сравнению со «стандартными» виртуальными активами), что одновременно повышает вероятность их использо-

[1] Сегодня группа FATF опубликовала финальную версию рекомендаций по регулированию криптовалют и деятельности операторов криптовалютных сервисов. URL: https://bits.media/finalnaya-versiya-rekomendatsiy-fatf-birzhi-kriptovalyut-budut-obyazany-obmenivatsya-informatsiey-o-/(дата обращения: 28.05.2020).

вания преступными элементами»[1]. Именно они потенциально способны изменить «экосистему» виртуальных активов и создать предпосылки для роста рисков легализации (отмывания) преступных доходов и противодействия финансированию терроризма[2].

Здесь же был утвержден Годовой обзор имплементации стандартов ФАТФ в части регулирования деятельности провайдеров услуг в сфере виртуальных активов, в котором обращается внимание на успешную реализацию в большинстве юрисдикций обновленных стандартов Группы, касающихся регулирования сферы виртуальных активов и деятельности провайдеров услуг в сфере виртуальных активов, а также о текущих подходах этих стран к работе с виртуальными активами.

Все вышеизложенное свидетельствует о значительном объеме работы, которая проделана Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ) с момента ее создания в сфере противодействия легализации (отмывании) преступных доходов, финансирования терроризма и предотвращения финансирования распространения оружия массового уничтожения.

Контрольные вопросы

1. Дайте понятие виртуальной валюты (криптовалюты), которое дано в отчете ФАТФ «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ».

2. Определите основные направления деятельности ФАТФ по противодействию легализации (отмыванием) преступных доходов.

3. В каких сферах деятельности ФАТФ предлагает на национальном уровне странам-участницам обеспечить строгий контроль с целью противодействия преступной деятельности с использованием виртуальной валюты (криптовалюты)?

4. Руководство по применению риск-ориентированного подхода к виртуальным валютам: роль и значение.

5. Какую роль на международном уровне выполняют Рекомендации ФАТФ по противодействию преступной деятельности с использованием виртуальной валюты?

---

[1] Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем и финансированию терроризма. 1–30 июня 2020 г. // Банк России. Июнь 2020. С. 4–5.

[2] *Там же.*

Глава 5. Организация международного сотрудничества по предупреждению преступной деятельности с использованием криптовалюты

Все большее число преступлений, совершаемых с использованием цифровых технологий, носят международный характер. Одна из причин этого явления заключается в том, что в современном обществе существует очень малая необходимость физического присутствия лица, совершившего преступление в месте, где предоставляется услуга. Как следствие, преступникам необязательно присутствовать там, где находится жертва. Ввиду мобильности преступников, необязательности их присутствия на месте совершения преступления, а также с учетом последствий подобных правонарушений, правоохранительным и судебным органам следует действовать сообща и оказывать содействие государству, в юрисдикции которого было совершено то или иное преступление.

Принимая во внимание различия в национальном законодательстве и ограниченное количество имеющихся правовых инструментов, налаживание международного сотрудничества считается одной из главных задач в контексте глобализации преступности. Это касается как традиционных форм транснациональной преступности, так и цифровой. Одним из ключевых требований следователей в транснациональных расследованиях является немедленная реакция коллег в стране нахождения преступника. В этом отношении традиционные инструменты международного сотрудничества судебных органов по уголовным вопросам очень часто не соответствуют требованиям в части скорости расследований в Интернете.

Применительно к расследованиям цифровых преступлений, основными формальными механизмами обеспечения международного сотрудничества являются взаимная правовая помощь и экстрадиция. Другие механизмы, такие как передача заключенных, передача уголовного производства, конфискация доходов от преступлений и восстановление активов, не имеют такой практической важности. Наряду с формальными механизмами, существуют также и неформальные способы сотрудничества, такие как обмен оперативной информацией между правоохранительными органами разных стран.

1. Правовые основы международного сотрудничества

При определении применимого документа, регулирующего международное сотрудничество, возможно три варианта. Во-первых, соответствующие процедуры могут быть оговорены в международных соглашениях, таких как Конвенция ООН против транснациональной организованной преступности и три протокола к ней, а также в региональных конвенциях, таких как: Межамериканская конвенция о взаимной правовой помощи по уголовным делам, Европейская конвенция о взаимной правовой помощи по уголовным делам и Конвенция Совета Европы о преступности в сфере компьютерной информации. Во-вторых, процедуры могут регулироваться двусторонними соглашениями. Такие соглашения, как правило, относятся к конкретным запросам и определяют соответствующие процедуры и формы контакта, а также права и обязанности запрашивающей и запрашиваемой стороны. Например, Англия подписала с другими странами более 20-ти двусторонних соглашений, регулирующих различные аспекты экстрадиции. Некоторые из таких соглашений обращаются к теме цифровой преступности, хотя неясно, насколько объективно существующие соглашения регламентируют эту сферу. Если не применяется ни одностороннее, ни двусторонне соглашение, международное сотрудничество должно основываться на международном этикете и принципе взаимности.

Нижеследующий обзор посвящен международным и региональным конвенциям, т. к. сотрудничество, основанное на двусторонних соглашениях и этикете, в значительной степени зависит от обстоятельств каждого конкретного дела и задействованных стран.

Основным международным документом, регламентирующим оказание взаимной правовой помощи по уголовным делам, является Конвенция ООН против транснациональной организованной преступности (UNTOC). Эта Конвенция содержит важные положения о международном сотрудничестве, но она не направлена исключительно на решение вопросов, касающихся цифровой преступности. В ней также не содержатся конкретные положения, посвященные необходимости сохранения данных.

§ 1 ст. 3 Конвенции указывает на то, что она применима к цифровым преступлениям только в том случае, если они совершены при участии организованной преступной группы. Ст. 2 Конвенции определяет организованную преступную группу как оформленную группу в составе трех или более лиц.

Следовательно, Конвенция особенно релевантна для дел, связанных с организованной преступностью. Без сомнения, ОПГ совер-

шают цифровые преступления. Тем не менее, степень их участия и, следовательно, релевантность данной Конвенции в отношении расследований транснациональных киберпреступлений, неясны. Следует отметить, что определение активности ОПГ очень важно.

Однако анализ связи между преступлениями против идентичности и цифровыми преступлениями представляет некоторые трудности. Первой главной проблемой является отсутствие объективных научных исследований в этой области. В отличие от технической стороны преступлений, их связь с организованной преступностью анализируется менее активно. Известны расследования, успешно обнаружившие ряд преступных групп, совершавших цифровые преступления. Но структура таких групп не всегда идентична структуре традиционных ОПГ. Цифровые преступные группы, как правило, имеют более свободную и гибкую структуру. Кроме того, такие группы нередко значительно меньше по размеру, чем традиционные ОПГ. Интернет дает возможность тесно сотрудничать с другим лицами и координировать их действия без необходимости когда-либо встречаться с ними лично. Таким образом, преступники могут работать вместе в свободных, неустойчивых группах.

Положения, регламентирующие взаимную правовую помощь, приведены в ст. 18. Эта статья содержит целый ряд процедур.

В § 3 ст. 18 перечислены конкретные случаи запросов правовой помощи. Список достаточно сложный – от получения свидетельских показаний до отслеживания доходов от преступлений. Как уже упоминалось выше, Конвенция ООН против транснациональной организованной преступности не содержит конкретных положений по запросам, связанным с данными, например, по запросам о перехвате коммуникации или сохранении данных. Тем не менее, в § 3 (i) ст. 18 говорится о прочих запросах, поэтому данная Конвенция может регулировать запросы, связанные с данными. Хотя в целом можно говорить о преимуществах конкретного регулирования запросов, аналогичные региональные документы, посвященные конкретным запросам, таким как Конвенция Совета Европы о преступности в сфере компьютерной информации, обычно ссылаются лишь на процессуальные положения национального законодательства, без определения конкретных процедур, регулирующих взаимные правовые запросы.

§ 4–5 ст. 18 посвящены обмену оперативной информацией. В них оговаривается форма сотрудничества, осуществляемого на добровольной основе, без необходимости подачи получающей стороной запроса о взаимной юридической помощи. Эти параграфы покрывают информацию, относящуюся к области уголовного

правосудия, например данные о потенциальных покупателях криптовалют, находящихся в другой стране, обнаруженные в ходе проведения расследования. Особенно в случаях со сложными расследованиями, – когда обращение к формальным инструментам взаимной юридической помощи требует времени и потому мешает ходу расследования, правоохранительные органы обычно склоняются к неформальным средствам сотрудничества. Однако обмен информацией может иметь место, только если государство-получатель информации сможет собрать все необходимые доказательства самостоятельно. В противном случае требуется официальное сотрудничество для обеспечения правил передачи ответственности. Выступая за переход международного сотрудничества от формальных запросов к спонтанному обмену информацией, следует помнить, что формальные процедуры были разработаны для защиты целостности страны и прав обвиняемых. Следовательно, обмен информацией не должен нарушать догматическую структуру взаимной юридической помощи.

§ 6–12 ст. 18 посвящены процессуальным аспектам взаимной юридической помощи. Особый интерес представляют § 8 и 9. § 9 разрешает странам отклонить запрос о взаимной юридической помощи на основании отсутствия обоюдного признания соответствующего деяния преступлением. Это особенно важно, поскольку гармонизация уголовной ответственности по цифровым преступлениям – например, с помощью Конвенции Совета Европы о преступности в сфере компьютерной информации – в данный момент ограничена. По состоянию на середину 2020 г., лишь сорок стран ратифицировали этот документ и установили соответствующие минимальные стандарты по цифровым преступлениям. Это может затруднить применение Конвенции ООН против транснациональной организованной преступности.

§ 13–16 ст. 18 определяют форму и содержание запросов, а также каналы коммуникации. Что касается каналов коммуникации, Конвенция предполагает передачу запросов от центрального органа к центральному органу. Конвенция подчеркивает важность этой процедуры для обеспечения быстрого и надлежащего выполнения запроса. Роли центральных органов могут различаться: от непосредственного вовлечения в процесс обработки и выполнения запросов до перенаправления их компетентным органам. Конвенция оставляет передачу запросов по дипломатическим каналам на усмотрение государства. Так как такой способ передачи представляет собой длительный процесс, он может сильно замедлить передачу информации и, в особенности, препятствовать оперативным мерам,

например, сохранению данных о трафике. В отличие от Конвенции Совета Европы о преступности в сфере компьютерной информации, Конвенция ООН против транснациональной организованной преступности не оперирует понятием об оперативном сотрудничестве, хотя содержит общую процедуру по срочным делам. При согласии стран, в качестве канала коммуникации можно использовать Международную организацию уголовной полиции (Интерпол). Чтобы облегчить определение необходимого органа в другой стране, Управление ООН по наркотикам и преступности (ЮНОДК) имеет онлайн-директорию, которая предоставляет запрашивающему государству данные о центральном органе в запрашиваемой стране, каналы коммуникации и другую необходимую информацию.

При подаче запроса необходимо обеспечить его соответствие формальным критериям, оговоренным в § 14 и 15. Запросы в устной форме допускаются только при чрезвычайных обстоятельствах и должны быть продублированы в письменном виде. Отчеты государств-участников о применении данной Конвенции демонстрируют, что, хотя законодательство многих стран требует направления запросов о взаимной правовой помощи в письменном виде, лишь несколько стран сообщили о том, что направляют запросы по электронной почте заранее. В этом отношении Конвенция ООН против транснациональной организованной преступности отличается от Конвенции Совета Европы о преступности в сфере компьютерной информации, которая призывает государства к использованию средств электронной коммуникации в экстренных случаях. Конвенция ООН против транснациональной организованной преступности предлагает использовать для запросов специальное программное обеспечение, призванное обеспечить корректное заполнение запросов (Программа составления просьб об оказании взаимной правовой помощи).

В Конвенции Совета Европы о преступности в сфере компьютерной информации говорится о растущей значимости международного сотрудничества в ст. 23–25.

2. Общие принципы международного сотрудничества и меры взаимной помощи в международном сотрудничестве

Ст. 23 Конвенции Совета Европы о преступности в сфере компьютерной информации (далее – Конвенция) определяет *три основных принципа, касающихся международного сотрудничества в расследовании цифровых преступлений* среди ее членов.

Во-первых, предполагается, что участники обеспечивают наиболее широкое сотрудничество в области международного расследования. Это обязательство отражает важность международного сотрудничества в расследовании цифровых преступлений. Во-вторых, в ст. 23 отмечается, что общие принципы применимы не только в расследовании цифровых преступлений, а в любых расследованиях с необходимостью сбора доказательств в электронной форме. Это включает расследования цифровых преступлений, а также расследования в традиционных случаях. Если подозреваемый в убийстве использовал услугу электронной почты за рубежом, ст. 23 будет применяться в отношении расследований, связанных с данными, хранимыми поставщиком услуг хостинга. Третий принцип отмечает, что положения, касающиеся международного сотрудничества, не подменяют положений международных соглашений в том, что касается взаимной правовой помощи и экстрадиции или соответствующих положений внутреннего законодательства, касающихся международного сотрудничества.

Составители Конвенции подчеркивают, что взаимопомощь должна в целом осуществляться на основе применения соответствующих договоров и аналогичных соглашений о взаимопомощи. Как следствие, данная Конвенция не намерена создать отдельный общий режим взаимопомощи. Таким образом, только в тех случаях, когда существующие договоры, законы и механизмы еще не содержат таких положений, каждая Сторона должна создать правовую основу для осуществления международного сотрудничества, как определено в Конвенции.

Экстрадиция граждан остается одним из самых трудных аспектов международного сотрудничества. Запросы об экстрадиции очень часто приводят к конфликту между необходимостью защищать граждан и необходимостью оказывать поддержку проводимого расследования в зарубежной стране. Ст. 24 определяет принципы экстрадиции. В отличие от ст. 23, это положение ограничено в отношении правонарушений, указанных в Конвенции, и не применяется в случаях, являющихся незначительными (лишение свободы на максимальный срок не менее одного года). Во избежание конфликтов, которые могут воз-

никнуть с учетом способности сторон делать оговорки, ст. 24 основана на принципе двойной уголовной ответственности.

Относительно взаимопомощи, ст. 25 дополняет принципы, изложенные в ст. 23. Одним из наиболее важных положений ст. 25 является п. 3, в котором подчеркивается важность быстрой связи в расследовании цифровых преступлений. Как отмечалось ранее, ряд расследований цифровых преступлений на национальном уровне провалился по причине того, что расследования шли слишком долго и важные данные были удалены, прежде чем процедурными мерами предписали сохранить их и изъять. Расследования, которые требуют оказания взаимной правовой помощи, в целом занимают еще больше времени из-за требующих времени формальных условий по установлению связи с органами охраны правопорядка. Конвенция решает эту проблему, подчеркнув важность создания требований для ускоренного использования средств коммуникации.

В ходе расследования цифровых преступлений, осуществляемых на национальном уровне, могут быть обнаружены связи с преступлениями, относящимися к другой стране. Если органы охраны правопорядка, например, расследуют дела, связанные с оборотом криптовалюты, они могут найти информацию из других стран, которые участвовали в обмене криптовалют. Ст. 26 устанавливает положения, которые являются необходимыми для органов охраны правопорядка по информированию иностранных органов охраны правопорядка без угрозы для своего собственного расследования.

Как отмечалось выше, существуют некоторые опасения, связанные с возможной заменой взаимной правовой помощи предоставлением внеплановой информации. Обмен информацией сработает только тогда, когда государство-получатель сможет самостоятельно собрать все значимые доказательства. В любых других случаях официальное сотрудничество, как правило, необходимо так или иначе для того, чтобы обеспечить сохранность вещественных доказательств при их передаче. В дискуссиях о переходе от официальных запросов к внеплановому обмену информацией следует помнить о том, что официальные процедуры разрабатывались для защиты целостности государства, а также прав обвиняемого. Таким образом, обмен информацией не должен нарушать догматических основ взаимной правовой помощи.

Одно из наиболее важных положений ст. 26 связано с конфиденциальностью информации. В связи с тем что ряд расследований может быть проведен успешно, если преступник не знает о происходящем расследовании, ст. 26 разрешает предоставляющей стороне требовать конфиденциальности в отношении передаваемой информации. Если

конфиденциальность не может быть гарантирована, предоставляющая сторона может отказаться от информационного процесса.

Так, ст. 25 основывается на идее о том, что взаимная правовая помощь должна осуществляться на основе применения соответствующих договоров и аналогичных соглашений, а не ссылок только на настоящую Конвенцию. Составители Конвенции решили не создавать режим отдельной обязательной взаимной правовой помощи в ее рамках, если другие документы уже нашли свое место, ст. 27 и 28 не имеют отношения к конкретным запросам.

Только в тех случаях, когда другие правила не применяются, ст. 27 и 28 предусматривают ряд механизмов, которые могут быть использованы для осуществления взаимной правовой помощи.

Наиболее важные аспекты, регулируемые ст. 27, включают обязательства по созданию назначенных контактных центров для запросов на оказание взаимной правовой помощи; требование прямой связи между контактными центрами во избежание долгой процедуры и создание баз данных со всех контактных центров Генеральным секретарем Совета Европы.

Кроме того, ст. 27 определяет ограничения, относящиеся к запросам на оказание помощи. Сторона Конвенции может отказать в сотрудничестве в случае политических преступлений и/или если она считает, что сотрудничество может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим жизненно важным интересам.

Составители Конвенции видели необходимость того, чтобы стороны в некоторых случаях могли отказаться от сотрудничества, с одной стороны, а с другой, – отметили, что стороны должны осуществлять отказ от сотрудничества с осторожностью во избежание противоречий с изложенными ранее принципами. Поэтому особенно важно определить термин «другие жизненно важные интересы» в узком смысле. В пояснительном отчете к Конвенции определено, что это может быть в том случае, если сотрудничество может привести к радикальным трудностям для запрашиваемой стороны. С точки зрения составителей, проблемы, связанные с неадекватными законами о защите данных, не считаются проблемами, имеющими жизненно важное значение.

Ст. 28–33 являются отражением процессуальных документов Конвенции, которые призваны улучшить расследования в государствах-членах. Что касается принципа национального суверенитета, эти инструменты могут быть использованы только для проведения расследований на национальном уровне. Если следователи понимают, что доказательства должны быть собраны за пределами их терри-

тории, они должны сделать запрос об оказании взаимной правовой помощи. В дополнение к ст. 18, каждый из документов, установленных ст. 16–21, имеет соответствующее положение в ст. 28–33, что позволяет органам охраны правопорядка применять процессуальные документы по запросу иностранного органа охраны правопорядка.

В дополнение к чистому отражению процедурных положений составители Конвенции обсудили обстоятельства, при которых органы охраны правопорядка могут получить доступ к компьютерным данным, которые не хранятся и не находятся под контролем какого-либо лица на их территории. Им удалось договориться только о двух случаях, когда расследование должно быть проведено одним органом охраны правопорядка без необходимости в запросе об оказании взаимной правовой помощи. Дальнейшие соглашения невозможны, и даже достигнутое решение еще критикуется государствами-членами Совета Европы.

Эти два случая, когда органы охраны правопорядка могут получить доступ к данным, хранящимся вне их территории, связаны с общедоступной информацией и/или доступом с согласия управляющего лица.

Другие формы трансграничного доступа не подпадают под действие ст. 32, но также не исключаются. Ст. 32 отмечает, что, если соответствующие данные являются общедоступными, иностранные органы охраны правопорядка имеют право доступа к этой информации. Примером общедоступной является информация на веб-сайтах без контроля доступа, например, паролей. Если следователям не будет, в отличие от любого другого пользователя, разрешен доступ к этим веб-сайтам, это может серьезно затруднить их работу. Таким образом, первая ситуация, рассмотренная в ст. 32, широко распространена.

Вторая ситуация, при которой органы охраны правопорядка могут получить доступ к данным, хранящимся на компьютере за пределами их территории, – когда следователи получили законное и добровольное согласие лица, которое имеет законные полномочия раскрывать данные.

Больше всего вопросов вызывает тот факт, что вышеприведенное положение в своей текущей формулировке может противоречить фундаментальным принципам международного права, согласно которым следственные органы во время проведения расследований обязаны уважать национальный суверенитет. В частности, им не разрешается осуществлять следственные действия в другом государстве без согласия уполномоченных органов этого государства. Решение о том, давать такое согласие или нет, зависит не от какого-то отдельного лица, а от органов государственной власти, поскольку вмеша-

тельство в национальный суверенитет затрагивает не только права подозреваемого, но также интересы государства. Ратифицируя Конвенцию, страны частично пренебрегают этим принципом и позволяют другим странам проводить расследования на своей территории.

Еще одна проблема состоит в том, что ст. 32 (b) не определяет процедуры, необходимые для проведения расследований. Исходя из текста положения, во время проведения международных расследований применение тех же ограничений, которые существуют в национальном законодательстве в отношении аналогичных внутригосударственных расследований, является необязательным.

В ст. 18 составители Конвенции разрешили следственным органам требовать представления данных в рамках внутригосударственных расследований. Если бы этот инструмент разрешалось использовать следственным органам при проведении международных расследований, этого было бы достаточно, чтобы включить его в перечень инструментов, упоминаемых в контексте взаимной правовой помощи. Однако, ст. 18 нельзя применить при проведении международных расследований, поскольку в гл. 3 Конвенции отсутствует соответствующее положение, касающееся международного сотрудничества. Вместо того чтобы ослаблять фундаментальные принципы, разрешая следственным органам другой страны напрямую контактировать с лицом, владеющим определенными данными, и требовать их предъявления, авторы могли бы просто ввести в действие соответствующие положения гл. 3 Конвенции.

Главным отличием является процедура уведомления, предусмотренная в п. 6 (b). Цель положения состоит в обмене разведывательной информацией. Однако после небольших изменений такое положение могло бы гарантировать, что затрагиваемые государства будут знать о проводимых на их территории расследованиях. В этом случае противоречия международному праву не удалось бы избежать, однако была бы обеспечена определенная степень прозрачности.

Расследования цифровых преступлений часто требуют немедленной реакции. Как указывалось выше, это особенно актуально, когда речь идет о получении данных о трафике (транзакциях), которые необходимы для идентификации подозреваемых, поскольку они часто удаляются в течение довольно короткого периода времени. Для увеличения скорости международных расследований Конвенция подчеркивает важность создания условий для усиленного использования средств коммуникации в ст. 25. В целях дальнейшего повышения эффективности запросов об оказании взаимопомощи Конвенция обязывает стороны назначить контактные центры для запроса об оказании взаимопомощи, которые будут доступны

без каких-либо временных ограничений. Составители Конвенции подчеркнули, что создание контактных центров является одним из наиболее важных инструментов, предусмотренных Конвенцией. Однако недавнее исследование показывает, что в странах, ратифицировавших Конвенцию о киберпреступности, использование Сети 24/7 носит очень ограниченный характер.

Идея Сети 24/7 основана на существующей сети для круглосуточных контактов по цифровой преступности. При создании контактных центров Сети 24/7 составители Конвенции сосредоточились на решении проблем борьбы с цифровой преступностью, особенно тех, которые имеют отношение к процессам скорости обмена данными и имеют международный масштаб. Стороны Конвенции обязаны создать такие контактные центры и обеспечить возможность их немедленного реагирования, равно как и среди других основных услуг. Как указывается в подп. 3 ст. 34 Конвенции, это включает подготовку и оснащение персонала.

Относительно процесса создания контактного центра и в особенности основополагающих принципов данной структуры, Конвенция дает максимальную гибкость государствам-членам. Конвенция не требует создания нового органа и не определяет, какие из существующих органов могут или должны быть наделены полномочиями контактного центра. Составители Конвенции также указывают на тот факт, что точки Сети 24/7 предназначены для оказания как технической, так и юридической помощи, что приведет к различным вариантам возможных решений ее осуществления.

Применительно к расследованию цифровых преступлений, создание контактных центров преследует две основные цели, а именно: ускорение обмена информацией в результате обращения в единый контактный центр и ускорение расследований путем предоставления контактному центру полномочий по немедленному проведению определенных следственных действий. Сочетание двух функций является потенциалом для приближения скорости международных расследований к уровню, достигаемому в рамках национальных расследований.

Ст. 32 Конвенции определяет минимально необходимые показатели узла сети. Помимо технической помощи и предоставления правовой информации, основные задачи контактного пункта включают сохранение данных, сбор доказательств и определение местоположения подозреваемых.

В этом контексте еще раз важно подчеркнуть, что эта Конвенция не определяет, какой орган должен отвечать за эксплуатацию контактного центра 24/7. Если контактным центром управляет один орган, обладающий компетенцией в целях сохранения данных, а иностран-

ный контактный центр запросил такие данные, эта мера может быть немедленно выполнена местным контактным центром. Если контактный центр находится в ведении органа, который не является самостоятельно компетентным в целях сохранения данных, важно, чтобы контактный центр имел возможность сразу обратиться в компетентные органы для обеспечения немедленного осуществления этой меры.

На втором совещании комитета Конвенции было четко указано, что участие в работе сети связи 24/7 не требует подписания и ратификации Конвенции.

Совет Европы проанализировал эффективность международного сотрудничества в борьбе с цифровой преступностью. Была дана оценка эффективности функционирования контактных центров 24/7 по противодействию цифровой преступности. Было констатировано, что не все страны, ратифицировавшие Конвенцию, создали действующие контактные центры, как того требует Конвенция. Помимо этого, выяснилось, что те страны, которые все-таки их создали, используют контактные центры в очень ограниченных целях, таких, например, как сохранение данных о трафике.

Краткий анализ международного опыта противодействия преступной деятельности с использованием криптовалюты позволил прийти к выводу о том, что в данном направлении на международном уровне проделан значительный объем работы.

В настоящее время правовая база в сфере киберпространства и противодействия преступности в сфере цифровых технологий в полной мере не отвечает современным требованиям. Это обусловлено существованием ряда проблем, в т. ч. и правового характера. Отсутствие единого подхода и легального толкования сущности цифровых технологий и криптовалют на международном уровне не способствуют принятию законодательных решений по определению криптовалют на региональном уровне.

Пока не выработаны базовые документы на международном уровне, положенные в основу формирования нормативно-правовых актов, направленных на противодействие преступной деятельности с использованием криптовалюты, но следует признать, что уже предпринят ряд шагов в этом направлении (Четырнадцатый Конгресс ООН). Заметную роль в предупреждении преступной деятельности с использованием криптовалюты играют международные органы и организации.

В этой связи нельзя не отметить работу по противодействию преступной деятельности с использованием криптовалюты Интерпола, Европола и ФАТФ. Они не только осуществляли и продолжают осуществлять подготовку методических рекомендаций, проведение конференций и обучающих семинаров, но и оказывают

серьезную помощь в раскрытии и расследовании тяжких преступлений в экономической сфере, в т. ч. легализации (отмывании) преступных доходов, в финансировании терроризма, торговле людьми, незаконном обороте оружия и наркотиков, и других преступлений, проводят мониторинг преступной деятельности с использованием криптовалюты, расширяют сотрудничество с международными организациями правоохранительной направленности и пр.

ФАТФ с момента ее создания в сфере противодействия легализации (отмыванию) преступных доходов, финансирования терроризма и предотвращения финансирования распространения оружия массового уничтожения проделала значительный объем работы, заложив международные правовые и институциональные основы противодействия легализации (отмывания) преступных доходов, финансирования терроризма в тесной взаимосвязи с иными международными организациями, разработала эффективный механизм мониторинга.

Вместе с тем эффективное регулирование, надзор и правоприменение в отношении криптовалюты и лиц, оказывающих услуги в сфере виртуальных активов, требуют глобального подхода и международного уровня нормативной базы в разных юрисдикциях, которая позволила бы снизить риски, связанные с легализацией (отмыванием) преступных доходов и противодействием финансированию терроризма.

Как свидетельствуют результаты исследования, практика взаимодействия по противодействию противоправному использованию криптовалюты требует разработать на международном уровне правовые инструменты, необходимые для международного сотрудничества и оказания взаимной правовой помощи, для обмена информацией, для проведения расследований и осуществления иного международного сотрудничества, связанного с противоправным использованием виртуальной валюты и пр.

Контрольные вопросы

1. Назовите основные направления международного сотрудничества по предупреждению преступной деятельности с использованием криптовалюты.
2. Какие инструменты противодействия преступной деятельности с использованием криптовалюты разработаны на международном уровне?
3. Каковы особенности международного опыта противодействия преступной деятельности с использованием криптовалюты?

Заключение

Анализ международного опыта противодействия преступной деятельности с использованием криптовалюты позволил прийти к выводу о том, что в данном направлении на международном уровне проделан значительный объем работы. Но, несмотря на это, пока не выработаны базовые документы, которые могли бы быть положены в основу формирования нормативно-правовых актов, направленных на противодействие преступной деятельности с использованием криптовалюты, хотя следует признать, что уже предпринят ряд шагов в этом направлении.

Заметную роль в предупреждении преступной деятельности с использованием криптовалюты играют международные органы и организации. В этой связи нельзя не отметить взаимодействие по противодействию преступной деятельности с использованием криптовалюты Интерпола, Европола и ФАТФ. Они не только создали методическую базу, но и продолжают развивать деятельность по подготовке методических рекомендаций, проводят научно-практические семинары, активно выполняют контролирующие функции в рамках своих компетенций.

Вместе с тем эффективное регулирование, надзор и правоприменение в отношении криптовалюты и лиц, оказывающих услуги в сфере виртуальных активов, требуют глобального подхода и международного уровня нормативной базы в разных юрисдикциях, которая позволила бы снизить риски, связанные с преступной деятельностью с использованием криптовалюты, легализацией (отмыванием) преступных доходов и противодействием финансированию терроризма.

Список литературы

Международные документы

XIII Программа правовой реформы (Thirteenth Program of Law Reform. Law Com №. 377). URL: https://www.lawcom.gov.uk/project/13th-programme-of-law-reform/ (дата обращения: 20 марта 2020).

Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 20 марта 2020).

Виртуальные валюты. Руководство по применению риск-ориентированного подхода. Июль 2015 г. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (дата обращения: 28 марта 2020).

Восьмой Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, Гавана, 27 августа – 7 сентября 1990 г. URL: https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/001_ACONF.144.INF.1_Information_for_Participants_R.pdf (дата обращения: 26 марта 2020).

Всемирный доклад о наркотиках, 2017 год: Взаимосвязь между наркотиками и организованной преступностью, незаконными финансовыми потоками, коррупцией и терроризмом. URL: https://www.unodc.org/doc/wdr2017/WDR2017_Booklet5_Russian.pdf (дата обращения: 25 марта 2020).

Декларация о сотрудничестве в рамках европейского партнерства в сфере блокчейн-технологий (принята в г. Брюсселе 10 апреля 2018 г.). URL: http: www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=57270#03891223908118764 (дата обращения: 02.12.2019).

Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», Женева, 2003 г. URL: https://online.zakon.kz/Document/?doc_id=30170561#pos=7;129 (дата обращения: 20.11.2019).

Директивы ЕС 2015/849 и 2009/138/ЕС и 2013/36/ЕС13 о предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского Парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского Парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской Комиссии. URL: https://base.garant.ru/71279458/ (дата обращения: 02.05.2020).

Доклад Конференции Организации Объединенных Наций по проблеме незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах, Нью-Йорк, 9–20 июля 2001 г. (A/CONF.192/15), гл. IV, п. 24. URL: https://undocs.org›pdf?symbol=ru/A/RES/74/60/ (дата обращения: 12.05.2020).

Доклад ООН: криптовалюты и блокчейн – это «важная часть глобальной финансовой системы». URL: http://cryptoconsulting.info/ru/doklad-oon-kriptovalyutyi-i-blokcheyn-eto-vazhnaya-chast-globalnoy-finansovoy-sistemyi/ (дата обращения: 12.05.2020).

Итоги Саммита G20: криптовалюты важны для глобальной экономики, но необходимо регулирование и налогообложение. URL: https://btcinfor.com/mine/itogi-sammita-g20-kriptovalyuty-vajny-dlia-globalnoi-ekonomiki-no-neobhodimo-regylirovanie-i-nalogooblojenie.html (дата обращения: 12.05.2020).

Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. (с изм. от 28 января 2003 г.) // СПС «КонсультантПлюс».

О признании утратившим силу распоряжения Президента РФ от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» [Электронный ресурс]: распоряжение Президента РФ от 22 марта 2008 г. № 144-рп. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=417185#05091896676102123 (дата обращения: 18.11.2019).

Обзор мирового экономического и социального положения, 2018 год: передовые технологии в интересах устойчивого развития. URL: https://www.un.org/development/desa/dpad/publication/обзор-мирового-экономического-и-соци/ (дата обращения: 02.05.2020).

Применение риск-ориентированного подхода для банковского сектора: Руководство ФАТФ. URL: https://eurasiangroup.org/files/FATF_docs/Rukovodstvo_FATF_ROP_v_bankovskom_sektore.pdf (дата обращения: 28.05.2020).

Публичное заявление о виртуальных активах и связанных с ними провайдерах. URL: http://www.fedsfm.ru/content/files/bulleten38_ru_print.pdf/ (дата обращения: 12.06.2020).

Рамочное решение Совета от 13 июня 2002 г. «О европейском ордере на арест и процедурах передачи лиц между государствами-членами» (2002/584/JAI). URL: http://eulaw.edu.ru/documents/legislation/law_defence/euro_order.htm#_ftnref1/ (дата обращения: 12.06.2020).

Регулирование виртуальных активов. URL: https://cbr.ru/counteraction_m_ter/international/fatf/doc_fatf/ (дата обращения: 12.06.2020).

Резолюция Совета Безопасности ООН, принята Советом Безопасности на его 5244-м заседании 29 июля 2005 г. URL: https://undocs.org/ru/S/RES/1617(2005)/ (дата обращения: 02.06.2020).

Резолюция 2462 (2019), принята Советом Безопасности на его 8496-м заседании 28 марта 2019 г. URL: http://www.fedsfm.ru/content/files/documents/international/2019/s_res_2462(2019)_r.pdf/ (дата обращения: 02.06.2020).

Резолюция 69/196 Генеральной Ассамблеи, приложение. URL: https://maintenance.un.org/ (дата обращения: 17.05.2020).

Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 января 1999 г. URL: https://www.ifap.ru/ofdocs/un/5753.pdf (дата обращения: 20.11.2019).

Резолюция Европарламента от 16 февраля 2017 г. 2015/2013(INL) P8_TA-PROV (2017)0051, включает текст Хартии робототехники. URL: http://robopravo.ru/riezoliutsiia_ies (дата обращения: 28.11.2019).

Рекомендации ФАТФ (FATF) по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг в сфере виртуальных активов (VASP). Отчет. URL: https://mgimo.ru/upload/2020/02/rekomendacii-fatf-fatf-po-regulirovaniyu-oborota-virtualnyh-aktivov-i-deyatelnosti-provajderov-uslug-v-sfere-virtualnyh-aktivov.pdf/ (дата обращения: 22.05.2020).

Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / пер. с англ. Москва: МУМЦФМ, 2012.

Решение ЕС от 6 апреля 2009 г. № 2009/371/ПВД «О создании Европейского полицейского ведомства (Европол)». URL: http://docs.pravo.ru/document/view/24869591/ (дата обращения: 22.05.2020).

Руководство «О риск-ориентированном подходе в секторе виртуальных активов и провайдеров услуг в сфере виртуальных активов», июнь 2019 г. URL: https://mumcfm.ru/biblioteka/mezdunarodnye-dokumenty/fatf/ (дата обращения: 12.06.2020).

Руководство «О цифровой идентификации личности» от 6 марта 2020 г. URL: www.fatf-gafi.org (дата обращения: 02.06.2020).

Совместный доклад ФАТФ и Группы Эгмонт «Сокрытие информации о бенефициарных собственниках», июль 2018 г. URL: https://cbr.ru/Content/Document/File/48583/FATF-Egmont-Concealment-beneficial-ownership.pdf/ (дата обращения: 18.06.2020).

Соглашение о сотрудничестве между Российской Федерацией и Европейской полицейской организацией (заключено в Риме 6 ноября 2003 г.) // СПС «КонсультантПлюс».

Устав Международной организации уголовной полиции (ИНТЕРПОЛ) (вступил в силу 13 июня 1956 г., с изм. по сост. на 1 января 1986 г.). URL: https://base.garant.ru/1306105// (дата обращения: 27.05.2020).

Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Киото, Япония, 20–27 апреля 2020 г. URL: https://undocs.org/ru/A/RES/69/313 (дата обращения: 20.06.2020).

Морнографии, учебники, учебные пособия

Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2001.

Ларина Е. С., Овчинский В.С. Искусственный интеллект. Большие данные. Преступность. Москва: Книжный мир, 2018.

Овчинский В.С. Кибервойны XXI века (О чем умолчал Эдвард Сноуден). Москва: Книжный мир, 2014.

Овчинский В.С. Криминал будущего уже здесь. Москва: Книжный мир, 2018.

Овчинский В.С. Технологии будущего против криминала. Москва: Книжный мир, 2017.

Овчинский В.С. Криминология цифрового мира: учебник. Москва: Норма: ИНФРА-М, 2018.

Уткин В.А. Международное право борьбы с преступностью. Томск: Изд-во НТЛ, 2017.

Уткин В.А. Международное право борьбы с преступностью: учеб. пособие. Москва: ЮСТИЦИЯ, 2019.

Диссертации

Мелкумян К.С. Эффективность деятельности Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в противодействии финансированию терроризма: дис. ... канд. полит. наук. 2019.

Статьи

Ализаде В.А. Оборот криптовалюты в Европейском союзе: на пороге правового регулирования // Библиотека криминалиста. Научный журнал. 2018. № 2 (37).

Асмаков А. Европол и Интерпол объединили усилия в борьбе с отмыванием денег через криптовалюты. URL: https://forklog.

com/evropol-i-interpol-obedinili-usiliya-v-borbe-s-otmyvaniem-deneg-cherez-kriptovalyuty/(дата обращения: 20.06.2020).

Болотаева О.С. Основные направления правового регулирования систем распределенного реестра в условиях формирования цифровой экономики // Вестник СВФУ им. М.К. Аммосова. 2017. № 4 (08).

Быкова Е.В. Проблемы и перспективы сотрудничества Российской Федерации с международными организациями в сфере уголовного судопроизводства // Международное уголовное право и международная юстиция. 2016. № 5.

Генеральный секретарь ООН Антониу Гутерриш (Ant*ó*nio Guterres) уверен, что возглавляемая им организация должна применять технологию блокчейна. URL: https://coinspot.io/technology/oon-kriptovalyuty-otkryvayut-novye-gorizonty-v-cifrovyh-finansah/ (дата обращения: 20.04.2020).

Глава МВФ: регулирование операций с криптовалютами неизбежно. URL: https://incrussia.ru/news/glava-mvf-regulirovanie-operatsij-s-kriptovalyutami-neizbezhno/ (дата обращения: 20.06.2020).

Глава Организации Объединенных Наций рекламирует технологию блокчейна как важнейший компонент эпохи цифровых технологий: URL: https://cryptonews.one/blockchain/glava-organizacii-obedinennykh-nacijj-reklamiruet-tekhnologiju-blokchejjna-kak-vazhnejjshijj-komponent-ehpokhi-cifrovykh-tekhnologijj/ (дата обращения: 20.06.2020).

Давыдов Д. Интерпол придумал, как бороться с киберпреступностью. URL: https://teknoblog.ru/2018/07/06/90797 (дата обращения: 20.06.2020).

Демидов О. Связанные одним блокчейном: Обзор международного опыта регулирования криптовалют // Индекс безопасности. 2015. № 2 (113).

Достов В.Л. Консультации ФАТФ с частным сектором: диалог продолжается // Финансовая безопасность. 2014. № 5.

Европол анализирует Bitcoin-преступления в новом докладе. URL: https://bits.media/evropol-analiziruet-bitcoin-prestupleniya-v-novom-doklade/ (дата обращения: 27.05.2020).

Желудков М.А. Особенности реализации в России международного опыта по защите от корыстных преступлений, совершаемых в киберпространстве // Вестник экономической безопасности. 2016. № 5.

Интерпол создает собственную криптовалюту. URL: https://ru.secnews.gr/92170/Интерпол-создает-собственную-криптовалюту/ (дата обращения: 20.06.2020).

Интерпол усилит борьбу с криминальным использованием криптовалюты в дарквебе. URL: https://novator.io/blokchejn/interpol-usilit-borbu-s-kriminalnym-ispolzovaniem-kriptovalyuty-v-darkvebe (дата обращения: 20.06.2020).

Исламов Р. А., Акаев А. М. Интерпол в борьбе с международной преступностью // Вестник Евразийской юридической академии им. Д. А. Кунаева. 2012.

Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / отв. ред. М. Б. Касенова; сост. О. В. Демидов и М. Б. Касенова. Москва: Статут, 2013.

Кузнецов И. Сотрудничество государств в борьбе с наркоманией в рамках Совета Европы// URL: http://www.observer.materik.ru/observer/N10_2007/ 044_052.pdf (дата обращения: 20.06.2020).

Ларина Е., Овчинский В. С. Криптовалюта, блокчейн и преступность. URL: https://zavtra.ru/blogs/kriptovalyuta_blokchejn_i_prestupnost_ (дата обращения: 20.06.2020).

Лукоянов Н. В. Правовые аспекты заключения, изменения и прекращения смарт-контрактов // Юридические исследования. 2018. № 11.

МВФ и Всемирный банк выпустили собственную криптовалюту. URL: https://ru.ihodl.com/topnews/2019-04-15/mvf-i-vsemirnyj-bank-vypustili-sobstvennuyu-kriptovalyutu/ (дата обращения: 20.06.2020).

МВФ и Всемирный банк обучат сотрудников работе с криптовалютами через Learning Coin. URL: https://decenter.org/ru/mvf-i-vsemirnyi-bank-learning-coin (дата обращения: 20.06.2020).

МВФ признает факт важности криптовалюты в мировой финансовой системе. URL: https://mining-cryptocurrency.ru/mvf-kriptovalyuty-v-mirovoj-finansovoj-sisteme/ (дата обращения: 20.06.2020).

Международный альянс J5 будет бороться с «криптовалютной угрозой» в сфере отмывания денег и уклонения от налогов. URL: https://news.myseldon.com/ru/news/index/191224059 (дата обращения: 20.06.2020).

Новикова О. Европол и Интерпол повысят меры по борьбе с отмыванием денег через криптовалюты. URL: https://zen.yandex.ru/media/freedmanclub/evropol-i-interpol-povysiat-mery-po-borbes-otmyvaniem-deneg-cherez-kriptovaliuty-5a70fc4b3dceb766bcd8fbc1 (дата обращения: 20.06.2020).

Новый, бессрочный мандат ФАТФ. URL: http://www.fedsfm.ru/content/files/bulleten38_ru_print.pdf (дата обращения: 14.05.2020).

Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем и финансированию терроризма. 1–30 июня 2020 г. // Банк России. 2020. Июнь.

Общая информация (сотрудничество в сфере борьбы с преступностью и незаконным оборотом наркотических средств в СНГ). URL: http://www.cis.minsk.by/page.php?id=18780 (дата обращения: 20.06.2020).

ООН обвиняет Северную Корею в обтывании денег через криптовалюты. URL: https://crypto-news.space/kriptovalyuty/oon-obvinyaet-severnuyu-koreyu-v-obmyvanii-deneg-cherez-kriptovalyuty/ (дата обращения: 20.06.2020).

ООН: блокчейн и криптовалюты – новый рубеж в бизнесе и госуправлении. URL: https://roskomsvoboda.org/44455// (дата обращения: 02.05.2020).

Пять стран начинают совместную борьбу с финансовыми преступлениями с участием криптовалют. URL: https://bits.media/pyat-stran-nachinayut-sovmestnuyu-borbu-s-finansovymi-prestupleniyami-s-uchastiem-kriptovalyut/ (дата обращения: 20.06.2020).

Северная Корея накапливает криптовалюту для оружейных программ. URL: https://neovesting.com/security/оон-северная-корея-накапливает-крипт/2019/08/06/ (дата обращения: 20.06.2020).

Сегодня группа FATF опубликовала финальную версию рекомендаций по регулированию криптовалют и деятельности операторов криптовалютных сервисов. URL: https://bits.media/finalnaya-versiya-rekomendatsiy-fatf-birzhi-kriptovalyut-budut-obyazany-obmenivatsya-informatsiey-o-/ (дата обращения: 20.06.2020).

США возглавили международный альянс силовиков по борьбе с отмыванием денег. URL: https://hashtelegraph.com/ssha-vozglavili-mezhdunarodnyj-aljans-cilovikov-po-borbe-s-otmyvaniem-deneg/ (дата обращения: 14.06.2020).

Теткин М. Нил Уолш, ООН: криптовалюты помогают террористам. URL: https://www.rbc.ru/crypto/news/5d68caa79a79472991ab5e9c (дата обращения: 14.06.2020).

Тропина Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3.

ФАТФ опубликовала рекомендации по развертыванию систем цифровой идентификации. URL: https://bits.media/fatf-opublikovala-rekomendatsii-po-razvertyvaniyu-sistem-tsifrovoy-identifikatsii (дата обращения: 27.05.2020).

Филиппова И.А. Правовое регулирование искусственного интеллекта: регулирование в России, иностранные исследования и практика // Государство и право. 2018. № 9.

Зарубежная литература

Council Decision 2009/902/JHA of 30 November 2009 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA. URL: http://eur-lex.europa.eu/ (дата обращения: 18.05.2020).

B.S. Alper, J.F. Boren with a Forew by W. Clifford. Crime: International Agenda. Concern and Action in the Prevention of Crime and Treatment of Offenders, 1946–1972. United Nations. Toronto – London, 1972. P. 24.

FATF Report to G20 Finance Ministers and Central Bank Governors. P. 3–4.

Electronic Communications Privacy Act of 1986, ECPA. URL: http://dorothy.as.arizona.edu/ LAW/ref5.html (дата обращения: 05.05.2019).

Money-Laundering and Globalization // Официальный сайт ООН. URL: http://www.unodc.org/unodc/en/money-laundering/globalization.html (дата обращения: 18.05.2020).

Site of the Council of Europe. URL: https://search.coe.int (дата обращения: 05.01.2020).

State Cybersecurity Strategies. URL: https://www.securitylab.ru (дата обращения: 05.05.2019).

The European Crime Prevention Network (EUCPN). URL: http://www.rikoksentorjunta.fi/ (дата обращения: 05.05.2019).

The National Strategy to Secure Cyberspace. URL: http://www.whitehouse.gov/pcipb/ (дата обращения: 15.04.2019).

United Nations, Treaty Series, vol. 823, No. 11806. URL: https://www.un-ilibrary.org/united-nations/treaty-series-2518_a6f68f29-en-fr (дата обращения: 15.04.2019).

United Nations, Treaty Series, vol. 993, No. 14537. URL: https://www.un-ilibrary.org/united-nations/treaty-series-2331_6bc2d018-en-fr (дата обращения: 15.04.2019).

Список рекомендованных Интернет-ресурсов

https://мвд.рф – официальный сайт МВД России.

http://genproc.gov.ru/ – официальный сайт Генеральной прокуратуры Российской Федерации.

http://www.vsrf.ru/ – официальный сайт Верховного Суда Российской Федерации.

http://www.gks.ru/ – официальный сайт Федеральной службы государственной статистики (Росстат).

http://www.chinaspace.ru – информационный ресурс «China Space».

http://www.garant.ru – информационно-правовой портал «Гарант».

http://www.consultant.ru – справочно-правовая система «КонсультантПлюс».

Приложения

Приложение 1

Генеральная Ассамблея. Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию

Киото, Япония, 20–27 апреля 2020 г. Проведение Конгресса перенесено в связи с пандемией COVID–19 на сентябрь 2021 г.

(Проект. Извлечение)

Руководство для дискуссий

Семинар-практикум 4. Современные тенденции в области преступности, последние изменения и новые решения, в частности – использование современных технологий как средства совершения преступлений инструмента борьбы с преступностью

Содержание

Стремительное развитие технологических инноваций, распространение новых информационно-коммуникационных технологий и расширение доступа к ним, а также беспрецедентный прогресс в таких областях, как информатика, робототехника и искусственный интеллект преобразовали общества во всем мире или способны сделать это. В то же время достижения в области информационно-коммуникационных технологий могут быть использованы для совершения уголовных преступлений, либо для деяний, направленных непосредственно против компьютерных данных и систем, или деяний, связанных с компьютерами, либо для облегчения взаимодействия и контактов между преступниками. Технологии и глобализация позволяют преступникам координировать их действия между регионами как никогда прежде, расширяя круг деятельности, преступлений и жертв, а также помогая увеличить прибыль. Если хищение данных или повреждение информации представляет собой одно из направлений преступной деятельности, то другое направление состоит в использовании технологий для непосредственного содействия деятельности организованных преступных групп. Незаконная деятельность, основанная на применении передовых техноло-

гий, является столь же разнообразной, как и сами технологии. Ядерный шантаж можно привести в качестве примера наиболее серьезной преступной угрозы, связанной с применением технологий, а телефонное мошенничество или киберпреступность в целях традиционных форм нарушения закона являются примерами преступлений «меньшего воздействия», для совершения которых требуются современные технологии.

Однако, как представляется, прогресс в развитии технологий имеет как негативные последствия, так и положительный эффект: хотя он может расширить возможности для преступников, он также способствует достижению целей, изложенных в Повестке дня в области устойчивого развития на период до 2030 г. Так, в области верховенства права как важнейшего фактора устойчивого развития технологический прогресс помогает укрепить общественную безопасность и обеспечить надлежащее отправление правосудия, облегчая работу правоохранительных органов и системы уголовного правосудия в области предупреждения, выявления и пресечения преступности. Для этого можно использовать арсенал высокотехнологичных устройств, таких как дротики, оснащенные приборами слежения глобальной навигационной спутниковой системы (GPS) и используемые при преследовании автомобиля подозреваемого, и трехмерное изображение места преступления. Кроме того, рост зависимости общества от Интернета и возможность общения с помощью компьютеров побудили правоохранительные органы разработать методы расследования правонарушений в режиме реального времени или использовать, например, компьютерные программы, специально разработанные для анализа картины преступления. Правоохранительные органы также используют социальные сети для налаживания взаимодействия и отношений с местными общинами и привлечения общественности к сотрудничеству в проведении уголовных расследований. Кроме того, в суде можно использовать доказательства, полученные с помощью таких инноваций, как видеонаблюдение, современные методы дактилоскопии или экспертиза ДНК, для более эффективного рассмотрения уголовного дела или обеспечения того, чтобы подверженные опасности потерпевшие могли давать показания, не опасаясь угроз. Национальные компетентные органы все чаще сталкиваются с трудностями при осуществлении мер по борьбе с транснациональными организованными преступными группами, которые имеют в своем распоряжении передовые информационные технологии. Самая насущная задача состоит в обеспечении необходимой адаптации мер уголовного правосудия и правоохранительных органов, с тем

чтобы они могли надлежащим образом бороться с преступлениями, совершаемыми с помощью таких технологий.

В силу очевидной роли технологий в создании благоприятных условий для совершения преступлений, в изменении форм преступности и в мерах противодействия, принимаемых обществом в целях охраны правопорядка и обеспечения безопасности, необходимы согласованные усилия для предотвращения использования этих технологий в преступных целях или его адекватного пресечения. На международном уровне, в п. 3 ст. 27 Конвенции об организованной преступности предусмотрено, что государства должны стремиться сотрудничать с целью противодействия транснациональным организованным преступлениям, совершаемым с использованием современных технологий На национальном уровне все больше внимания уделяется правовым мерам и укреплению потенциала наряду со стратегическим планированием, что может также включать, в соответствующих случаях, партнерские отношения между государственным и частным сектором.

В связи с этим представляют интерес шесть тематических областей, некоторые из которых взаимосвязаны друг с другом, и ниже они классифицируются по условным признакам для того, чтобы лучше понять влияние и роль технологий как в качестве фактора, способствующего преступности, так и в качестве средства защиты от нее. Эти тематические области добавляются к другой соответствующей тематической области, т. е. более широкому использованию информационно-коммуникационных технологий для террористических целей, которая рассматривается в рамках п. 6 повестки дня в настоящем руководстве. Все из них можно описать с помощью сравнения с Янусом: люди могут воспользоваться преимуществами технологий, при этом рискуя столкнуться с их негативной стороной, как у двуликого бога Януса в древнеримской мифологии.

1. Криптовалюта

Криптовалюты, определяемые как конвертируемые, действующие между равноправными субъектами, децентрализованные сетевые цифровые валюты, в т. ч. биткоин и эфириум, используют методы криптографии для регулирования генерации денежных единиц и проверки перевода средств, обращаясь при этом независимо от Центрального банка. Обеспеченная ими высокая степень анонимности в сочетании с низким уровнем обнаружения позволяет избежать многих рисков, связанных с операциями по отмыванию денежных средств и финансированию терроризма, и, таким

образом, создает благоприятные условия для совершения этих преступлений в виртуальной среде. Кроме того, криптовалюты могут облегчить совершение других преступлений, таких как вымогательство и мошенничество.

Следовательно, использование криптовалют является испытанием на способность компетентных органов принимать адекватные меры регулирования и укреплять международное сотрудничество с учетом также законного применения технологии биткоина, включая использование криптовалют в качестве средства сохранения сбережений и способа оплаты законных товаров и услуг. Поэтому крайне важно, чтобы государства рассмотрели возможность разработки междисциплинарных стратегий (включая меры регулирования, директивные инициативы по предупреждению и подготовку сотрудников компетентных органов) с целью решения проблем и повышения потенциала для успешного и эффективного расследования и судебного преследования в соответствующих делах. Такие меры будут способствовать выполнению, насколько это применимо в виртуальной среде, задачи сокращения масштабов незаконных финансовых потоков, связанных с различными формами преступности, включая транснациональную организованную преступность.

В рамках своей Глобальной программы борьбы с киберпреступностью УНП ООН разработало курс обучения специалистов по расследованиям, связанным с криптовалютами, и активно проводило подготовку в области расследований по криптовалютам в различных регионах. Цель подготовки состоит в повышении уровня квалификации сотрудников правоохранительных органов, прокуроров и судей с целью более глубокого понимания, что такое криптовалюта, отслеживания биткоинов при проведении финансовых расследований, поиска ресурсов для получения дополнительной информации и взаимодействия в изучении материалов международных судебных дел. Кроме того, УНП ООН налаживает партнерские отношения с субъектами сектора регулятивных технологий (“RegTech”) и сектора финансовых технологий (“FinTech”) и сотрудничает с отраслевыми лидерами в области криптовалют, такими как Chainalysis Inc., для оказания помощи сотрудникам правоохранительных органов и аналитикам в отслеживании незаконных финансовых потоков.

Хотя в настоящее время в этой области существуют ходы, технологии, лежащие в основе криптовалют, они открывают некоторые потенциально интересные возможности для следователей. Некоторые аспекты технологии «блокчейн», которые позволяют существо-

вать биткоину и другим цифровым криптовалютам, могут сделать его полезным инструментом правоприменения. Помимо выявления подозрительных транзакций, правоохранительные органы могут также использовать программное обеспечение технологии «блокчейн» для сбора доказательств.

2. Роль технологий в создании рынков наркотиков с низким уровнем риска

Темный сегмент Интернета открывает новые возможности для незаконного оборота наркотиков, поскольку он позволяет пользователям покупать наркотики с использованием криптовалюты и получать купленный товар скрытым образом. Таким образом, он выступает в качестве анонимного открытого рынка, что позволяет розничным наркоторговцам преодолевать географические ограничения закрытых внесетевых рынков наркотиков и потенциально расширять распространение наркотиков. Кроме того, анонимный характер этого сегмента снижает риск ареста как дилеров, так и пользователей, а также устраняет опасности, связанные с покупкой наркотиков, такие как возможность стать жертвой других форм преступности в окрестностях, где процветает торговля наркотиками[1]. Несмотря на распространение и феноменальный рост, темный сегмент Интернета по-прежнему составляет, согласно *Всемирному докладу о наркотиках, 2017 г.*, лишь незначительную часть мирового объема торговли наркотиками. Тем не менее он открывает новые возможности для «ведения бизнеса» и еще больше меняет характер незаконной торговли наркотиками и категории ее участников, когда все более значительными становятся более самостоятельные горизонтальные сети и более мелкие группы.

С правоохранительной точки зрения, потенциальные способы выявления торговли наркотиками с помощью Интернета включают традиционные методы расследования, применяемые в отношении поставок наркотиков; выявление и перехват почтовых отправлений; и обнаружение, и пресечение операций в онлайновом режиме. Расследование и уголовное преследование в соответствующих случаях требуют наличия специальных навыков проведения уголовного

[1] Взаимосвязь между наркотиками и организованной преступностью, незаконными финансовыми потоками, коррупцией и терроризмом // Всемирный доклад о наркотиках, 2017 г. (издание Организации Объединенных Наций, в продаже под № R.17.XI.11). С. 19.

расследования, которые должны применяться в виртуальной среде. Возросшая зависимость от компьютерных технологий вызвала необходимость в создании специальных подразделений по борьбе с киберпреступностью, которые должны отвечать на просьбы об экспертном поиске доказательств с помощью компьютера и, таким образом, повысить оперативные возможности государства в решении соответствующих проблем.

3. Незаконный оборот огнестрельного оружия в темном сегменте Интернета

Все большее внимание уделяется потенциальной роли темного сегмента Интернета в облегчении незаконного оборота огнестрельного оружия и боеприпасов через рынки криптовалют и интернет-магазины поставщиков.

Правоохранительные органы сталкиваются с рядом оперативных проблем в борьбе с этим явлением. Хотя некоторые из указанных проблем возникают в связи с техническими функциями темного сегмента Интернета, другие могут быть преодолены с помощью активного участия заинтересованных сторон, занимающихся разработкой политики, как на национальном, так и на международном уровне. На национальном уровне директивные ведомства должны обеспечить, чтобы правоохранительные органы были укомплектованы кадрами, подготовлены для эффективного противодействия и соответствующим образом оснащены. Возможно, потребуется рассмотреть вопрос о принятии стратегий в области образования и профилактики.

На международном уровне эффективные меры борьбы с незаконным оборотом огнестрельного оружия в темном сегменте Интернета также основаны на строгом соблюдении существующих международных документов, направленных на решение общей проблемы незаконного оборота оружия, таких как Протокол против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему, дополняющий Конвенцию об организованной преступности, и Договор о торговле оружием. На уровне мер профилактики и обеспечения безопасности важно уменьшить незаконные поступления и оборот огнестрельного оружия через темный сегмент Интернета. Соответствующие меры предусмотрены в применимых международно-правовых документах и служат основой для разработки комплексных подходов к борьбе с этим явлением.

4. Роль технологий в торговле людьми

Технологии традиционно применяются в ущерб жертвам торговли людьми. Торговцы используют социальные сети, веб-сайты, анонимные приложения и сети для вступления в контакт со своими жертвами и их вербовки и без затруднений общаются на анонимной основе с покупателями и участниками сговора в рамках своего объединения, контролирующего рынок торговли людьми. Однако в то же время технологический прогресс открывает правоохранительным органам беспрецедентные возможности для отслеживания незаконной деятельности, поиска и спасения жертв торговли, сбора и анализа данных, необходимых для уголовного преследования лиц, занимающихся такой торговлей, и упрощения взаимодействия между субъектами и учреждениями по борьбе с торговлей людьми.

Для обеспечения эффективности расследования и уголовного преследования важно иметь более полное представление о масштабах и способах использования технологий торговцами, жертвами и потребителями на различных этапах процесса торговли людьми (вербовка, провоз или передача, размещение, осуществление финансовых операций, реклама и методы контроля).

Основанные на технологиях меры по борьбе с торговлей людьми требуют сотрудничества между секторами в целях рационализации усилий, направленных на выполнение задачи 8.7, установленной в Повестке дня на период до 2030 года, и, насколько это применимо, задачи 17.17. Просветительские кампании среди общественности и прочные партнерские отношения между государственным и частным сектором должны основываться на общем понимании потенциальных результатов применения инновационных технологий в борьбе с торговлей людьми.

5. Связь современных информационных технологий с надругательствами над детьми и эксплуатацией детей

Расширение доступа детей к информационно-коммуникационным технологиям в сочетании с их незащищенностью и неспособностью в полной мере осознать угрозы, связанные с неправильным использованием таких технологий, являются причиной резкого увеличения числа случаев надругательств и эксплуатации в отношении детей.

Хотя использование информационно-коммуникационных технологий в преступлениях в отношении детей создает много проблем, в т. ч. в том, что касается выявления и установления личности преступника, оно может также обеспечить системе уголовного

правосудия ряд возможностей в плане расследования и сбора доказательств. Как подчеркивается в исследовании УНП ООН "Effects of New Information Technologies on the Abuse and Exploitation of Children" («Последствия применения современных информационных технологий в аспекте надругательств и эксплуатации в отношении детей»), следователи, разбирающиеся в цифровых технологиях, имеют все больше возможностей для получения электронных доказательств надругательств с помощью информационно-коммуникационных технологий, выявления жертв и предоставления им поддержки и помощи.

В рамках усилий по выполнению задачи 16.2, которая состоит в том, чтобы положить конец надругательствам и эксплуатации в отношении детей, меры по борьбе с надругательствами и эксплуатацией в отношении детей с помощью информационно-коммуникационных технологий требуют участия многочисленных сторон для активного вовлечения детей, семей, общин, правительств, гражданского общества и частного сектора.

6. Роль технологий в расследовании дел, связанных с незаконным ввозом мигрантов

Наряду с ошеломляющим ростом незаконного ввоза мигрантов, который наблюдался в последние годы, также резко возросла степень изощренности этого вида преступности. Лица, занимающиеся незаконным ввозом мигрантов, используют новейшие коммуникационные технологии в целях получения информации об изменении мер пограничного контроля и адаптации к ним и, в ответ на меры ограничения, они быстро меняют свои маршруты.

Социальные сети и цифровые коммуникации обеспечивают лицам, занимающимся незаконным ввозом мигрантов, невиданный способ поставок: возможность осуществлять прямой сбыт и привлекать клиентов с помощью современных социальных сетей, а также в меньшей степени зависеть от местных посредников.

С другой стороны, внедрение цифровых технологий явно сокращает информационные пробелы, которыми могут воспользоваться лица, занимающиеся незаконным ввозом мигрантов. Мобильные и сетевые технологии можно использовать для оказания помощи мигрантам, с тем чтобы они могли установить контакты в важнейших социальных сетях для получения поддержки и информации. Кроме того, надлежащее использование технологий может помочь правительствам, деловым кругам и неправительственным организациям в предотвращении и смягчении последствий этого бедствия.

Отчет ФАТФ к саммиту лидеров G20: 28–29 июня 2019 г.

1. Под председательством Японии Группа двадцати продолжала выражать свою поддержку ФАТФ в целях содействия быстрому и эффективному осуществлению стандартов ФАТФ во всем мире. Группа двадцати вновь заявила о своей поддержке ФАТФ как глобального органа по борьбе с отмыванием денег, финансированием терроризма (ПОД/ФТ) и нормотворчеством в области финансирования распространения и приветствовала его постоянные усилия по укреплению своей институциональной базы. Группа двадцати также призвала ФАТФ активизировать свои усилия по противодействию финансированию распространения и просила ФАТФ разъяснить, каким образом ее стандарты применяются к финансовой деятельности виртуальных активов и связанным с ней поставщикам.

2. Под председательством США, с 1 июля 2018 г. ФАТФ успешно выполнила призыв G20 к уточнению глобальных стандартов регулирования и надзора за финансовой деятельностью и поставщиками виртуальных активов, с тем чтобы помочь странам разработать эффективные рамки ПОД/ФТ, балансируя при этом инновации и финансовую доступность.

3. ФАТФ уделила приоритетное внимание своей деятельности по борьбе с финансированием терроризма и принятию дополнительных мер по борьбе с финансированием распространения оружия массового уничтожения. ФАТФ также проводит работу по поддержке использования цифровых удостоверений личности и продолжает содействовать обеспечению прозрачности и доступности информации о бенефициарных владельцах.

4. 12 апреля 2019 г. министры ФАТФ согласовали открытый мандат ФАТФ и подтвердили ее роль в руководстве глобальными действиями по борьбе с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения. Принятие открытого мандата в связи с 30-й годовщиной ФАТФ отражает тот факт, что эти угрозы представляют собой непреходящую угрозу целостности финансовой системы и что необходима устойчивая политическая приверженность.

5. В новой министерской декларации и мандате ФАТФ признается необходимость того, чтобы ФАТФ продолжала руководить решительными, скоординированными и эффективными глобальными действиями по противодействию злоупотреблениям финансовой системой со стороны преступников и террористов и укреплять

свой потенциал реагирования на эти угрозы, с которыми сталкиваются все страны.

6. Министры определили приоритетные задачи ФАТФ по борьбе с этими угрозами, а также по укреплению ее руководства и потенциала. Они приняли открытый мандат для подтверждения того, что эти угрозы являются непреходящими проблемами и что необходима устойчивая политическая приверженность. Министры также приняли решение проводить встречи каждые два года, договорились продлить срок полномочий председателя ФАТФ (президента и вице-президента) до двухлетнего периода и договорились о более сильной модели финансирования организации.

7. Это ключевые инициативы, которые позволят повысить эффективность ФАТФ в глобальном масштабе и повысить ее авторитет и известность среди глобальных органов управления и соответствующих заинтересованных сторон. Эти усовершенствования направлены на признание и развитие более широкого участия ФАТФ в международных форумах, в т. ч. в рамках G7/G20, органов ООН и региональных органов типа ФАТФ, а также на поддержку реагирования ФАТФ на текущие и возникающие угрозы и возможности.

8. После принятия министрами ФАТФ открытого мандата ФАТФ проведет стратегический обзор своей основной работы, с тем чтобы обеспечить ее пригодность в будущем и поддержать дальнейшие усилия по повышению ее эффективности в качестве ведущего глобального органа по установлению стандартов в области предотвращения отмывания денег, финансирования терроризма и финансирования распространения и борьбы с ними.

Программа работы ФАТФ виртуальные активы (криптовалюты)

9. Технологические инновации, в т. ч. лежащие в основе виртуальных активов, таких как блокчейн и другие технологии распределенной бухгалтерской книги, могут принести значительные выгоды финансовой системе и экономике в целом. Это включает в себя потенциальные выгоды для расширения доступа к финансовым услугам и трансграничные денежные переводы.

10. Однако виртуальные активы также создают серьезные риски отмывания денег и финансирования терроризма, которыми пользуются преступники, отмыватели денег, террористы и другие незаконные субъекты. В июне 2019 г. ФАТФ завершила разработку руководства по финансовым расследованиям, связанным с виртуальными активами, для правоохранительных и других оперативных

органов, в котором рассматривается рассматривается ряд проблем передовой практики, связанных с выявлением, расследованием и конфискацией случаев, касающихся виртуальных активов, когда преступники используют виртуальные активы в целях отмывания денег и финансирования терроризма.

11. В октябре 2018 г. ФАТФ приняла изменения к своим рекомендациям, чтобы четко разъяснить, что они применяются в случае финансовой деятельности, связанной с виртуальными активами, и к соответствующим поставщикам услуг. ФАТФ также добавила в глоссарий два новых определения: «виртуальный актив» и «поставщик услуг виртуальных активов». Измененная рекомендация 15 ФАТФ требует, чтобы поставщики услуг виртуальных активов регулировались для целей ПОД/ФТ, лицензировались или регистрировались и подчинялись эффективным системам мониторинга или надзора.

12. С тех пор ФАТФ приняла пояснительную записку к рекомендации 15 в июне 2019 г. В пояснительной записке излагаются обязательные меры для эффективного регулирования и надзора или мониторинга поставщиков услуг виртуальных активов. Это требует, в частности: применения риск-ориентированного подхода к финансовой деятельности виртуальных активов и поставщикам услуг виртуальных активов; лицензионных или регистрационных обязательств. ФАТФ использует термин «виртуальные активы» для обозначения цифровых представлений стоимости, которые могут быть проданы в цифровом формате или переданы и могут использоваться для платежных или инвестиционных целей, охватывая как конвертируемые, так и неконвертируемые, централизованные и децентрализованные формы, а также первоначальные предложения монет. Это включает в себя, но шире, чем криптоактивы, как их обычно называют в G20, компетентный орган страны, а не саморегулируемый орган, обладающий достаточными полномочиями, в т. ч. для проведения инспекций и принуждения к производству информации; ряд эффективных, соразмерных и сдерживающих санкций в отношении поставщиков услуг по виртуальным активам, которые не соответствуют их требованиям в области ПОД/ФТ, включая полномочия надзорных органов отзывать, ограничивать или приостанавливать действие лицензии или регистрации поставщиков услуг по виртуальным активам; применение всех превентивных мер ФАТФ, включая должную осмотрительность клиентов, ведение учета и мониторинг подозрительных операций, в частности, поставщиками услуг по обслуживанию виртуальных активов; обеспечение максималь-

но широкого круга международного сотрудничества между странами, особенно между надзорными органами.

13. В июне 2019 г. ФАТФ также выпустила Руководство по применению риск-ориентированного подхода к виртуальным активам и поставщикам услуг виртуальных активов. В обновленном руководстве далее разъясняется применение требований ФАТФ в контексте виртуальных активов и поставщиков услуг виртуальных активов (а также для других обязанных организаций, которые занимаются финансовой деятельностью, продуктами или услугами по виртуальным активам или предоставляют их поставщикам). Они призваны помочь как национальным органам власти в понимании и разработке нормативных и надзорных мер в отношении деятельности по виртуальным активам и поставщиков услуг по виртуальным активам, так и организациям частного сектора, стремящимся участвовать в деятельности или операциях по виртуальным активам, в понимании своих обязательств по ПОД/ФТ и того, как они могут эффективно выполнять эти требования.

14. ФАТФ немедленно приступит к работе по пересмотру своей методологии оценки в соответствии со своими новыми пересмотренными стандартами. Эта работа будет продолжаться в приоритетном порядке, с тем чтобы ФАТФ могла приступить к оценке соблюдения странами новых стандартов, применимых к виртуальным активам и поставщикам виртуальных активов.

15. В свете стремительного развития ряда финансовых функций, выполняемых виртуальными активами, ФАТФ рассмотрит вопрос о выполнении странами и поставщиками услуг требований, применимых к виртуальным активам и поставщикам услуг виртуальных активов, в июне 2020 г. Это будет включать в себя мониторинг выполнения новых требований на национальном уровне, мониторинг прогресса поставщиков услуг виртуальных активов в разработке технологических решений для безопасного представления информации об отправителе/бенефициаре между поставщиками услуг виртуальных активов при осуществлении передачи виртуальных активов и оценку необходимости дальнейшего обновления для обеспечения того, чтобы стандарты ФАТФ оставались актуальными и эффективными. ФАТФ также создала контактную группу, которая будет заниматься промышленностью и контролировать отраслевые усилия по повышению соответствия стандартам ФАТФ и лучшей защите окружающей среды.

Борьба с финансированием терроризма

16. Терроризм по-прежнему представляет собой серьезную угрозу глобальному миру и безопасности, от которой не застрахован ни один регион. Несмотря на территориальное поражение ИГИЛ в Ираке и Сирии, оно продолжает представлять угрозу, вдохновляя и потенциально проводя нападения по всему миру. Подрыв финансовых потоков ИГИЛ, Аль-Каиды и других террористических организаций, и отдельных террористов остается одним из наиболее эффективных способов выявления и пресечения террористической деятельности.

17. Резолюция 2462 Совета Безопасности ООН, принятая в марте 2019 г., подчеркивает важность международного сообщества в борьбе с финансированием терроризма и центральную роль ФАТФ в установлении глобальных стандартов и мониторинге рисков финансирования терроризма. Однако оценки ФАТФ показали, что большинство стран не имеют адекватного представления о своих рисках финансирования терроризма и примерно две трети из них не имеют возможности эффективно расследовать и преследовать в судебном порядке деятельность по финансированию терроризма.

18. В период председательства США ФАТФ уделяла приоритетное внимание работе в трех областях: эффективное осуществление, понимание рисков и межведомственная координация. ФАТФ подготовила и опубликовала руководящие указания, призванные помочь странам оценить и понять свои риски в области ТФ, а также провела глобальный семинар, призванный помочь повысить способность стран эффективно осуществлять судебное преследование за финансирование терроризма.

19. ФАТФ решила сосредоточить свой следующий этап работы на развитии потенциала стран по пониманию риска финансирования терроризма, повышении эффективности осуществления стандартов ФАТФ и поддержке развития режимов борьбы с финансированием терроризма и активизации диалога в регионах с более высоким риском. В соответствии с этими приоритетами, ФАТФ подготовит руководящие указания по эффективному расследованию и судебному преследованию случаев финансирования терроризма, а также оценит, каким образом ФАТФ может поддержать разработку режимов борьбы с финансированием терроризма в регионах с высоким уровнем дохода.

20. ФАТФ будет продолжать совершенствовать эффективное осуществление стандартов ФАТФ. Он будет и впредь привлекать

страны к ответственности за неспособность устранить свои недостатки путем публикации надежных и всеобъемлющих докладов о взаимной оценке и последующей деятельности, а также публично перечислять те страны со стратегическими недостатками, которые представляют опасность для глобальной финансовой системы.

Противодействие 21. Финансирование распространения оружия массового уничтожения остается одной из ключевых угроз международному миру и безопасности. Совет Безопасности ООН уже давно признал эту угрозу, что нашло отражение в многочисленных резолюциях, призывающих уделять больше внимания мерам по борьбе с финансированием распространения. ФАТФ по-прежнему привержена продолжению дальнейшей работы по укреплению глобальных ответных мер по борьбе с финансированием распространения оружия массового поражения.

22. Под эгидой США. Председательствуя в июне 2019 г., ФАТФ согласилась продолжить дальнейшую работу по укреплению стандартов ФАТФ по противодействию финансированию распространения оружия массового поражения, требуя от юрисдикций и организаций частного сектора понимания и смягчения их рисков, а также повышения требований к внутреннему сотрудничеству и координации в области их финансирования. ФАТФ провела обширный анализ целого ряда предложений, но согласилась с тем, что эта работа будет продвигаться вперед в приоритетном порядке. Другие рассмотренные варианты включали новые требования к использованию мер уголовного правосудия и финансовой разведки, расширению инструментов целенаправленных финансовых санкций и более эффективных механизмов обеспечения международной информации, обмена информацией о деятельности по финансированию распространения оружия массового поражения. ФАТФ согласилась потенциально рассмотреть эти и другие варианты на более позднем этапе.

23. ФАТФ будет продолжать повышать прозрачность и доступность информации о бенефициарных собственниках посредством продолжения работы в этой области, процесса ее взаимной оценки и сотрудничества с глобальным форумом по вопросам транспарентности и обмена информацией для целей налогообложения.

24. ФАТФ опубликовала Руководство по риск-ориентированному подходу для юристов, бухгалтеров и поставщиков услуг трастовых компаний в июне 2019 г. Основное внимание уделяется тому, как эти профессии должны применять гарантии, основанные на риске, чтобы предотвратить злоупотребление их услуг преступниками; и как надзорные органы должны предотвра-

щать деятельность соучастников или небрежных профессионалов. Эта работа проводилась в партнерстве с частным сектором.

25. С февраля 2019 г. ФАТФ занимается выявлением наилучшей практики в отношении бенефициарного владения, опираясь на практические примеры, представленные ее делегациями, и свои взаимные оценки на сегодняшний день. Это будет способствовать осуществлению юрисдикциями эффективных мер по обеспечению того, чтобы юридические лица не использовались не по назначению для отмывания денег и финансирования терроризма.

26. На консультативном форуме частного сектора ФАТФ, состоявшемся 6–7 мая 2019 г., участники обменялись мнениями о ключевых особенностях различных систем и обменялись мнениями о ключевых факторах эффективной системы содействия прозрачности бенефициарной собственности в соответствии со стандартами ФАТФ. С учетом замечаний государственного и частного секторов, ФАТФ продолжит работу над этим проектом, который, как ожидается, будет опубликован к концу текущего года.

Цифровая идентичность 27. ФАТФ признает финансовые инновации и решительно поддерживает ответственные технологические разработки, которые укрепляют национальные механизмы борьбы с отмыванием денег и финансированием терроризма. Цифровая идентификация имеет потенциал для расширения доступа к финансовым услугам и снижения затрат на привлечение клиентов, а также для более эффективного управления рисками отмывания денег и финансирования терроризма.

28. В рамках работы по приоритетной повестке дня G20 на тему «Возможности и вызовы финансовых инноваций» ФАТФ, совместно с МВФ и G20, провела 2 апреля 2019 г. специальную совместную сессию по финансовым технологиям, борьбе с отмыванием денег и финансированием терроризма. Эта сессия высветила целый ряд возможностей и проблем, возникающих в связи с финансовыми технологиями в области борьбы с отмыванием денег и финансированием терроризма.

29. Консультативный форум частного сектора ФАТФ от 2019 г. предоставил дополнительную возможность для обмена мнениями о том, как частный сектор может шире использовать технологии (такие как машинное обучение, интеллектуальный анализ данных, искусственный интеллект) для управления рисками ПОД/ФТ, содействия должной осмотрительности клиентов, скрининга санкций и других мер. Особое внимание уделено мониторингу транзакций, а также тому, как государственные органы используют новые технологии для повышения эффективности и результативности.

30. ФАТФ готовит Руководство по применению рекомендаций ФАТФ в отношении должной осмотрительности клиентов в контексте цифровых удостоверений личности. Хотя стандарты ФАТФ являются технологически нейтральными, это руководство направлено на обеспечение комфорта для тех, кто стремится использовать ответственные инновации, разъясняя, как цифровые формы идентификации, верификации и аутентификации могут использоваться в процессе должной осмотрительности клиентов. В руководстве будут рассмотрены возможности, предоставляемые этой технологией, включая расширение доступа к финансовым услугам, а также освещены потенциальные риски и меры по их смягчению. Данные материалы были опубликованы в марте 2020 г.

31. В более широком плане ФАТФ продолжает отслеживать риски и возможности финансовых инноваций для обеспечения того, чтобы стандарты ФАТФ оставались актуальными и гибкими, и ФАТФ отчитается о своей деятельности перед Группой двадцати в 2021 г.

32. Снижение риска остается сложной задачей для ряда стран, секторов и предприятий по всему миру. Хотя факторы снижения риска носят сложный характер, ФАТФ активно разъясняет стандарты ФАТФ, чтобы избежать недоразумений, которые могут способствовать снижению риска. Кроме того, ФАТФ вносит свой вклад в глобальные усилия по решению проблемы сокращения объема банковских услуг в секторе денежных переводов, поскольку потоки денежных переводов являются ключом к обеспечению жизнедеятельности людей в ряде стран.

33. ФАТФ рассматривает решение проблемы снижения риска как стратегический приоритет для международного сообщества. В июне 2019 г. ФАТФ обсудила обновленную информацию о международных усилиях по мониторингу и решению проблем снижения риска, в т. ч. в рамках инициатив ФСБ, МВФ, Всемирного банка и региональных органов ФАТФ в стиле ЦГФМ. ФАТФ будет продолжать следить за этими тенденциями и вносить свой вклад в международные усилия в этой области.

34. ФАТФ надеется внести свой вклад в работу «Большой двадцатки» под председательством Японии и Королевства Саудовская Аравия и доложить о своем прогрессе по этим вопросам министрам финансов «Большой двадцатки» и управляющим центральными банками, а также на следующем саммите лидеров «Большой двадцатки».

Приложение 3

Официальное заявление ФАТФ о виртуальных активах и провайдерах услуг в сфере виртуальных активов, 21 июня 2019 г. (Извлечение)

Орландо, Флорида, США, 21 июня 2019 г. Публичное заявление о виртуальных активах и связанных с ними поставщиках Целевая группа по финансовым мероприятиям (ФАТФ) сегодня приняла и опубликовала пояснительную записку к Рекомендации 15 о новых технологиях (МНО. 15), которая дополнительно разъясняет предыдущие поправки ФАТФ к международным стандартам, касающимся виртуальных активов, и описывает то, каким образом страны и обязанные субъекты должны соблюдать соответствующие рекомендации ФАТФ по предотвращению неправомерного использования виртуальных активов для отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения.

Ранее, в октябре 2018 г., ФАТФ обновила свои стандарты, чтобы уточнить их применение к виртуальным активам и поставщикам услуг виртуальных активов, внеся поправки в Рекомендацию 15 и добавив два новых определения в глоссарий ФАТФ. Совет Безопасности ООН приветствовал эти и другие продолжающиеся усилия ФАТФ по решению проблемы регулирования и надзора за деятельностью в области виртуальных активов и поставщиками услуг в области виртуальных активов, в т. ч. в своей резолюции 2462 от 28 марта 2019 г. Сегодняшние действия ФАТФ основаны на этих событиях. Она устанавливает обязательные меры, имеющие отношение как к странам, так и к поставщикам услуг виртуальных активов (а также к другим обязанным субъектам, которые занимаются или предоставляют продукты и услуги виртуальных активов), с тем чтобы создать более равные условия для всех участников экосистемы виртуальных активов.

Эти обязательства требуют от стран оценивать и смягчать свои риски, связанные с деятельностью виртуальных актив. Далее, Рекомендация 15 требует от стран обеспечить, чтобы поставщики услуг также оценивали и снижали свои риски отмывания денег и финансирования терроризма и осуществляли полный комплекс превентивных мер ПОД/ФТ в соответствии с рекомендациями ФАТФ, включая должную осмотрительность клиентов, ведение учета, отчетность о подозрительных сделках и проверку всех сделок на предмет соблюдения целевых финансовых санкций среди про-

чих мер, как и другие субъекты, подпадающие под регулирование ПОД/ФТ. Это включает в себя координацию с соответствующими органами для обеспечения совместимости требований ПОД/ФТ с правилами защиты данных и конфиденциальности, и аналогичными положениями. Кроме того, сегодня ФАТФ опубликовала обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов, основанное на новаторском руководящем документе ФАТФ за 2015 г., с тем чтобы еще больше помочь странам и поставщикам продуктов и услуг виртуальных активов понять и выполнить свои обязательства по ПОД/ФТ.

Угроза преступного и террористического неправомерного использования виртуальных активов является серьезной и неотложной, и ФАТФ ожидает, что все страны примут оперативные меры для выполнения рекомендаций ФАТФ в контексте деятельности по использованию виртуальных активов и поставщиков услуг. ФАТФ будет следить за выполнением новых требований странами и поставщиками услуг и проведет 12-месячный обзор в июне 2020 г.

Развитие МНО. 15 и обновленное руководство в значительной степени выиграло от диалога с частным сектором для лучшего понимания технологии, лежащей в основе виртуальных активов и их различных типов, связанных с ними бизнес-моделей, существующих технологических решений для потенциального повышения соответствия требованиям ПОД/ФТ, а также рисков отмывания денег и финансирования терроризма, которые злоупотребляют виртуальными активами, – что может происходить в отсутствие эффективного регулирования, надзора и отраслевого контроля ПОД/ФТ. Как ФАТФ, так и ее члены будут продолжать диалог с частным сектором по мере того, как правительства и промышленность будут выполнять рекомендации ФАТФ, с тем чтобы обеспечить эффективное реагирование на эти риски.

ФАТФ создаст контактную группу для привлечения промышленности и контроля за предпринимаемыми под ее руководством усилиями по улучшению соблюдения стандартов ФАТФ и более эффективной защите международной финансовой системы от злоупотреблений. Министры финансов и управляющие центральными банками на встрече G20 в Фукуоке приветствовали и выразили свою поддержку действиям ФАТФ по регулированию и надзору за виртуальными активами и поставщиками услуг виртуальных активов. Сегодня ФАТФ успешно выполнила призыв «Большой двадцатки» к регулированию и надзору за деятельностью виртуальных активов и связанных с ними поставщиков услуг в области ПОД/ФТ, а так-

же к дальнейшему уточнению ожиданий ФАТФ относительно того, как страны должны разрабатывать надежные механизмы ПОД/ФТ в этой связи. ФАТФ будет продолжать принимать меры по обеспечению эффективного регулирования и надзора за использованием новых технологий, в т. ч. в контексте виртуальных активов, в целях снижения связанных с этим рисков отмывания денег и финансирования терроризма, и поддержки ответственных инноваций в секторе финансовых услуг.

Париж, Франция, 19 октября 2018 г. Виртуальные активы и связанные с ними финансовые услуги обладают потенциалом для стимулирования финансовых инноваций и повышения эффективности и расширения доступа к финансовым услугам, но они также создают новые возможности для преступников и террористов отмывать свои доходы или финансировать свою незаконную деятельность. Поэтому ФАТФ активно отслеживает риски в этой области и в 2015 г. выпустила Руководство по применению риск-ориентированного подхода к виртуальным валютам. Существует настоятельная необходимость в том, чтобы все страны приняли скоординированные меры по предотвращению использования виртуальных активов в преступных и террористических целях.

Рекомендации ФАТФ устанавливают всеобъемлющие требования по борьбе с отмыванием денег и финансированием терроризма, которые применяются ко всем формам финансовой деятельности, включая те, которые используют виртуальные активы. Однако правительства и частный сектор обратились с просьбой о большей ясности в отношении того, к каким именно видам деятельности применяются стандарты ФАТФ в этом контексте. Подход, основанный на учете рисков, требует от юрисдикций выявления рисков отмывания денег и финансирования терроризма и принятия соответствующих мер по снижению этих рисков. Это включает в себя выявление и смягчение рисков незаконного финансирования, связанных с новыми продуктами или деловой практикой, а также другие виды деятельности, прямо не упомянутые в рекомендациях ФАТФ.

Учитывая настоятельную необходимость эффективного глобального, основанного на учете рисков реагирования на риски ПОД/ФТ, связанные с финансовой деятельностью, которая, в свою очередь, связана с виртуальными активами, ФАТФ приняла изменения к рекомендациям и глоссарию ФАТФ, которые разъясняют, как эти рекомендации применяются в случае финансовой деятельности, связанной с виртуальными активами. Эти изменения добавляют в глоссарий новые определения «виртуальных активов» и «поставщиков услуг виртуальных активов» – таких как биржи,

некоторые типы поставщиков кошельков и поставщиков финансовых услуг для первичного размещения монет (ICO). Эти изменения четко указывают на то, что юрисдикции должны обеспечить, чтобы поставщики услуг виртуальных активов подпадали под действие правил ПОД/ФТ, например, проведение должной проверки клиентов, включая постоянный мониторинг, ведение учета и отчетность о подозрительных сделках. Они должны быть лицензированы или зарегистрированы и подлежать мониторингу для обеспечения соответствия требованиям. ФАТФ дополнительно уточнит, каким образом эти требования должны применяться в отношении виртуальных активов.

Все юрисдикции должны в срочном порядке принять правовые и практические меры для предотвращения неправомерного использования виртуальных активов. Это включает в себя оценку и понимание рисков, связанных с виртуальными активами в их юрисдикциях, применение основанных на рисках правил ПОД/ФТ к поставщикам услуг виртуальных активов и определение эффективных систем для проведения основанного на рисках мониторинга или надзора за поставщиками услуг виртуальных активов. Некоторые юрисдикции уже регулируют деятельность с виртуальными активами в соответствии с руководством 2015 г. Сегодняшние разъяснения к стандартам ФАТФ в значительной степени совместимы с их существующими нормативными требованиями. ФАТФ подчеркивает, что юрисдикции обладают гибкостью в принятии решений о том, в рамках какой категории регулируемых видов деятельности должны регулироваться поставщики услуг виртуальных активов, например, в качестве финансовых учреждений, DNFBPs или в качестве другой, отличительной категории.

ФАТФ использует термин «виртуальный актив» для обозначения цифровых представлений стоимости, которые могут быть проданы в цифровом виде или переданы и могут использоваться для платежных или инвестиционных целей, включая цифровые представления стоимости, которые функционируют в качестве средства обмена, расчетной единицы и/или хранилища стоимости. ФАТФ подчеркивает, что виртуальные активы отличаются от фиатной валюты (она же «реальная валюта», «реальные деньги» или «национальная валюта»), которая является деньгами страны, обозначенной в качестве ее законного платежного средства.

Рекомендации ФАТФ требуют мониторинга или надзора только для целей ПОД/ФТ и не подразумевают, что поставщики услуг виртуальных активов подпадают (или должны быть) под гарантии стабильности или защиты потребителей/инвесторов, а также

не подразумевают каких-либо гарантий защиты потребителей или инвесторов. В настоящее время поставщики услуг по обслуживанию виртуальных активов в большинстве юрисдикций не регулируются в целях обеспечения финансовой стабильности или защиты инвесторов и потребителей.

Стандарты ФАТФ позволяют юрисдикциям запрещать определенные виды деятельности, основанные на риске и сфере охвата в этой юрисдикции (например, казино в юрисдикциях, где азартные игры являются незаконными), и при условии соблюдения запрета не требуют от юрисдикций принятия мер по регулированию этих запрещенных видов деятельности. Некоторые страны могут принять решение о запрете виртуальных активов, основываясь на своей собственной оценке риска.

ФАТФ будет предоставлять разъяснения юрисдикциям в области управления рисками ОД и ТФ виртуальных активов, одновременно создавая надежную регулятивную среду ПОД/ФТ, в которой компании могут свободно внедрять инновации. В условиях поэтапного подхода, ФАТФ подготовит обновленное Руководство по основанному на риске подходу к регулированию деятельности поставщиков услуг виртуальных активов, включая их надзор и мониторинг; а также руководство для оперативных и правоохранительных органов по выявлению и расследованию незаконной деятельности, связанной с виртуальными активами.

В свете быстрого развития ряда финансовых функций, выполняемых виртуальными активами, ФАТФ также рассмотрит сферу деятельности и операций, охватываемых измененными рекомендациями и глоссарием в течение следующих 12 мес. и рассмотрит вопрос о необходимости дальнейшего обновления для обеспечения того, чтобы стандарты ФАТФ оставались актуальными.

Действия ФАТФ по выявлению и пресечению финансирования ИГИЛ, «Аль-Каиды» и их филиалов

Действия ФАТФ по выявлению и пресечению деятельности ИГИЛ, «Аль-Каиды» и ее филиалов, финансирующих Республику Конго, а также по всему миру, свидетельствуют о том, что, несмотря на свое территориальное поражение в Ираке и Сирии, ИГИЛ продолжает расширять свою сеть, совершая нападения на ни в чем не повинных гражданских лиц и разрушая мирные общества. Кроме того, «Аль-Каида» и ее филиалы остаются угрозой международной стабильности и безопасности, от которой не застрахован ни один регион.

Для оказания поддержки своим государствам-членам в борьбе с финансированием этих террористических организаций целевая группа по финансовым мероприятиям (ФАТФ) создала механизм, который будет способствовать пониманию рисков финансирования терроризма (ТФ), исходящих от ИГИЛ. Публичный доклад ФАТФ, озаглавленный «Финансирование террористической организации: Исламское государство в Ираке и Леванте» (февраль, 2015 г.), стал первым итогом этих учений. Эти усилия были расширены в октябре 2017 г., чтобы охватить «Аль-Каиду», а также филиалы обеих групп. С 2015 г. ФАТФ регулярно публикует закрытые обновленные данные для оперативных органов и разведывательных служб, которые обеспечивают оперативное информирование органов всей глобальной сети ФАТФ о смене деятельности ТФ, связанной с этими группами, а также о мерах, принимаемых юрисдикциями для борьбы с сопутствующими рисками.

На пленарном заседании ФАТФ в Орландо, штат Флорида, в июне 2019 г. ФАТФ приняла свою десятую обновленную информацию о финансировании ИГИЛ, «Аль-Каиды» и связанных с ними группировок. В связи с устойчивым международным давлением в течение последних лет, включая осуществление ряда мер, предусмотренных стандартами ФАТФ (например, трансграничные правоохранительные усилия, целенаправленные финансовые санкции и т. д.), ИГИЛ наблюдает значительное снижение своих доходов. Это привело к фундаментальному сдвигу в финансовой структуре ИГИЛ к пониманию того, как основная группировка, остающаяся в Ираке и Сирии, связана со своими филиалами и филиалами по всему миру.

ИГИЛ продолжает оказывать финансовую поддержку своим филиалам, но также дает им возможность собирать свои собствен-

ные средства на местном уровне и даже полагается на некоторые филиалы для распределения средств в пределах своего собственного региона. ИГИЛ продолжает использовать сектор услуг по переводу денег или ценностей (MVTS), особенно незарегистрированных поставщиков услуг, для перемещения средств для финансирования своего терроризма по всему миру. Несмотря на свое территориальное поражение в Ираке и Сирии, ИГИЛ и связанные с ним группировки по-прежнему обладают накопленными денежными средствами и другими финансовыми ресурсами и предпринимают попытки инвестировать эти незаконные доходы в законный бизнес и другие инвестиции. Например, мы видели свидетельства того, что новая сеть ИГИЛ в Центральной Африке, возможно, пытается создать предприятия для покупки золота и продажи его на внешних рынках. «Аль-Каида» продолжает извлекать выгоду из средств, собранных в результате незаконной деятельности, а также из сочувствующих ей людей по всему миру.

ФАТФ продолжает следить за изменениями в риске ТФ, создаваемом этими и другими террористическими группами. Под председательством США ФАТФ добилась многочисленных успехов в улучшении результатов оценки рисков ТФ в глобальном масштабе; в усилении расследований и судебного преследования ТФ и других незаконных источников финансирования с помощью новых платежных методов, таких как виртуальные активы; и в содействии эффективному осуществлению стратегий срыва ТФ.

Информация и разведданные, передаваемые через механизм внутренней отчетности ФАТФ, не только способствуют пониманию рисков ТФ оперативными органами во всем мире, но и служат основой для дальнейших действий ФАТФ по борьбе с возникающими рисками ТФ. Принимая во внимание недавно принятую Резолюцию 2462 СБ ООН, которая требует от государств-членов срывать и криминализировать финансирование терроризма в любых целях, даже при отсутствии связи с конкретным террористическим актом, членам глобальной сети ФАТФ настоятельно рекомендуется использовать результаты этих обновлений и продолжать принимать быстрые и скоординированные меры по борьбе с ТФ в соответствии со стандартами ФАТФ. ФАТФ будет продолжать оказывать поддержку государственным органам посредством распространения информации о текущем риске ТФ сведений об ИГИЛ, «Аль-Каиде» и связанных с ними группах, обеспечивающей оперативное реагирование на новые и возникающие риски ТФ по мере их развития на местах.

Учебное издание

МЕЖДУНАРОДНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Учебно-практическое пособие

Редактор *В. А. Яровая*
Верстка *А. А. Мельникова*

Подписано в печать 12.03.2021. Формат 60 x 84 $^{1}/_{16}$.
Усл. печ. л. 6,3. Уч.-изд. л. 6,05. Тираж 90 экз. Заказ № 09у.

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России.
125993, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907187-60-3