

Научная статья

Original article

УДК 343

doi: 10.55186/2413046X_2022_7_8_487

**ВЛИЯНИЕ НОВЫХ ТЕХНОЛОГИЙ НА ФИНАНСИРОВАНИЕ
ТЕРРОРИЗМА
THE IMPACT OF NEW TECHNOLOGIES ON THE FINANCING OF
TERRORISM**



Лашин Григорий Алексеевич, Финансовый университет при Правительстве РФ, г. Москва, Россия, E-mail: lashin.grigoriy@mail.ru

Охотников Илья Викторович, доцент, кандидат экономических наук, доцент кафедры «Экономическая теория и менеджмент» Российского университета транспорта (МИИТ), Россия, Москва, e-mail: roat.miit@mail.ru

Сибирко Иван Владимирович, доцент, кандидат экономических наук, доцент кафедры «Экономическая теория и менеджмент» Российского университета транспорта (МИИТ), Россия, Москва, e-mail: roat.miit@mail.ru

Lashin Grigoriy Alekseevich, Financial University under the Government of Russian Federation, Moscow, Russia

Okhotnikov Ilya Viktorovich, Docent, Candidate of Economic Sciences, Assistant Professor of the Economic Theory and Management Department of the Russian University of Transport (MIIT), Russia, Moscow

Sibirko Ivan Vladimirovich, Docent, Candidate of Economic Sciences, Assistant Professor of the Economic, Theory and Management Department of the Russian University of Transport (MIIT), Russia, Moscow

Аннотация. Данная работа посвящена изучению роли, которую новые технологии - от финтех-сервисов до социальных сетей могут играть в

процессе финансирования терроризма. Проблема финансирования терроризма вызывает растущее беспокойство международного истеблишмента, также подпитываемое нестабильной политической повесткой, что подчеркивает актуальность выбранной темы исследования. Эмпирическая база включает обзор литературы из открытых источников, научные статьи, отчеты аналитических центров и СМИ. Террористическая деятельность, вдохновленная исламистским и крайне правым экстремизмом, рассматривалась в международном контексте, учитывая транснациональный характер интернет-технологий и ограниченность освещения выбранной темы. Задачей данной работы является исследование вопроса влияния новых технологий на существующие риски финансирования терроризма. Сделан вывод о том, что финансовые технологии действительно использовались при организации и финансировании терактов, но стоит учесть, что краудфандинг в социальных сетях и виртуальные активы стали инструментами для более широкого организационного финансирования и были добавлены, а не заменили традиционные методы сбора денежных средств.

Abstract. This work is devoted to the study of the role that new technologies - from fintech services to social networks can play in the process of financing terrorism. The problem of financing terrorism is a growing concern of the international establishment, also fueled by an unstable political agenda, which underlines the relevance of the chosen research topic. The empirical base includes a review of open source literature, scientific articles, think tank and media reports. Terrorist activities inspired by Islamist and far-right extremism were considered in an international context, given the transnational nature of Internet technologies and the limited coverage of the chosen topic. The objective of this work is to study the issue of the impact of new technologies on the existing risks of terrorist financing. It is concluded that financial technology was indeed used in organizing and financing terrorist attacks, but it is worth considering that social media crowdfunding and virtual assets have become tools for broader organizational

funding and have been added to rather than replaced traditional fundraising methods.

Ключевые слова: финансовые технологии, международная безопасность, экономическая безопасность, противодействие финансированию терроризма, цифровые активы

Key words: financial technologies, international security, economic security, countering the financing of terrorism, digital assets

Введение

С момента создания британцем пакистанского происхождения Бабаром Ахмадом веб-сайта для освещения событий в Боснии и Чечне в 90-ых годах XX-го века и последующего размещения на данном сайте призывов к финансовой и иной поддержке талибов в Афганистане, использование Интернета для финансирования терроризма развивалось вместе с дальнейшей популяризацией новых интернет-технологий [11]. Ориентируясь на скорость, эффективность и положительный пользовательский опыт, в перспективе, новые технологии могут существенно снизить уровень сопротивления для действий лиц, финансирующих терроризм, посредством поддержки атак и организационной деятельности. Эта статья призвана внести свой вклад в существующую базу знаний касательно уровня реальной угрозы, формирующегося в результате эксплуатации новых технологий, и ответить на вопрос в какой степени она повлияла на появление новых и/или усугубление существующих рисков финансирования терроризма. В настоящее время, по-видимому, одержимость предполагаемыми уязвимостями новых технологий, вкупе с растущим, хотя и ограниченным, объемом доказательств, преувеличивает уровень реальной угрозы.

Финансирование терроризма: цели и методы (Terrorism financing: aims and methods)

Термин «новые технологии» широко используется, но при этом не имеет точного определения и теоретически может обозначать любой финансовый инструмент, разработанный в недавнем прошлом для

осуществления разнопланового перечня действий, начиная с обмена мгновенными сообщениями до эксплуатации систем искусственного интеллекта. Наиболее релевантный к процедуре финансирования терроризма сектор известен как «фин-тех». Представляющие его фирмы используют новые технологии для осуществления основных финансовых услуг, требующих обработки больших массивов данных, быстро, безопасно и с минимальными издержками. Отказавшись от традиционных посредников в пользу онлайн-платформ, фирмы фин-тех сектора обеспечивают себе доступ к более объемной выборке пользователей, которых привлекает удобство ведения финансовой деятельности онлайн, посредством новейших достижений в области мобильных технологий и сетей сотовой связи. Вышеупомянутые фирмы развивались практически во всех сферах обслуживания финансовой системы, включая следующие:

Таблица 1. Секторы финансовых технологий, сопряженные с риском финансирования терроризма

Цифровой банкинг	В настоящее время существует несколько хорошо зарекомендовавших себя онлайн-банков или «необанков», таких как "N26" в Германии и "Тинькофф Банк" в России. Эти банки предлагают ряд тех же услуг, что и традиционные розничные банки, но исключительно в цифровом формате.
Платежные сервисы	Американская технологическая компания Stripe, предоставляющая решения для приема и обработки платежей между физическими лицами, предприятиями и/или финансовыми учреждениями как внутри страны, так и за ее пределами.
Кредитование	предоставление целевого онлайн-кредита на личные или бизнес-цели, некоторые компании лидирующие в отрасли, такие как базирующаяся в Великобритании FundingCircle, используют подход «равный-равному» (P2P) для финансирования своих кредитов, позволяя физическим лицам кредитовать непосредственно малый и средний бизнес
Краудфандинг	Вдохновленный прогрессом микрофинансовых организаций в развивающихся странах, по принципу краудсорсинга знаний и услуг через Интернет, краудфандинг включает в себя использование специальных онлайн-платформ для продвижения индивидуальных проектов, позволяя напрямую агрегировать и быстро отправлять средства предполагаемому получателю. Средства привлекаются по принципу пожертвований и изначально были разработаны для поддержки благотворительных и иных некоммерческих мероприятий и

	организаций [4, с. 2].
Инвестиции	Инвестиционная индустрия пострадала от роста спроса на приложения, позволяющие инвесторам управлять своими портфелями напрямую или с помощью автоматических «робо-советников», а не традиционных брокеров.
Страхование	Как и в случае с инвестициями, финтех-фирмы вышли на страховой рынок с намерением использовать большие массивы данных и машинное обучение для улучшения оценки рисков и снижения страховых взносов [3, С. 3-8].
Поставщики услуг виртуальных активов (VASP)	Сектор VASP развился в следствие роста криптовалют, таких как биткойн, основанных на технологии распределенного реестра (DLT) или блокчейн. Эти валюты разрабатывались с момента зарождения Биткойна в 2008 г. и рост популярности «конфиденциальных монет» с более надежными протоколами шифрования и стейблкоинов, привязанных к базовому активу, не заставил себя ждать. Ядром сектора VASP в настоящее время являются хранение валюты в криптокошельках, а также их покупка и продажа (через биржи). Даркнет где криптовалюта является основным платежным средством, предоставляет альтернативное место для их использования.

Помимо фин-тех, необходимо также учитывать финансовую значимость социальных сетей ввиду возможности поддерживать обмен финансовой информацией способами, позволяющими финансировать терроризм. Согласно совместному отчету за 2019 год Азиатско-Тихоокеанской группы по борьбе с отмыванием денег и Группы разработки финансовых мер борьбы с отмыванием денег на Ближнем Востоке и в Северной Африке, социальные сети включают четыре субдомена: службы социальных сетей (Facebook или Twitter); услуги хостинга контента: сайты, позволяющие пользователям создавать, загружать и потреблять контент (YouTube или Vimeo); краудфандинговые услуги: сайты, позволяющие пользователям финансировать проект, запрашивая небольшие суммы у многих людей (GoFundMe и JustGiving); Интернет-мессенджеры: также известные как обмен мгновенными сообщениями (WhatsApp или Signal). Все чаще, такие службы используют сквозное шифрование, чтобы предотвратить слежку за разговорами. Некоторые даже начали внедрять услуги интернет-платежей или мобильных платежей, например, как WeChat Pay, что в

конечном итоге затрудняет процессы надзора и противодействия финансирования терроризма [8, С. 353-363].

Концептуализация финансирования терроризма и его реальные проявления имеют разительные отличия в контексте восприятия термина "новые технологии". Резолюция 2463 о противодействии финансированию терроризма, принятая Советом Безопасности ООН 28 марта 2019 года, определяет сбор, перемещение, передачу и предоставление доступа к средствам террористическим организациям как практическое понимание финансирования терроризма [10]. В то же время, Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) фокусирует внимание на целевом использовании средств "финансировании террористических актов, а также деятельности террористов и террористических организаций" [2, с. 88]. Актуальные научные труды на данную тему позволяют разрешить вышеуказанный спор посредством объединения мер, предпринимаемых лицами, финансирующими терроризм и целями ими преследуемыми для формирования более наглядного представления процесса финансирования терроризма. Мартин Навиас идентифицирует три основных категории действий [6, с. 49] (создание фондов, перевод и использование средств) - в то время как Джессика Дэвис [5, с. 5] дополняет его еще тремя ключевыми видами деятельности: сбор, использование, хранение, перемещение и сокрытие средств, а также управление фондами.

Данная интерпретация обращает внимание на то, что финансирование терроризма- это не просто кратко- и среднесрочные виды деятельности (привлечение, использование и перемещение средств) - а также и долгосрочные соображения о надзоре и управлении финансовыми ресурсами. Помимо этого, исследователи акцентируют внимание на операционном и организационном финансировании. Первое направлено на поддержку готовящихся и потенциальных атак (включая процессы подготовки боевиков, проведение исследований и разведывательной деятельности, приобретение оружия и иных материалов) [9, С. 12-23]. Организационное финансирование,

напротив, является более широкомасштабным и разноплановым по своим целям, покрывая расходы на техническое обслуживание террористических групп или сетей, вербовку обучение, оперативные нужды, создание и распространение тактической и стратегической пропаганды, а зачастую и оперативную поддержку симпатизирующих группировок. Такое разделение является основополагающим для понимания специфики финансирования терроризма, так как цели привлечения не только идентифицируют используемые виды финансовой деятельности, но при более детальном рассмотрении определяют типы финансовых инструментов, которые можно задействовать. Например, финансирование отдельных атак, вероятно будет менее затратным, что исключает необходимость привлечения, использования и перемещения существенных объемов финансирования. В настоящее время такой сценарий действий наиболее характерен для Европы, учитывая степень распространения самоактивирующегося терроризма, обозначенного Европоллом (полицейская служба ЕС) главной угрозой, стоящей перед континентом [12, с. 13], а также составляющей 74% выборки атак и заговоров, в рамках анализируемого массива данных. Исследования показывают, что такие злоумышленники как правило проводят более дешевые, самофинансируемые атаки, привлекая средства законными и банальными методами, используя заработную плату, государственные льготы или частные накопления, либо за счет доходов от уголовных преступлений, таких как незаконный оборот наркотических средств.

Напротив, организационное финансирование потребует более разнообразные методы сбора денежных средств, большую часть которых будет необходимо переместить через границу и управлять ими в течение продолжительного периода времени, обращая отдельное внимание на процессы перевода, хранения и сокрытия средств. Таким образом, финансовые операции ливанской шиитской организации и политической партии Хезболла включали в себя отмывание денег через подставные предприятия и преступную деятельность [7].

Представители Хамас, Харакаташ-Шабаб и других исламистских экстремистских группировок собирают пожертвования от своих сторонников из Европы, эти денежные средства в последствие переводятся за пределы Европы с помощью курьеров, подставных компаний, банковских переводов, услуг по переводу денег и ценностей, таких как MoneyGram и Western Union, а также традиционной системы перевода ценностей «хавала», функционирующей как неформальная финансово-расчетная система на основе взаимозачета требований и обязательств между брокерами. Ультраправые группировки, проживающие в Европе, сделали то же самое, включая группировки из Финляндии и Швеции которые привлекают финансирование посредством членских взносов и пожертвований своих сторонников. Каналы косвенного организационного финансирования все чаще вызывают опасения у представителей контролирующих органов по вопросам финансирования терроризма, ведь зачастую средства переводятся в зоны конфликта, но не предназначены для финансовой поддержки операций террористической группы. В разгар территориального контроля Исламского государства (запрещенная в России террористическая организация) в Ираке и Сирии, присутствие иностранных боевиков в зоне конфликта побуждало их друзей или членов семьи переводить средства по неофициальным каналам для обеспечения благополучия своих близких. Отправители этих переводов очень редко разделяли идеологические взгляды получателей, но тем не менее, предоставление средств террористу привело к нескольким обвинительным приговорам за финансирование терроризма в ЕС. Так в 2019 году британская пара была признана виновной в финансировании терроризма за отправку 233 фунтов стерлингов через ливанского посредника их сыну, поддерживающему Исламское государство в Сирии [1, с. 2]. Совсем недавно аналогичные переводы были сделаны из Швейцарии, Швеции, Испании, Нидерландов и других европейских держав в целях финансирования возвращения иностранных боевиков на родину или поддержки лиц, содержащихся в лагерях для сторонников Исламского государства, в том

числе в целях перевода суммы выкупа контрабандистам и посредникам за вывоз женщин и детей, связанных с Исламским государством из мест содержания под стражей. Операции по извлечению стали осуществимы благодаря сложным системам обмена информации с участием связанных с ИГ и Аль-Каидой (запрещенная в России террористическая организация) террористических групп, таких как Хайат Тахрираш-Шам (запрещенная в России террористическая организация), получающих прибыль от контрабанды людей. Таким образом, в качестве исходного уровня, относительно которого можно измерить степень изменения риска, связанного с появлением и использованием новых технологий, с точки зрения оперативного финансирования терроризма в Европе преобладает самофинансирование небольшими объемами за счет мелкой преступности прочими "консервативными" способами [13, с. 4]. Организационное финансирование - более сложный процесс, зависящий от сбора пожертвований и перевода средств.

Новые технологии и их появление в этом ландшафте может разрушить устоявшуюся модель восприятия финансирования терроризма во многом так же, как они подорвали эффективность регулирующих инструментов в рамках контроля финансовой активности. В актуальной литературе и интервью на эту тему, идея новых технологий, трансформирующих процесс финансирования терроризма, выражается тремя основными способами:

- предложение новых каналов - появление множества новых поставщиков финансовых услуг, предоставляет террористам обилие возможностей для осуществления финансирования терроризма, таких как развитие формальных и неформальных краудфандинговых платформ (при использовании социальных сетей) [14];
- цифровые активы - часто воспринимаются как идеальное средство для перемещения средств, вырученных незаконной деятельностью, по причине их учета в децентрализованной системе, P2P-характера операций,

высокой скорости обращения, низкого уровня транзакционных издержек и предполагаемой анонимности, что потенциально упрощает процессы организационного финансирования;

- низкий уровень контроля - учитывая относительную незрелость большинства финтех-компаний в формировании собственных мер по борьбе с финансовыми преступлениями и рисками финансирования терроризма, с которыми они сталкиваются, очевидно, что такие платформы предоставляют возможность финансистам террористов действовать в условиях несовершенного контроля, в отличие от унаследованного финансового сектора, имеющего больше опыта в контроле за соблюдением требований ПОД/ФТ.

Исследование позволило структурировать развернувшиеся в экспертном сообществе дискуссии касательно функций, роли и влияния новых финансовых технологий на развитие процессов финансирования терроризма, а также более четко интерпретировать термин "новые технологии", не ограничивая представление исключительно на экзотических финансовых инструментах, рассмотрев риски финансирования терроризма, при условии использования этих инструментов в tandem с социальными сетями и схожими по функционалу платформами. В данной работе были выявлены основные сегменты рынка фин-тех услуг, наиболее предрасположенные к использованию в рамках финансирования терроризма, что обусловлено сложностью и новизной цифровых активов, а также их существованием вне рамок международного правового поля. Результаты исследования также указывают на острую необходимость Росфинмониторингу совместно с Советом Безопасности РФ и Национальным антитеррористическим комитетом при взаимодействии с ФАТФ разработать комплекс мер по регулированию операций с использованием цифровых активов и, в частности, криптовалюты, как инструмента наиболее подверженному риску финансирования терроризма.

Список литературы

1. Вавилов А.И. «Исламское государство»: феномен, эволюция, перспективы: Аналитические доклады / Вавилов А.И. [и др.]. Москва: МГИМО-Университет МИД РФ. Вып. 1 (45). – 2016 - 26 с.
2. Мелкумян К.С. ФАТФ в противодействии финансированию терроризма (специфика подхода) // Вестник МГИМО-Университета. – 2014 -N1. - 88 с.
3. Пичков О.Б., Уланов А.А. Риски и несовершенства развития цифровой экономики на современном этапе // Страховое дело. – 2017 - N11. - С. 3–8.
4. Francesca Di Pietro, "Deciphering Crowdfunding", in Theo Lynn et al. (eds), *Disrupting Finance: FinTech and Strategy in the 21st Century* (Cham: Palgrave Macmillan, 2019), p. 2.
5. Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (London: Lynne Rienner, 2021), p. 5.
6. Martin S Navias, *Finance & Security: Global Vulnerabilities, Threats and Responses* (London: C Hurst & Co., 2019), p. 49.
7. Matthew Levitt, "The Lebanese Hizbullah Financing Threat in Europe", Research Briefing N. 1, Project CRAAFT, 2020.
8. Michael Jacobson, "Terrorist Financing and the Internet", *Studies in Conflict and Terrorism* (Vol. 33, No. 4, 2010), P. 353–363.
9. Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Edward Elgar, 2012), P. 12-23.
10. "Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast)", July 2021 [Электронный ресурс] URL: https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.pdf (дата обращения 21.05.2022).
11. Robert Verkaik, "The Trials of Babar Ahmad: From Jihad in Bosnia to a US Prison via Met Brutality", *The Observer*, 19 March 2016. URL: <https://www.theguardian.com/uk-news/2016/mar/12/babar-ahmad-jihad-bosnia-us-police-interview> (дата обращения: 25.06.2022).

12. Stephen Reimer and Matthew Redhead, "A New Normal: Countering the Financing of Self-Activating Terrorism in Europe", RUSI Occasional Papers (May 2021), p. 13.

13. The Financing of Terrorism, Insurgency, and Irregular Warfare (Santa Barbara, CA: ABC-CLIO, 2015), p. 4.

14. Tom Keatinge, David Carlisle and Florence Keen, "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses", May 2018. URL:

[https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).(дата обращения: 24.05.2022).

References

1. Vavilov A.I. "Islamic State": Phenomenon, Evolution, Prospects: Analytical Reports / Vavilov A.I. [and etc.]. Moscow: MGIMO-University of the Ministry of Foreign Affairs of the Russian Federation. Issue. 1 (45). -2016- 26 p.

2. Melkumyan K.S. FATF in combating the financing of terrorism (specific approach) // Bulletin of MGIMO-University. - 2014 - N 1. - 88 p.

3. Pichkov O.B., Ulanov A.A. Risks and imperfections in the development of the digital economy at the present stage // Insurance business. - 2017 - N 11. - S. 3–8.

4. Francesca Di Pietro, "Deciphering Crowdfunding", in Theo Lynn et al. (eds), *Disrupting Finance: FinTech and Strategy in the 21st Century* (Cham: Palgrave Macmillan, 2019), p. 2.

5. Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (London: Lynne Rienner, 2021), p. 5.

6. Martin S Navias, *Finance & Security: Global Vulnerabilities, Threats and Responses* (London: C Hurst & Co., 2019), p. 49.

7. Matthew Levitt, "The Lebanese Hizbullah Financing Threat in Europe", Research Briefing N. 1, Project CRAAFT, 2020.

8. Michael Jacobson, "Terrorist Financing and the Internet", *Studies in Conflict and Terrorism* (Vol. 33, No. 4, 2010), pp. 353–363.

9. Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Edward Elgar, 2012), pp. 12-23.

10. "Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast)", July 2021 [Electronic resource] URL: https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.pdf (Accessed 21.05.2022).

11. Robert Verkaik, "The Trials of Babar Ahmad: From Jihad in Bosnia to a US Prison via Met Brutality", *The Observer*, 19 March 2016. URL: <https://www.theguardian.com/uk-news/2016/mar/12/babar-ahmad-jihad-bosnia-us-police-interview> (accessed 25.06.2022).

12. Stephen Reimer and Matthew Redhead, "A New Normal: Countering the Financing of Self-Activating Terrorism in Europe", *RUSI Occasional Papers* (May 2021), p. 13.

13. *The Financing of Terrorism, Insurgency, and Irregular Warfare* (Santa Barbara, CA: ABC-CLIO, 2015), p. four.

14. Tom Keatinge, David Carlisle and Florence Keen, "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses", May 2018. URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf). (dateofaccess: 05/24/2022).

Для цитирования: Лашин Г.А., Охотников И.В., Сибирко И.В. Влияние новых технологий на финансирование терроризма // *Московский экономический журнал*. 2022. № 8. URL: <https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-8-2022-37/>

© Лашин Г.А., Охотников И.В., Сибирко И.В., 2022 *Московский экономический журнал* № 8.