DOI: 10.22394/2070-8378-2019-21-1-81-85

Риски цифровизации и новые направления финансового контроля

ЭЛИНА ЛЕОНИДОВНА СИДОРЕНКО, **доктор юридических наук, доцент, профессор кафедры уголовного права, уголовного процесса и криминалистики, директор Центра цифровой экономики и финансовых инноваций, руководитель рабочей группы Государственной Думы Российской Федерации по оценкам рисков оборота криптовалюты**

Московский государственный институт международных отношений Министерства иностранных дел Российской Федерации (Российская Федерация, 119454, Москва, проспект Вернадского, 76). E-mail: 12011979@list.ru

Аннотация: В статье рассматриваются основные риски использования новых цифровых инструментов в российской и международной финансовой системе. Автор обращает особое внимание на динамику использования криптовалюты в преступных схемах: при продаже наркотиков, порнографии, при совершении мошенничества, легализации преступных доходов и финансировании терроризма. Отмечается, что пока не будут разработаны национальные и международные меры защиты от негативных тенденций, черный рынок оборота криптовалют и связанных с ним преступлений будет только расти. На основе проведенного криминологического анализа выделены основные направления деятельности по легализации новых финансовых инструментов и установлению финансового контроля за их оборотом, обращено внимание на необходимость корректировки системы финансового контроля ввиду активного развития искусственного интеллекта. Особого внимания заслуживает авторский подход к оценке рисков удаленной идентификации и использования искусственного интеллекта для подготовки финансовых заключений. Сделан вывод об отставании государственного правового регулирования от темпов развития цифрового пространства и о необходимости детальной проработки всех вопросов, связанных с цифровизацией.

Ключевые слова: цифровые финансовые активы, криптовалюта, законодательное регулирование, финансовый контроль, финансовый мониторинг

Статья поступила в редакцию 11 февраля 2019 года.

Сидоренко Э. Л. Риски цифровизации и новые направления финансового контроля. *Государственная служба.* 2019. № 1. С. 81-85.

DIGITALIZATION RISKS AND NEW DIRECTIONS OF FINANCIAL CONTROL

ELINA L. SIDORENKO, **Dr. Sci. (Law), Associate Professor**

Professor of the Chair of criminal law, criminal procedure and criminalistics, Director of the Center for Digital Economy and Financial Innovation, Head of the working group of the state Duma of the Russian Federation on cryptocurrency turnover risk assessment.

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of Russia (76, prospekt Vernadskogo, Moscow, Russian Federation, 119454). E-mail: 12011979@list.ru

Abstract: The article discusses the main risks of using new digital tools in the Russian and international financial system. The author pays special attention to the dynamics of the use of cryptocurrency in criminal schemes: the sale of drugs, pornography, fraud, money laundering and terrorist financing. It is noted that until national and international measures are developed to protect against negative trends, the black market for the circulation of cryptocurrencies and related crimes will only grow. On the basis of the conducted criminological analysis, the main activities for the legalization of new financial instruments and the establishment of financial control over their turnover were highlighted; attention was drawn to the need to adjust the financial control system due to the active development of artificial intelligence. Special attention should be given to the author's approach to assessing the risks of remote identification and using artificial intelligence to prepare financial statements. It was concluded that the state legal regulation is lagging behind the pace of development of the digital space and the need for a detailed study of all issues related to digitalization.

Keywords: digital financial assets, cryptocurrency, legislative regulation, financial control, financial monitoring

The article was received on February 11, 2019.

Sidorenko, E. L., Digitalization risks and new directions of financial control. *Gosudarstvennaya sluzhba*. 2019. № 1. P. 81-85. In Russian

Риски использования новых финансовых инструментов

Вопросы развития цифровой экономики находятся в центре внимания российской экономической политики. Однако, признавая важность и своевременность внедрения цифровых технологий в систему государственного управления и бизнеса, государство вынуждено решать и ряд острых вопросов, связанных с отсутствием необходимых механизмов правового регулирования и контроля не существовавших ранее финансовых институтов и процедур.

В первую очередь, обращают на себя внимание криминологические риски использования новых финансовых инструментов, которые активно используются в сети интернет для:

– приобретения запрещенных товаров и услуг в теневом сегменте интернета (Даркнете);

– хищения активов с электронных кошельков и организации мошеннических схем краудинвестинга (сбора инвестиций под проект);

– легализации преступных доходов и финансирования терроризма.

Согласно данным проведенного нами исследования, только на одном русскоязычном ресурсе «Hydra» зарегистрировано продавцов: марихуаны – 1430, каннабиноидов – 154, стимуляторов – 1265, эйфоретиков – 825, психоделиков – 341, энтеогенов – 4, экстази – 440, диссоциативов – 55, опиатов – 143. Помимо наркотических средств и психотропных веществ, теневой интернет активно предлагает химические реактивы и «конструкторы», которые позволяют изготовить наркотики в домашних условиях, а также порнографические материалы, сексуальные услуги и даже заказные убийства. В этой бизнес-схеме покупателей привлекает относительно низкая цена и безопасность, а продавцов – сложности доказывания состава преступления.

По данным А. Леумана, в 2016 году существовало около 3 тыс. доменов, предлагающих психотропные вещества[1]. Чтобы получить доступ к ресурсу, следует создать специальную учетную запись и с ее помощью просматривать предложения[2]. Использование зашифрованного канала связи делает обмен данными безопасным, что, в свою очередь, позволяет преступникам расширять свой бизнес как за счет увеличения аудитории пользователей, так и за счет расширения спектра продаваемых наркотиков. Согласно данным Всемирного доклада ООН о наркотиках (2016 год), возросший объем предложения наркотиков и других запрещенных товаров через интернет позволяет не только безнаказанно расширять теневые интернет-рынки, но и привлекать новые группы наркопотребителей, в первую очередь, за счет облегчения доступа к психоактивным веществам и возможности сохранять анонимность через использование «лукового» маршрутизатора передачи данных (TOR)[3]. Рост объемов наркоторговли в «Даркнете» продолжает увеличиваться примерно со скоростью 44 миллиона долларов в год[4].

Серьезную опасность для правоохранительной системы вызывает использование цифровых технологий при совершении хищений. Примечательно, что в этом случае цифровые финансовые активы выступают обновременно и способом, и предметом преступных посягательств. Так, согласно докладу Cipher Trace «О противодействии легализации (отмыванию) денежных средств Q2 2018», в настоящее время отмечен тренд увеличения количества и повышения качества хищений цифровых финансовых активов (криптовалют). Только за 2016–2017 годы было украдено 1,21 млрд долларов США в криптовалюте из обменников[5]. А за первую половину 2018 года динамика этих преступлений перекрыла годовые показатели предыдущего, 2017 года.

Во многом это объясняется отсутствием правового статуса цифровых финансовых активов, что не позволяет квалифицировать деяния как хищения. Так, в Российской Федерации до настоящего времени не вынесен ни один обвинительный приговор суда по краже и (или) хищению криптовалюты и токенов.

Серьезную опасность представляет и высокая распространенность преступлений, связанных с легализацией преступных доходов.

По данным Европола, в Европе около четырех процентов преступных доходов отмывается при помощи криптовалюты. Процент может показаться небольшим, однако он составляет примерно $5 млрд доходов, легализуемых преступниками. При этом нельзя не учитывать и те обстоятельства, что, во-первых, эти преступления обладают высокой степенью латентности, и, во-вторых, ввиду отсутствия легального статуса криптовалют и иных цифровых финансовых активов, они пока не очень охотно используются для отмывания преступных доходов. В случае же придания им соответствующего правового статуса в отсутствии налаженной системы финансового контроля мы сможем наблюдать ситуацию стремительного роста преступлений в границах 150–550% в год[6].

Схемы, используемые для легализации криптовалют

Схемы легализации с использованием криптовалют отличаются от традиционных схем отмывания. Они предполагают наличие нескольких этапов:

размещение «грязных» денег на цифровые платформы;

1 Lewman A. Tor and links with cryptomarkets. In Internet and Drug Markets, EMCDDA Insights. www.emcdda.europa.eu

2 Martin J. Lost on the silk road: Online drug distribution and the "cryptomarket". www.researchonline.mq.edu.au; Van Slobbe, J. The drug trade on the deep web: A law enforcement perspective. In Internet and Drug Markets, EMCDDA Insights. www.emcdda.europa.eu

3 Всемирный доклад о наркотиках 2016 год. www.unodc.org

4 www.unodc.org

5 ciphertrace.com

6 /www.europol.europa.eu

использование смесителей, цепных прыжков, тумблеров и других технических средств для запутывания цепочек транзакций. Фактически эти операции приобретают псевдонимный характер: возможность их отслеживания сохраняется, но существенно затрудняется, прежде всего в плане доказывания;

на третьем этапе происходит смешение отмываемых денег с законными доходами на легальных сервисах;

на четвертом этапе смешанные средства выводятся на счета клиентов с оплатой от 1% до 15% за услуги.

Терроризм и цифровые финансовые рынки

В связи с активным развитием цифрового финансового рынка при отсутствии механизмов финансового контроля возрастает опасность использования новых инструментов в поддержке терроризма. Пока отмечаются лишь отдельные случаи использования криптовалюты в такого рода операциях, но есть серьезные предпосылки, указывающие на их рост в самой ближайшей перспективе.

Так, по данным исследования Департамента политики Европейского парламента по правам граждан и конституционным вопросам, в обозримом будущем основными направлениями использования криптовалют террористами будут:

– сбор средств или закупка незаконных предметов на теневом киберрынке;

– привлечение пожертвований в рамках краудфандинговых кампаний, проводимых в социальных сетях и на зашифрованных платформах обмена сообщениями;

– передача средств на международном уровне между членами террористических сетей[7].

По оценке Интерпола, основание для неблагоприятных прогнозов роста финансирования терроризма с использованием новых цифровых инструментов дают: планируемое увеличение кибератак малыми группами с 10% в 2018 году до 78% в 2025 году, увеличение числа молодых людей с радикальными взглядами и навыками использования криптовалют с 35% до 75% соответственно, рост кибератак на децентрализованные сети с 20% до 90%. Ожидается, что криптовалюта для финансирования в 2025 году будет использоваться в 30 раз чаще. Очевидно, что этот прогнозный показатель может быть увеличен даже втрое, если мировое сообщество и отдельные государства не разработают систему правового и финансового контроля над новым цифровым рынком[8].

Рекомендации по предотвращению возможных рисков

Для предотвращения возможных рисков, в первую очередь, следует:

• провести на уровне ФАТФ оценку рисков, представляемых продуктами и услугами на основе новых цифровых финансовых активов;

• принять меры по наложению на финансовые учреждения и иные учреждения, являющиеся провайдерами услуг, обязанности по принятию эффективных мер для снижения своих рисков ПОД/ФТ, связанных с платежными продуктами и услугами на основе виртуальной валюты;

• принять решение о введении режима регулирования обмена цифровых активов на фиатную валюту и наоборот. В том числе разработать режим лицензирования и сертификации деятельности, а также установить максимальный порог транзакций без идентификации клиента;

• важно разработать механизмы идентификации лиц, участвующих в обороте новых финансовых инструментов на основе традиционных методик ФАТФ применительно к фиатной валюте и ценным бумагам. Но прежде всего важно установить нормативный запрет на анонимность транзакций.

Данные меры активно обсуждаются на площадке ФАТФ и находят выражение в проекте Федерального закона РФ «О цифровых активах», подготовленного Центром цифровой экономики и финансовых инноваций МГИМО МИД России [Сидоренко, 2018. С. 29–34]. Однако, даже в случае разработки мер контроля по отношению к криптовалюте и другим цифровым финансовым активам (токенам, стейбкойнам и др.) [Федоров, 2018. С. 30–74], останется ряд неурегулированных вопросов, решение которых должно осуществляться в принципиально иных правовых плоскостях финансового контроля [Перов, 2018. С. 58–60].

Обозначим основные из них. Установление финансового контроля за оборотом криптовалюты [Макарчук, 2018. С. 21–24], к сожалению, не решит задачи борьбы с аватарами, которые получают от клиентов банка доступ к интернет-банкингу и цифровым кошелькам. Современные цифровые технологии существенно затрудняют процесс обнаружения плательщика: агент финансового мониторинга попросту не может установить его при проведении онлайн платежей и платежей с использованием интернет-банкинга. Предполагается, что механизмы идентификации клиента не позволят решить проблему аватаров в банкинге, а это значит, что криптопреступность будет охотно обходить запреты, прибегая к этой схеме.

Важно обратить внимание и на то обстоятельство, что любое правовое регулирование должно быть подкреплено обоснованными и адекватными мерами ответственности. В этой связи на первый план выходят вопросы установления уголовной ответственности за передачу прав доступа к интернет-порталам, электронным и цифровым кошелькам, позволяющим проводить финансовые операции без волеизъявления лица – владельца соответствующего банковского счета или цифрового кошелька. Если ответственное лицо – служащий финансовой компании – передает такую информацию аватару, он должен нести ответственность за нарушение законодательства о финансовом контроле.

Не меньше вопросов вызывает удаленная идентифи-

7 www.europol.europa.eu

8 www.europol.europa.eu

кация клиентов[9]. В настоящее время активно внедряется первичная биометрическая идентификация клиентов, но уже очень скоро она будет преодолеваться преступниками с использованием новых цифровых технологий.

Возникает ряд прикладных рисков идентификации в сфере осуществления государственного финансового контроля. Например, риск использования поддельных изображений клиентов. Технологии в этом смысле продвинулись далеко вперед. В частности, в феврале 2019 года был запущен сайт, на котором раз в несколько секунд генерируется человеческое лицо с помощью алгоритма генеративных нейронных сетей StyleGan. Разработчикам удалось преодолеть эффект «зловещей долины» благодаря генеративной нейронной сети[10]. В итоге искусственное лицо невозможно отличить от реального. Кроме того, сложно определить степень влияния (давления) на клиента третьих лиц при удаленной идентификации. Агенту финансового контроля сложно определить, насколько принимаемое лицом решение соответствует его собственной воле. Нельзя исключать и тот факт, что увеличение скорости обработки межбанковских транзакций может привести к увеличению числа экономически необоснованных движений денежных средств и, как следствие, к росту фактов легализации преступных доходов и финансирования терроризма.

В этой связи обоснованным видится кардинальный пересмотр системы контроля при первоначальной визуальной идентификации клиента. Возможно, следует рассмотреть возможность введения режимов контроля через установление высоких и низких рисков причастности клиента к преступной деятельности (прежде всего к мошенничеству, легализации преступных доходов и финансированию терроризма).

Искусственный интеллект: безопасность и ответственность

Говоря о рисках цифровых технологий в системе финансового мониторинга и контроля, нельзя не упомянуть и об использовании искусственного интеллекта.

По мере развития этой технологии в геометрической прогрессии увеличивается опасность несанкционированного вмешательства в процесс обработки и анализа данных сложных технических алгоритмов. В отдельных случаях искусственный интеллект в режиме удаленной идентификации клиента сможет переводить средства с одного счета на другой, тем самым запутывая цепочку расчетов с преступными целями. В этом случае государство должно обеспечить, в первую очередь, гарантии признания данных сделок незаконными и предусмотреть ответственность за их осуществление. Непонятно, однако, кто в случае причинения вреда должен нести ответственность: разработчик программы, ее пользователь или банк (кредитная организация), допустившая возможность такого вторжения. Думается, этот вопрос должен получить разрешение в самой ближайшей перспективе.

Не меньше вопросов возникает и к идее внедрения искусственного интеллекта в систему государственного финансового контроля. Плюсы такого рода инноваций очевидны: сокращение временных и финансовых издержек, высвобождение человеческих ресурсов, сокращение «бумажной» работы, возможность проведения контроля дистанционно и др. Но вместе с тем, имеется и ряд юридических вопросов обеспечения безопасности такой работы.

Первый и самый очевидный из них – это вопрос доверия к заключениям, даваемым искусственным интеллектом. Степень доверия напрямую зависит от тех правовых гарантий, которые лежат в основе взаимоотношений. В случае же с искусственным интеллектом они напрямую отсутствуют.

Второй вопрос касается механизмов интеграции искусственного интеллекта в систему финансового мониторинга агента финансового мониторинга[11]. В настоящее время государство не только не решило его, но даже и не занялось его решением. А между тем, пока не будут урегулированы проблемы эффективности работы искусственного интеллекта, границ его использования, гарантий добросовестности разработчиков, верификации и дополнительного контроля полученных данных, говорить о правовой возможности полной «оцифровки» системы финансового контроля вряд ли возможно.

В заключение отметим, что активная цифровизация финансовой сферы вынуждает государство качественно и серьёзно подходить к решению юридических вопросов [Леднева, Черникова, 2017. С. 27–29], прежде всего связанных с определением правового статуса новых финансовых инструментов, к определению границ и стандартов их применения и установлением мер ответственности за использование этих инструментов в преступных целях.

9 Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Нормативную основу финансово-правового регулирования биометрической идентификации и верификации составляют изменения, вносимые Федеральным законом от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

10 www.thispersondoesnotexist.com

11 Speech by Rob Gruppetta, Head of the Financial Crime Department at the FCA, delivered to the FinTech Innovation in AML and Digital ID regional event, London. www.fca.org.uk

Литература

Леднева Ю.В., Черникова Е.В. Законы для блага экономики. *Государственная служба.* 2017. № 1. С. 27–29.

Макарчук Н.В. Публично-правовые ограничения использования криптовалют как способ минимизации возможных рисков цифровизации экономики. *Право и цифровая экономика.* 2018. № 1. С. 21–24.

Перов В.А. Об особенностях правового регулирования правоотношений в сфере оборота криптовалют на территории Рос-

сийской Федерации. *Российская юстиция.* 2018. № 3. С. 58–60.

Сидоренко Э.Л. Криминологические риски криптовалюты: основные тенденции и прогнозы. *Государственная служба*. 2018. № 3. С. 29–34.

Федоров Д.В. Токены, криптовалюта и смарт-контракты в отечественных законопроектах с позиции иностранного опыта. *Вестник гражданского права*. 2018. № 2. С. 30–74.

Lewman, A., Tor and links with cryptomarkets. In Internet and Drug Markets, EMCDDA Insights. Available at: http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf (assessed 21.10.2018).

Martin, J. Lost on the silk road: Online drug distribution and the 'cryptomarket'. Criminology and Criminal Justice 14:351–67. Available at: https://www.researchonline.mq.edu.au/vital/access/manager/Repository/mq:34686 (assessed 21.10.2018).

Van Slobbe, J. The drug trade on the deep web: A law enforcement perspective. In Internet and Drug Markets, EMCDDA Insights. Available at: http://www.emcdda.europa.eu/publications/insights/internet-drug-markets_en (assessed 21.10.2018).

References

Fedorov, D.V. Tokens, cryptocurrency and smart contracts in domestic bills from the position of foreign experience. *Vestnik grazhdanskogo prava*. 2018. № 2. P. 30–74. In Russian

Ledneva, J.V., Chernikova, E.V. Laws for the good economy. *Gosudarstvennaya sluzhba*. 2017. № 1. P. 27–29. In Russian

Lewman, A. Tor and links with cryptomarkets. In Internet and Drug Markets, EMCDDA Insights. Available at: http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf (assessed 21.10.2018). In English

Makarchuk, N. V. Public-legal restrictions on the use of cryptocurrencies as a way to minimize the possible risks of digitalization of the economy. *Pravo i tsifrovaya konomika*. 2018. № 1. P. 21–24. In Russian

Martin, J. Lost on the silk road: Online drug distribution and the 'cryptomarket'. Criminology and Criminal Justice 14:351–67. Available at: https://www.researchonline.mq.edu.au/vital/access/manager/Repository/mq:34686 (assessed 21.10.2018). In English

Perov, V.A. On the peculiarities of legal regulation of legal relations in the sphere of turnover of cryptocurrencies in the territory of the Russian Federation. *Rossijskaya justitsija*. 2018. № 3. P. 58–60. In Russian

Sidorenko, E.L. Criminological risks of crypto-currencies: main trends and forecasts. *Gosudarstvennaya sluzhba*. 2018. №3. P. 29–34. In Russian

Van Slobbe, J. The drug trade on the deep web: A law enforcement perspective. In Internet and Drug Markets, EMCDDA Insights. Available at: http://www.emcdda.europa.eu/publications/insights/internet-drug-markets_en (assessed 21.10.2018). In English

ЧТО ЧИТАТЬ

Презентация книг Вито Танци

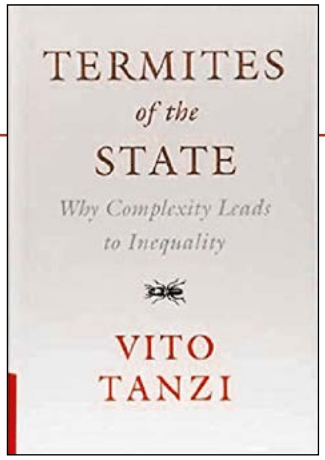


16 января в рамках Гайдаровского форума прошла презентация книг Вито Танци – известного экономиста, который более двух десятков лет работал в МВФ и почти 15 лет в правительстве Италии. Одна из них уже опубликована на русском языке в издательстве Института Гайдара – «Правительство и рынки: меняющаяся экономическая роль государства». Другая вышла в свет на английском и тоже посвящена теме участия государства в экономике – «Termites of The State: Why Complexity Leads to Inequality».

Автор всесторонне исследовал новые роли государства в XX веке, сделал обзор экономических теорий и их трансформаций в условиях глобализации мира, представил проблемы государственных расходов, политики налогообложения, а также влияние социальных обязательств государства на экономику.

Главная мысль автора – государство не может и не должно полностью покрывать потребность в защите от рисков с экономическими последствиями [Танци, 2018. С. 200]. Государство обременено многочисленными обязанностями, но должны быть и зоны ответственности участников рынка за собственные действия, должна быть свобода для хозяйствующих субъектов. Вслед за Адамом Смитом Вито Танци повторяет: задача государства заключается в том, чтобы «сделать работу рынка настолько эффективной, насколько это возможно» [Танци, 2018. С. 545].

Эта мысль была на Гайдаровском форуме сквозной. И на презентацию книг Вито Танци пришло немало заинтересованных специалистов и студентов.



Литература

Танци В. Правительство и рынки: меняющаяся экономическая роль государства. М.: Издательство Института Гайдара, 2018.

Tanzi V. Termites of The State: Why Complexity Leads to Inequality. Cambridge: Cambridge University Press, 2018.