Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2021, 4: 12–19
© А.А. Бордюговская, 2021

DOI 10.26163/GIEF.2021.50.94.002
УДК (336.74:004):343.359

A.A. Bordyugovskaya

OFFENSES IN THE FIELD OF ELECTRONIC MONEY FLOW

Anastasiya Bordyugovskaya – Lecturer, the Department of Civil Law Disciplines, State Institute of Economics, Finance, Law and Technology, Gatchina; **e-mail: an.alekseevna19@yandex.ru**.

Implementation of IT technologies covering different areas of life has made human existence more comfortable on the one hand and on the other hand, it gave rise to offenses in the realm of Information Security. The article focuses on major problematic issues and challenges revealed currently in the field of Information Security. It sets out key lines of the development of legislation in the sphere of financial security, the ones, which among other things might have a positive impact on the cyber skills of the population.

Keywords: *Information Security; financing of terrorism; e-money; fishing; swindling with the use of electronic means of payment; financial operations; virtual assets; money-laundering; electronic money operator; FATF (financial action task force); cryptocurrency; social engineering; financial organizations customers; cybercrime; FinCERT (credit and finance-related computer emergency response team).*

А.А. Бордюговская

ПРАВОНАРУШЕНИЯ В СФЕРЕ ОБОРОТА ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Анастасия Алексеевна Бордюговская – преподаватель кафедры гражданско-правовых дисциплин, Государственный институт экономики, финансов, права и технологий, г. Гатчина; **e-mail: an.alekseevna19@yandex.ru**.

Внедрение IT-технологий в различные сферы жизни человека, с одной стороны, сделало ее более комфортной, а с другой – послужило предпосылкой к увеличению количества преступлений в области информационной безопасности.

В статье рассмотрены основные проблемы и угрозы информационной безопасности, выявленные за последние годы. Сформулированы основные направления совершенствования законодательства в сфере финансовой безопасности, которые, в том числе, способны оказать положительное влияние на киберграмотность населения в целом.

Ключевые слова: *информационная безопасность; электронные денежные средства; фишинг; мошенничество с использованием электронных средств платежа; финансовые операции; финансирование терроризма; виртуальные активы; отмывание доходов; оператор электронных денежных средств; ФАТФ (группа разработки финансовых мер борьбы с отмыванием денег); криптовалюта; социальная инженерия; клиенты финансовых организаций; киберпреступность; ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере).*

Под угрозами информационной безопасности следует понимать потенциально возможные деяния, события или процессы, способные оказать отрицательное влияние на систему или на информацию, которая в ней хранится [1]. Данное положение в полной мере относится и к информации, касающейся ЭДС. Особую опасность здесь представляет то обстоятельство, что ЭДС – это не просто денежные средства, предоставленные их владельцем оператору ЭДС, а возможный источник финансирования незаконной деятельности.

Немаловажную роль в обнаружении именно такой деятельности играет частота совершаемых платежных операций, когда Банк может посчитать, что владелец ЭСП финансирует деятельность, запрещенную законом. За этим следует требование предъявить подтверждающие документы (в том числе налоговые), в противном случае Банк вправе блокировать операции и приступить к выявлению противоправной цели оборота денежных средств. Надо сказать, что судебная практика в отношении наложения ограничений на проведение транзакций в большинстве случаев предпочитает становиться на сторону кредитной организации [12].

Отметим, что за последние 6–8 лет одной из основных угроз информационной безопасности в сфере перевода ЭДС являются фишинговые сайты, преследующие своей целью сбор персональных данных и платежной информации пользователей сетей через поддельные сайты банков, социальных сетей и др., которые внешне полностью копируют оригинальный ресурс. Это происходит путем кражи логинов и паролей пользователей, при этом пользователь после совершения такого деяния перенаправляется на оригинальный сайт, где пройдена авторизация. Именно поэтому жертва даже не подозревает о совершении в отношении неё преступления.

Следует отметить, что государство принимает активное участие в контроле и обеспечении безопасности сетей, однако этого явно недостаточно, т.к. не все сегменты Всемирной паутины подконтрольны государству. Одним из таких сегментов являются частные сети, т.е. сети, позволяющие обеспечить одно или несколько сетевых подключений (например, локальная сеть) поверх другой сети, к которой, например, относится частная сеть «Tor»[1].

На нелегальных площадках достаточно распространены деяния, которые могут повлечь наступление ответственности по таким статьям уголовного законодательства РФ, как:

1) ст. 159.3 УК РФ, предусматривающая наказание за мошенничество с использованием ЭСП, а именно хищение чужого имущества, совершенное с использованием поддельной кредитной карты путем обмана уполномоченного работника кредитной, торговой или иной организации;

2) ст. 272 УК РФ, ответственность по которой наступает за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;

3) ст. 274 УК РФ, а именно за деяние, совершенное в форме нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации;

4) ст. 174.1 УК РФ, наказание по которой наступает за совершение такого деяния, как совершение финансовых операций и других сделок с денежными средствами (в том числе ЭДС) или иным имуществом, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или

[1] TOR (от англ. – The Onion Router) – это система частных прокси-серверов, которая частично формируется из пользователей и серверов, разбросанных по всему миру. Обмен данными происходит в зашифрованном виде в целях повышения анонимности и безопасности пользователей сети, которые обеспечиваются недоступными для публики IP-адресами. Именно поэтому пользователи могут общаться, не опасаясь государственного вмешательства.

Ввиду этого TOR часто воспринимается как некий инструмент, к которому невозможно подключиться через обычный браузер и с помощью которого можно осуществлять коммуникации в целях сохранения приватности общения. Это позволяет использовать TOR в различных видах как легальной, так и нелегальной деятельности, в том числе таких, как торговля оружием, наркотиками, банковскими картами и др.

иным имуществом.

Действующее уголовное законодательство РФ не предусматривает наказание за создание фишинговых сайтов и их содержание. В связи с этим представляется необходимым дополнить Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятием «фишинг» и «фишинговый сайт», а также внести изменения в действующий Уголовный кодекс РФ, дополнив гл. 28 УК РФ статьей, предусматривающей уголовную ответственность за создание фишинговых сайтов и владение ими. Также необходимо при обнаружении подобных сайтов производить их блокировку. На данный момент правомочиями по блокированию фишинговых сайтов Роскомнадзор не обладает. Актуальность реализации предложенных мер подтверждается данными, ежемесячно публикуемыми на сайте Центрального Банка России о событиях в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма [6; 7; 8]. Так, за январь–апрель 2021 г. новости стран Европы, Европейского Союза и Российской Федерации таковы:

1) 25.01.2021 г.: Министерство юстиции Люксембурга публикует отчёт о результатах оценки рисков отмывания доходов, полученных преступным путем, и финансирования терроризма [22] (далее – ОД/ФТ), присущих виртуальным активам и провайдерам услуг в сфере виртуальных активов (далее – ВА)[2] [20].

Отчет был подготовлен на основании результатов национальных оценок рисков за 2018, 2020 гг. Результаты удручающие: сфера ВА с точки зрения ОД/ФТ является высокорисковой[3] ввиду их анонимности, технологической сложности, возможности использования при построении «дистанционных», в том числе международных, отношений. Наиболее высокие риски были отмечены в отношении «биткоинов» и «монеро» [4], «эфириумов», «стейблкоинов»[5] [4].

Основными видами преступлений, совершаемых с помощью ВА, согласно отчету, стали незаконная торговля наркотиками, фальсификация документов, удостоверяющих личность, кража ВА, кибермошенничество;

2) 03.02.2021 г.: Полицейская служба Европейского Союза (Европол) публикует пресс-релиз о результатах международного расследования по делу о мошенничестве и отмыванию доходов [15].

Итоги расследования таковы: раскрыта международная сеть по отмыванию доходов, полученных преступных путем в результате совершения мошеннических действий и хищения денежных средств у финансовых учреждений Америки[6] на

[2] Виртуальный актив (virtualasset) означает 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.

[3] По информации Cipher Trace, в 2019 г. в Люксембурге в целях ОД/ФТ преступниками использовались виртуальные активы на сумму более 10 млрд долл. США (Cipher Trace Cryptocurrency Anti-Money Laundering Report. 2018 Q3). (Cipher Trace – американская компания, которая специализируется на вопросах кибербезопасности и является одной из ведущих компаний-разработчиков решений в сфере противодействия ОД, в частности, с использованием криптовалют. Cipher Trace была разработана платформа с искусственным интеллектом для определения потенциальных источников ОД, в которой отображаются следы финансовых потоков и информация о текущем нахождении денежных средств, включая страны и биржи, которые были использованы в целях ОД).

[4] Monero – появившаяся в 2014 г. криптовалюта на основе протокола Crypto Note, ориентированная на повышенную конфиденциальность транзакций. Сумма транзакций, а также адреса отправителя и получателя известны только участникам транзакций и тем, кому предоставляется особый ключ доступа.

[5] Стейблкоин – это криптовалюта, обеспеченная определенным традиционным активом: фиатной валютой (долларом, евро, рублем, юанем), драгоценным металлом (золотом, серебром, бронзой), природным ресурсом (газом, нефтью и т.д.).

[6] По информации Европола, указанной преступной организацией на территории США создавались «компании-оболочки» и открывались для них счета в американских банках. Для формирования доверительного отношения со стороны указанных

общую сумму около 14,5 млн долл.; арестовано 105 физических лиц-участников сети; заморожено 87 банковских счетов, денежные средства на которых составляли около 1,3 млн долл.

Поскольку выявленная схема носила международный характер, постольку в расследовании было задействовано несколько компетентных ведомств под общим руководством Европола: Секретная служба США, Национальная полиция Испании, Министерство юстиции США, Сеть по борьбе с финансовыми преступлениями США, правоохранительные ведомства Австрии, Дании и Греции;

3) 16.02.2021 г.: Целевой группой по финансовым действиям (далее – ФАТФ)[7] публикуется отчет о принятии Данией мер по борьбе с ОД/ФТ (после оценки в 2017 г. и последующих докладов в 2018–2019 гг.) [17]. В отчете отмечается, что по одним показателям зафиксировано повышение рейтинга по Рекомендациям [11] (например, Рекомендация 6 (С6) – финансовые санкции, связанные с терроризмом), по другим – понижение (например, Рекомендация 15 (D15) новые технологии) ввиду неприведения Рекомендаций в соответствие с новым стандартом в части обеспечения должного регулирования деятельности провайдеров услуг в сфере виртуальных активов[8] [20], их лицензирования или регистрирования. Ввиду этого Дания остается на особом контроле со стороны ФАТФ и обязана отчитываться об устранении недостатков;

4) 03.03.2021 г.: Европейским банковским управлением (European Banking Authority, EBA) публикуется заключение о рисках ОД/ФТ для финансовой системы ЕС[9] [23], в котором рассматриваются риски ОД/ФТ, связанные с виртуальными валютами, услугами, оказываемыми финтех-компаниями, решениями в области Reg Tech[10], риски, связанные с недостатками в системах внутреннего контроля по противодействию финансированию терроризма субъектов исполнения «противолегализационного» законодательства, а также риски, связанные с дерискингом[11] [14];

С 2019 г., когда Европейским банковским управлением было подготовлено предыдущее заключение, отмечается рост рисков, связанных с виртуальными валютами, прежде всего в связи с постоянным ростом криптовалютного рынка по объёму осуществляемых операций и количеству клиентов. К факторам повышения рисков ОД/ФТ можно отнести непрозрачность операций с криптовалютой, отсутствие информации о лицах, осуществляющих соответствующие операции. Таким рискам наиболее подвержены эмитенты электронных денег, платежные ор-

американских банков на открытые у них счета членами преступной организации осуществлялись переводы денежных средств из различных европейских стран. После этого американскими банками по указанным счетам выпускались дебетовые и кредитные карты, которые впоследствии использовались преступниками для хищения и последующего отмывания денежных средств.

[7] Целевая группа по финансовым действиям (ФАТФ) является глобальной организацией по борьбе с отмыванием денег и финансированием терроризма. Межправительственный орган устанавливает международные стандарты, которые направлены на предотвращение этой незаконной деятельности и ущерба, который она наносит обществу. Будучи директивным органом, ФАТФ работает над созданием необходимой политической воли для проведения национальных законодательных и нормативных реформ в этих областях.

[8] Виртуальный актив (virtualasset) означает 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.

[9] Заключение подготовлено EBA совместно с Европейской службой по ценным бумагам и рынкам (European Securities and Markets Authority, ESMA) и Европейской службой страхования и пенсионного обеспечения (European Insurance and Occupational Pensions Authority, EIOPA).

[10] Reg Tech – инновационные методы регулирования, используемые для упрощения и более эффективного выполнения финансовыми организациями требований законодательства о ПОД/ФТ.

[11] Под «дерискингом» ФАТФ понимает ситуации, когда кредитно-финансовые учреждения прекращают или ограничивают деловые отношения с целыми странами или классами клиентов во избежание рисков, вместо управления рисками в соответствии с риск-ориентированным подходом.

ганизации, кредитные организации;

5) 16.03.2021 г.: Управлением по контролю за соблюдением правил поведения на финансовых рынках Великобритании (Financial Conduct Authority, FCA) опубликован пресс-релиз [18] об инициировании уголовно-процессуальных действий в отношении лондонского отделения National Westminster Bank Plc (Nat West)[12] по делу о нарушении требований законодательства о ПОД/ФТ. Дело связано с обработкой средств, внесенных на счета, управляемые британским инкорпорированным клиентом Nat West;

6) 25.03.2021 г.: на сайте торговой ассоциации сектора банковских и финансовых услуг Великобритании UKFinance опубликован отчет о трендах финансовых преступлений в 2020 г., в том числе мошенничества и отмывания денег [19], спонсируемый Lexis Nexis Risk Solutions. Из содержания отчета следует, что на фоне пандемии COVID-19 рост онлайн-мошенничества увеличился. Речь идет о преступлениях, совершаемых с использованием криптовалют, а также о киберпреступлениях, совершаемых с применением технологий, позволяющих обходить современные системы безопасности банков. Кроме того, отмечается рост «денежных мулов»[13], завербованных при помощи вебсайтов;

7) 10.03.2021 г.: на сайте Росфинмониторинга публикуется информационный бюллетень за 2020 г. «Итоги информационного взаимодействия с организациями, осуществляющими операции с денежными средствами или иным имуществом» [3], в котором содержится информация о форматах предоставления обратной связи о качестве взаимодействия, сведения об анализе сообщений о подозрительных операциях за отчетный период (снижение на 30% в целом, повышение показателей в бюджетной сфере и по незаконному обороту наркотиков), информация о динамике количества отказов кредитных организаций в части выполнения распоряжений клиентов и заключения (расторжения) договоров банковского счета (фиксируется уменьшение);

8) 23.03.2021 г.: на сайте Центрального банка России публикуется обзор об основных видах атак в кредитно-финансовой сфере. Аналогично отчету о трендах финансовых преступлений в 2020 г., в обзоре отмечается значительный рост мобильного мошенничества в отношении граждан в период пандемии COVID-19. Наибольший рост отмечен в отношении фишинговых сайтов, а именно сайтов, дублирующих страницы интернет-магазинов и социальных служб. За период пандемии было выявлено 5011 таких сайтов, из которых 4314 перестали быть доступными для пользователей ввиду снятиях их с делегирования [9].

Активная противоправная деятельность с использованием смс-рассылки, фишинга, установки вредоносного оборудования, звонков привела к резкому росту объема и числа попыток операций без согласия клиента в период начала пандемии примерно в два раза по сравнению с аналогичным периодом 2019 г. В период пандемии злоумышленники пользовались как старыми, так и новыми способами вывода денежных средств:

- через операторов ЭДС: мошенники, вводя потерпевших в заблуждение, указывают номер виртуальной карты оператора ЭДС, после получения денежных средств выводят их на «обменники» с целью сокрытия следов дальнейшего движения денежных средств;

- через операторов сотовой связи: мошенники осуществляют перевод на баланс мобильного телефона с дальнейшим переводом через оператора ЭДС, либо указывают потерпевшему номер виртуальной карты, привязанной к счету мобильного телефона;

- переводы с карты на карту с исполь-

[12] National Westminster Bank Plc (Nat West) является крупным розничным коммерческим банком в Великобритании. С 2000 г. входит в состав Nat West Group Plc (ранее – Royal Bank of Scotland Group Plc); имеет широкую филиальную сеть в Великобритании (более 960 отделений).

[13] Денежные мулы (moneymules) – физические лица, завербованные преступными организациями в качестве посредников ОД и использующие свои банковские счета для получения и перевода денежных средств, полученных преступным путём.

зованием сервисов перевода денежных средств: мошенники, предварительно получив данные карты потерпевшего, осуществляют перевод денежных средств на заранее подготовленную «дроп»-карту[14];

- вывод денежных средств на «обменники» (криптообменники) [15]. Курс для осуществления операций по обмену устанавливается непосредственно «обменником» и чаще всего превышает рыночный на 5–10%. Отслеживание цепочки вывода денежных средств весьма затруднительно ввиду осуществления переводов с множества заключенных в разных кредитных организациях счетов [9].

9) 12.04.2021 г.: на сайте Центрального банка России публикуется обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 г. Данный обзор содержит информацию о динамике количества и объема операций с использованием ЭСП. Так, количество операций, совершенных с использованием ЭСП без согласия клиента – физического лица, составило 770075 единиц, суммарный объем которых составляет 8757,2 млн руб. Основной причиной совершенных хищений операторы по переводу ЭДС называют социальную инженерию (основываясь на информации, полученной от клиентов). Тем не менее, в сравнении с 2019 г. ее доля уменьшилась на 6,8% (68,6% случаев в 2019 г. против 61,8% случаев в 2020 г.), что объясняется повышением уровня киберграмотности населения. С клиентами – юридическими лицами ситуация обстоит следующим образом: количество операций, совершенных без согласия клиента с использованием ЭСП, снизилось на 36,4% (4609 операций в 2019 г. против 2933 операций в 2020 г.), однако их объем увеличился на 45,5% (701 млн руб. против 1020 млн руб.). Основными причинами доступа к информационной инфраструктуре операторов ЭДС стали: несанкционированный доступ работников и иных уполномоченных лиц к объектам информационной инфраструктуры, информации о банковских счетах, автоматизированным банковским системам, программно-аппаратному обеспечению банкоматов и электронных терминалов; компьютерные атаки; несанкционированный доступ к автоматизированным банковским системам и информации о банковских счетах [5]. Таковы данные за первые четыре месяца 2021 г.

Говоря о киберпреступности в финансовой сфере, нельзя не затронуть тему DDoS-атак[16] на финансовые организации, информация о которых поступала в ФинЦЕРТ [13] в течение 2019–2020 гг. Чаще всего им были подвержены системы дистанционного банковского обслуживания и сервисы онлайн-банкинга, а также иные сервисы для перевода денежных средств.

Кроме того, в 2019 г. замечена активность злоумышленников, проявляющаяся в совершении телефонных звонков клиентам банков от имени финансовых организаций. Клиентам сообщалось о приостановлении «банком» операции, возможно, совершаемой без согласия клиента, и под этим предлогом собирались данные карт и коды из SMS-сообщений.

Количество операций, совершенных с использованием ЭСП и без согласия клиента, в 2019 г. составило 576566, суммарным объемом 6426,5 млн руб. Большая часть операций была проведена путем обмана клиентов либо с применением методов несанкционированного доступа к информации и системам ее хранения без использования технических средств. Речь идет о социальной инженерии, методы которой основаны на так называемом «человеческом факторе» и являются довольно эффективными.

В 2020 г., соответственно, основной угрозой для информационной и финансовой безопасности при совершении опера-

[14] Фактически, это подставная карта. Дропы – это подставные лица, позволяющие злоумышленникам оставаться «в тени». Карты, с которыми работают дропы, называются дроп-картами.

[15] Обменники – сервисы, которые предоставляют возможность покупки/продажи валюты (криптовалюты), при которой сервис выступает в роли покупателя/продавца.

[16] Distributed Denial of Service, или «Распределенный отказ от обслуживания» – подавление веб-ресурса или сервера трафиком из огромного количества источников, что делает его недоступным.

ций клиентами стали CNP – транзакции[17] при оплате товаров и услуг через Интернет, суммарный объем которых предполагается еще выше, чем в 2019 г., поскольку пандемия, когда люди стали ещё более чаще прибегать к оплате товаров/услуг посредством сети Интернет, сыграла отнюдь не последнюю роль.

В 2019 г. ФинЦЕРТом на базе АСОИ (автоматизированная система обработки инцидентов) была введена в действие автоматизированная система «Фид-АнтиФрод» (далее – АС «Фид-АнтиФрод»), позволяющая формировать базу данных случаев и попыток проведения операций по переводу денежных средств без согласия клиентов. Статистика работы АС «ФИД-АнтиФрод» по состоянию на декабрь 2020 г. показывает следующее:

- выявлено более 43 тысяч уникальных признаков операций, совершенных без согласия клиента;
- выявлено 23444 карты, участвующие в совершении операций без согласия клиента;
- выявлено 1237 счетов, задействованных в совершении операций без согласия клиента;
- выявлено 1100 электронных кошельков, задействованных в совершении операций без согласия клиента [5].

Банк России ведет активную политику по противодействию операциям, совершаемым без согласия клиента, путем противодействия социальной инженерии [16], повышения цифровой культуры населения страны и популяризации киберграмотности [10]. Вместе с этим необходимо уделить особое внимание совершенствованию как законодательства в области обеспечения информационной безопасности финансовых организаций в целом, так и отдельных актов Банка России в частности.

ЛИТЕРАТУРА

1. *Бордюговская А.А., Бозиев Т.О.* К вопросу о современных информационных угрозах // Современное общество: наука, техника, образование: сб. трудов по материалам Всерос. науч. конф. с международ. участием. Уфа: Башкирский государственный университет, 2016. С. 274–281.

2. Виртуальные активы получили криминальное определение // Ежедневная деловая газета РБК. 2019. 26 февраля. № 018(2973)(2702): [сайт]. URL: https://www.rbc.ru/newspaper/2019/02/27/5c74f3fa9a7947500e19cd24 (дата обращения: 19.04.2021).

3. Итоги информационного взаимодействия с организациями, осуществляющими операции с денежными средствами или иным имуществом // Росфинмониторинг: [сайт]. URL: https://www.fedsfm.ru/content/files/documents/2021/итоги%20информационного%20взаимодействия%20с%20организациями,%20осуществляющими%20операции%20с%20денежными%20средствами%20или%20иным%20имуществом.pdf (дата обращения: 23.04.2021).

4. Не призрачный доход. Как заработать на стейблкоинах // РБК: [сайт]. URL: https://www.rbc.ru/crypto/news/5da589ac9a7947a5c8bba667 (дата обращения: 19.04.2021).

5. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год // Центральный банк РФ: [сайт]. URL: http://www.cbr.ru/ Collection/Collection/File/32190/Review_of_transactions_2020.pdf (дата обращения: 12.10.2021).

6. Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Январь 2021: [сайт]. URL: https://cbr.ru/Collection/Collection/File/32099/january_2021.pdf (дата обращения: 15.04.2021).

7. Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Февраль 2021 /// Центральный банк РФ: [сайт]. URL: https://cbr.ru/Collection/Collection/File/32100/february_2021.pdf (дата обращения: 15.04.2021).

[17] Транзакция CNP – это любая транзакция с использованием кредитной карты, при которой владелец карты отсутствует и физически не может предъявить свою карту для оплаты.

8. Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Март 2021 // Центральный банк РФ: [сайт]. URL: https://cbr.ru/Collection/Collection/File/32245/March_2021.pdf (дата обращения: 15.04.2021).

9. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах // Центральный банк РФ: [сайт]. URL: http://www.cbr.ru/collection/collection/file/32122/attack_2019-2020.pdf (дата обращения: 23.04.2021).

10. Правовые проблемы использования электронных денежных средств // Арбитражная практика для юристов: [сайт]. URL: https://www.arbitr-praktika.ru/article/2269-problemy-elektronnyh-denejnyh-sredstv (дата обращения: 24.04.2021).

11. Рекомендации ФАТФ: Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения // Росфинмониторинг: [сайт]. URL: https://www.fedsfm.ru/content/files/documents/2018/рекомендации%20фатф.pdf (дата обращения: 19.04.2021).

12. Решение Арбитражного суда Санкт-Петербурга и Ленинградской области от 03.02.2020 г. по делу № А56-86956/2019 // Судебные и нормативные акты РФ: [сайт]. URL: https://sudact.ru/arbitral/doc/ghlNw1ktwNbq/ (дата обращения: 08.01.2021).

13. ФинЦЕРТ // Центральный банк РФ: [сайт]. URL: https://cbr.ru/information_security/fincert/ (дата обращения: 23.04.2021).

14. Шпаргалка: «дерискинг» применительно к корреспондентским отношениям – что рекомендует ФАТФ? URL: https://xco.news/methodology/2020/02/28/shpargalka-derisking-primenitelno-k-korrespondentskim-otnosheniyam-chto-rekomenduet-fatf (дата обращения: 20.04.2021).

15. 105 arrestedforstealingover €12 millionfromus-basedbanks // Europol. 03.02.2021. URL: https://www.europol.europa.eu/newsroom/news/105-arrested-for-stealing-over-%E2%82%AC12-million-us-based-banks (дата обращения: 17.04.2021).

16. *Boziev T.O., Korotkov A.V., Sipyagina M.N., Intykbaev M.K.* IT crime: a virtual threat with real consequences. // SHS Web of Conferences. IX Baltic Legal Forum «Law and Order in the Third Millennium». 2021. P. 03011.

17. Denmark's progress in strengthening measures to tackle money laundering and terrorist financing. URL: https://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-denmark-2021.html(дата обращения: 19.04.2021).

18. FCA starts criminal proceedings against NatWest Plc. // Financial conduct authority. URL: https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc (дата обращения: 22.04.2021).

19. Fraud – the Facts 2021. URL: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021 (дата обращения: 22.04.2021).

20. Interpretive Note to Recommendation 15 on New Technologies (INR. 15). URL: https://alrf.msk.ru/files/03654e0d164907fc4b7d1eae061779767.pdf (дата обращения: 19.04.2021);

21. Interpretive Note to Recommendation 15 on New Technologies (INR. 15). URL: https://alrf.msk.ru/files/03654e0d164907fc4b7d1eae061779767.pdf (дата обращения: 19.04.2021).

22. ML/TF Vertical Risk Assessment: Virtual Asset Service Providers. December 2020. URL: https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf (дата обращения: 15.04.2021).

23. The EBA highlights key money laundering and terrorist financing risks across the EU // European Banking Authority: [site]. URL: https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks-across-eu (дата обращения: 20.04.2021).