УДК 336.02 JEL E58; O16 DOI 10.26425/1816-4277-2023-5-151-160

Повышение устойчивости информационной безопасности финансового сектора экономики

Качурин Владимир Вячеславович

Ассистент Высшей инженерной школы новых материалов и технологий
ORCID: 0009-0009-2496-0560, e-mail: vova.kachurin.02@mail.ru

Ахмадеев Равиль Габдуллаевич

Канд. экон. наук, доц. каф. государственных и муниципальных финансов
ORCID: 0000-0002-7526-0144, e-mail: Ahm_rav@mail.ru

Российский экономический университет имени Г.В. Плеханова, г. Москва, Россия

Аннотация

Правовая определенность действующих в Российской Федерации законодательных актов относительно организационно-правовых основ противодействия отмыванию средств преступного происхождения и четкая регламентация процедуры финансового мониторинга, а также взаимодействие органов власти являются основополагающими элементами в целях финансового контроля. Вместе с тем противодействие легализации доходов, полученных преступным путем, считается глобальным аспектом, который напрямую затрагивает как общество, так и экономическую систему большинства экономически развитых государств. В исследовании проанализированы основные мероприятия Банка России, направленные на обеспечение устойчивости информационной безопасности финансового сектора экономики, а также проводимые мероприятий, направленные на ограничение масштабов распространения киберпреступлений на основе автоматизированной системы обработки инцидентов. В целях решения стратегических задач в области финансовой безопасности субъектов рынка предложены практические рекомендации по совершенствованию механизма противодействия киберопреступлений на основе проведения финансового мониторинга по операциям эквайринга и корпоративных банковских карт.

Ключевые слова

Кибербезопасность, кибератаки, финансовые операции, кредитные организации, финансовые преступления

Для цитирования: Качурин В.В., Ахмадеев Р.Г. Повышение устойчивости информационной безопасности финансового сектора экономики// Вестник университета. 2023. № 5. С. 151–160.

Improving the information security sustainability of the economy financial sector

Vladimir V. Kachurin
Assistant at the Higher Engineering School of New Materials and Technologies
ORCID: 0009-0009-2496-0560, e-mail: vova.kachurin.02@mail.ru

Ravil G. Akhmadeev
Cand. Sci. (Econ), Assoc. Prof. At the Department of State and Municipal Finance
ORCID: 0000-0002-7526-0144, e-mail: Ahm_rav@mail.ru

Russian University of Economics named after G.V. Plekhanov, Moscow, Russia

Abstract

The legal certainty of the legislative acts in force in the Russian Federation concerning the organizational and legal basis for countering the funds laundering of criminal origin and clear regulation of the financial monitoring procedure, as well as the interaction of authorities are fundamental elements for the purpose of financial control. At the same time, countering the money laundering is a global aspect that directly affects both society and the economic system of most economically developed countries. The study analyzes the main activities of Russia Bank, aimed at ensuring the sustainability of information security in the financial sector of the economy, as well as ongoing activities aimed at limiting the spread of cybercrime based on an automated incident handling system. In order to solve strategic tasks in the financial security field of market entities, practical recommendations are proposed to improve the mechanism of countering to cyber crimes on the basis of financial monitoring of acquiring operations and corporate bank cards.

Keywords

Cybersecurity, cyber attacks, financial transactions, credit institutions, financial crimes

For citation: Kachurin V.V., Akhmadeev R.G. (2023) Improving the information security sustainability of the economy financial sector. *Vestnik universiteta*, no. 5, pp. 151–160.

ВВЕДЕНИЕ

Процесс глобализации и интеграция финансовой системы национальной юрисдикции последовательно способствуют интенсификации свободного движения капиталов. Одним из наиболее важных аспектов современной тенденции развития мировой экономики является интернационализация преступности, непосредственно влияющая на экономическую безопасность государства, включая элементы косвенного влияния на финансовую сферу, так и непосредственно в форме экономических отношений субъектами денежно-кредитных отношений при осуществлении операций с сокрытием бенефициарных владельцев сделок с использованием офшорных юрисдикций [1; 2].

Расширение масштабов интернационализации киберпреступлений, несовершенство нормативно-правовой базы в области противодействия легализации доходов, полученных преступным способом, непрозрачные схемы ведения деятельности некоммерческих организаций и финансовых операций, незаконное перемещение активов за пределы национальных юрисдикций с использованием офшорных компаний в большей степени формируют предпосылки к осуществлению «инвестирования и развития» международных преступных группировок, что, соответственно, негативно отражается на развитии экономической и финансовой политики как в отдельной стране, так и по секторам народного хозяйства [3; 4]. Вместе с тем противодействие легализации доходов, полученных преступным путем, является глобальным аспектом, напрямую затрагивает как общество, так и экономическую систему большинства экономически развитых государств [5].

Современные способы отмывания денежных средств в глобальной экономике основываются на использовании различных видов финансовых операций, которые предоставляют посредством поставщиков финансовых услуг (кредитные организации, микрофинансовые организации, брокеры и др.). Основой киберпреступлений, связанных с легализацией доходов, являются как денежные переводы с использованием международных платежных систем, электронные деньги, так и традиционные срочные переводы. Доходы, полученные преступным путем, в большей своей части стараются быстро и эффективно легализовать [6; 7]. В этой связи одним из актуальных направлений в области устойчивости информационной безопасности финансового сектора экономики является расширение текущих мероприятий, проводимых для ограничения масштабов распространения киберпреступлений и для внедрения IT-решений по контролю за участниками финансового рынка: от кредитных организаций до физических лиц. Такие мероприятия нацелены на предупреждение и своевременное выявление реализуемых мошеннических схем бизнес-структурами для последующего отмывания полученных денежных средств в результате таких операций с учетом развития блокчейн технологий и финансовых инструментов на основе применения различных цифровых валют [8].

МЕТАДАННЫЕ И МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

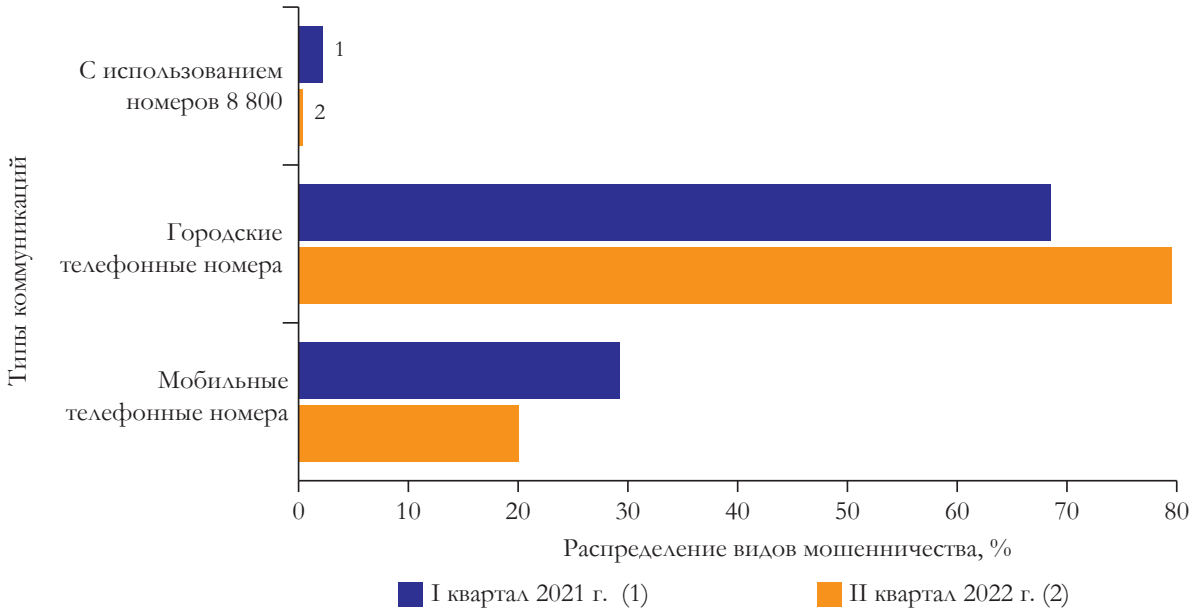
В 2018 г. Банком России было зафиксировано свыше 700 различных кибератак в отношении кредитных и финансовых компаний, в том числе 177 из них носили целевой характер. В большинстве случаев в качестве несанкционированного проникновения использовался способ поддельной маскировки адресов электронной почты для отправки вредоносного программного обеспечения (далее – ПО) или вредоносных программ. При этом наибольшее количество кибератак зафиксировано в конце календарного года по причине внедрения автоматизированной системы обработки инцидентов ФинЦЕРТ (англ. CERT – computer emergency response team, группа реагирования на компьютерные инциденты, далее – ФинЦЕРТ) в качестве основного способа передачи информации между участниками финансового сектора, правоохранительными органами, провайдерами и операторами связи, а также иными IT-компаниями, занимающимися разработкой и внедрением специализированного ПО в сфере информационной безопасности. Вместе с тем привлечение независимых экспертов к внедрению автоматизированной системы обработки инцидентов ФинЦЕРТ позволило сформировать более полную картину кибератак и побудило участников рынка объединить свои усилия в борьбе с киберпреступлениями.

В практическом применении на основе процессионговой автоматизированной поисковой системы (далее — АИПС) регулятор получил от участников рынка свыше 500 образцов вредоносных программ, которые в качестве несанкционированного проникновения использовались при организации кибератак, а свыше 50 % выявленных вредоносных программ отнесены к категории «программ-вымогателей»

и «шифровальщиков». Системой ФинЦЕРТ в последующие периоды было распространено финансовым учреждениям и иным участникам информационного обмена свыше 150 практических бюллетеней с индикаторами, указывающими на возможную компрометацию систем и сетей. Практическая значимость информационных бюллетеней позволила участникам информационного обмена находиться в курсе наиболее актуальных киберугроз на финансовом рынке и разрабатывать свои собственные эффективные мероприятия с применением современных IT-решений. При этом полученные аналитические данные от участников информационного обмена через АИПС позволили обобщить информацию и выявить свыше 540 интернет-ресурсов, которые распространяли вредоносное ПО или осуществляли деятельность в качестве серверов, контролирующих вредоносное ПО. В то же время более 500 таких ресурсов были зарегистрированы за пределами юрисдикции Российской Федерации (далее – РФ). Тот факт, что такие ресурсы размещаются в доменных зонах, выходящих за рамки полномочий ФинЦЕРТ, которая является организацией, уполномоченной выявлять нарушения, усложняет возможность приостановления деятельности соответствующих веб-сайтов.

ПРАКТИЧЕСКИЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

На законодательном уровне с 01 декабря 2021 г. регулятор имеет право в заявительном порядке обращаться в суд в целях ограничения доступа к интернет-ресурсам, позволяющим пользователям получать неправомерный доступ к информационным системам как кредитных организаций, так и некредитных финансовых организаций. Вместе с тем действие регулятора направлено, прежде всего, в отношении ограничения финансовой деятельности нелегальных форекс-дилеров, финансовых пирамид и незаконных кредиторов, особенно активизирующихся в период распространения мировой пандемии и перехода физических лиц в режим онлайн-торговли, а также во время осуществления электронных, бесконтактных платежей, удаленной трудовой деятельности и т.д. В этой связи в целях повышения устойчивости информационной безопасности между субъектами финансовых отношений важным аспектом взаимодействия бизнеса со своими клиентами и партнерами, а также с кредитными организациями является обеспечение, прежде всего, элементов внутренней сетевой безопасностью с учетом внедрения мероприятий, позволяющих в режиме текущего времени выявлять следы кибератак в собственной IT-инфраструктуре (рис. 1).



Составлено авторами по материалам источника [9]

Рис. 1. Сравнительная характеристика основных видов финансового мошенничества посредством применения телефонной коммуникации, %

Технический прогресс, постоянное совершенствование IT-технологий, конкуренция в цифровом бизнесе позволяют киберпреступникам использовать в целях совершения преступлений и последующей легализации различные механизмы и инструменты. В частности, при отмывании доходов от киберпреступлений характерной чертой является использование следующих подходов:

– открытие счетов по утраченным документам или документам подставных лиц, а также их дальнейшее использование (данный механизм в основном используется для открытия карточных счетов и оформление банковских карт на «дропов»);

– проведение операций по счетам разных фирм с целью сокрытия источника их происхождения (часто используется при выводе бюджетных средств и воровстве со счетов юридических фирм);

– открытие электронных кошельков и покупка электронных денег, а также использование международных платежных систем (МИР, Visa, Mastercard и т.д.), что позволяет быстро переводить денежные средства между участниками платежной системы;

– приобретение товаров через сеть «Интернет» (далее – Интернет) за счет краденных денежных средств;

– использование фиктивных (транзитных) предприятий.

В этой связи механизм легализации доходов, или вывод похищенных денежных средств в наличность до последнего времени являлся основной конечной точкой цепочки легализации, поскольку перемещение наличных вне банковской системы практически невозможно отследить, а в последние годы широко практикуется легализация через цифровые валюты (криптовалюты). Цифровые активы, в свою очередь, конвертируются в фиатные деньги и уже «очищенными» обратно попадают в банковскую систему. Международные платежные системы имеют ряд неоспоримых преимуществ, которые и обуславливают их быстрое развитие, а именно:

– доступность – открыть банковскую карту, в том числе виртуальную, электронный кошелек физическому лицу возможно за короткий промежуток времени и достаточно иметь необходимые документы;

– простота использования – работать с современными финансовыми инструментами довольно легко, а в целях увеличения количества пользователей все поставщики финансовых услуг стараются сделать свои сервисы интуитивно понятными;

– мобильность – доступ к финансовым инструментам очень прост. Достаточно иметь стабильное интернет-соединение, а с учетом развития и доступности мобильных устройств отсутствует необходимость в наличии персонального компьютера или ноутбука;

– оперативность – большинство транзакций осуществляется в течении нескольких секунд, а в случае использования роботизированных устройств крупные суммы денежных средств можно раздробить на мелкие платежи и транзитом через несколько счетов вывести в любую точку мира и т.д.

Если основным преимуществом использования электронных денег изначально являлась возможность анонимного открытия и пополнения электронных кошельков, то за последние годы Банком России внесены изменения в законодательные акты в отношении ужесточения требований к использованию электронных денежных средств. В частности, на текущий момент пополнить электронный кошелек можно только с идентифицированного средства платежа, а наличными денежными средствами электронный кошелек может пополнить только его владелец. Соблюдение данных требований возложено как на кредитную организацию, которая осуществляет пополнение электронного кошелька, так и на организацию, которая открыла данный кошелек физическому лицу. Сотрудники финансового мониторинга кредитных организаций выявляют подозрительные операции, которые могут быть связаны с киберпреступностью. Их основные отличия следующие:

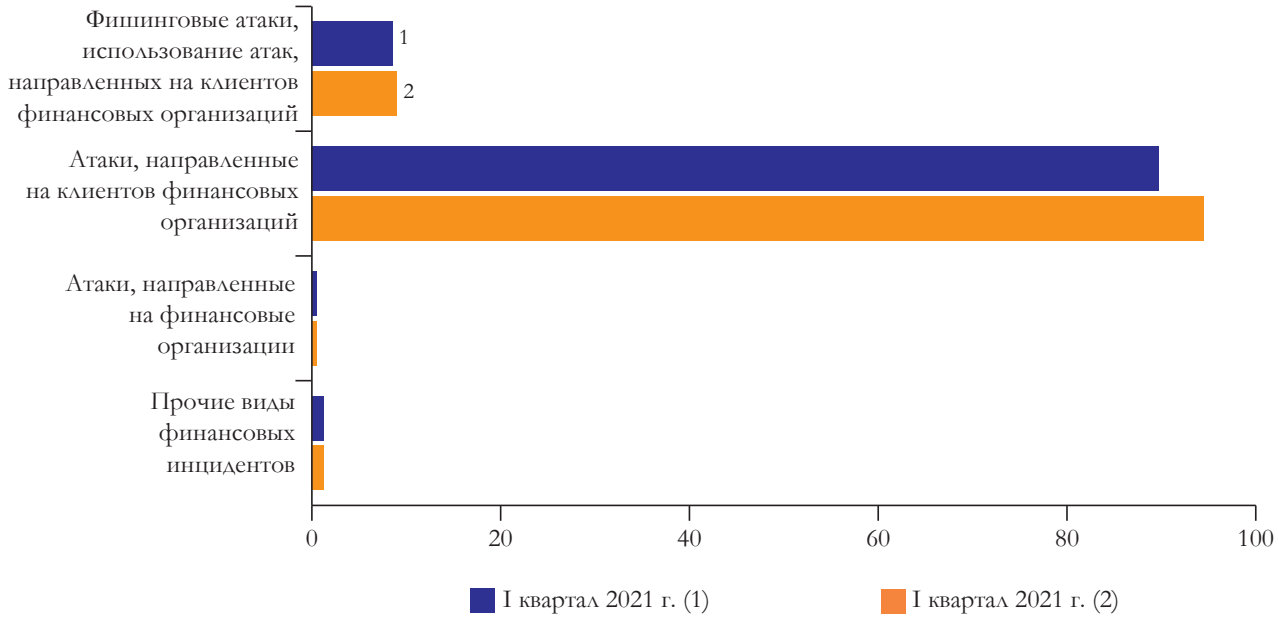
1) отсутствие прямой взаимосвязи между отправителем и получателем денежных средств, а также осуществление частых (периодических) переводов в отношении физических лиц;

2) перевод финансовых средств из территорий на территорию, не имеющих прямой или очевидной взаимосвязи с предпринимательской сферой или счетами физических, юридических лиц, индивидуальных предпринимателей;

3) посреднические операции, являющиеся получателями денежных средств от физических лиц или юридических лиц, а также вовлечение в финансовую сферу обращения компаний, относящихся к категории фирм-однодневок и т.д.

Следует учесть то, что киберпреступники используют широкий инструмент в схемах кражи и легализации незаконных доходов, имеется возможность поделить все типы операций по уровням риска. Если брать во внимание, что деятельность операторов денежных средств и операторов электронных кошельков находится под пристальным вниманием регулятора, и длительное время эта часть финансового рынка вычленялась от схем, которые использовали киберпреступники, то в сложившейся текущей ситуации в экономике к сферам повышенного риска можно отнести микрокредитование, площадки маркетплейс,

ломбарды, потребительские кооперативы, сервисы по оказанию услуг денежных переводов с использованием банковских карт [10]. Вместе с тем потенциальные финансовые субъекты (преступники и организованные преступные группировки) стремительно адаптируются в постпандемийном периоде. В целях реализации мошеннических схем создаются легальные бизнес-структуры для распространения и сбыта контрафактной продукции, а затем и последующего отмывания полученных в результате этого процесса денежных средств. С целью легализации доходов, полученных преступных путем, в большей мере используются современные IT-технологии, в том числе, основанные на механизме блокчейн операций по следующим основным видам финансовых атак (рис. 2).



Составлено авторами по материалам исследования [9]

Рис. 2. Сравнительная характеристика основных видов финансовых атак, %

В этой связи проработка и постоянное совершенствование нормативных актов является одним из важнейших действий для обеспечения информационной безопасности. Государственные, финансовые и иные учреждения должны иметь внутренние регламенты, составленные на основании нормативной документации государственных органов, включающие ответственность сотрудников данного учреждения или организации за несоблюдение правил информационной безопасности. Цифровое пространство на текущий момент является не только тем местом, где совершается большое количество экономических преступлений, но и является местом, где происходит легализация дохода, полученного в результате этих и других преступлений [11; 12].

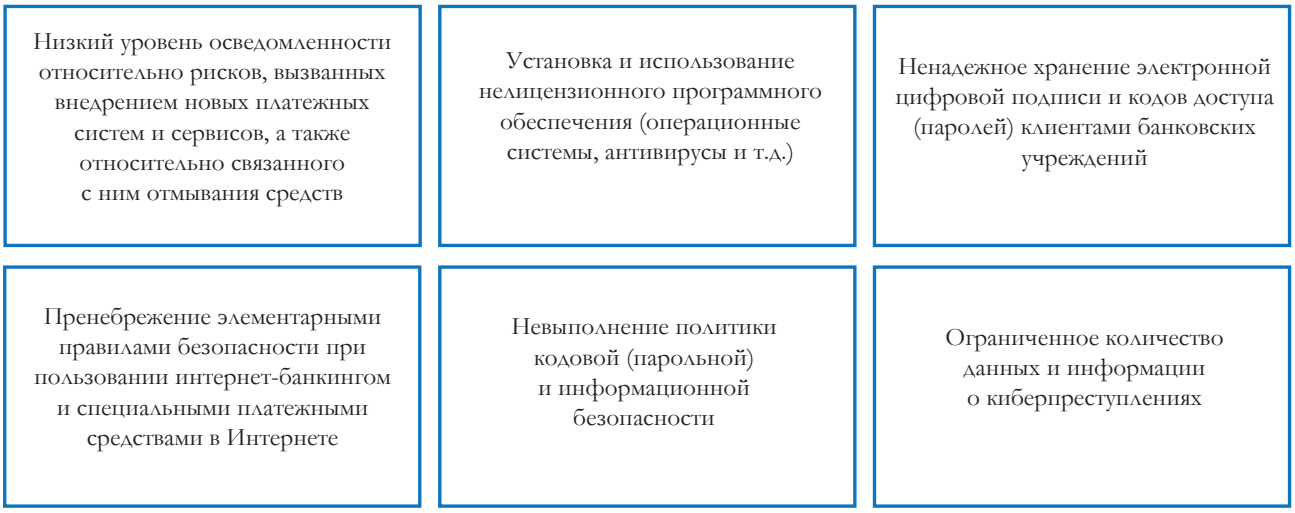
ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Важно отметить, что наиболее популярные схемы и механизмы преступлений в цифровом пространстве, которые были выявлены за последнее время, заключаются в использовании современных систем денежных переводов, в применении электронных кошельков, использовании электронных платежных систем, а также традиционных способов в форме срочных денежных переводов. Денежные средства, полученные в результате экономических преступлений в цифровом пространстве, или средства, полученные другим незаконным способом, а также денежные средства, которые требуется легализовать для уклонения от налогов, используются с целью приобретения предоплаченных карт (на российском рынке финансовых услуг данный инструмент предоставляют всего несколько кредитных организаций, что позволяет Банку России четко осуществлять регулирование этого направления банковского бизнеса), товаров или услуг в Интернете посредством приобретения этих товаров у подставных фирм или фирм-однодневок, а также путем перевода денежных средств в игровые фишки онлайн-казино или электронные деньги. Данные средства в дальнейшем перечисляются между электронными кошельками, банковскими картами, счетами организаций с последующей конвертацией в иную валюту (иностранная валюта,

электронные деньги, эмитированные различными кредитными организациями, а также в цифровые валюты) и обналичиваются [13].

Противодействие киберпреступности, а также способам легализации доходов от этих и других преступлений является первоочередным в современном цифровом мире. Для целей противодействия и легализации доходов, полученных преступным путем, кредитные организации и государство должны проводить мероприятия различного характера. Прежде всего, в процессе работы финансового подразделения, отвечающего за противодействие легализации доходов, полученным преступным путем. С учетом действующих нормативных документов в данной области можно выдвинуть следующие предложения для использования другими участниками рынка: регулярный осмотр банкоматов в целях выявления незаконно установленных устройств; расширение для клиентов банковских карт на основе микропроцессоров; внесение дополнительных требований, учитывающих двухфакторную аутентификацию пользователей и режим использования токенов при хранении электронных цифровых документов; осуществление генерации клиентских ключей и их привязка к серийному номеру жесткого накопителя, банка-клиента пользователя, а также анализ статистики интернет-трафика [14; 15].

Эффективное противодействие отмыванию преступных доходов и снижение уровня преступности в цифровом пространстве в большей степени возможны на основе постоянного сотрудничества финансового сообщества, а также осуществления специализированных мероприятий, направленных на передачу накопленного опыта, приводящего к своевременному выявлению финансовых операций, которые могут быть связаны с отмыванием доходов, полученных преступным способом. В связи с тем, что существенная доля населения не осведомлена о потенциальных возможностях киберпреступников, происходит огромное количество хищения денежных средств со счетов физических и юридических лиц. При этом по инициативе Банка России население периодически информируется о киберпреступлениях и фактах, наиболее применяемых в сфере мошеннических операций (рис. 3).



Составлено авторами по материалам исследования [9]

Рис. 3. Агрегированные сведения видов совершаемых киберпреступлений

Таким образом, законодательная определенность относительно организационно-правовых основ противодействия отмыванию средств преступного происхождения, принятие необходимых нормативно правовых актов, согласование положений таких актов между собой, четкая регламентация процедуры финансового мониторинга, взаимодействие органов власти являются основополагающими шагами для формирования контроля за финансовыми потоками. Достижение целей и выполнение задач, таких как усиление конструктивного взаимодействия РФ с иностранными (дружественными) государствами, а также развитие национальной системы механизмов мониторинга рисков и киберугроз на основе ресурсов Федеральной службы по финансовому мониторингу позволит применять эффективные способы и меры противодействия легализации доходов, полученных преступным путем, и финансированию терроризма. Такие задачи, прежде всего, направлены на предупреждение реализации угроз финансовой

безопасности и учитывают риски совершения операций без создания искусственных регулятивных барьеров для достижения устойчивости экономики.

ЗАКЛЮЧЕНИЕ

В качестве основных вариантов по решению проблемных задач, с которыми сталкиваются российские финансовые организации, следует выделить следующие аспекты.

1. Киберпреступники, как правило, создают «зеркало» популярного интернет-сайта по предоставлению товаров (работ, услуг), на основании которого осуществляется подмена одной интернет-страницы на страницу иного сайта, где имеются перезаполненные данные, например, номер мобильного телефона/карты. Пользователь сайта зеркала, не подозревая ничего, выбирает товар или услугу, переходит к странице оплаты и ввода карточных данных, совершает оплату. В момент оплаты денежные средства не списываются с карты плательщика и отправляются по реквизитам злоумышленников. Кредитные организации как эквайер интернет-страниц, где оказываются услуги по переводам и платежам, несет все риски, связанные с данной операций, так как в случае оспаривания операции со стороны плательщика денежные средства будут возвращены, а компания может быть привлечена к штрафам со стороны Банка России за нарушение правил финансового мониторинга. В качестве мер по противодействию киберопреступлений в данной ситуации возможно ввести лимитирование по количеству и сумме переводов и/или количеству переводов на одну банковскую карту в течение дня, а также установить ограничения на подключение к интернет-странице с одного и того же IP-адреса, в том числе блокировать иностранные IP-адреса.

2. Банк России активно осуществляет контроль за нелегальными онлайн-казино путем блокировки различных подставных компаний, через которые происходит движение денежных средств. В свою очередь, на финансовом рынке появляются различные схемы маскировки деятельности нелегальными онлайн-казино под деятельность микрофинансовых компаний и/или ломбардов, коллекторских агентств и прочих компаний, ведущих аналогичную деятельность. С учетом того, что микрофинансовые компании активно развивают свою деятельность в IT-каналах (выдача и погашение займов без похода в оффлайн отделения), часто пользуются услугами банков эквайеров при осуществлении переводов денежных средств на банковские карты (выдача займа) и с использованием банковских карт обратно на счет компании (погашение займа), денежные средства осуществляемых переводов в обе стороны практически идентичны суммам среднестатистического выигрыша или ставки. Аналогичным образом происходит процедура переводов в пользу компании под видом погашения денежных займов, но по факту все переводы являются ставками. Игрок казино даже не подозревает, что совершает перевод в адрес микрофинансовой компании, так как совершает все действия на сайте виртуального казино. Избежать ситуаций, когда эквайер обслуживает нелегальные онлайн-казино, возможно на основе введения процедуры идентификации юридического лица, а также при осуществлении мониторинга операций клиентов для выявления мошеннических действий. Операции по переводу на карты не должны превышать суммы, указанные в правилах выдачи микрозаймов. При этом частота погашений займа и общей суммы за максимально возможный срок займа с одной карты не может превышать сумму выданного займа с учетом максимально возможной суммы начисленных процентов.

3. Эквайринг все чаще используется мошенниками и организаторами схем легализации доходов для отмывания денежных средств. Одним из способов обналичивания денежных средств является так называемый «обратный эквайринг» – возврат денежных средств на банковскую карту физического или юридического лица без оригинальной операции покупки. Крупные торгово-сервисные предприятия могут использовать данную схему для частичного ухода от налогообложения. Избежать вовлечение банка-эквайера в схему с «обратным эквайрингом» возможно только при постоянном анализе операций торгово-сервисных предприятий. А в случае возрастающего количества операций возврата покупки без оригинальной операции покупки следует принять меры со стороны сотрудников подразделения финансового мониторинга. При этом регулятор должен анализировать весь денежный поток, проходящий через конкретный банк эквайер, и в случаях высокой концентрации таких типов операций принимать необходимые ограничительные меры.

4. Эквайринг используется не только как конечное звено в цепочке по обналичиванию денежных средств, но и как инструмент для транзита денежных средств в схеме легализации доходов, полученных незаконным путем. Во избежание вовлеченности в легализацию денежных средств необходимо

организовывать внутренние проверки системных настроек соответствующего ПО. Для эквайера также необходимо анализировать типы карт, с которых осуществляются операции в торгово-сервисных предприятиях, с которыми заключен договор по обслуживанию. И в случае высокой концентрации платежей с использованием корпоративных карт необходимо принять меры со стороны сотрудников подразделения финансового мониторинга.

Библиографический список

1. Лужнова Л.А. Защита прав и законных интересов потребителей банковских услуг как фактор повышения их финансовой безопасности. *Банковские услуги*. 2022; 9: 22–27 с. https://doi.org/10.36992/2075-1915_2022_9_22
2. Бронц Э.А. Внедрение технологии блокчейн в государственно-финансовый контроль Российской Федерации. *Финансовая экономика*. 2023; 1: 8–10 с.
3. Шумилин В.П., Лысенко Е.С., Острякова А.Ф. Проблемы законодательства о киберпреступности. *Аграрное и земельное право*. 2022; 5(209): 137–140 с. https://doi.org/10.47643/1815-1329_2022_5_137
4. Намиот Д.Е. О кибербезопасности систем Интернета Вещей. *International Journal of Open Information Technologies*. 2023; 11(2):85–97 с.
5. Филиппов Н.В. Подход к созданию экспертной системы оценки информационной безопасности телекоммуникационных систем. *Электросвязь*. 2022; 2: 61–66 с. https://doi.org/10.34832/ELSV.2022.27.2.009
6. Михайленко Н.В., Мурадян С.В., Вихляев А.А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях. *Аудиторские ведомости*. 2022; 1: 140–145 с. https://doi.org/10.24411/1727-8058-2022-1-140-145
7. Маслов С.Н., Щербакова И.В. К вопросу определения сущности понятий киберпространства и киберпреступлений. *Закон и право*. 2022; 6: 169–171 с. https://doi.org/10.24412/2073-3313-2022-6-169-171
8. Федотова Г.В., Орлова Е.Р., Бочарова И.Е. Вопросы кибербезопасности цифровых финансовых сервисов. *Информационные технологии и вычислительные системы*. 2022; 2: 37–45 с. https://doi.org/10.14357/20718632220205
9. Центральный банк России. *Обзор операций, совершенных без согласия клиентов финансовых организаций. Ежегодный аналитический отчет Банка России*. https://cbr.ru/analytics/ib/operations_survey_2022// (дата обращения: 11.03.2023).
10. Гусев А.И. Новые технологии Private banking как защита от уэйлинга. *Банковское дело*. 2022; 8: 64–68 с.
11. Крусс И.А. Развитие технологий искусственного интеллекта в банковском секторе. *Банковское дело*. 2022; 9: 62–65 с.
12. Антропов К.Ю., Ахмадеев Р.Г., Косов М.Е. Кибербезопасность и сохранение цифрового суверенитета экономики. *Вестник экономической безопасности*. 2021; 5: 268–273. https://doi.org/10.24412/2414-3995-2021-5-268-273
13. Минбалеев А.В. Правовое обеспечение кибербезопасности как фактор устойчивого развития и реализации ESG-стандартов. *Информационное право*. 2022; 1: 35–38 с. https://doi.org/10.55291/1999-480X-2022-1-35-38
14. Шарипов Ф.Ф., Дьяконова М.А., Сюй М. Особенности цифрового управления современной экономикой. *Вестник университета*. 2022; 7: 138–144 с. https://doi.org/10.26425/1816-4277-2022-7-138-144
15. Богданова М.В. Профилактика киберпреступлений с использованием информационных технологий. *Управленческий учет*. 2022; 11(3): 674–679 с. https://doi.org/10.25806/uu11-32022674-679

References

1. Luzhnova L.A. Protection of the rights and legitimate interests of consumers of banking services as a factor in increasing their financial security. *Banking services*. 2022; 9: 22–27 pp. https://doi.org/10.36992/2075-1915_2022_9_22 (In Russian).
2. Brontz E. A. Introduction of blockchain technology in state-financial control of the Russian Federation. *Financial Economics*. 2023; 1: 8–10 pp. (In Russian).
3. Shumilin V.P., Lysenko E.S., Ostryakova A.F. Problems of cybercrime legislation. *Agrarian and Land Law*. 2022; 5(209): 137–140 pp. https://doi.org/10.47643/1815-1329_2022_5_137 (In Russian).
4. Namiot D.E. On the cybersecurity of Internet of Things systems. *International Journal of Open Information Technologies*. 2023; 11(2):85–97 pp. (In Russian).
5. Filippov N.V. An approach to creating an expert system for assessing the information security of telecommunications systems. *Telecommunications*. 2022; 2: 61–66 pp. https://doi.org/10.34832/ELSV.2022.27.2.009 (In Russian).
6. Mikhailenko N.V., Muradyan S.V., Vikhlyaev A.A. Topical issues of monitoring and countering cyber threats in peer-to-peer networks. *Auditorskie vedomosti*. 2022; 1: 140–145 pp. https://doi.org/10.24411/1727-8058-2022-1-140-145 (In Russian).
7. Maslov S. N., Shcherbakova I. V. To the question of determining the essence of the concepts of cyberspace and cybercrime. *Law and Law*. 2022; 6: 169–171 pp. https://doi.org/10.24412/2073-3313-2022-6-169-171 (In Russian).
8. Fedotova G.V., Orlova E.R., Bocharova I.E. Issues of cybersecurity of digital financial services. *Information technologies and computing systems*. 2022; 2: 37–45 pp. https://doi.org/10.14357/20718632220205 (In Russian).

9. The Central Bank of the Russian Federation. *Review of transactions made without the consent of clients of financial organizations. Annual Analytical Report of the Bank of Russia. https://cbr.ru/analytics/ib/operations_survey_2022//* (accessed 11.03.2023).
10. Gusev A.I. New technologies of Private banking as a defense against wailing. *Banking*. 2022; 8: 64–68 pp. (In Russian).
11. Kruss I.A. Development of artificial intelligence technologies in the banking sector. *Banking*. 2022; 9: 62–65 pp. (In Russian).
12. Antropov K.Y., Akhmadeev R.G., Kosov M.E. Cybersecurity and the preservation of digital sovereignty of the economy. *Vestnik ekonomicheskoi bezopasnosti*. 2021; 5: 268–273 pp. https://doi.org/10.24412/2414-3995-2021-5-268-273 (In Russian).
13. Minbaleev A.V. Legal provision of cybersecurity as a factor of sustainable development and implementation of ESG-standards. *Information Law*. 2022; 1: 35–38 pp. https://doi.org/10.55291/1999-480X-2022-1-35-38 (In Russian).
14. Sharipov F.F., Diakonova M.A, Xu M. Features of digital management of modern economy. *Vestnik Universiteta*. 2022; 7: 138–144 pp. https://doi.org/10.26425/1816-4277-2022-7-138-144 (In Russian).
15. Bogdanova, M. V. Cybercrime prevention using information technology. Management *Accounting*. 2022; 11(3): 674–679 pp. https://doi.org/10.25806/uu11-32022674-679 (In Russian).