Юлия Сергеевна Евлахова

доктор экономических наук, доцент, заведующий кафедрой финансового мониторинга и финансовых рынков Ростовского государственного экономического университета (РИНХ), г. Ростов-на-Дону, evlahova@yandex.ru

Анастасия Сергеевна Клабукова

студентка направления «Финансовая безопасность и финансовые рынки в цифровой экономике» Ростовского государственного экономического университета (РИНХ), г. Ростов-на-Дону, klabukova1406@gmail.com

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ КАК УГРОЗА ФИНАНСОВОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА И ГРАЖДАНИНА

Аннотация. Сегодня в связи с появлением новых информационных технологий появляются и новые, более совершенные каналы проникновения преступников в финансовую систему государства. Поэтому своевременное их выявление дает возможность пойти на опережение и разработать ответные меры. В данной работе рассмотрена специфика угроз финансовой безопасности в контексте цифровизации, понятие киберпреступности и ее направления. Реализован обзор схем отмывания доходов, полученных преступных путем, с использованием современных технологий, выявлены риски использования электронных средств платежа в преступных целях. Проведен анализ развития цифровизации экономики и динамики совершения киберпреступлений в России, а также представлены направления развития информационных технологий в борьбе с киберпреступностью и легализацией преступных доходов.

Ключевые слова: финансовая безопасность, цифровизация, угрозы, киберпреступность, криптовалюты, отмывание преступных доходов.

Yulia Sergeevna Yevlakhova

Doctor of Economics, Associate Professor, Head of the Department Financial Monitoring and Financial Markets of Rostov State University of Economics (RINH), Rostov-on-Don, evlahova@yandex.ru

Klabukova Anastasia Sergeevna

Student of the specialty "Financial Security and Financial Markets in the Digital Economy", Rostov State University of Economics (RINH), Rostov-on-Don, klabukova1406@gmail.com

DIGITALIZATION OF THE ECONOMY AS A THREAT TO THE FINANCIAL SECURITY OF THE STATE AND CITIZEN

Abstract. Today, due to the emergence of new information technologies, new, more advanced channels for criminals to penetrate the financial system of the state are also emerging. Therefore, timely detection of them makes it possible to go ahead and develop response measures. This paper examines the specifics of threats to financial security in the context of digitalization, the concept of cybercrime and its directions. An overview of schemes for laundering proceeds from crime using modern technologies has been implemented, the risks of using electronic means of payment for criminal purposes have been identified. The analysis of the development of the digitalization of the economy and the dynamics of cybercrime in Russia is carried out, as well as the directions of the development of information technologies in the fight against cybercrime and the legalization of criminal proceeds are presented.

Keywords: financial security, digitalization, threats, cybercrime, cryptocurrencies, money laundering.

Финансовая безопасность — одна из важнейших составляющих национальной безопасности государства. От того, насколько страна финансово устойчива, зависит уровень и динамика ее социально-экономического развития. В то же время финансовая устойчивость любого государства подвержена различным угрозам, как со стороны внешних, так и со стороны внутренних факторов. Одной из таких угроз является стремительное развитие цифровых

технологий. Несмотря на очевидную пользу цифровизации для развития финансовой системы, способствующего укреплению финансовой безопасности, цифровые технологии становятся незаменимым инструментом преступников, позволяя им совершать все более продуманные и филигранные схемы финансовых махинаций, мошенничества и отмывания преступных доходов. Расширение масштабов теневой экономики, значительно растущей в эпоху компьютерных инноваций, оказывает, несомненно, деструктивное влияние на финансовую безопасность государства и каждого его гражданина.

Под финансовой безопасностью понимают такое состояние экономики и финансовых отношений, при котором создаются оптимальные условия для стабильного развития страны, позволяющие сохранять целостность финансовой системы и обеспечивать эффективную нейтрализацию рисков и угроз в экономической сфере, а также деятельность государства по защите национальных интересов через поддержание финансовой стабильности [1, с. 20-22]. Финансовая безопасность личности — это социально-экономическое состояние человека, при котором гарантированы материальные условия защиты его жизненных интересов, обеспечение социальной защищенности [2, с. 64]. Она зависит от политики государства, включающей в себя способы предотвращения угроз и ликвидации последствий отрицательных составляющих внешней и внутренней среды.

Для того чтобы обеспечить в стране достаточный уровень финансовой безопасности, необходимо своевременно выявлять ее угрозы. Это различные кризисные ситуации, способные нанести ущерб финансовой системе государства, национальным и личным интересам граждан. Многие авторы (В.С. Кудряшов, В.Ю. Доберчук [3, с. 5-6], Н.Н. Губернаторова [1, с. 32] и др.) сходятся на том, что значительной угрозой финансовой безопасности является расширение масштабов теневой экономики. А в современных условиях стремительной информатизации темпы роста криминализации экономики все сильнее повышаются из-за появления новых орудий совершения экономических и финансовых преступлений. В этой связи цифровизация экономики является не только трамплином для ее развития, но и одной из наиболее значительных угроз ее безопасности. Финансовая безопасность отдельно взятой личности также подвержена ряду угроз. К ним можно отнести, например, дифференциацию по уровню доходов, низкий уровень ВВП на душу населения, бедность и безработицу. Не менее значительной угрозой является криминогенная обстановка. Подверженность граждан становиться жертвами мошенничества и других экономических преступлений может быть вызвана недостаточным уровнем финансовой грамотности или слабо развитой системой нормативного регулирования. Финансовая безопасность личности связана с финансовой безопасностью государства, поэтому нейтрализация этих угроз зависит от направлений государственной политики.

Влияние цифровизации на финансовую безопасность: риски использования электронных платежных средств для легализации преступных доходов

Цифровая трансформация, проникшая во все сферы жизнедеятельности, оказывает существенное влияние и на развитие экономики, в результате чего в ней выделилась особая ветвь — цифровая экономика. В.И. Глотов и А.У. Альбеков [4, с.154] отмечают, что цифровизация мировой экономики создает

новый формат взаимодействия участников хозяйственных отношений, формирует особую инновационную среду для бизнеса, способствует наращиванию государствами конкурентных преимуществ и обеспечению роста производительности предприятий.

Однако необходимо учитывать и риски, которые несет за собой данное явление. Так, Э. А. Золаев [5, с. 577-578] считает значительной проблемой зависимость процесса информатизации российской экономики от иностранных технологий. Это означает прирост инвестиций в иностранные экономики и утечку капитала за рубеж, что приведет к недостаточному развитию собственной экономики. В условиях санкционного давления и напряженной политической обстановки в мире проблема зависимости от зарубежных программных продуктов особенно актуальна. Этим обусловлена необходимость налаживания собственных отечественных разработок, поддержка импортозамещающего производства программного обеспечения и необходимой техники. Среди социальных угроз автор акцентирует внимание на росте структурной безработицы. Очевидно, что вместе с активным внедрением информационных процессов в различные сферы производства снижается потребность в некоторых устаревших профессиях. При этом возникает спрос на новые специальности, требующие особых компетенций в цифровой сфере, однако недостаточный уровень квалификации может препятствовать полной занятости. Как итог, растет социальная напряженность, криминализация общества и развитие теневого сектора.

Среди угроз финансовой безопасности многие авторы особое внимание уделяют рискам использования информационных технологий, в том числе виртуальных валют, в преступных целях. ФАТФ определяет [6] виртуальные валюты как средство выражения и хранения стоимости, предназначенное для обмена в цифровой форме, которое не обладает статусом законного платежного средства и может выполнять свои функции только по соглашению в рамках сообщества ее пользователей. Федеральный закон «О цифровых финансовых активах» [7] признает ее как «цифровую валюту» и определяет как совокупность электронных данных, содержащихся в информационной системе, которые могут быть приняты в качестве средства платежа, не являющегося денежной единицей РФ или другого государства или в качестве инвестиций. Наибольшую популярность сегодня приобрели децентрализованные цифровые валюты — криптовалюты. Безусловно, их развитие приносит мировой финансовой системе определенную пользу. Виртуальные валюты обладают возможностью увеличить эффективность платежей и снизить их издержки, стимулировать международные переводы, используются в качестве средства инвестиций. Однако многие особенности виртуальных активов могут нести за собой определенные риски.

Так, Бекетнова Ю.М [8, с. 2 14-215] выделяет четыре типа уязвимостей виртуальных валют и электронных денег. Первая уязвимость связана с высокой скоростью перемещения денежных средств, большими объемами платежей и отсутствием лимитов на количество операций перевода. Во-вторых, операции с виртуальными валютами не требуют личного контакта между плательщиком, получателем и самой системой. Третья уязвимость состоит в международном характере электронных сделок. Отсутствие границ в платежных системах мо-

гут привести к такой ситуации, что отправитель, получатель и сама система могут располагаться в совершенно разных юрисдикциях, что препятствует контролю над такими операциями и расследованиям особо подозрительных из них. И в-четвертых, некоторые системы онлайн-платежей могут находиться в странах со слабо развитой системой ПОД/ФТ, что ведет к снижению эффективности борьбы с незаконными операциями.

В отчете ФАТФ [6] в качестве главной уязвимости данных активов выделяют их анонимность. В децентрализованных системах адреса, которые используются в качестве счетов, не содержат идентификационной информации, которая могла бы установить личность пользователя, и в них не обеспечивается учет данных о прошлых операциях, с которыми связан данный пользователь. Кроме того, отсутствует контролирующий орган для выявления схем подозрительных операций, и правоохранительные структуры не в силах определить одно центральное место или администратора для проведения расследований. Таким образом, виртуальные активы дают преступникам большие возможности для их незаконного использования в целях отмывания денег и финансирования терроризма.

В. И. Глотов, А.У. Альбеков [4, с. 180-182] выделяют три основные группы рисков, связанных с использованием криптовалюты в целях ОД/ФТ. Среди технологических рисков отмечаются анонимность, транснациональность, децентрализованность. К экономическим рискам относятся уход от налогообложения, сложность определения бенефициара, а к правовым — пробелы в законодательстве в сфере обращения криптовалют, отсутствие должного надзора за обращением и недостаточная подготовка правоохранительных органов к расследованиям в данной сфере. Усложнилась ситуация с появлением инновационных блокчейн-технологий: «анонимайзеров», тумблеров («смесителей») и прочих, способствующих легализации преступных доходов путем запутывания цепочек операций, смешивания и перемены местами адресов кошельков. Для снижения и нейтрализации данных рисков необходимо разработать единый подход к контролю и обеспечить эффективное нормативно-правовое регулирование использования виртуальных валют.

Понятие, виды и направления киберпреступности

Распространение цифровых технологий коррелирует с расширением масштабов киберпреступности, что несет в себе безусловную угрозу финансовой безопасности государства в виде отмывания доходов, полученных от данных видов преступности.

Под киберпреступлением понимается акт социальной девиации, имеющий целью нанесение экономического, политического, культурного и других видов ущерба индивиду, организации или государству при помощи любого технического средства, имеющего доступ в Интернет [8, с. 223]. Так как оно относится к числу предикатных преступлений, выделяется несколько направлений легализации доходов, полученных от киберпреступлений:

– обналичивание (в том числе с использованием «денежных мулов»), использование мобильных платежных систем, открытие счетов в банках;

– покупка высоколиквидных товаров для последующей перепродажи;

– покупка билетов и других товаров через интернет с целью возврата (или перепродажи) с целью получения наличных денег.

Ю.М. Бекетнова [8, с. 234-241] приводит примеры схем кибермошенничества. Так, существует схема массового маркетинга, при котором создается сайт-одностраничник интернет-магазина с очень низкими ценами, отсутствием отзывов и скудными контактными данными. Переписка с псевдопродавцом ведется по электронной почте, затем покупатель перечисляет деньги с использованием электронных платежных систем за границу на имена подставных лиц, и после получения денег псевдопродавец исчезает.

Особое внимание автор уделяет мошенничеству с банковскими картами. Это могут быть как операции без присутствия карты (когда преступники пользуются украденными с помощью скимминга реквизитами карты для покупок в сети Интернет), так и изготовление дубликатов настоящей карты, открытие банковского счета с использованием поддельных или украденных документов и т. д. Особым рискам подвержена система дистанционного банковского обслуживания (ДБО). В процессе атаки на нее злоумышленники получают удаленный доступ к учетным записям физических или юридических лиц, переводят их денежные средства на счета подставных лиц, а затем отмывают с использованием тех же банковских операций и дальнейшего обналичивания с помощью «дропов». К признакам легализации доходов от кибермошенничества относятся, например, совершение сделок в вечернее или ночное время, участие большого количества иностранных физических и юридических лиц, IP-адресов; отсутствие очевидных деловых связей между участниками сделки; конвертацию в электронные деньги посредством обменных площадок и др.

Согласно типологическому исследованию ЕАГ о киберпреступности [9], среди киберпреступлений, направленных на обогащение злоумышленников путем кражи денежных средств, выделяются три группы:

1. Мошенничество в сети Интернет (финансовые пирамиды, Интернет-аукционы, ПО для хищения финансовой, коммерческой или персональной информации).

2. Мошенничество в системах ДБО (вирусы для перехвата доступа клиентов к Системе, проведение несанкционированных операций в Системе и др.).

3. Мошенничество с банкоматами и картами (клонирование, кража карт; скимминг — установка на банкоматы считывающих устройств с целью получения реквизитов; вмешательства в работу банкоматов с целью присвоения чужих наличных).

Для отмывания средств, полученных от данного вида преступлений, используются как традиционные методы легализации (использование фиктивных компаний-однодневок, счетов на подставных лиц или по украденным документам, обналичивание с помощью «денежных мулов» и т. д.), так и методы с использованием цифровых технологий, таких как электронные кошельки, онлайн-покупки товаров через Интернет и др.

И.П. Заварзина [10, с. 5] отмечает, что наиболее рискованной сферой для киберпреступности является кредитно-финансовая система, в которой сосредоточены масштабные объемы денежных средств. Она упоминает о рисках, связанных с интернет-банкингом, при котором все данные клиента хранятся в его мобильном телефоне. На сегодняшний день распространена схема рассылок

вредоносных поддельных ссылок через социальные сети. Это связано с тем, что социальные сети сейчас разрабатывают собственные платежные системы (например, VK Pay), которые пользователь может использовать как электронный кошелек, привязав к нему свою карту. Таким образом, пользователь социальной сети просто переходит по неизвестной ссылке, которую злоумышленники могут умело замаскировать нейтральным контекстом, и все реквизиты банковского счета, который был привязан к аккаунту, оказываются в руках мошенников, что позволяет им получить доступ ко всем имеющимся на данном счете денежным средствам.

Динамика развития цифровизации и распространения киберпреступности в России

Развитие информационных технологий является одной из приоритетных национальных целей РФ. Так, одним из 14 национальных проектов является проект «Цифровая экономика», цели которого — создание условий для высокотехнологичного бизнеса, повышение конкурентоспособности на мировом рынке и другие. Не менее важно внедрение IT-решений в работу различных сегментов финансовой системы. Рынок цифровых технологий в финансовой сфере — финтех — один самых быстроразвивающихся рынков в мире. По некоторым исследованиям [11], к 2035 г. около 96% всех финансовых операций будут осуществляться с помощью инновационных технологий. По данным исследования РБК [12], финтех-рынок в России с 2017 по 2021 гг. вырос с 31,7 млрд руб. до 67,1 млрд руб., то есть почти в два раза.

Как отмечают специалисты «Сколково» [13], в 2021 г. уровень распространенности финтех-услуг в России достиг 82%, что относит нашу страну к числу лидеров в этой сфере (данный показатель выше только в Индии и Китае). Проследить за динамикой этого показателя можно, обратившись к исследованию С.В. Ештокина [14, с.1927] (рис. 1)

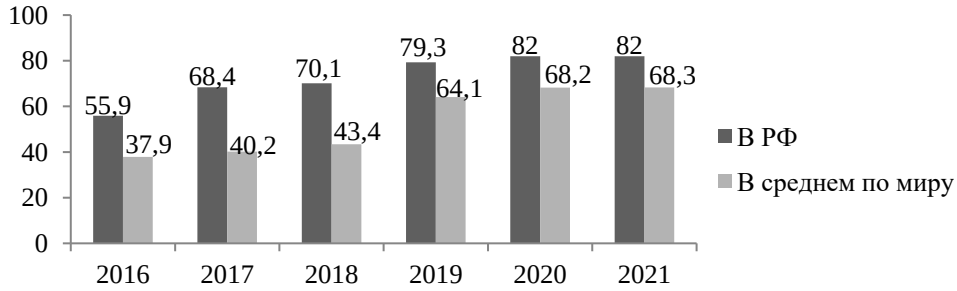

Рис. 1. Динамика проникновения финтех-услуг (в %)

Источник: составлено автором по данным [14, с. 1927].

Таким образом, по рисунку 1 наблюдается положительная динамика внедрения финтех-трендов в России, что говорит о высоких темпах роста интегрирования цифровых технологий в финансовую сферу. Данный показатель и в динамике превышает среднемировой медианный уровень, что свидетельствует

о том, что наша страна занимает лидирующие позиции в этой отрасли. Новейшие цифровые технологии задействованы практически во всех направлениях деятельности финансовых организаций: необанкинг и платежные сервисы, финансовые маркетплейсы и электронные кошельки, а также прикладные решения для кредитных организаций: программы лояльности, автоматизация банковских процессов и облачные технологии. Что касается финансирования финтех-направления, согласно исследованию «Сколково», объем инвестиций в финтех-стартапы только за первое полугодие 2021 г. составил 78 млн долларов, что составило 7,8% от общего объема венчурных инвестиций в 1 млрд долларов. (В 2020 г. общий объем составил всего 500 млн долларов, то есть на 50% меньше).

Любые инновации могут иметь и отрицательные последствия. Цифровые технологии, в особенности виртуальные валюты, могут быть задействованы преступниками в наркобизнесе, коррупционных схемах, на рынке поддельных денежных средств и документов и т. д. Так, по данным МВД РФ [15], за 2022 год всего было зарегистрировано 522 065 преступлений с использованием компьютерных технологий. Сопоставив эту цифру с данными за прошлые годы из исследования А.В. Пахарева [16, с.461], можно увидеть следующую динамику (рис. 2).

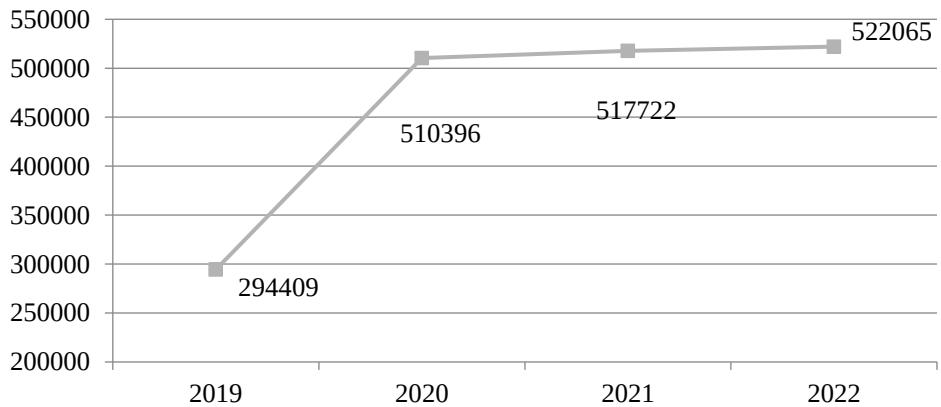

Рис. 2. Динамика зарегистрированных IT-преступлений в России

Источник: составлено автором по данным [15, 16, с .461].

Согласно рис. 2, число IT-преступлений на 2022г, по сравнению с 2021 увеличилось на 4 343 шт., или на 0,84%. В целом по прошлым годам наблюдается положительная динамика, поэтому можно говорить о тенденции к росту числа IT-преступлений. Для оценки уровня преступности важно оценивать не только объем совершенных нарушений, но и уровень их раскрываемости. На основе отчета МВД [15] рассмотрим динамику выявления и раскрываемости по некоторым отдельным видам преступлений, в которых были использованы цифровые технологии (см. табл. 1).

Таблица 1

Сравнительная таблица о результатах деятельности органов внутренних дел РФ по противодействию преступлениям за 2022 и за 2021 гг.

Виды преступлений	*Количество преступлений*		*Раскрыто*		*Раскрываемость, %*	
	2022	*2021*	*2022*	*2021*	*2022*	*2021*
С использованием пластиковых карт	127149	165658	42682	40369	32,4	23,6
Кража	113565	156792	42706	41961	36,3	25,8
Мошенничество	257606	249249	30232	21610	12,0	9,0
Связанные с незаконным оборотом наркотиков	62209	51444	27979	19697	48,4	40,9
Всего преступлений, совершенных в сфере компьютерной информации	522065	517722	142384	118920	27,8	23,4

Источник: составлено автором по данным [15].

Как видно из табл. 1, наибольший объем у преступлений с мошенническими схемами (они составляют около 50% от общего числа), и при этом их процент раскрываемости наименьший. Это значит, что мошенничество является одной из глобальных угроз с точки зрения преступлений в компьютерной сфере. Говоря о динамике, объем зарегистрированных преступлений по таким направлениям, как мошенничество и преступления, связанные с НОН, увеличивается, что следует оценивать негативно. Процент раскрываемости как по отдельным статьям, так и в целом, растет, однако он не превышает даже 50% и все еще остается на низком уровне.

Очевидно, что правоохранительная система не успевает адаптироваться к цифровой трансформации преступного мира. Значительное влияние могут оказывать пробелы в законодательстве, которое не успевает корректироваться со скоростью, равной скорости развития технологий, а в этой сфере особенно важна оперативность. В частности, в сфере регулирования криптовалют до сих пор не существует единого нормативного подхода к их регулированию. В России еще идет процесс выработки правовых рамок для майнинга, выпуска и обращения цифровых валют в стране. Так, 17 ноября 2022 г. в Государственную Думу был внесен законопроект (О внесении изменений в Федеральный закон «О цифровых финансовых активах») [17], регулирующий процедуру майнинга криптовалют и их последующую продажу. Но пока еще нет четких границ регулирования, и обращение криптовалют остается без контроля государства, они несут серьезную угрозу финансовой безопасности ввиду своей привлекательности для криминальных структур.

Так, согласно отчету о криптопреступлениях Chainalysis 2021 [18], в России оборот криптовалют на рынках даркнета на 2020 год составил 288 млн долларов, что значительно выше объема криптовалютных транзакций в других странах (см. рис. 3).

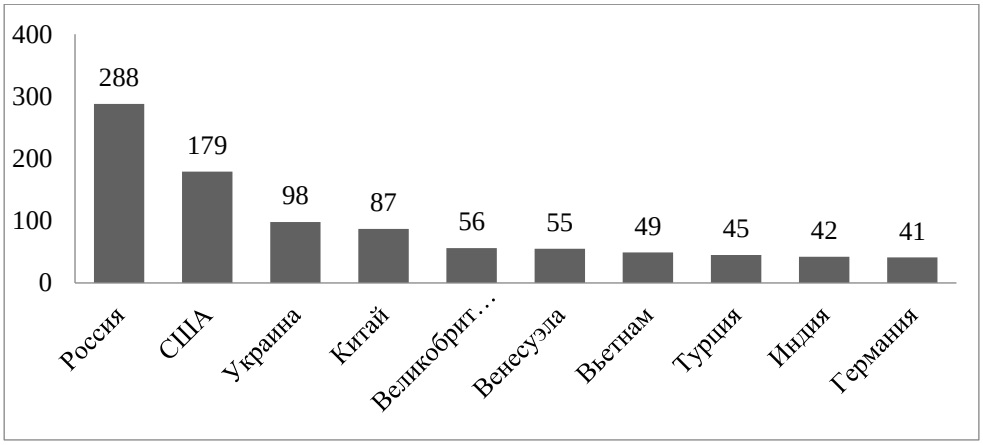

Рис. 3. Объем оборота криптовалют на рынках даркнета в 2020 г. (млн долл.)

Источник: составлено автором по данным [18].

Из рис. 3 мы видим, что Россия с большим отрывом занимает абсолютную лидирующую позицию в данном антирейтинге, что говорит о высокой криминализации использования криптовалют в нашей стране.

Таким образом, несмотря на высокие темпы роста цифровой экономики и финтеха, которые способствуют общему социально-экономическому развитию страны, высокая активность теневых структур и неспособность правоохранительных органов оперативно реагировать на их деятельность наносят серьезную угрозу финансовой устойчивости нашей страны и ее граждан.

Современные направления борьбы с киберпреступлениями и ОД/ФТ с использованием цифровых технологий

Для обеспечения должного уровня финансовой безопасности в контексте новых угроз, возникших в эпоху цифровизации, необходим комплекс мероприятий по их нейтрализации.

Так, А.В. Пахарев в своей работе [16, с.466] представляет комплекс мер в области кибербезопасности. Во-первых, необходимо создание эффективного государственного института по разработке и координации исполнения данных мер. Во-вторых, автор предлагает наладить международное сотрудничество в процессе разработки нормативной базы и инструментария для раскрытия киберпреступлений, совершенных из-за рубежа.

Также рекомендуется создать оптимальные условия для частно-государственного партнерства, обеспечить достаточный уровень инвестиций в собственное производство высокотехнологичных отраслей, выработать четкую государственную политику в отношении регулирования цифровых валют. Кроме того, одним из главных условий поддержания уровня финансовой безопасности является повышение уровня финансовой грамотности в обществе.

Для того чтобы пресекать рост теневого сектора за счет цифровой трансформации, государству необходимо идти на опережение — разрабатывать собственные инновационные технологии, препятствующие проникновению преступности в экономическую сферу. Так, одним из направлений в области

цифровизации российской экономики является проект Банка России «Цифровой рубль» как создание третьей формы денег. На данный момент уже производится тестирование прототипа платформы цифрового рубля. Как считает Помулев А.А. [19, с. 272-273], основной задачей цифрового рубля может быть контроль за деятельностью хозяйствующих субъектов и государственными расходами. Действительно, его целесообразно использовать в сфере государственных закупок, например. При отсутствии наличных и безналичных расчетов легко будет прослеживаться цепочка транзакций, и будет возможно отслеживать, на что потрачен каждый цифровой рубль, выявлять и пресекать незаконные операции. Однако необходимо еще заинтересовать частный бизнес и физические лица хранить свои деньги и производить расчеты в цифровом рубле (так как на размещенные в кошельках цифровые рубли не будет начисляться процентный доход), потому что отсутствие их мотивации может нивелировать все преимущества нововведения.

В сфере ПОД/ФТ стремительно внедряются такие технологии, как, например, искусственный интеллект и нейронные сети. Особенно они актуальны для работы комплаенс-отделов кредитных организаций, повышая точность и оперативность при выявлении подозрительных операций и рисков, позволяя анализировать множество источников и помогая человеку принимать более качественные решения. Не менее важен проект Банка России, действующий с 1 июля 2022 г. — платформа «ЗСК» («Знай своего клиента»). Он подразумевает взаимодействие регулятора с коммерческими банками, в формате которого все поднадзорные организации в ежедневном режиме получают реестры клиентов в форме «банковского светофора», то есть распределенные по уровню риска участия в подозрительных операциях. Еще до своего внедрения, в ходе пилотирования платформа была высоко оценена [20, с. 15] за достоверность и полезность оценок, а значит, она имеет потенциал для поднятия эффективности антиотмывочной системы. Стоит также отметить стремительный рост блокчейн-технологий, с помощью которых, например, был создан новый инструмент контроля за транзакциями — «Прозрачный блокчейн». Его функционал направлен на достижение централизованного контроля и деанонимизации лиц, совершающих незаконные операции, с целью выявления и пресечения незаконной деятельности. Таким образом, данный сервис также направлен на снижение экономической преступности и может стать действенным инструментом в деятельности по ПОД/ФТ.

Ю.А. Чиханчин и А.Г. Братко [21, с. 473-475] в качестве направлений внедрения технологий в деятельность надзорных органов рассматривают перспективу разработки централизованного облачного решения, обеспечивающего для Федеральной службы по финансовому мониторингу, Банка России и подотчетных организаций автоматизированное выполнение различных задач и информационное взаимодействие между собой. Для этого необходима интеграция их информационных систем, внедрения различных технологий анализа, машинного обучения и искусственного интеллекта. Как отмечают авторы, эффективное технологическое развитие российской антиотмывочной системы — это главный фактор ее соответствия новым угрозам.

Таким образом, технологические инновации обладают большим потенциалом для препятствования развития киберпреступности и легализации преступных доходов. Главное — грамотно просчитывать риски и использовать качественные решения, чтобы эти решения не смогли использовать в противоправных целях.

В заключении отметим, что научно-технический прогресс, стремительный рост цифровых технологий, выводящий развитие всего мирового общества на новый уровень, открывает новые горизонты для развития экономики и финансовых институтов, однако в столь же равной степени несет в себе и множество рисков. Сложившееся информационное пространство стало не только местом получения и обмена цифровых данных, но также и инструментом новых типов мошенничества и преступлений, образующим серьезную угрозу как отдельным личностям, попадающим в руки злоумышленников и несущим материальные потери, так и финансовой безопасности государства в целом в виде разрастающихся масштабов теневой экономики.

В нашей стране IT-технологии активно развиваются и внедряются в различные отрасли экономики и звенья финансовой системы. Цифровая экономика финансируется государством, финтех-стартапы получают поддержку от инвесторов. По уровню распространения инноваций в этой сфере наша страна занимает лидирующие позиции. Однако вместе с этим наблюдается стремительный рост различных преступлений, совершаемых с использованием цифровых технологий. При этом неподготовленность правоохранительных органов к такого рода новшествам и пробелы в нормативно-правовом регулировании препятствуют результативному их раскрытию.

Для того, чтобы продуктивно бороться с возникшими видами преступлений, а лучше их не допускать и пресекать заранее, необходимо развивать и внедрять инновационные технологии в работу контролирующих органов и поднадзорных им финансовых институтов. Ведь эффективно и оперативно работающая система ПОД/ФТ означает устойчивость финансовой системы к новым вызовам и угрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Губернаторова Н.Н. Финансовая безопасность : учебное пособие / Н.Н. Губернаторова. — Москва: КноРус, 2021. — 181 с.
2. Астахова Е.А. Финансовые аспекты безопасности личности / Е.А. Астахова, С.Н. Калюгина, Н.А. Ларионова, М.В. Симанкина // Вестник Северо-Кавказского федерального университета — 2018. — № 2 (65). — С. 63-71.
3. Кудряшов В. С. Современные угрозы финансовой безопасности России / В. С. Кудряшов, В. Ю. Доберчук // Juvenis Scientia — 2018. — № 6. — С. 4-7.
4. Финансовый мониторинг : учебник / коллектив авторов / под ред. В.И. Глотова, А.У. Альбекова. — Москва : КНОРУС, 2022. — 198 с.
5. Золаев Э.А. Экономическая безопасность государства: понятие и угрозы цифровизации. / Золаев Э.А. // Экономическая безопасность — 2022. — То. 5, № 2. — С. 571-582.
6. Отчет ФАТФ «Виртуальные валюты — ключевые определения и риски в сфере ПОД/ФТ», июнь 2014 г. // Федеральная служба по финансовому мониторингу: сайт. — URL: https://www.fedsfm.ru/content/files/documents/fatf/rop_virtualnye_valyuty.pdf (дата обращения: 02.02.2023).

7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон 31.07.2020 № 259-ФЗ: ред. от 14.07.2022 : принят Государственной думой 22 июля 2020 г. : одобрен Советом Федерации 24 июля 2020 г. // КонсультантПлюс: надежная правовая поддержка : сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 02.02.2023).
8. Бекетнова Ю.М. Типологический анализ в финансовом мониторинге: учебное пособие / Ю.М. Бекетнова. — М.: Прометей, 2020. — 260 с.
9. Киберпреступность и отмывание денег. Проект типологического исследования // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма: сайт. — URL: https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf (дата обращения: 04.02.2023).
10. Заварзина И.П. Киберпреступность как одна из главных проблем российского финансового сектора / И.П. Заварзина // COLLOQUIUM-JOURNAL — 2019. — № 47. — С. 4-7.
11. Легкие финансы. Как живет российский финтех // Научно-образовательный портал IQ: сайт. — URL: https://iq.hse.ru/news/334262759.html (дата обращения: 05.02.2023).
12. Анализ рынка финансовых технологий (FinTech) в России в 2017-2021 гг, прогноз на 2022-2026 гг. Перспективы рынка в условиях санкций // РБК: сайт. — URL: https://marketing.rbc.ru/articles/13460/ (дата обращения: 05.02.2023).
13. Этот дивный мир российского финтеха // Финансовая сфера. Банковское обозрение: сайт. — URL: https://bosfera.ru/bo/etot-divnyy-mir-rossiyskogo-finteha (дата обращения: 05.02.2023).
14. Ештокин С.В. Российский финтех в национальной финансовой системе: защитник интересов или скрытая угроза? / С.В. Ештокин // Экономика, предпринимательство и право. — 2021. — Т. 11, № 8. — С. 1915–1944.
15. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2022 г. // Официальный сайт Министерства внутренних дел Российской Федерации: сайт. — URL: https://xn--b1aew.xn--p1ai/reports/item/35396677 (дата обращения: 09.02.2023).
16. Пахарев А.В. Влияние цифровых валют и киберпреступности на экономическую безопасность страны / А.В. Пахарев // Экономическая безопасность. — 2022. — Том 5. — № 2. — С. 457–472.
17. О внесении изменений в Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»: Законопроект № 237585-8 // СОЗД ГАС «Законотворчество»: сайт. — URL: https://sozd.duma.gov.ru/bill/237585-8 (дата обращения: 09.02.2023).
18. Geographic Distinctions in Crypto Darknet Market Activity // Chainalysis: сайт. — URL: https://blog.chainalysis.com/reports/crypto-darknet-markets-2021-geographic-breakdown/ (дата обращения: 09.02.2023).
19. Помулев А.А. Цифровая валюта — инструмент противодействия теневой экономической деятельности? / А.А. Помулев // Теневая экономика. — 2021. — Т. 5, № 4. — С. 267 — 274.
20. Ясинский И.В. Новые инструменты и технологии контрольно-надзорной деятельности Банка России в сфере противодействия легализации (отмыванию) доходов, полученных преступных путем, и финансированию терроризма. / Ясинский И.В. // Финансовая безопасность — сентябрь 2022. — № 35. — С. 14-16.
21. Финансовый мониторинг : т. 2 : учебное пособие для бакалавриата и магистратуры / Ю.Ф. Короткий, П.В. Ливадный, В.И. Глотов [и др.] ; под ред. Ю.А. Чиханчина, А. Г. Братко. — Москва : Юстицинформ, 2018. — 480 с.